EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych w sprawie komunikatu Komisji dotyczącego planu działania na rzecz wdrażania inteligentnych systemów transportowych w Europie i towarzyszącego mu wniosku w sprawie dyrektywy Parlamentu Europejskiego i Rady ustanawiającej ramy wdrażania inteligentnych systemów transportowych w dziedzinie transportu drogowego oraz ich interfejsów z innymi rodzajami transportu

(2010/C 47/02)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

uwzględniając Traktat ustanawiający Wspólnotę Europejską, w szczególności jego art. 286,

uwzględniając Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 8,

uwzględniając dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych,

uwzględniając dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej,

uwzględniając rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, w szczególności jego art. 41,

uwzględniając wniosek o wydanie opinii zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001, otrzymany od Komisji Europejskiej w dniu 11 lutego 2009 r.,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. WPROWADZENIE

1. W dniu 16 grudnia 2008 r. Komisja przyjęła komunikat określający plan działania na rzecz wdrażania inteligentnych systemów transportowych w Europie („komunikat") ([1]). Komunikatowi towarzyszy wniosek w sprawie dyrektywy Parlamentu Europejskiego i Rady ustanawiającej ramy wdrażania inteligentnych systemów transportowych w dziedzinie transportu drogowego oraz ich interfejsów z innymi rodzajami transportu („wniosek") ([2]). Komunikat wraz z towarzyszącym wnioskiem zostały przesłane przez Komisję do Inspektora do konsultacji zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 ([3]).

2. EIOD z zadowoleniem przyjmuje fakt przeprowadzania z nim konsultacji i zaleca, aby odniesienia do tych konsultacji zamieścić w motywach tego wniosku, podobnie jak włączono je do kilku innych tekstów ustawodawczych, w sprawie których konsultowano się z Inspektorem zgodnie z rozporządzeniem (WE) nr 45/2001.

I.1. Komunikat Komisji w sprawie planu działania na rzecz wdrażania inteligentnych systemów transportowych w Europie

3. „Inteligentne systemy transportowe" („ITS") to zaawansowane aplikacje używające technologii informacyjno-komunikacyjnych (ICT), które są wbudowane w różnych środkach transportu z myślą o wzajemnych powiązaniach między nimi. W dziedzinie transportu drogowego ITS zapewnią innowacyjne usługi w zakresie środków transportu i zarządzania ruchem podróżnym, użytkownikom i operatorów infrastruktury transportu drogowego, osobom zarządzającym flotą oraz podmiotom służb ratowniczych.

4. Stwierdzając rosnące rozpowszechnienie ITS w różnych środkach transportu ([4]) w Unii Europejskiej, Komisja przyjęła plan działania, aby przyspieszyć wprowadzenie

([1]) COM(2008) 886 wersja ostateczna. Rada przyjęła konkluzje dotyczące komunikatu na 2935. posiedzeniu Rady ds. Transportu, Telekomunikacji i Energii w dniach 30 i 31 marca 2009 r.

([2]) COM(2008) 887 wersja ostateczna.

([3]) Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz. U. L 8 z 12.1.2001, s. 1).

([4]) Na szczeblu UE działa wiele inicjatyw polegających na integracji ITS w różnych środkach transportu, w tym transporcie lotniczym (SESAR), żegludze śródlądowej (RIS), kolejach (ERTMS, TAF-TSI), żegludze morskiej (VTMIS, AIS, LRIT) i w transporcie drogowym (eToll, eCall), zob. COM(2008) 886 wersja ostateczna, s. 3.

i stosowanie aplikacji i usług ITS w dziedzinie transportu drogowego. Plan ten służy również zapewnieniu ich interakcji z innymi środkami transportu, co ułatwi świadczenie usług multimodalnych. Spójne rozmieszczenie ITS w Europie będzie służyć różnym celom wspólnotowym, w tym efektywności, ekologiczności oraz ochronie i bezpieczeństwu transportu, przy jednoczesnym wsparciu wewnętrznego rynku i konkurencyjności UE. W związku z różnorodnością celów rozmieszczenia ITS komunikat wymienia sześć priorytetowych obszarów działań na okres 2009–2014. Aby zrealizować ten plan, Komisja proponuje, aby na szczeblu UE określić ramy prawne za pomocą dyrektywy, w której określone zostaną pewne środki w wybranych obszarach priorytetowych.

I.2. **Wniosek dotyczący dyrektywy ustanawiającej ramy wdrażania inteligentnych systemów transportowych w dziedzinie transportu drogowego oraz ich interfejsów z innymi rodzajami transportu**

5. Wniosek zawiera ramy transnarodowego wdrażania aplikacji ITS, którego celem jest ułatwienie świadczenia zharmonizowanych usług transgranicznych, zwłaszcza w zakresie informacji o ruchu i podróży oraz zarządzania ruchem. Wymaga od państw członkowskich podjęcia pewnych środków technicznych służących ułatwieniu wymiany danych między użytkownikami, organami publicznymi, odpowiednimi zainteresowanymi stronami i dostawcami usług ITS, a także wprowadzenia w pojazdach i infrastrukturze drogowej systemów ITS, które są związane z ochroną i bezpieczeństwem. Techniczne specyfikacje aplikacji i systemów ITS w czterech obszarach priorytetowych ([5]) wymienionych w planie działania zostaną określone w drodze procedury komitetowej ([6]); główne elementy tych specyfikacji sformułowano w załączniku II. Konkretne cele stosowania ITS w tych obszarach nie są jednak jasne. Ponadto wdrażanie ITS może być rozszerzone na o wiele więcej obszarów niż cztery początkowo wybrane obszary rozwoju zharmonizowanych technicznych specyfikacji. Wniosek dotyczy głównie wdrożenia przyszłych aplikacji i systemów ITS, ale w miarę możliwości powinien on także objąć istniejące lub obecnie rozwijające się technologie w tej dziedzinie (takie jak eCall, eToll itd.).

6. Wniosek został przesłany do Parlamentu Europejskiego, który przyjął swoje stanowisko w pierwszym czytaniu ([7]) w dniu 23 kwietnia 2009 r. W następstwie wniosku o przeprowadzenie konsultacji zgłoszonego przez Radę w dniu 29 stycznia 2009 r. Europejski Komitet Ekonomiczno-Społeczny przyjął opinię w sprawie wniosku w dniu 13 maja 2009 r. ([8])

I.3. **Zakres opinii**

7. EIOD z zadowoleniem przyjmuje fakt, że skonsultowano się z nim w sprawie proponowanego planu wdrożenia ITS opracowanego przez Komisję. Nie jest to pierwszy raz, kiedy EIOD zajmuje się kwestiami, których dotyczy plan działania w sprawie ITS. EIOD wydał opinię na temat wniosku Komisji wprowadzającego ułatwienia w transgranicznym egzekwowaniu prawa dotyczącego bezpieczeństwa drogowego ([9]) oraz wziął udział w pracach grupy roboczej art. 29 nad dokumentem dotyczącym eCall ([10]).

8. Inteligentne systemy transportowe opierają się na gromadzeniu, przetwarzaniu i wymianie szerokiego wachlarza danych pochodzących z publicznych i prywatnych źródeł; stanowią zatem obszar dużego skupienia danych. Wdrażanie ITS będzie polegać w dużej mierze na technologiach geolokalizacyjnych, takich jak nawigacja satelitarna i technologie bezstykowe, takie jak RFID, które ułatwią świadczenie różnych publicznych lub komercyjnych usług lokalizacyjnych (np. informacje na temat ruchu w czasie rzeczywistym, eFreight, eCall, eToll, rezerwacje parkingów itd.). Niektóre informacje, które będą przetwarzane za pośrednictwem ITS, są zagregowane – np. informacje dotyczące ruchu, wypadków i możliwości – i nie dotyczą żadnych konkretnych osób, natomiast inne informacje są związane z zidentyfikowanymi lub dającymi się zidentyfikować osobami i dlatego można je określić jako dane osobowe w rozumieniu art. 2 lit. a) dyrektywy 95/46/WE.

9. EIOD uważa za ważne, by planowane działania w związku z wdrażaniem ITS były spójne z istniejącymi ramami prawnymi przytoczonymi we wniosku, w szczególności z dyrektywą 95/46/WE w sprawie ochrony danych ([11]) i dyrektywą 2002/58/WE o e-prywatności ([12]).

([5]) Artykuł 4 wniosku przewiduje określenie środków technicznych w następujących obszarach: (i) optymalne wykorzystanie danych dotyczących dróg, ruchu i podróży; (ii) ciągłość usług ITS związanych z zarządzaniem ruchem i przewozami towarowymi w ramach europejskich korytarzy transportowych i w konurbacjach; (iii) bezpieczeństwo i ochrona ruchu drogowego; oraz (iv) integracja pojazdu w ramach infrastruktury transportowej.

([6]) Wniosek przewiduje procedurę regulacyjną połączoną z kontrolą zgodnie z art. 5a ust. 1–4 i art. 7 decyzji 1999/468/WE.

([7]) Rezolucja legislacyjna Parlamentu Europejskiego z dnia 23 kwietnia 2009 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady ustanawiającej ramy wdrażania inteligentnych systemów transportowych w dziedzinie transportu drogowego oraz ich interfejsów z innymi rodzajami transportu, T6-0283/2009.

([8]) Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady ustanawiającej ramy wdrażania inteligentnych systemów transportowych w dziedzinie transportu drogowego oraz ich interfejsów z innymi rodzajami transportu, TEN/382, 13.5.2009.

([9]) Opinia Europejskiego Inspektora Ochrony Danych na temat wniosku w sprawie dyrektywy Parlamentu Europejskiego i Rady wprowadzającej ułatwienia w transgranicznym egzekwowaniu prawa dotyczącego bezpieczeństwa drogowego, 2008/C 310/02, Dz.U. C 310 z 5.12.2008, s. 9.

([10]) Dokument roboczy grupy roboczej art. 29 w sprawie implikacji inicjatywy eCall dla ochrony danych i prywatności, WP 125, 26.9.2006. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp125_en.pdf

([11]) Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.U. L 281 z 23.11.1995, s. 31.

([12]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz.U. L 201 z 31.7.2002, s. 37.

10. Komisja określiła nierozstrzygnięte kwestie prywatności i ochrony danych jako jedną z głównych przeszkód w promowaniu ITS. Kwestie te omówiono w niniejszej opinii w następujący sposób:

— w rozdziale II ramy prawne opracowane przez Komisję do celów wdrażania ITS zostaną przeanalizowane z punktu widzenia ochrony danych,

— w rozdziale III przedstawione zostaną obawy związane z ochroną danych, które muszą zostać uwzględnione przy odpowiednim wdrażaniu ITS:

— w pierwszym punkcie opinia skupi się na potrzebie „poszanowania prywatności od samego początku" w rozwoju ITS i dokładniej przedstawi istotne kwestie, które należy rozwiązać przy projektowaniu aplikacji ITS i systemów przetwarzających dane,

— drugi punkt skoncentruje się na pewnych rozważaniach dotyczących prywatności, które muszą zostać uwzględnione następnie do celów świadczenia usług ITS.

II. ANALIZA RAM PRAWNYCH ZAPROPONOWANYCH DO CELÓW WDRAŻANIA ITS

11. Wniosek Komisji w sprawie dyrektywy zawiera dwa przepisy (motyw 9 i artykuł 6) dotyczące prywatności, ochrony i ponownego wykorzystania informacji. Artykuł 6 ust. 1 wniosku Komisji wymaga, aby działanie ITS było prowadzone zgodnie z zasadami ochrony danych zawartymi między innymi w dyrektywie 95/46/WE i dyrektywie 2002/58/WE. We wniosku Komisji art. 6 ust. 2 przewiduje konkretne środki ochrony danych głównie z punktu widzenia bezpieczeństwa: art. 6 ust. 2 wniosku stwierdza, że „państwa członkowskie zapewniają ochronę danych i zapisów ITS przeciwko nadużyciom, w tym bezprawnemu dostępowi, zmianom i utracie". Na koniec, art. 6 ust. 3 wniosku Komisji przewiduje, że „zastosowanie ma dyrektywa 2003/98/WE".

12. Parlament Europejski zaproponował w pierwszym czytaniu zmiany art. 6. W szczególności w art. 6 ust. 1 zostały dodane trzy nowe akapity, które odnoszą się do użycia w stosownych przypadkach danych anonimowych do przetwarzania szczególnie chronionych danych wyłącznie za wyraźną i świadomą zgodą osoby, której dane dotyczą, oraz do zapewnienia, by dane osobowe były przetwarzane tylko „w zakresie, w którym przetwarzanie to jest konieczne do korzystania z aplikacji lub usług ITS". Ponadto art. 6 ust. 2 został zmieniony przez dodanie stwierdzenia, że dane i zapisy ITS „nie mogą być wykorzystywane do celów innych niż określone w niniejszej dyrektywie".

13. EIOD z zadowoleniem przyjmuje fakt, że podczas opracowywania wniosku uwzględniono ochronę danych i że określono ją jako ogólny warunek właściwego wdrażania ITS w Europie. EIOD uznaje, że potrzebna jest spójna harmonizacja przetwarzania danych na szczeblu UE, tak aby zapewnić możliwość działania aplikacji i usług ITS w całej Europie.

14. EIOD odnotowuje jednak, że proponowane ramy prawne są zbyt szerokie i ogólne, aby w odpowiedni sposób rozwiązać problemy związane z prywatnością i ochroną danych wiążące się z wdrażaniem ITS w państwach członkowskich. Nie jest jasne, kiedy świadczenie usług ITS będzie prowadzić do gromadzenia i przetwarzania danych osobowych, jakie są konkretne cele przetwarzania danych ani to, jaka jest podstawa prawna uzasadniająca takie przetwarzanie. Ponadto stosowanie technologii lokalizacyjnych do celów wdrażania ITS zwiększa ryzyko rozwoju usług, które ingerują w prywatność, jeżeli wiążą się z gromadzeniem i wymianą danych osobowych. Ponadto wniosek nie określa jasno ról i zadań różnych operatorów działających w obrębie łańcucha wdrażania ITS i w związku z tym trudno jest określić, którzy operatorzy będą administratorami danych i będą dlatego odpowiedzialni ([13]) za zgodność z obowiązkami w zakresie ochrony danych. Operatorzy ITS natkną się na znaczne problemy, jeżeli wszystkie te kwestie nie zostaną wyjaśnione w przepisach prawnych, ponieważ to oni będą odpowiadać za stosowanie środków zawartych w proponowanej dyrektywie.

15. Istnieje zatem ryzyko, że brak jasności proponowanych ram prawnych spowoduje rozbieżności we wprowadzaniu ITS w Europie i że zamiast zmniejszania różnic między państwami członkowskimi doprowadzi, przeciwnie, do znacznej niepewności, fragmentacji i niespójności z powodu różnych poziomów ochrony danych w Europie. Może także doprowadzić do niespełnienia podstawowych gwarancji ochrony danych. EIOD podkreśla potrzebę dalszej harmonizacji w tych kwestiach na szczeblu UE. EIOD zaproponuje przy tym zmiany do proponowanych ram prawnych z punktu widzenia ochrony danych. Z naciskiem zaleca, aby Parlament i Rada wprowadziły do wniosku proponowane zmiany, a także, jeżeli jest to wykonalne, dodatkowe przepisy wyjaśniające nierozstrzygnięte kwestie (takie jak definicja i zadania podmiotów ITS, opracowanie zharmonizowanych umów o świadczenie usług ITS itd.). Podkreśla ponadto, że państwa członkowskie będą również odpowiedzialne za wykonanie dyrektywy w odpowiedni sposób, tak aby operatorzy

([13]) Zgodnie z art. 2 lit. d), art. 6 ust. 2 i art. 23 dyrektywy 95/46/WE wspomnianej w przypisie 11.

mogli opracować systemy i usługi, które zapewniają odpowiedni poziom ochrony danych osobowych w całej Europie.

II.1. **Działania związane z przetwarzaniem danych muszą opierać się na odpowiedniej podstawie prawnej**

16. Nie wiadomo, kiedy rozpocznie się przetwarzanie danych, gdy sprzęt ITS zostanie zintegrowany z pojazdem, i na jakiej podstawie prawnej odbywać się będzie to przetwarzanie. Do celów przetwarzania danych operatorzy mogą opierać się na różnych podstawach prawnych, między innymi na jednoznacznej zgodzie użytkowników, umowie lub prawnym zobowiązaniu, które musi wypełnić administrator. Konieczne jest zharmonizowanie podstawy prawnej, według której przeprowadzane będzie przetwarzanie danych za pośrednictwem ITS, tak aby dopilnować, by systemy działały w całej Europie i by różnice w sposobach przetwarzania stosowanych w poszczególnych krajach UE nie szkodziły użytkownikom.

17. W wielu przypadkach systemy ITS będą z założenia zintegrowane z pojazdami. Tak jest zwłaszcza w przypadku systemów ITS związanych z ochroną i bezpieczeństwem, które muszą być wbudowane w pojazdach na mocy przedmiotowego wniosku. Wniosek nie definiuje jednak, co należy rozumieć przez „systemy związane z ochroną i bezpieczeństwem", dlatego należy doprecyzować, jakie konkretne aplikacje i systemy ITS muszą być wbudowane w pojazdach. Ponadto należy wyjaśnić, czy użytkownicy będą aktywować i stosować urządzenie na zasadzie dobrowolności czy też obowiązku. Decyzja, aby dokonywać przetwarzania danych na zasadzie obowiązku, powinna zostać podjęta jedynie do konkretnych, należycie uzasadnionych celów (np. śledzenie towarów w zarządzaniu transportem towarowym) i z zachowaniem odpowiednich gwarancji w zakresie przetwarzania danych dotyczących poszczególnych osób. Jeżeli stosowanie ITS następuje na zasadzie dobrowolności, należy wprowadzić odpowiednie gwarancje, aby zapobiec sytuacji, w której z samej obecności systemu w pojeździe wynika zgoda użytkowników na ich stosowanie.

18. EIOD opowiada się za tym, by usługi ITS były świadczone na zasadzie dobrowolności. Wiąże się to z tym, że użytkownicy muszą mieć swobodę wyrażenia zgody na stosowanie systemu i na szczególne cele, do których będzie on używany. Jeżeli świadczona usługa opiera się na danych dotyczących lokalizacji, należy przekazać odpowiednie informacje użytkownikowi (zgodnie zwłaszcza z art. 9 dyrektywy 2002/58/WE), który musi mieć możliwość wycofania tej zgody. Od strony praktycznej wymaga to wprowadzenia łatwego – bez technicznych lub finansowych ograniczeń dla użytkownika ([14]) – sposobu dezaktywacji urządzenia lub funkcji, gdy użytkownik nie zgadza się już na użycie systemu lub danej funkcji. Należy wprowadzić dalsze gwarancje, tak aby użytkownicy nie byli dyskryminowani, w przypadku gdy odmówią korzystania z usługi.

([14]) Zob. WP 125 w sprawie eCall, s. 4, wspomniany w przypisie 10.

19. W przypadkach gdy pewne działania związane z przetwarzaniem są obowiązkowe, a inne podlegają zgodzie użytkownika, należy zapewnić przejrzystość odnośnie do różnych wykonywanych operacji przetwarzania danych poprzez przekazanie odpowiednich informacji użytkownikom na temat obowiązkowego lub dobrowolnego charakteru każdej konkretnej operacji przetwarzania oraz zakresu tego przetwarzania. Ponadto kluczowe znaczenie będzie mieć wprowadzenie odpowiednich gwarancji bezpieczeństwa, tak aby żadne dane nie były gromadzone i przetwarzane poza zakresem tego, co zostało prawnie zdefiniowane lub na co dobrowolnie wyrażono zgodę.

20. Rozważając transnarodowy skutek usług ITS, EIOD zaleca ponadto opracowanie paneuropejskich standardowych umów, aby usługi świadczone za pośrednictwem ITS oferowały te same gwarancje ochrony danych w całej Europie i w szczególności aby użytkownikom przekazywane były wystarczająco jasne informacje na temat konkretnych używanych funkcji, wpływu używania konkretnych technologii na ochronę ich danych oraz tego, jak użytkownicy mogą korzystać ze swoich praw. Gdy dodawane są nowe funkcje, dostawcy usług powinni podjąć dalsze kroki, aby zapewnić użytkownikom jasne i konkretne informacje dotyczące tych dodatkowych funkcji oraz aby uzyskać ich wymaganą zgodę na użycie tych nowych funkcji.

II.2. **Należy doprecyzować cele i warunki przetwarzania danych**

21. EIOD odnotowuje, że wniosek nie definiuje dokładnie konkretnych usług i celów, dla których aplikacje ITS mogłyby być używane, jest to więc kwestia otwarta. Pozwala to w praktyce na elastyczność, ale oznacza też, że nierozstrzygnięte kwestie prywatności i ochrony danych – określone przez Komisję jako jedna z przeszkód w promowaniu ITS (zob. pkt 10) – mogą pozostać nierozwiązane i mogą zaszkodzić zrównoważonej realizacji proponowanych środków.

22. EIOD podkreśla, że szczególnie ważne jest, aby operacje przetwarzania do celów świadczenia konkretnych usług ITS dokonywane były nie tylko na mocy odpowiedniej podstawy prawnej, ale również do konkretnych, wyraźnych i uzasadnionych celów, oraz by przewidziane przetwarzanie było proporcjonalne i konieczne do tych celów (art. 6 dyrektywy 95/46/WE). Należy zatem rozważyć ewentualną konieczność dalszego uregulowania na szczeblu UE w odniesieniu do konkretnych użyć ITS, tak aby zapewnić zharmonizowaną i adekwatną podstawę prawną działań związanych z przetwarzaniem, które należy podjąć, oraz aby uniknąć różnic między państwami członkowskimi we wdrażaniu usług ITS.

23. W proponowanych ramach nie ma jeszcze decyzji o warunkach przetwarzania danych i wymiany danych do celów używania ITS. Wiele parametrów technicznych, których wybór będzie miał różne skutki dla prywatności i ochrony danych, zostanie wybranych na późniejszym etapie drogą procedury komitetowej. Biorąc pod uwagę szczególną ochronę przyznaną prywatności i ochronie

danych jako podstawowym prawom chronionym w art. 8 Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności oraz w art. 7 i 8 Karty praw podstawowych Unii Europejskiej, można się zastanawiać, czy i w jakim zakresie definicja operacji przetwarzania danych powinna zostać określona drogą procedury komitetowej.

24. W społeczeństwie demokratycznym decyzje dotyczące podstawowych zasad i warunków, które mają wpływ na prawa podstawowe, powinny być podejmowane drogą pełnej procedury ustawodawczej, która obejmuje odpowiednie kontrole i oceny. W tym przypadku oznacza to, że decyzje, które mają duży wpływ na prywatność i ochronę danych osób, takie jak cele i warunki obowiązkowych działań związanych z przetwarzaniem danych oraz definicja warunków wdrażania ITS w nowych obszarach, powinny być podejmowane przez Parlament Europejski i Radę, a nie drogą procedury komitetowej.

25. W tej perspektywie EIOD z naciskiem zaleca, aby w stosownych przypadkach włączyć grupę roboczą art. 29 i EIOD do prac komitetu stworzonego na mocy art. 8 wniosku i do przyszłych podejmowanych działań dotyczących wdrażania ITS na zasadzie konsultacji na dostatecznie wczesnym etapie przed opracowaniem odpowiednich środków.

26. Ponadto EIOD odnotowuje zmiany przyjęte przez Parlament Europejski w związku z art. 6 wniosku. EIOD odnotowuje najpierw, że zmiana związana z zachęcaniem do wykorzystania w stosownych przypadkach danych anonimowych, choć co do zasady jest słuszna, nie rozwiąże wszystkich problemów związanych z ochroną danych, ponieważ wiele danych gromadzonych i wymienianych za pośrednictwem ITS może się kwalifikować jako dane osobowe. Aby przetwarzanie danych następowało w sposób anonimowy, nikt nie może na żadnym etapie przetwarzania – uwzględniając wszystkie środki, które mogą być rozsądnie używane albo przez administratora, albo przez jakąkolwiek inną osobę – połączyć danych z danymi dotyczącymi zidentyfikowanej osoby, w przeciwnym wypadku dane te stanowią dane osobowe w rozumieniu art. 2 lit. a) dyrektywy 95/46/WE ([15]). Ponadto na podstawie poprawek zaproponowanych przez Parlament Europejski EIOD zaleca, aby art. 6 wniosku został zmieniony następująco:

— ocena konieczności przetwarzania danych osobowych za pośrednictwem ITS powinna być dokonana w świetle uzasadnionych i konkretnych celów, do których dane są przetwarzane (zgodnie z art. 6 i 7 dyrektywy 95/46/WE). Działanie aplikacji ITS ([16]) samo w sobie nie może być uzasadnionym celem przetwarzania danych, ponieważ aplikacja ta jest jedynie środkiem gromadzenia i wymiany danych, którego użycie powinno być zasadniczo ukierunkowane na szczególne cele,

— poprawka ([17]) odnosząca się do zakazu używania danych i zapisów ITS „do celów innych niż określone w niniejszej dyrektywie" nie przewiduje dostatecznych gwarancji, w szczególności ponieważ konkretne cele i usługi, dla których ITS będą używane, nie są jasno i wyczerpująco określone w dyrektywie. Uznając, że różne działania związane z przetwarzaniem danych będą prowadzone za pośrednictwem ITS do bardzo różnych celów, należy dopilnować, aby dane gromadzone podczas przetwarzania do jednego konkretnego celu nie były używane do innych celów, które nie są kompatybilne, jak przewiduje art. 6 ust. 1 lit. b) dyrektywy 95/46/WE. EIOD zaleca zatem, aby art. 6 ust. 2 został zmieniony, tak aby dopilnować, aby dane i zapisy ITS nie były używane „do celów innych niż cele, do których zostały zgromadzone, w sposób niekompatybilny z tymi celami".

III. OCHRONA DANYCH W INTELIGENTNYCH SYSTEMACH TRANSPORTOWYCH

27. Szczególnie ważne jest, aby role różnych podmiotów zaangażowanych w ITS były sprecyzowane, tak aby określić, kto ponosi odpowiedzialność za zapewnienie właściwego działania systemów z punktu widzenia ochrony danych. Należy zatem doprecyzować, kto powinien być odpowiedzialny za realizację aplikacji i systemów, których budowa zostanie określona w drodze procedury komitetowej, oraz kto spośród łańcucha podmiotów będzie odpowiedzialny za zgodność przetwarzania danych z prawem dotyczącym ochrony danych (tj. administratorzy danych). EIOD zwróci poniżej uwagę na pewne obawy związane z prywatnością i ochroną danych, którymi należy się zająć w drodze procedury komitetowej i które powinni uwzględnić administratorzy danych podczas projektowania architektury aplikacji i systemów. Ponadto poruszy on niektóre kwestie dotyczące ochrony danych, którymi muszą się zająć ustawodawca i administratorzy danych w związku ze świadczeniem usług ITS.

III.1. „Poszanowanie prywatności od samego początku"

28. Właściwe stosowanie zasad ochrony danych zawartych w dyrektywie 95/46/WE jest podstawowym warunkiem powodzenia wdrażania ITS we Wspólnocie. Zasady te mają konsekwencje dla budowy architektury systemów i aplikacji. EIOD zaleca, aby na wczesnym etapie projektowania ITS przyjąć podejście „poszanowania prywatności od

([15]) Jak określono w motywie 26 dyrektywy 95/46/WE, „w celu ustalenia, czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owej osoby".

([16]) Poprawka 34 wprowadzająca nowy art. 6 ust. 1 lit. b) przewiduje: „Dane osobowe są przetwarzane tylko w zakresie, w którym przetwarzanie to jest konieczne do korzystania z aplikacji lub usług ITS".

([17]) Poprawka 36 dodaje do art. 6 ust. 2 następujący fragment: „oraz dbają, aby nie wykorzystywano ich do celów innych niż określone w niniejszej dyrektywie".

samego początku", aby określić architekturę oraz działanie aplikacji i systemów oraz zarządzanie nimi. Podejście to zostało zwłaszcza podkreślone w dyrektywie 1999/5/WE ([18]) w odniesieniu do urządzeń radiowych i końcowych urządzeń telekomunikacyjnych.

29. Projekt aplikacji i systemów ITS będzie opracowywany w kilku etapach przez różne podmioty, z których wszystkie powinny uwzględnić kwestie prywatności i ochrony danych. Komisja i komitet ds. ITS będą w pierwszym etapie ponosić szczególną odpowiedzialność za zdefiniowanie – w drodze procedury komitetowej – środków, inicjatyw standaryzacyjnych, procedur i najlepszych praktyk, które powinny promować „poszanowanie prywatności od samego początku".

30. Na wszystkich etapach procesów i we wszystkich formach procesów należy wspierać „poszanowanie prywatności od samego początku":

— na szczeblu organizacyjnym należy uwzględnić zasadę poszanowania prywatności przy definiowaniu koniecznych procedur wymiany danych między wszystkimi odpowiednimi punktami wymiany – może mieć to bezpośredni wpływ na rodzaj wymiany i rodzaj wymienianych danych,

— wymogi dotyczące prywatności i bezpieczeństwa powinny zostać włączone do standardów, najlepszych praktyk, specyfikacji technicznych i systemów,

— na poziomie technicznym EIOD zaleca rozwój, na przykład drogą procedury komitetowej, najlepszych dostępnych technik ([19]) (BAT) dotyczących prywatności, ochrony danych i bezpieczeństwa w konkretnych sektorach lub do szczególnych celów, w których różne parametry bezpieczeństwa, które muszą być wprowadzone w całym cyklu życia systemu, byłyby zdefiniowane, aby zagwarantować zgodność z ramami regulacyjnymi UE.

31. EIOD przedstawia poniżej niektóre kwestie, które należy uwzględnić przy projektowaniu aplikacji i architektury systemów. Odnoszą się one do zgromadzonych danych, interoperacyjności systemów oraz do bezpieczeństwa danych.

III.1.a) *Ograniczanie ilości danych do minimum i anonimowość*

32. Zgodnie z art. 6 ust. 1 lit. c) dyrektywy 95/46/WE jedynie dane osobowe, które są niezbędne i właściwe dla konkretnych celów, mogą być gromadzone i przetwarzane.

33. EIOD podkreśla znaczenie przyjęcia odpowiedniej klasyfikacji informacji i danych, które mają być przetwarzane za pośrednictwem ITS przed zaprojektowaniem aplikacji i systemów, tak aby uniknąć masowego i nieodpowiedniego gromadzenia danych osobowych. W związku z tym należy wziąć pod uwagę:

— źródło danych (ze źródła publicznego, dostawcy telekomunikacyjnego, dostawcy usług ITS, innych operatorów, pojazdu, użytkownika pojazdu lub innych osób, których dane dotyczą),

— charakter danych (np. zagregowane informacje, dane anonimowe, dane osobowe, dane szczególnie chronione),

— cel(e), dla którego(-ych) dane mają być użyte, oraz

— w odniesieniu do systemów współpracujących należy doprecyzować, które dane pochodzą z pojazdu, które są do niego dostarczane na zasadzie *push*/*pull*, które są wymieniane z innym pojazdem lub infrastrukturą i które przechodzą z jednej infrastruktury do drugiej i do jakich celów.

34. Poszczególne funkcje należy uważnie przeanalizować zgodnie z realizowanymi celami, tak aby ocenić konieczność gromadzenia danych osobowych. EIOD podkreśla znaczenie zachowania właściwej równowagi między prawami podstawowymi osób, których dane dotyczą, i interesami różnych zaangażowanych podmiotów, co zakłada, że przetwarzanych jest jak najmniej danych osobowych. W jak największym zakresie architektura aplikacji i systemów powinna być zaprojektowana w taki sposób, aby gromadzone były jedynie te dane osobowe, które są ściśle potrzebne do realizacji celów, które należy osiągnąć.

35. Jeżeli dane osobowe nie są konieczne lub są konieczne jedynie na wstępnym etapie przetwarzania, nie powinny być gromadzone lub powinno się je jak najszybciej uczynić anonimowymi. Jest zatem szczególnie ważne, aby nie tylko ocenić konieczność gromadzenia danych, ale także konieczność ich zatrzymywania w różnych systemach. Należy dla poszczególnych podmiotów w łańcuchu usług określić konkretne limity czasowe przechowywania danych osobowych; powinny one być zróżnicowane stosownie do rodzaju danych i celu, dla którego zostały zgromadzone ([20]). W rezultacie, jeżeli przechowywanie danych nie jest już potrzebne do osiągnięcia celów, dla których zostały zgromadzone lub następnie przetworzone, powinny one stać się anonimowe, tj. nie powinny więcej wiązać się z zidentyfikowaną lub dającą się zidentyfikować osobą.

36. Projekt architektury systemów i procedury wymiany danych powinien wspierać przetwarzanie jak najmniejszych ilości danych osobowych. W tym względzie należy uwzględnić wszystkie etapy przetwarzania i wszystkie podmioty w łańcuchu świadczenia usług ITS. Niektóre

([18]) Głównie art. 3 ust. 3 lit. c) dyrektywy 1999/5/WE Parlamentu Europejskiego i Rady z dnia 9 marca 1999 r. w sprawie urządzeń radiowych i końcowych urządzeń telekomunikacyjnych oraz wzajemnego uznawania ich zgodności.

([19]) Najlepsze dostępne techniki oznaczają najwydajniejszy i najbardziej zaawansowany etap rozwoju działań i ich metod operacji, które wskazują praktyczną odpowiedniość konkretnych technik dostarczania – co do zasady – podstawy aplikacji i systemów ITS, która byłaby zgodna z wymogami dotyczącymi prywatności, ochrony danych i bezpieczeństwa określonymi w ramach regulacyjnych UE.

([20]) Na przykład zatrzymywanie danych dotyczących ruchu drogowego i lokalizacji przetwarzanych w związku ze świadczeniem publicznie dostępnych elektronicznych usług komunikacyjnych w publicznych sieciach komunikacyjnych jest regulowane dyrektywą 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającą dyrektywę 2002/58/WE.

dane mogą być wymieniane i przetwarzane na zasadzie anonimowości, natomiast inne dane, nawet jeżeli są wymieniane jako niezidentyfikowane, mogą być połączone z danymi dotyczącymi zidentyfikowanych osób i dlatego stanowią dane osobowe w rozumieniu art. 2 lit. a) dyrektywy 95/46/WE ([21]). W związku z celami, dla których ITS będą używane, trudne wydaje się zapewnienie przetwarzania dużych ilości danych zgromadzonych za pośrednictwem ITS na zasadzie anonimowości, skoro w pewnym momencie do konkretnych celów, takich jak fakturowanie, potrzebna będzie tożsamość danej osoby. Skutkowałoby to co najmniej koniecznością podjęcia specjalnych – technicznych, organizacyjnych i prawnych – środków, aby zapewnić anonimowość w niektórych dziedzinach.

III.1.b) *Interoperacyjność, jakość danych i ograniczenie do celu*

37. Interoperacyjność aplikacji i systemów jest kluczowym elementem udanego wdrożenia ITS. Przeprowadzone zostaną prace na rzecz harmonizacji, dzięki którym określone zostaną techniczne specyfikacje interfejsów, które należy włączyć do aplikacji i systemów, tak aby mogły one działać wspólnie z innymi aplikacjami wbudowanymi w innych środkach lub systemach transportu. Interoperacyjność systemów pomoże ułatwić świadczenie różnych usług i przyczyni się do zapewnienia ich ciągłości w całej Europie, stwarza jednakże pewną liczbę zagrożeń z perspektywy ochrony danych, takich jak ryzyko niewłaściwego użycia lub nadużycia danych. Każde wzajemne połączenie baz danych powinno nastąpić z właściwym poszanowaniem zasad ochrony danych ([22]) i praktycznych gwarancji w zakresie bezpieczeństwa (zob. również sekcja III.1.c).

38. Zasada jakości danych przytoczona w art. 6 lit. d) dyrektywy 95/46/WE jest szczególnie istotna w kontekście interoperacyjności aplikacji i systemów. Techniczne specyfikacje, które należy zdefiniować do celów budowy interfejsów, powinny zapewniać dokładność danych, które zostaną uzyskane w wyniku wzajemnego połączenia aplikacji i systemów.

39. W związku z tym, że interoperacyjność systemów ułatwi wzajemne połączenie baz danych i powiązanie danych do dalszych celów, EIOD podkreśla, że każde wzajemne połączenie powinno być nawiązywane ze szczególnym uwzględnieniem zasady ograniczenia do celu zawartej w art. 6 ust. 1 lit. b) dyrektywy 95/46/WE. Szczególnie ważne jest, aby projekt architektury systemów ITS zapobiegał jakiemukolwiek dalszemu użyciu danych do innych celów niż te, dla których zostały zgromadzone. W systemie muszą być wbudowane odpowiednie zabezpieczenia, tak aby zapobiegać niewłaściwemu użyciu, niedozwolonemu ujawnieniu lub dostępowi, jak również skutkom ubocznym działania urządzeń. Na przykład, należy wprowadzić wystarczające zabezpieczenia, tak aby nieuprawnione strony trzecie nie miały dostępu do urządzeń przenośnych i aby urządzenia te nie były używane do identyfikowania i śledzenia ludzi do celów innych niż cele systemu.

40. Jeżeli chodzi o zasadność samego wzajemnego połączenia, będzie ono musiało być oceniane w poszczególnych przypadkach przy uwzględnieniu charakteru danych, które są udostępniane i wymieniane za pośrednictwem systemów, oraz celów, dla których są pierwotnie używane.

III.1.c) *Bezpieczeństwo danych*

41. Bezpieczeństwo danych osobowych jest kluczowym elementem wdrażania ITS. EIOD z zadowoleniem przyjmuje fakt, że bezpieczeństwo jest wyraźnie wspomniane w planie działania i we wniosku dotyczącym dyrektywy. Bezpieczeństwo powinno być przewidziane nie tylko podczas działania urządzeń ITS (w systemach zainstalowanych w pojazdach i w komunikacyjnym protokole transportowym), ale również poza czasem działania tych urządzeń – w bazach danych, w których dane są przetwarzane lub przechowywane. Na wszystkich etapach przetwarzania należy zdefiniować odpowiednie techniczne, administracyjne i organizacyjne wymogi, które zapewnią odpowiedni poziom bezpieczeństwa zgodnie z art. 16 i 17 dyrektywy 95/46/WE (jak również art. 4 i 5 dyrektywy 2002/58/WE, w stosownych przypadkach).

42. Definicja odpowiednich środków bezpieczeństwa powinna być sporządzana wyłącznie po uważnej ocenie szczególnych celów, dla których ITS będą używane, i warunków przetwarzania. W tym względzie EIOD zaleca, aby ocenę skutków dla prywatności i ochrony danych przeprowadzić w związku z konkretnymi sektorami lub celami użycia (np. systemy ITS związane z bezpieczeństwem, systemy zarządzania transportem towarowym itd.). Przeprowadzenie oceny skutków dla prywatności i ochrony danych oraz użycie najlepszych dostępnych technik w odniesieniu do prywatności i ochrony danych przyczyni się do zdefiniowania najodpowiedniejszych środków bezpieczeństwa właściwych dla konkretnego przetwarzania.

III.2. **Dalsze rozważania dotyczące ochrony danych oraz prywatności w związku ze świadczeniem usług ITS**

43. Dalsza harmonizacja warunków wdrażania usług ITS jest konieczna na szczeblu UE, aby zapobiegać rozbieżnościom we wdrażaniu tych usług. W tym względzie EIOD chciałby poniżej zwrócić uwagę na dwie kwestie, które szczególnie wymagają dalszych rozważań z perspektywy prywatności i ochrony danych:

— użycie narzędzi lokalizacyjnych do celów świadczenia publicznych i komercyjnych usług dotyczących lokalizowania wymaga wprowadzenia dodatkowych gwarancji. W tym kontekście szczególną uwagę należy zwrócić na to, czy i kiedy usługi ITS dotyczące lokalizowania będą używane do celów prywatnych lub celów zawodowych oraz jakie konsekwencje będzie miało użycie takiego systemu dla osób używających pojazdu w kontekście zawodowym,

— w systemach zintegrowanych szczególnie ważne jest, aby sprecyzowane były role i zadania różnych stron zaangażowanych we wdrażanie ITS.

([21]) Zob. przypis 15.

([22]) Zob. również uwagi Inspektora do komunikatu Komisji w sprawie interoperacyjności między europejskimi bazami danych, 10.3.2006. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

III.2.a) *Gwarancje dotyczące użycia narzędzi lokalizacyjnych do celów świadczenia usług ITS dotyczących lokalizowania*

44. Wdrażanie ITS będzie wspierać rozwój aplikacji służących śledzeniu ruchu i pochodzenia towarów i pozwoli na wdrażanie komercyjnych i publicznych usług dotyczących lokalizowania. Usługi te będą polegać na użyciu technologii takich jak nawigacja satelitarna i identyfikatory RFID ([23]). Nawigacja, systemy śledzenia ruchu i pochodzenia mają być w zamierzeniu używane do różnych celów, takich jak zdalne monitorowanie pojazdów i ładunku na trasie (np. w przypadku transportu towarów niebezpiecznych lub żywych zwierząt), fakturowanie pojazdów w oparciu o różne parametry, w tym przebyta odległość i pora dnia (np. opłaty drogowe, elektroniczne systemy opłat drogowych) oraz monitoring kierowców do celów egzekwowania, na przykład przez sprawdzanie czasu jazdy (za pomocą cyfrowych tachografów) i nakładanie kar (za pomocą elektronicznej identyfikacji pojazdów).

45. Użycie technologii lokalizacyjnych w szczególny sposób ingeruje w prywatność, ponieważ pozwala na śledzenie kierowców i gromadzenie różnych danych związanych z nawykami w zakresie kierowania pojazdami. Jak podkreślono na forum grupy roboczej art. 29 ([24]), przetwarzanie danych lokalizacyjnych jest szczególnie wrażliwą kwestią obejmującą główny problem związany ze swobodą anonimowego przemieszczania się i wymaga wdrożenia szczególnych gwarancji, tak aby zapobiegać nadzorowi osób i niewłaściwemu użyciu danych.

46. EIOD podkreśla, że użycie narzędzi lokalizacyjnych musi być prawomocne, tj. oparte na właściwej podstawie prawnej do jasnych i uprawnionych celów, i proporcjonalne do celów, które mają być osiągnięte. Prawne uzasadnienie podejmowanego przetwarzania danych będzie w dużej mierze zależeć od sposobu i celów używania narzędzi lokalizacyjnych. Jak grupa robocza art. 29 podkreśliła w opinii w sprawie eCall, „z perspektywy ochrony danych nie byłoby do przyjęcia, by urządzenia te były na stałe połączone i w związku z tym pojazdy były na stałe możliwe do wyśledzenia z myślą o ewentualnej aktywacji urządzeń eCall" ([25]). Dlatego ważne jest, aby doprecyzować konkretne okoliczności, w których pojazd będzie śledzony, oraz wpływ na użytkownika. W każdym wypadku użycie urządzeń lokalizacyjnych powinno być uzasadnione uprawnioną potrzebą (np. monitorowaniem transportu towarów) i ściśle ograniczone do tego, co jest potrzebne do tego celu. Dlatego ważne jest, aby dokładnie określić, jakie dane lokalizacyjne będą gromadzone, gdzie będą przechowywane i jak długo będą trzymane, z kim i do jakich celów będą wymieniane, oraz aby podjąć wszelkie niezbędne kroki w celu uniknięcia niewłaściwego użycia lub nadużycia danych.

47. Ponadto przetwarzanie danych lokalizacyjnych odnoszących się do użytkowników publicznych sieci komunikacyjnych lub publicznie dostępnych elektronicznych usług komunikacyjnych jest ściśle regulowane w art. 9 dyrektywy 2002/58/WE. Wymaga to zwłaszcza, aby przetwarzanie danych dotyczących lokalizacji było przeprowadzane na zasadzie anonimowości lub za zgodą użytkownika. Oznacza to, że użytkownicy, zanim zgodzą się na użycie narzędzia lokalizacyjnego, muszą otrzymać odpowiednie informacje, w tym dotyczące rodzaju przetwarzanych danych dotyczących lokalizacji, celów i czasu trwania przetwarzania oraz tego, czy dane zostaną przekazane stronie trzeciej do celu świadczenia usługi stanowiącej wartość dodaną. Użytkownicy muszą mieć możliwość, w prosty sposób i bezpłatnie, tymczasowej odmowy przetwarzania danych dotyczących lokalizacji w odniesieniu do każdego połączenia do sieci lub każdej transmisji komunikatu. Przetwarzanie danych dotyczących lokalizacji powinno być ściśle ograniczone do osób działających z upoważnienia dostawcy publicznej sieci komunikacyjnej lub publicznie dostępnej usługi komunikacyjnej lub trzeciej strony świadczącej usługę stanowiącą wartość dodaną.

48. Należy przyjąć dodatkowe gwarancje, gdy dane dotyczące lokalizacji są zbierane z pojazdów, które są używane podczas działalności zawodowej, aby zapobiec używaniu technologii lokalizacyjnej do niewłaściwego monitorowania pracowników. W każdym przypadku przetwarzanie powinno być ograniczone do zbierania danych dotyczących lokalizacji podczas czasu pracy – pracownicy powinni mieć zatem możliwość wyłączenia funkcji lokalizacyjnej poza godzinami pracy lub w momencie używania pojazdu do prywatnych celów.

49. Istnieje ryzyko, że strony trzecie (takie jak przedsiębiorstwa ubezpieczeniowe, pracodawcy i organy ścigania) będą wymagać dostępu do danych zebranych za pośrednictwem systemów nawigacji i śledzenia do uprawnionych i określonych celów (takich jak śledzenie towarów, elektroniczne uiszczanie opłat itd.), aby wykorzystać je do drugorzędnych celów, takich jak sprawdzanie czasu jazdy i okresów odpoczynku lub weryfikacja zgodności z przepisami drogowymi i nakładanie kar. Co do zasady dostęp do danych do celów drugorzędnych nie jest

([23]) Zob. kwestie prywatności i ochrony danych związane ze stosowaniem RFID w opinii Europejskiego Inspektora Ochrony Danych w sprawie komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie „Identyfikacji radiowej (RFID) w Europie: w stronę ram polityki" COM(2007) 96, Dz.U. C 101 z, 23.4.2008, s. 1. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EN.pdf

([24]) Grupa robocza art. 29, opinia w sprawie użycia danych lokalizacyjnych w celu świadczenia usług stanowiących wartość dodaną, WP 115, listopad 2005 r. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf

([25]) Zob. WP 125 w sprawie eCall, s. 5, wspomniany w przypisie 10.

dozwolony, jeżeli dostęp ten służy celom, które są niekompatybilne z celami, dla których dane zostały zgromadzone. Dostęp może być dozwolony na zasadzie odstępstwa od tej zasady, jedynie jeżeli warunki tego dostępu spełniają ścisłe wymogi art. 13 dyrektywy 95/46/WE. W rezultacie każdy dostęp do danych dotyczących lokalizacji dla stron trzecich powinien być udzielany zgodnie z prawem i w sposób przejrzysty na podstawie środka prawnego, który określa odpowiednie procedury i warunki dostępu do danych do konkretnych celów oraz który przewiduje odpowiednie gwarancje osobom zgodnie z dalszymi celami, dla których ich dane mogłyby być użyte.

III.2.b) *Role i zadania podmiotów ITS*

50. Nie jest jeszcze jasne, kto będzie administratorem danych na każdym etapie przetwarzania. W wielu wypadkach dostawcy usług ITS będą prawdopodobnie administratorami danych sami w odniesieniu do danych osobowych przetwarzanych do celów świadczenia ich własnych usług ITS albo wspólnie, w przypadku gdy przetwarzanie jest przeprowadzane wraz z innymi administratorami danych. Rola i zadania wypełniane przez operatorów zaangażowanych w ITS w różnym charakterze, jako administratorzy danych lub przetwórcy danych, są jasno określone w odniesieniu do każdego etapu przetwarzania (np. operatorzy komunikacyjni dostarczający usługi komunikacyjne, a także usługi ITS).

51. Osoby te działające jako administratorzy danych są odpowiedzialne ([26]) za zapewnienie zgodności systemów i usług ze wszystkimi obowiązkami dotyczącymi ochrony danych, w szczególności za wdrażanie systemów, które zakładają „poszanowanie prywatności od samego początku", które przestrzegają jakości danych i zasad ograniczenia do celu oraz gwarantują odpowiedni poziom bezpieczeństwa danych, jak opisano w III.1.

52. Administratorzy danych będą musieli dopilnować, aby obowiązywały odpowiednie gwarancje na wszystkich szczeblach łańcucha podmiotów zaangażowanych we wdrażanie ITS. Będzie to zwłaszcza wymagać, aby zawarli oni odpowiednie umowy ze wszystkimi podmiotami zaangażowanymi w wymianę i przetwarzanie danych, co powinno zapewnić odpowiednie gwarancje ochrony danych (w szczególności w odniesieniu do art. 16 i 17 dyrektywy 95/46/WE oraz art. 4 i 5 dyrektywy 2002/58/WE). Ważne jest, aby odnotować, że podczas gdy z perspektywy ochrony danych administratorzy danych muszą zapewniać ochronę danych na wszystkich etapach przetwarzania, to pozostają oni odpowiedzialni za przetwarzanie i nie mogą wyłączyć tej odpowiedzialności umową.

IV. **WNIOSKI**

53. EIOD z zadowoleniem przyjmuje zaproponowany plan wdrażania ITS przekazany przez Komisję, którego celem jest zharmonizowanie przetwarzania danych w całej Europie, tak aby ułatwić świadczenie usług ITS, i w którym ochrona danych jest określona jako podstawowy warunek właściwego wdrażania ITS w Europie.

54. EIOD odnotowuje fakt, że proponowana dyrektywa wyznacza ogólne ramy, które przywołują pewne problemy związane z prywatnością i ochroną danych, którymi należy się dalej zająć na szczeblu UE i krajowym:

— istnieje ryzyko, że brak jasności proponowanych ram prawnych spowoduje rozbieżność wprowadzania ITS w Europie, co doprowadzi do różnych poziomów ochrony danych w Europie. EIOD podkreśla potrzebę dalszej harmonizacji w odniesieniu do tych zagadnień na szczeblu UE, aby wyjaśnić nierozstrzygnięte kwestie (takie jak definicja ról i zadań podmiotów ITS, które konkretne aplikacje i systemy ITS muszą być wbudowane w pojazdy, rozwój zharmonizowanych umów do celów świadczenia usług ITS, konkretne cele i warunki używania ITS itd.). Szczególnie istotne jest, aby określić, kto będzie administratorem danych w odniesieniu do dokonywanego przetwarzania danych, ponieważ administratorzy ci będą ponosić odpowiedzialność za uwzględnienie uwag dotyczących prywatności i ochrony danych na wszystkich szczeblach łańcucha przetwarzania,

— decyzje dotyczące pewnych warunków przetwarzania, które mogłyby poważnie wpłynąć na prawa osób związane z prywatnością i ochroną danych, powinny być podjęte przez Parlament Europejski i Radę, a nie w drodze procedury komitetowej,

— kluczowe jest, aby prywatność i ochronę danych uwzględniać od wczesnego etapu przetwarzania i na wszystkich etapach przetwarzania; przy projektowaniu aplikacji i systemów ITS należy zachęcać do „poszanowania prywatności od samego początku" i włączać tę zasadę do standardów, najlepszych praktyk, specyfikacji technicznych i systemów,

— każde wzajemne połączenie aplikacji i systemów powinno nastąpić z właściwym poszanowaniem zasad ochrony danych i praktycznych gwarancji w zakresie bezpieczeństwa,

— w odniesieniu do niepewności, które pozostają na tym etapie, dotyczących warunków wdrażania ITS, EIOD przyjmuje w szczególności z zadowoleniem zgłoszoną przez Komisję w jej komunikacie inicjatywę, aby do 2011 roku przeprowadzić ocenę w zakresie prywatności. Ponadto z naciskiem zaleca, aby ocenę skutków dla prywatności i ochrony danych przeprowadzić w związku z konkretnymi sektorami lub celami użycia w celu określenia odpowiednich środków bezpieczeństwa oraz aby opracowane zostały najlepsze dostępne techniki dotyczące prywatności, ochrony danych i bezpieczeństwa ITS,

— EIOD podkreśla ponadto, że państwa członkowskie będą odpowiedzialne za wykonanie dyrektywy w odpowiedni sposób, tak aby operatorzy ITS wdrożyli systemy i usługi, które zapewniają odpowiedni poziom ochrony danych osobowych w całej Europie,

([26]) Zob. przypis 13.

— administratorzy danych świadczący usługi ITS powinni wprowadzić odpowiednie gwarancje, tak aby użycie technologii lokalizacyjnych, takich jak nawigacja satelitarna i identyfikatory RFID, nie ingerowało w prywatność osób używających pojazdów zarówno w ściśle prywatnym, jak i zawodowym kontekście. Będzie to zwłaszcza wymagać ograniczenia przetwarzania danych do danych ściśle koniecznych do tego celu przy zapewnieniu, że odpowiednie środki bezpieczeństwa są wbudowane w systemy, tak aby dane dotyczące lokalizacji nie były ujawniane osobom nieupoważnionym, oraz przy dostarczaniu użytkownikom skutecznych środków dezaktywacji urządzenia/funkcji lokalizacyjnej.

55. EIOD zaleca, aby zmienić art. 6 wniosku zgodnie z dyrektywą 95/46/WE, w sposób następujący:

— należy zachęcać do użycia minimalnej ilości danych do celów przetwarzania danych dokonywanego za pośrednictwem ITS. W związku z tym zaleca się zmianę art. 6 ust. 1b wniosku w następujący sposób: „Dane osobowe są przetwarzane tylko w zakresie, w którym przetwarzanie to jest konieczne do konkretnego celu, dla którego ITS jest używane, i zgodnie z odpowiednią podstawą prawną”,

— ważne jest, aby dane osobowe przetwarzane za pośrednictwem interoperacyjnych systemów nie były używane do innych celów, które nie są kompatybilne z celami, dla których zostały zgromadzone. Dlatego zaleca się zmianę art. 6 ust. 2 w sposób następujący: „i nie mogą być używane do celów innych niż cele, do których zostały zgromadzone, w sposób niekompatybilny z tymi celami”,

— zaleca dodanie wyraźnego odniesienia w art. 6 wniosku do pojęcia „poszanowania prywatności od samego początku” przy projektowaniu aplikacji i systemów ITS. Ponadto zaleca, aby informowano grupę roboczą art. 29 i EIOD oraz by konsultowano się z nimi w przypadku dalszych działań podejmowanych w tej kwestii w drodze procedury komitetowej.

56. EIOD zaleca ponadto, by w motywach wniosku zawrzeć odniesienie do niniejszej konsultacji.

57. Biorąc pod uwagę powyższe rozważania, EIOD zaleca, aby organy ochrony danych, w szczególności za pośrednictwem grupy roboczej art. 29, oraz EIOD byli ściśle zaangażowani w inicjatywy związane z wdrażaniem ITS oraz by konsultowano się z nimi na dostatecznie wczesnym etapie rozwoju odpowiednich środków.

Sporządzono w Brukseli dnia 22 lipca 2009 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych