

Dziennik Urzędowy C 280

Unii Europejskiej



Wydanie polskie

Informacje i zawiadomienia

Tom 53

16 października 2010

<u>Powiadomienie nr</u>	Spis treści	Strona
I <i>Rezolucje, zalecenia i opinie</i>		
OPINIE		
Europejski Inspektor Ochrony Danych		
2010/C 280/01	Opinia Europejskiego Inspektora Ochrony Danych w sprawie wspierania zaufania w społeczeństwie informacyjnym poprzez działanie na rzecz ochrony danych i prywatności	1
2010/C 280/02	Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie zużytego sprzętu elektrycznego i elektronicznego (WEEE) ...	16
II <i>Komunikaty</i>		
KOMUNIKATY INSTYTUCJI, ORGANÓW I JEDNOSTEK ORGANIZACYJNYCH UNII EUROPEJSKIEJ		
Komisja Europejska		
2010/C 280/03	Zatwierdzenie pomocy państwa zgodnie z art. 107 i 108 TFUE – Sprawy, w których Komisja nie wnosi zastrzeżeń ⁽¹⁾	22
2010/C 280/04	Zatwierdzenie pomocy państwa zgodnie z art. 107 i 108 TFUE – Sprawy, w których Komisja nie wnosi zastrzeżeń ⁽¹⁾	26

PL

Cena:
3 EUR

⁽¹⁾ Tekst mający znaczenie dla EOG, z wyjątkiem działań wchodzących w zakres załącznika I do Traktatu

(Ciąg dalszy na następnej stronie)

<u>Powiadomienie nr</u>	Spis treści (ciąg dalszy)	Strona
2010/C 280/05	Zatwierdzenie pomocy państwa zgodnie z art. 107 i 108 TFUE – Sprawy, w których Komisja nie wnosi zastrzeżeń ⁽¹⁾	29
2010/C 280/06	Zatwierdzenie pomocy państwa zgodnie z art. 107 i 108 TFUE – Sprawy, w których Komisja nie wnosi zastrzeżeń ⁽¹⁾	30

IV *Informacje*

INFORMACJE INSTYTUCJI, ORGANÓW I JEDNOSTEK ORGANIZACYJNYCH UNII EUROPEJSKIEJ

Komisja Europejska

2010/C 280/07	Kursy walutowe euro	31
2010/C 280/08	Decyzja Komisji z dnia 14 października 2010 r. powołująca ponownie CARS 21 – grupę wysokiego szczebla ds. konkurencyjności i zrównoważonego rozwoju przemysłu motoryzacyjnego w Unii Europejskiej	32

V *Ogłoszenia*

POSTĘPOWANIA ZWIĄZANE Z REALIZACJĄ POLITYKI KONKURENCJI

Komisja Europejska

2010/C 280/09	Zgłoszenie zamiaru koncentracji (Sprawa COMP/M.5927 – BASF/Cognis) ⁽²⁾	35
2010/C 280/10	Zgłoszenie zamiaru koncentracji (Sprawa COMP/M.5982 – CVCII/Advance Properties/Huvepharma) – Sprawa, która może kwalifikować się do rozpatrzenia w ramach procedury uproszczonej ⁽²⁾	36
2010/C 280/11	Komunikat Ministra Gospodarki Królestwa Niderlandów wydany na podstawie art. 3 ust. 2 dyrektywy 94/22/WE Parlamentu Europejskiego i Rady w sprawie warunków udzielania i korzystania z zezwoleń na poszukiwanie, badanie i produkcję węglowodorów	37



⁽¹⁾ Tekst mający znaczenie dla EOG, z wyjątkiem działań wchodzących w zakres załącznika I do Traktatu

⁽²⁾ Tekst mający znaczenie dla EOG

(Ciąg dalszy na wewnętrznej tylnej stronie okładki)

I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych w sprawie wspierania zaufania w społeczeństwie informacyjnym poprzez działanie na rzecz ochrony danych i prywatności

(2010/C 280/01)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16,

uwzględniając Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 7 i 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⁽¹⁾,

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⁽²⁾,

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⁽³⁾, w szczególności jego art. 41,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. WPROWADZENIE

1. Technologie informacyjno-komunikacyjne (TIK) dają ogromne możliwości w praktycznie każdym aspekcie naszego życia – pracy, rozrywce, życiu towarzyskim i edukacji. Są one niezbędne w dzisiejszej gospodarce informacyjnej i ogólnie w społeczeństwie.

⁽¹⁾ Dz.U. L 281 z 23.11.1995, s. 31.

⁽²⁾ Dz.U. L 201 z 31.7.2002, s. 37.

⁽³⁾ Dz.U. L 8 z 12.1.2001, s. 1.

2. Unia Europejska jest światową potęgą w zaawansowanych TIK i jest zdecydowana utrzymać taki stan rzeczy. Oczekuje się, że aby sprostać temu wyzwaniu, Komisja Europejska niedługo przyjmie nową europejską agendę cyfrową, której priorytetowe znaczenie potwierdziła komisarz Kroes⁽⁴⁾.

3. EIOD uznaje korzyści wynikające ze stosowania TIK i zgadza się, że UE powinna dołożyć wszelkich starań, aby promować rozwój tych technologii i ich powszechne przyjmowanie. EIOD w pełni popiera także poglądy komisarzy Kroes i Reding, zgodnie z którymi podstawą tego nowego środowiska powinny być osoby fizyczne⁽⁵⁾. Osoby fizyczne powinny mieć możliwość polegania na zdolności TIK do zapewnienia bezpieczeństwa informacji i kontrolowania ich wykorzystania, a także powinny mieć pewność, że ich prawa do prywatności i ochrony danych będą respektowane w przestrzeni cyfrowej. Poszanowanie tych praw jest niezbędne do zwiększania zaufania konsumentów. Zaufanie to jest z kolei istotne, aby obywatele korzystali z nowych usług⁽⁶⁾.

⁽⁴⁾ Odpowiedzi na kwestionariusz Parlamentu Europejskiego dla komisarz Neelie Kroes w kontekście przesłuchania w Parlamencie Europejskim, które poprzedzało mianowanie komisarza.

⁽⁵⁾ Odpowiedzi na kwestionariusz Parlamentu Europejskiego dla komisarz Neelie Kroes w kontekście przesłuchania w Parlamencie Europejskim, które poprzedzało mianowanie komisarza; przemówienie komisarz Viviane Reding na temat europejskiej agendy cyfrowej dla nowych konsumentów cyfrowych, wygłoszone na wielostronnym forum Europejskiej Organizacji Konsumentów pt. „Prywatność konsumentów i marketing internetowy: tendencje rynkowe i perspektywy w zakresie polityki” (Consumer Privacy and Online Marketing: Market Trends and Policy Perspectives), Bruksela, dnia 12 listopada 2009 r.

⁽⁶⁾ Zob. np. sprawozdanie RISEPTIS pt. „Trust in the Information Society”, Sprawozdanie Rady Doradczej RISEPTIS (badania i innowacje na rzecz bezpieczeństwa, prywatności i wiarygodności w społeczeństwie informacyjnym). Dostępne pod adresem <http://www.think-trust.eu/general/news-events/riseptis-report.html> Zob. także: J. B. Horrigan, „Broadband Adoption and Use in America”, Inicjatywa Szerokopasmowa Omnibus (Omnibus Broadband Initiative) Federalnej Komisji Łączności (Federal Communications Commission), OBI Working Paper Series No 1.

4. UE ma silne ramy prawne w zakresie ochrony danych i prywatności, których zasady pozostają całkowicie uzasadnione w erze cyfrowej. Nie można jednak popadać w samozadowolenie. W wielu przypadkach TIK dają podstawy do nowych obaw, które nie są uwzględnione w istniejących ramach. Konieczne są zatem pewne działania, aby dopilnować, że poszczególne prawa przewidziane w prawodawstwie UE w dalszym ciągu zapewniają skuteczną ochronę w tym nowym środowisku.
5. W niniejszej opinii omówiono środki, które Unia Europejska może promować lub podejmować w celu zagwarantowania ochrony prywatności osób fizycznych i danych w zglobalizowanym świecie, którego siłą napędową nadal będą technologie. Przedstawiono tu instrumenty ustawodawcze i o charakterze nieustawodawczym.
6. Po przedstawieniu w ogólnym zarysie TIK jako nowych osiągnięć, które dają możliwości, ale i stwarzają zagrożenie, w opinii omówiono potrzebę zintegrowania – na poziomie praktycznym – ochrony danych i prywatności od samego powstania nowych technologii informacyjno-komunikacyjnych (co jest nazywane zasadą poszanowania prywatności od samego początku). Aby zapewnić zgodność z tą zasadą, w opinii omówiono potrzebę uwzględnienia – na co najmniej dwa różne sposoby – zasady poszanowania prywatności od samego początku w ramach prawnych dotyczących ochrony danych. Po pierwsze, poprzez włączenie jej jako ogólnej obowiązującej zasady, a po drugie – poprzez włączenie jej w konkretne obszary TIK stanowiące określone zagrożenia dla ochrony danych/prywatności, które to zagrożenia można zmniejszyć dzięki odpowiedniej architekturze technicznej i projektowi. Obszary te to identyfikacja radiowa (ang. radio frequency identification, RFID), aplikacje portali społecznościowych i aplikacje przeglądarek. Ponadto w opinii zawarto zalecenia dotyczące innych narzędzi i zasad mających na celu ochronę prywatności osób fizycznych i danych w sektorze TIK.
7. W odniesieniu do powyższych kwestii w niniejszej opinii omówiono niektóre uwagi grupy roboczej art. 29 poczynione w ramach wkładu do konsultacji publicznych na temat przyszłości prywatności⁽¹⁾. Niniejsza opinia jest ponadto oparta na wcześniejszych opiniach EIOD, takich jak: opinia z dnia 25 lipca 2007 r. w sprawie dyrektywy o ochronie danych, opinia z dnia 20 grudnia 2007 r.

w sprawie RFID i dwie opinie w sprawie dyrektywy o prywatności i łączności elektronicznej⁽²⁾.

II. TIK DAJĄ NOWE MOŻLIWOŚCI, ALE STANOWIĄ TAKŻE NOWE ZAGROŻENIA

8. TIK są porównywane z innymi ważnymi wynalazkami z przeszłości, takimi jak elektryczność. Chociaż może być zbyt wcześnie na ocenę ich rzeczywistego wpływu historycznego, związek pomiędzy TIK a rozwojem gospodarczym w krajach rozwiniętych jest wyraźny. TIK tworzą miejsca pracy, dają korzyści gospodarcze i przyczyniają się do wzrostu ogólnego dobrobytu. Wpływ TIK wykracza poza kwestie czysto gospodarcze, ponieważ technologie te odgrywają ważną rolę w stymulowaniu innowacyjności i kreatywności.
9. Ponadto TIK zmieniły sposób, w jaki ludzie pracują, prowadzą życie towarzyskie i nawiązują wzajemne kontakty. Na przykład ludzie w coraz większym stopniu polegają na TIK w relacjach społecznych i gospodarczych. Osoby fizyczne mogą korzystać z szeregu nowych zastosowań TIK, np. w dziedzinie e-zdrowia, e-transportu i e-administracji, a także z innowacyjnych interaktywnych systemów w zakresie rozrywki i nauki.
10. W świetle tych korzyści wszystkie instytucje Unii Europejskiej wyraziły zobowiązanie do wspierania TIK jako narzędzia niezbędnego do zwiększenia konkurencyjności przemysłu europejskiego i przyspieszenia tempa naprawy gospodarczej w Europie. W sierpniu 2009 r. Komisja przyjęła sprawozdanie w sprawie konkurencyjności Europy w dziedzinie technologii cyfrowych⁽³⁾ i rozpoczęła konsultacje społeczne na temat odpowiednich przyszłych strategii promujących TIK. W dniu 7 grudnia 2009 r. Rada przyjęła konkluzje stanowiące wkład do tych konsultacji pt. „Po strategii i2010 – ku otwartemu, zielonemu i konkurencyjnemu społeczeństwu wiedzy”⁽⁴⁾. Niedawno Parlament Europejski przyjął

⁽¹⁾ Opinia grupy roboczej art. 29 WP 168 „Przyszłość prywatności. Wspólny wkład w konsultacje Komisji Europejskiej w sprawie ram prawnych dotyczących podstawowego prawa do ochrony danych osobowych” (The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data), przyjęta w dniu 1 grudnia 2009 r.

⁽²⁾ Opinia EIOD z dnia 25 lipca 2007 r. w sprawie komunikatu Komisji dla Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych, Dz.U. C 255 z 27.10.2007, s. 1; opinia EIOD z dnia 20 grudnia 2007 r. 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; opinia EIOD z dnia 10 kwietnia 2008 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady zmieniającej m.in. dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz.U. C 181 z 18.7.2008, s. 1; druga opinia EIOD z dnia 9 stycznia 2009 r. w sprawie przeglądu dyrektywy 2002/58/WE dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej).

⁽³⁾ Sprawozdanie w sprawie konkurencyjności Europy w dziedzinie technologii cyfrowych – Najważniejsze osiągnięcia strategii i2010 w latach 2005–2009, (SEC(2009) 1060).

⁽⁴⁾ Konkluzje Rady „Po strategii i2010 – ku otwartemu, zielonemu i konkurencyjnemu społeczeństwu wiedzy” (17107/09), przyjęte w dniu 18.12.2009 r.

sprawozdanie mające na celu dostarczenie Komisji wskazań w zakresie określenia agendy cyfrowej⁽¹⁾.

11. Wraz z możliwościami i korzyściami towarzyszącymi rozwojowi TIK pojawiają się nowe zagrożenia, szczególnie dla prywatności i ochrony danych osobowych dotyczących osób fizycznych. TIK na ogół prowadzą do szybkiego wzrostu (dość często w sposób niewidoczny dla osób fizycznych) liczby informacji gromadzonych, przechowywanych, filtrowanych, przekazywanych lub w inny sposób zatrzymywanych, i dlatego mnożą się zagrożenia dla tych danych.
12. Na przykład procesory RFID zastępują kody kreskowe na (niektórych) produktach konsumenckich. Poprzez poprawę przepływu informacji w łańcuchu dostaw (a zatem zmniejszenie potrzeby utrzymywania bezpiecznego poziomu zapasów, zapewniania dokładniejszych prognoz itp.) nowy system ma przynosić korzyści zarówno przedsiębiorstwom, jak i konsumentom. Jednakże jednocześnie zwiększa się niepokojąca możliwość bycia śledzonym, dla różnych celów i przez różne podmioty, za pośrednictwem dóbr osobistych opatrzonych etykietami.
13. Innym przykładem jest tzw. „przetwarzanie w chmurze” (ang. cloud computing), które polega na świadczeniu za pośrednictwem Internetu usług konsumenckich i niekonsumenckich dostarczanych przez organizacje zewnętrzne. Zakres tych usług jest bardzo szeroki – od bibliotek fotografii, kalendarzy, poczty elektronicznej i baz danych konsumentów po bardziej złożone usługi okołobiznesowe. Korzyści zarówno dla przedsiębiorstw, jak i osób fizycznych są oczywiste – obniżenie kosztów (koszty są przyrostowe), mniejsze uzależnienie od lokalizacji (łatwy dostęp do informacji w dowolnym miejscu świata), automatyzacja (brak konieczności posiadania dedykowanych zasobów informatycznych i aktualizowania oprogramowania) itp. Jednocześnie istnieje bardzo realne zagrożenie zakłóceniami bezpieczeństwa i hakerstwem. Istnieje także obawa o utratę dostępu do własnych danych i kontroli nad nimi.
14. Wykazano, że korzyści i zagrożenia współistnieją w innych obszarach wykorzystujących TIK. Przykładem jest dziedzina e-zdrowia, która może zwiększać efektywność, obniżać koszty, zwiększać dostępność i ogólnie poprawiać jakość usług opieki zdrowotnej. Jednakże z e-zdrowiem często wiąże się kwestia legalności wtórnego wykorzystywania informacji dotyczących e-zdrowia, wymagająca dokładnej analizy celów każdego potencjalnego wtórnego wykorzystania⁽²⁾. Ponadto wraz z powszechniejszym stosowaniem elektronicznych kart zdrowia systemy takich kart stają się przedmiotem skandalów ujawniających wiele przypadków nieupoważnionego dostępu.

⁽¹⁾ Sprawozdanie w sprawie określenia nowej agendy cyfrowej dla Europy – od i2010 do digital.eu (2009/2225 (INI)), przyjęte w dniu 18.3.2010 r.

⁽²⁾ Na przykład sprzedaż lub wykorzystywanie informacji na temat stanu zdrowia gromadzonych na potrzeby prowadzenia leczenia nie mogą mieć na celu wybierania lokalizacji dla przychodni satelickich, tworzenia ośrodków leczenia ambulatoryjnego oraz innych rodzajów planowania przyszłych działań o skutkach finansowych, które wymagałyby dokładnego zbadania.

15. Podsumowując, prawdopodobnie pozostanie pewien poziom szczytkowego ryzyka nawet po dokonaniu odpowiednich ocen i zastosowaniu koniecznych środków. Całkowity brak zagrożenia byłby nierealny. Jednakże, jak omówiono poniżej, można i trzeba wdrożyć środki ograniczające takie zagrożenia do stosownego poziomu.

III. POSZANOWANIE PRYWATNOŚCI OD SAMEGO POCZĄTKU JAKO NAJWAŻNIEJSZE NARZĘDZIE ZWIĘKSZANIA INDYWIDUALNEGO POZIOMU ZAUFANIA DO TIK

16. Z potencjalnych korzyści wynikających z TIK można w praktyce korzystać tylko wtedy, gdy technologie te są w stanie zwiększać poziom zaufania – innymi słowy, gdy ze względu na swoje właściwości i korzyści mogą zapewnić gotowość użytkowników do polegania na TIK. Zaufanie będzie rosło jedynie wtedy, gdy TIK będą niezawodne, bezpieczne, pozostające pod kontrolą osób fizycznych i gdy gwarantowana będzie ochrona danych osobowych i prywatności użytkowników.
17. Powszechne zagrożenia i niepowodzenia, takie jak przedstawione poniżej, mogą szkodzić zaufaniu użytkownika do społeczeństwa informacyjnego, szczególnie gdy wiążą się z wykorzystaniem danych osobowych niezgodnie z przeznaczeniem lub ich naruszeniem ze szkodą dla prywatności osób fizycznych. Może to poważnie zagrażać rozwojowi TIK i korzyściom, które mogą przynosić.
18. Jednakże rozwiązanie problemu tych zagrożeń dla prywatności i ochrony danych nie może polegać na wyeliminowaniu, wykluczeniu ani odmowie wykorzystywania lub promowania TIK. Byłoby to niewykonalne i nierealne; uniemożliwiłoby osobom fizycznym korzystanie z korzyści płynących z TIK i poważnie ograniczyłoby ogólne korzyści, jakie można uzyskać dzięki tym technologiom.
19. EIOD uważa, że bardziej pozytywnym rozwiązaniem jest projektowanie i rozwijanie TIK z poszanowaniem prywatności i ochrony danych. Jest zatem niezwykle istotne, aby uwzględnić prywatność i ochronę danych w całym cyklu życia technologii, od najwcześniejszego etapu projektowania po jej ostateczne wprowadzenie, użytkowanie i ostateczne usunięcie. Rozwiązanie to jest zwykle nazywane „poszanowaniem prywatności od samego początku”. Poniżej omówiono je bardziej szczegółowo.
20. Poszanowanie prywatności od samego początku może wiązać się z różnymi działaniami w zależności od konkretnego przypadku lub zastosowania. W niektórych przypadkach może ono np. wymagać wyeliminowania/ograniczenia danych osobowych bądź zapobiegania zbędnemu lub niepożądanemu przetwarzaniu. W innych przypadkach może ono wiązać się z oferowaniem narzędzi zwiększających kontrolę użytkowników nad ich własnymi danymi osobowymi. Takie środki należy rozważać przy określaniu norm lub najlepszych praktyk. Mogą one także

być wprowadzone w architekturze systemów informacyjno-komunikacyjnych lub w strukturalnej organizacji podmiotów przetwarzających dane osobowe.

III.1. Zasada poszanowania prywatności od samego początku stosowana w różnych środowiskach TIK i ich wpływ

21. Potrzeba zasady poszanowania prywatności od samego początku występuje w wielu różnych środowiskach TIK. Na przykład sektor opieki zdrowotnej jest w coraz większym stopniu uzależniony od infrastruktury TIK, która często wiąże się ze scentralizowanym przechowywaniem informacji dotyczących stanu zdrowia pacjentów. Zastosowanie zasady poszanowania prywatności od samego początku w sektorze opieki zdrowotnej wymagałoby oceny stosowności różnych środków, takich jak: możliwość ograniczenia do minimum ilości danych przechowywanych centralnie lub ograniczenia ich do indeksu, stosowanie narzędzi szyfrujących, przyznawanie prawa dostępu na zasadzie ograniczonego dostępu, anonimizacja danych, gdy nie są już potrzebne itp.
22. Podobnie systemy transportowe są coraz częściej oferowane domyślnie z zaawansowanymi zastosowaniami TIK, które komunikują się z pojazdem i jego otoczeniem dla różnych celów i na potrzeby różnych funkcji. Na przykład samochody są coraz częściej wyposażane w nowe funkcje TIK (GPS, GSM, sieć czujników itd.), które rejestrują nie tylko ich lokalizację, ale także warunki techniczne w czasie rzeczywistym. Informacje te można wykorzystać na przykład w celu zastąpienia istniejącego systemu podatku drogowego opłatami drogowymi zależnymi od użytkownika. Zastosowanie zasady poszanowania prywatności od samego początku w projekcie architektury tych systemów powinno wspierać przetwarzanie i dalsze przekazywanie jak najmniejszej ilości danych osobowych⁽¹⁾. Zgodnie z tą zasadą zdecentralizowana lub połowicznie zdecentralizowana architektura ograniczająca ujawnianie danych dotyczących lokalizacji do punktu centralnego byłaby bardziej pożądana niż architektura scentralizowana.
23. Powyższe przykłady pokazują, że tworzenie technologii informacyjno-komunikacyjnych zgodnie z zasadą poszanowania prywatności od samego początku może znacznie ograniczyć zagrożenia dla prywatności i ochrony danych.

⁽¹⁾ Zob. opinia Europejskiego Inspektora Ochrony Danych z dnia 22 lipca 2009 r. 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, dostępna pod adresem: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_PL.pdf

III.2. Niewystarczające wprowadzenie TIK stosujących zasadę poszanowania prywatności od samego początku

24. Ważną kwestią jest to, czy podmioty gospodarcze, producenci/dostawcy TIK i administratorzy danych są zainteresowani marketingiem i wdrażaniem zasady poszanowania prywatności od samego początku w TIK. W tym kontekście ważne jest również ocenienie zapotrzebowania użytkowników na tę zasadę.
25. W 2007 r. Komisja wydała komunikat wzywający przedsiębiorstwa do wykorzystywania swojej siły innowacji do tworzenia i wdrażania technologii na rzecz ochrony prywatności w celu poprawienia ochrony prywatności i danych osobowych od samego początku cyklu rozwoju⁽²⁾.
26. Dostępne dowody wykazują jednak, że dotychczas ani producenci TIK, ani administratorzy danych (zarówno w sektorze prywatnym, jak i publicznym) nie byli w stanie spójnie wdrożyć zasady poszanowania prywatności od samego początku ani wprowadzić tej zasady na rynek. Wskazuje się różne przyczyny takiej sytuacji, w tym brak zachęt gospodarczych lub wsparcia instytucjonalnego, niewystarczające zapotrzebowanie itp.⁽³⁾.
27. Jednocześnie zapotrzebowanie użytkowników na poszanowanie prywatności od samego początku jest dość małe. Użytkownicy produktów i usług TIK mogą słusznie zakładać, że ich prywatność i dane osobowe są faktycznie chronione, chociaż w wielu przypadkach tak nie jest. W niektórych przypadkach zwykle nie są oni w stanie przyjąć środków bezpieczeństwa niezbędnych do ochrony własnych danych osobowych lub danych innych osób. Sytuacja ta często wynika z braku pełnej czy nawet częściowej wiedzy użytkowników na temat tych zagrożeń. Na przykład, ogólnie rzecz biorąc, młodzież lekceważy zagrożenia dla prywatności związane z udostępnianiem danych osobowych na portalach społecznościowych i często ignoruje ustawienia dotyczące prywatności. Inni użytkownicy zdają sobie sprawę z zagrożeń, ale mogą nie mieć wiedzy technicznej koniecznej do wdrożenia technologii ochronnych, np. zabezpieczających połączenie z Internetem, lub do zmiany ustawień wyszukiwarki w celu zminimalizowania możliwości tworzenia profilu w oparciu o monitorowanie czynności związanych z surfowaniem po Internecie.
28. Zagrożenia dla ochrony prywatności i danych są jednak bardzo realne. Jeżeli prywatność i ochrona danych nie są uwzględniane od samego początku, często jest za późno na naprawę systemów i jest ona zbyt droga; za późno też jest na naprawienie już spowodowanych szkód. Rosnąca liczba przypadków naruszenia danych osobowych

⁽²⁾ Komunikat Komisji dla Parlamentu Europejskiego i Rady w sprawie lepszej ochrony danych z wykorzystaniem technologii na rzecz ochrony prywatności, 2.5.2007 r., (COM(2007) 228 wersja ostateczna).

⁽³⁾ Badanie dotyczące korzyści gospodarczych wynikających z technologii na rzecz ochrony prywatności (privacy enhancing technologies — PETs), jls/2008/D4/036.

w ostatnich latach doskonale odzwierciedla ten problem i zwiększa potrzebę poszanowania prywatności od samego początku.

29. Powyższe stwierdzenia wyraźnie wskazują na to, że producenci i dostawcy TIK mających na celu przetwarzanie danych osobowych powinni być odpowiedzialni – wraz z administratorami danych – za projektowanie ich z uwzględnieniem ochrony danych i zabezpieczeń prywatności. W wielu przypadkach oznaczałoby to, że technologie te powinny być projektowane z domyślnymi ustawieniami prywatności.
30. W tym kontekście trzeba rozważyć, jakie kroki powinny podjąć osoby odpowiedzialne za wyznaczanie kierunków polityki w tej dziedzinie, aby wspierać poszanowanie prywatności od samego początku w rozwoju TIK. Pierwsze pytanie dotyczy tego, czy istniejące ramy prawne w dziedzinie ochrony danych zawierają odpowiednie przepisy mające na celu zapewnienie wdrożenia zasady poszanowania prywatności od samego początku przez zarówno administratorów danych, jak i producentów/twórców. Drugie pytanie odnosi się do tego, co należy zrobić w kontekście europejskiej agendy cyfrowej, aby zagwarantować, że sektor TIK zwiększy zaufanie konsumentów.

IV. WPROWADZENIE ZASADY POSZANOWANIA PRYMATNOŚCI OD SAMEGO POCZĄTKU DO PRAWA I POLITYKI UE

IV.1. Obecne ramy prawne dotyczące ochrony danych i prywatności

31. UE posiada szeroko zakrojone ramy dotyczące ochrony danych i prywatności, które zapisane są w dyrektywie 95/46/WE⁽¹⁾, dyrektywie 2002/59/WE⁽²⁾ oraz w praktyce sądowej Europejskiego Trybunału Praw Człowieka⁽³⁾ i Trybunału Sprawiedliwości.
32. Dyrektywa o ochronie danych stosuje się do „każdej operacji lub zestawu operacji dokonywanych na danych osobowych” (gromadzenia, przechowywania, ujawniania itd.). Nakłada na podmioty, które przetwarzają dane osobowe („administratorów danych”) wymóg zgodności z określonymi zasadami oraz obowiązki. Określono w niej prawa osób fizycznych, takie jak prawo dostępu do danych osobowych. Dyrektywa o prywatności i łączności elektronicznej dotyczy w szczególności ochrony prywatności w sektorze łączności elektronicznej⁽⁴⁾.

(1) Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady (zwana dalej „dyrektywą o ochronie danych”).

(2) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady (zwana dalej „dyrektywą o prywatności i łączności elektronicznej”).

(3) Zawierającej wykładnię głównych pojęć i warunków zawartych w art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (EKPC), przyjętej w Rzymie w dniu 4 listopada 1950 r., z zastosowaniem ich do różnych dziedzin.

(4) Traktat lizboński zwiększył tę ochronę poprzez uznanie poszanowania życia prywatnego i ochrony danych osobowych za odrębne prawa podstawowe w art. 7 i 8 Karta praw podstawowych Unii Europejskiej. Karta praw podstawowych Unii Europejskiej stała się obowiązująca z chwilą wejścia w życie traktatu lizbońskiego.

33. Obecna dyrektywa o ochronie danych nie zawiera jednoznacznego wymogu poszanowania prywatności od samego początku. Obejmuje jednak przepisy, które pośrednio, w różnych sytuacjach, mogą wymagać wprowadzenia zasady poszanowania prywatności od samego początku. W szczególności art. 17 wymaga od administratorów danych wprowadzenia odpowiednich środków technicznych i organizacyjnych w celu zapobiegania nielegalnemu przetwarzaniu danych⁽⁵⁾. Poszanowanie prywatności od samego początku jest zatem ujęte w bardzo ogólny sposób. Ponadto przepisy dyrektywy dotyczą głównie administratorów danych oraz przetwarzania przez nich danych osobowych. Przepisy te nie zawierają wyraźnego wymogu, aby technologie informacyjno-komunikacyjne były zgodne z zasadami ochrony danych i prywatności, co wymaga również uwzględnienia w przepisach projektantów i wytwórców TIK, w tym działań prowadzonych na etapie normalizacji.

34. Dyrektywa o prywatności i łączności elektronicznej jest bardziej jednoznaczna. Jej art. 14 ust. 3 stanowi, że „w miarę potrzeb, możliwe jest przyjęcie środków w celu zapewnienia, że terminal jest skonstruowany w sposób zgodny z prawem użytkowników do ochrony i kontroli używania ich danych osobowych, zgodnie z dyrektywą 1999/5/WE i decyzją Rady 87/95/EWG z dnia 22 grudnia 1986 r. w sprawie normalizacji w dziedzinie technologii informatycznych i telekomunikacji”. Przepis ten jednak nie został nigdy wykorzystany⁽⁶⁾.

35. Podczas gdy powyższe przepisy obu dyrektyw są pomocne w promowaniu poszanowania prywatności od samego początku, w praktyce nie są wystarczające do zapewnienia uwzględnienia prywatności w TIK.

36. W wyniku powyższej sytuacji w prawodawstwie nie wymaga się w wystarczająco precyzyjny sposób projektowania TIK zgodnie z zasadą poszanowania prywatności od samego początku. Również organy ochrony danych nie posiadają wystarczających kompetencji do zapewnienia wprowadzenia zasady poszanowania prywatności od samego początku. Powoduje to nieskuteczność. Na przykład organy ochrony danych mogą mieć uprawnienia do nakładania sankcji za brak odpowiedzi na wnioski osób fizycznych o udzielenie dostępu do danych i będą posiadały kompetencje do żądania wdrożenia określonych środków w celu zapobieżenia nielegalnemu przetwarzaniu

(5) Artykuł 17 brzmi następująco: „Państwa członkowskie zapewniają, aby administrator danych wprowadził odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub przypadkową utratą, zmianą, niepozwolonym ujawnieniem lub dostępem, szczególnie wówczas gdy przetwarzanie danych obejmuje transmisję danych w sieci, jak również przed wszelkimi innymi nielegalnymi formami przetwarzania”. Motyw 46 uzupełnia go stwierdzeniem: „Ochrona praw i wolności osób, których dotyczą przetwarzane dane osobowe wymaga przyjęcia odpowiednich rozwiązań technicznych i organizacyjnych, zarówno przy opracowywaniu systemu przetwarzania danych, jak i podczas samego ich przetwarzania, szczególnie w celu utrzymania bezpieczeństwa i niedopuszczenia do niedozwolonego przetwarzania danych”.

(6) Komisja ogłosiła, że planuje zaktualizować dyrektywę 1999/5/WE pod koniec 2010 r.

danych. Jednak nie zawsze jest w wystarczającym stopniu jasne, czy ich kompetencje rozciągają się także na żądanie zaprojektowania systemu w sposób ułatwiający osobom fizycznym korzystanie z ich praw do ochrony danych⁽¹⁾. Na przykład na podstawie istniejących przepisów prawnych nie jest oczywiste, czy można wymagać, aby architektura systemu informacyjnego była zaprojektowana w sposób, który ułatwi przedsiębiorstwom reagowanie na wnioski o udzielenie dostępu do danych wystosowane przez osoby fizyczne, tak aby takie wnioski były przetwarzane automatycznie i szybciej. Ponadto późniejsze próby zmiany technologii już po jej opracowaniu lub wprowadzeniu mogą skutkować niespójnymi rozwiązaniami, które nie będą w pełni działały, a poza tym będą uciążliwe gospodarczo.

37. Z punktu widzenia EIOD, który to punkty widzenia podziela także grupa robocza art. 29⁽²⁾, obecne ramy prawne pozostawiają możliwość wyraźniejszego zatwierdzenia zasady poszanowania prywatności od samego początku.

IV.2. Wprowadzenie poszanowania prywatności od samego początku na różnych poziomach

38. W świetle powyższego EIOD zaleca Komisji cztery następujące kierunki działania:
- zapropozowanie włączenia ogólnego przepisu o poszanowaniu prywatności od samego początku do ram prawnych dotyczących ochrony danych;
 - rozwińnięcie tego ogólnego przepisu w przepisach szczegółowych, gdy w różnych sektorach zaproponowane zostaną szczegółowe instrumenty prawne. Te przepisy szczegółowe już mogłyby zostać włączone do instrumentów prawnych; na podstawie art. 17 dyrektywy o ochronie danych (oraz innych istniejących przepisów);
 - uwzględnienie poszanowania prywatności od samego początku jako naczelnej zasady europejskiej agendy cyfrowej;
 - wprowadzenie poszanowania prywatności od samego początku jako zasady w innych inicjatywach UE (głównie o charakterze nieustawodawczym).

⁽¹⁾ Zob. sprawozdanie biura brytyjskiego komisarza ds. informacji pt. „Poszanowanie prywatności od samego początku” (Privacy by Design), opublikowane w listopadzie 2008 r.

⁽²⁾ Zob. opinia grupy roboczej art. 29 WP 168 „Przyszłość prywatności. Wspólny wkład w konsultacje Komisji Europejskiej w sprawie ram prawnych dotyczących podstawowego prawa do ochrony danych osobowych” (The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data), przyjęta w dniu 1 grudnia 2009 r.

Ogólny przepis o poszanowaniu prywatności od samego początku

39. EIOD proponuje jednoznacznie i wyraźnie włączyć zasadę poszanowania prywatności od samego początku do istniejących ram regulacyjnych w zakresie ochrony danych. Mogłoby to wzmocnić i sprecyzować poszanowanie prywatności od samego początku, a także przyczynić się do jej efektywnego wprowadzenia, dodatkowo dając więcej uprawnień organom egzekucyjnym w zakresie wymagania jej faktycznego stosowania w praktyce. Jest to szczególnie konieczne w świetle faktów przedstawionych powyżej, nie tylko ze względu na znaczenie samej zasady jako narzędzia promującego zaufanie, ale również jako zachęty dla zainteresowanych stron do wprowadzenia poszanowania prywatności od samego początku i rozszerzenia gwarancji przewidzianych w istniejących ramach prawnych.
40. Wniosek ten opiera się na zaleceniu grupy roboczej art. 29 dotyczącym wprowadzenia zasady „poszanowania prywatności od samego początku” jako ogólnej zasady w zakresie ram prawnych dotyczących ochrony danych, w szczególności dyrektywy o ochronie danych. Według grupy roboczej art. 29: „Zasada ta powinna być wiążąca dla projektantów i producentów technologii, jak również dla administratorów danych, którzy muszą podejmować decyzje odnośnie do nabywania i wykorzystywania TIK. Powinni być zobowiązani do uwzględnienia technicznej ochrony danych już na etapie planowania informacyjno-technologicznych procedur i systemów. Dostawcy takich systemów lub usług, a także administratorzy powinni wykazać, że podjęli wszelkie środki konieczne do spełnienia tych wymogów”.
41. EIOD z zadowoleniem przyjmuje także poparcie komisarzy Viviane Reding dla zasady poszanowania prywatności od samego początku, wyrażone w kontekście zapowiedzi przeglądu dyrektywy o ochronie danych⁽³⁾.
42. Kolejną kwestią jest treść takiego uregulowania. Przede wszystkim ogólna zasada poszanowania prywatności od samego początku powinna być neutralna technologicznie. Celem tej zasady nie powinno być regulowanie technologii, tj. nie powinna zalecać określonych rozwiązań technicznych. Powinna natomiast przewidywać wprowadzenie istniejących zasad prywatności i ochrony danych do systemów i rozwiązań informacyjno-komunikacyjnych. Umożliwi to zainteresowanym stronom, producentom, administratorom danych oraz organom ochrony danych

⁽³⁾ „Poszanowanie prywatności od samego początku to zasada leżąca w interesie zarówno obywateli, jak i przedsiębiorstw. Poszanowanie prywatności od samego początku doprowadzi do lepszej ochrony osób fizycznych, a także do zwiększenia zaufania do nowych usług i produktów, co z kolei będzie miało pozytywny wpływ na gospodarkę. Istnieją pewne zachęcające przykłady, lecz bardzo wiele pozostaje do zrobienia”. Przemówienie programowe w Dniu Ochrony Danych, dnia 28 stycznia 2010 r., Parlament Europejski, Bruksela.

interpretowanie zasady w każdym poszczególnym przypadku. Po drugie, zgodność z tą zasadą powinna być obowiązkowa na różnych etapach, od tworzenia norm i projektowania architektury, po ich wdrażanie przez administratora danych.

Przepisy w konkretnych instrumentach prawnych

43. Obecne i przyszłe instrumenty ustawodawcze muszą zawierać zasadę poszanowania prywatności od samego początku w oparciu o istniejące ramy prawne oraz – po przyjęciu ogólnego przepisu zaproponowanego powyżej – w oparciu o ten ostatni. Na przykład zgodnie z aktualnymi inicjatywami związanymi z inteligentnymi systemami transportu Komisja będzie ponosiła w pierwszym etapie szczególną odpowiedzialność za zdefiniowanie środków, inicjatyw standaryzacyjnych, procedur i najlepszych praktyk. W trakcie wykonywania tych zadań poszanowanie prywatności od samego początku powinno być zasadą naczelną.
44. EIOD zwraca także uwagę, że zasada poszanowania prywatności od samego początku jest również szczególnie ważna w obszarze wolności, bezpieczeństwa i sprawiedliwości, zwłaszcza w odniesieniu do celów strategii zarządzania informacjami przewidzianej w programie sztokholmskim ⁽¹⁾. W swojej opinii w sprawie programu sztokholmskiego EIOD podkreślił, że architektura wymiany informacji powinna być oparta na „poszanowaniu prywatności od samego początku” ⁽²⁾: „Oznacza to konkretnie, że systemy informatyczne służące zapewnieniu bezpieczeństwa publicznego powinny być zawsze tworzone zgodnie z zasadą poszanowania prywatności od samego początku”.
45. W swojej opinii dotyczącej przyszłości prywatności ⁽³⁾ grupa robocza art. 29 jeszcze bardziej stanowczo nalega, aby w obszarze wolności, bezpieczeństwa i sprawiedliwości – gdzie organy publiczne odgrywają główną rolę i gdzie środki nadzoru bezpośrednio wpływają na podstawowe prawa do poszanowania prywatności i ochrony danych – wymogi poszanowania prywatności od samego początku były obowiązkowe. Poprzez wprowadzenie tych wymogów do systemów informacyjnych rządy mogłyby wspierać poszanowanie prywatności od samego początku w ramach swoich zdolności jako „klientów pilotażowych”.

⁽¹⁾ Program sztokholmski – Otwarta i bezpieczna Europa dla dobra i ochrony obywateli, zatwierdzony przez Radę Europejską w grudniu 2009 r.

⁽²⁾ Opinia Europejskiego Inspektora Ochrony Danych z dnia 10 lipca 2009 r. w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady dotyczącego przestrzeni wolności, bezpieczeństwa i sprawiedliwości w służbie obywateli, Dz.U. C 276 z 17.11.2009, s. 8, pkt 60.

⁽³⁾ Opinia grupy roboczej art. 29 WP 168 „Przyszłość prywatności. Wspólny wkład w konsultacje Komisji Europejskiej w sprawie ram prawnych dotyczących podstawowego prawa do ochrony danych osobowych” (The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data), przyjęta w dniu 1 grudnia 2009 r.

Poszanowanie prywatności od samego początku jako naczelną zasadą europejskiej agendy cyfrowej

46. Technologie informacyjno-komunikacyjne są coraz bardziej złożone i wiążą się z większymi zagrożeniami dla prywatności i ochrony danych. Na ogół informacje w formie cyfrowej, które łatwiej jest uzyskać, powielić i przesłać, narażone są na znacznie większe zagrożenie niż informacje w formie papierowej. Wraz z rozwojem sieci połączonych obiektów zagrożenia te będą się nasilać. Im większe będzie zagrożenie dla prywatności/ochrony danych, tym większe będzie zapotrzebowanie na silniejsze środki ochrony danych/prywatności. Z tego względu argument za koniecznością wprowadzenia w sektorze TIK zasady poszanowania prywatności od samego początku jest nie do odparcia. Ponadto, jak stwierdzono powyżej, zaufanie osób fizycznych do TIK ma zasadnicze znaczenie, jeśli mają one korzystać z tych nowych usług, a prywatność i ochrona danych są niezbędnymi elementami tego zaufania.
47. Powyżej podkreślono, że w ramach strategii rozwoju TIK trzeba potwierdzić potrzebę projektowania tych technologii z nieodłącznym elementem prywatności i ochrony danych, tj. z uwzględnieniem zasady poszanowania prywatności od samego początku.
48. W europejskiej agendzie cyfrowej należy zatem jednoznacznie poprzeć zasadę poszanowania prywatności od samego początku jako element niezbędny do zapewnienia zaufania obywateli do TIK i usług online. W agendzie tej należy stwierdzić, że prywatność i zaufanie idą w parze i że poszanowanie prywatności od samego początku powinno być nadrzędnym czynnikiem w rozwijaniu wiarygodnego sektora TIK.
- #### *Poszanowanie prywatności od samego początku jako zasada w innych inicjatywach UE*
49. Poszanowanie prywatności od samego początku powinno być dla Komisji zasadą naczelną we wdrażaniu polityki, działań i inicjatyw w określonych sektorach TIK, w tym w dziedzinie e-zdrowia, e-zamówień, e-zabezpieczenia społecznego, e-nauczania itp. Wiele z tych inicjatyw będzie punktami działania w ramach europejskiej agendy cyfrowej.

50. Oznacza to na przykład, że inicjatywy mające na celu zapewnienie większej skuteczności i nowoczesności usług administracyjnych, tak aby osoby fizyczne mogły kontaktować się z administracją, powinny uwzględniać potrzebę zaprojektowania i działania tych usług zgodnie z zasadą poszanowania prywatności od samego początku. Dotyczy to również polityki i działań Komisji na rzecz szybszego Internetu, treści cyfrowych lub ogólnego promowania stałej, bezprzewodowej komunikacji i transmisji danych.

51. Powyższe stwierdzenia odnoszą się także do obszarów, w których Komisja jest odpowiedzialna za zakrojone na szeroką skalę systemy informatyczne, takie jak SIS i VIS, a także do przypadków, w których odpowiedzialność Komisji ogranicza się do utworzenia i utrzymywania wspólnej infrastruktury takiego systemu, na przykład europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS).
52. Szczegółowy sposób rozwinięcia zasady poszanowania prywatności od samego początku będzie zależał od danego sektora i sytuacji. Na przykład gdy inicjatywom Komisji towarzyszą wnioski ustawodawcze dotyczące określonego sektora TIK, w wielu przypadkach stosowne będzie zawarcie w nich jednoznacznego odniesienia do pojęcia poszanowania prywatności od samego początku, które ma zastosowanie do projektu konkretnej aplikacji/systemu TIK. W przypadku opracowywania planów działania dla określonego obszaru powinny one systematycznie zapewniać stosowanie ram prawnych, a dokładniej gwarantować tworzenie danych TIK z uwzględnieniem poszanowania prywatności od samego początku.
53. Jeżeli chodzi o badania, to siódmy program ramowy i kolejne programy powinny być wykorzystywane w charakterze narzędzi wspierających projekty, które mają na celu analizowanie norm, TIK i architektury przyczynających się do wzmocnienia prywatności, a zwłaszcza zasady poszanowania prywatności od samego początku. Ponadto poszanowanie prywatności od samego początku powinno również stanowić niezbędny element, który należy uwzględnić w szerzej zakrojonych projektach z dziedziny TIK mających na celu przetwarzanie danych osobowych osób fizycznych.

Obszary będące przedmiotem szczególnego zainteresowania

54. W niektórych przypadkach, ze względu na określone zagrożenia dla prywatności i ochrony danych osób fizycznych lub z powodu innych czynników (opór sektora przed oferowaniem produktów uwzględniających poszanowanie prywatności od samego początku, zapotrzebowanie konsumentów itp.), konieczne może być określenie – w instrumentach ustawodawczych lub nie – bardziej jednoznacznych i szczegółowych środków w zakresie poszanowania prywatności od samego początku, które muszą być zawarte w określonym rodzaju produktu/technologii TIK.
55. EIOD zidentyfikował różne obszary (RFID, portale społecznościowe i aplikacje przeglądarek), które jego zdaniem wymagają na tym etapie dokładnego rozważenia przez Komisję i podjęcia praktycznych działań interwencyjnych, o których mowa powyżej. Te trzy obszary omówiono bardziej szczegółowo poniżej.

V. IDENTYFIKACJA RADIOWA – RFID

56. Etykiety RFID mogą być zintegrowane z przedmiotami, zwierzętami i ludźmi. Mogą być wykorzystane do gromadzenia i przechowywania danych osobowych takich jak ewidencja medyczna, do śledzenia przemieszczania się

ludzi lub do tworzenia profilu ich zachowań w różnych celach. Może się to odbywać bez wiedzy osoby fizycznej⁽¹⁾.

57. Efektywne gwarancje dotyczące ochrony danych, prywatności oraz wszystkich powiązanych wymiarów etycznych mają zasadnicze znaczenie dla zaufania publicznego do RFID oraz przyszłego Internetu przedmiotów. Jedynie wówczas technologia dostarczy wielu korzyści gospodarczych i społecznych.

V.1. Luki w obowiązujących ramach prawnych dotyczących ochrony danych

58. Dyrektywa o ochronie danych oraz dyrektywa o prywatności i łączności elektronicznej stosują się do gromadzenia danych przy pomocy zastosowań RFID⁽²⁾. Wymagają m.in. wprowadzenia odpowiednich środków ochrony prywatności na potrzeby zastosowań RFID⁽³⁾.
59. Jednakże te ramy prawne nie uwzględniają w pełni wszystkich kwestii ochrony danych i prywatności wiążących się z tą technologią. Wynika to z faktu, że dyrektywy

(1) Skrót RFID oznacza identyfikację radiową (ang. *radio frequency identification*). Główne elementy technologii lub infrastruktury identyfikacji radiowej to etykieta (np. mikroprocesor), czytnik oraz aplikacja połączona z etykietami i czytnikami za pośrednictwem oprogramowania pośredniczącego i przetwarzająca wytworzone dane. Etykieta składa się z obwodu elektronicznego, w którym przechowywane są dane, oraz z anteny, dzięki której dane są przekazywane drogą radiową. Czytnik posiada antenę i demodulator, który przetwarza informacje analogowe otrzymywane z łącza radiowego na dane cyfrowe. Informacje te można następnie wysłać za pośrednictwem sieci do baz danych i serwerów w celu przetworzenia przy pomocy komputera.

(2) W dyrektywie o prywatności i łączności elektronicznej odniesienie do RFID znajduje się w art. 3: „Niniejsza dyrektywa ma zastosowanie do przetwarzania danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności we Wspólnocie włącznie z publicznymi sieciami łączności służącymi do zbierania danych i obsługi urządzeń identyfikacyjnych”. Uzupełnia to motyw 56 dyrektywy 2009/136/WE: „Postęp technologiczny pozwala na rozwój nowych aplikacji opartych na urządzeniach do gromadzenia danych i identyfikacji, którymi mogłyby być urządzenia bezkontaktowe wykorzystujące częstotliwości radiowe. Na przykład urządzenia do identyfikacji radiowej (»RFID«) wykorzystują częstotliwości radiowe do odczytu danych z etykiet towarowych z unikatowym kodem, które to dane następnie mogą być przekazywane do istniejących sieci łączności. Zastosowanie tego rodzaju technologii na szeroką skalę może przynieść istotne korzyści gospodarcze i społeczne, a tym samym w znaczący sposób przyczynić się do urzeczywistnienia rynku wewnętrznego, jeżeli ich stosowanie zostanie zaakceptowane przez obywateli. Aby osiągnąć ten cel, należy zapewnić ochronę wszystkich podstawowych praw jednostek, w tym prawa do prywatności i ochrony danych. W przypadku gdy takie urządzenia są przyłączone do publicznie dostępnych sieci łączności elektronicznej lub korzystają z usług łączności elektronicznej jako podstawowej infrastruktury, zastosowanie mają odpowiednie przepisy dyrektywy 2002/58/WE (dyrektywa o prywatności i łączności elektronicznej), wraz z przepisami dotyczącymi bezpieczeństwa, ruchu i danych dotyczących lokalizacji oraz przepisami dotyczącymi poufności”.

(3) Na przykład art. 17 dyrektywy o ochronie danych nakłada obowiązek wprowadzenia odpowiednich środków technicznych i organizacyjnych w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub niedozwolonym ujawnieniem.

nie są wystarczająco szczegółowe pod względem rodzajów zabezpieczeń, jakie powinny być wdrożone w zastosowaniach RFID. Istniejące zasady muszą być uzupełnione dodatkowymi, przewidującymi konkretne zabezpieczenia, w szczególności zobowiązującymi do wprowadzenia rozwiązań technicznych (poszanowanie prywatności od samego początku) do technologii RFID. Dotyczy to etykiet przechowujących dane osobowe, które powinny posiadać polecenie zakończenia procesu (ang. *kill command*), oraz zastosowania kryptografii w etykietach przechowujących określone rodzaje danych osobowych.

V.2. Samoregulacja jako pierwszy krok

60. W marcu 2007 r. Komisja przyjęła komunikat⁽¹⁾, w którym uznano m.in. potrzebę opracowania szczegółowych wytycznych dotyczących praktycznego wdrażania RFID, a także zalety przyjęcia kryteriów projektowania w celu uniknięcia zagrożeń dla prywatności i bezpieczeństwa.
61. Aby osiągnąć te cele, w maju 2009 r. Komisja przyjęła zalecenie w sprawie wdrażania zasad ochrony prywatności i ochrony danych w zastosowaniach wspieranych identyfikacją radiową⁽²⁾. W zastosowaniach RFID w sprzedaży detalicznej wymagane jest dezaktywowanie etykiet w punkcie sprzedaży, chyba że osoba fizyczna wyrazi zgodę na aktywność etykiety. Zasada ta ma zastosowanie, chyba że ocena skutków w zakresie ochrony danych i prywatności wykaże, że etykiety prawdopodobnie nie stanowią zagrożenia dla prywatności lub ochrony danych osobowych, w którym to przypadku mogą pozostać aktywne po opuszczeniu punktu sprzedaży, jeżeli osoba fizyczna nie zrezygnuje z tej możliwości bez ponoszenia kosztów.
62. EIOD zgadza się z podejściem Komisji zakładającym wykorzystanie instrumentów samoregulacyjnych. Jednakże, jak opisano poniżej, nie można wykluczyć, że samoregulacja nie dostarczy oczekiwanych wyników; dlatego apeluje do Komisji, aby była gotowa do przyjęcia innych środków.

V.3. Problematiczne obszary i możliwe dodatkowe środki na wypadek, gdyby zawiodła samoregulacja

63. EIOD obawia się, że organizacje obsługujące zastosowania RFID w sektorze sprzedaży detalicznej mogą pominąć możliwość monitorowania etykiet RFID przez niepożądane osoby trzecie. Takie monitorowanie może ujawniać dane osobowe przechowywane na etykiecie (jeżeli jakiegokolwiek istnieją), ale może również umożliwić osobom trzecim śledzenie lub rozpoznanie osoby w czasie po prostu poprzez wykorzystanie niepowtarzalnych identyfikatorów znajdujących się na jednej etykiecie lub większej liczbie etykiet noszonych przez osobę fizyczną w środowisku, które może nawet znajdować się poza

granicy działania zastosowania RFID. EIOD obawia się także, że operatorzy zastosowań RFID mogą odczuwać pokusę nadmiernego korzystania z wyjątku i tym samym pozostawiać etykiety aktywne po opuszczeniu punktu sprzedaży.

64. Jeżeli taka sytuacja nastąpi, może być za późno na zmniejszenie zagrożeń dla ochrony danych i prywatności osób fizycznych, na które już mogły zostać narażone. Ponadto biorąc pod uwagę charakter samoregulacji, krajowe organy egzekwowania prawa mogą znajdować się w trudniejszej sytuacji, gdy wymagają od organizacji obsługujących zastosowania RFID przyjęcia określonych środków poszanowania prywatności od samego początku.
65. W świetle powyższego EIOD apeluje do Komisji, aby była gotowa do zaproponowania instrumentów ustawodawczych regulujących podstawowe kwestie wykorzystywania RFID w przypadku gdyby nie powiodło się skuteczne wdrożenie istniejących ram prawnych. Ocena Komisji nie powinna być zbyt opóźniona; opóźnienie naraziłoby osoby fizyczne na zagrożenie i również wobec przemyśłu przyniosłoby skutek odwrotny do zamierzonego, ponieważ niepewność prawna jest zbyt duża i rozwiązanie trwałych problemów będzie prawdopodobnie trudniejsze i bardziej kosztowne.
66. W ramach środków, które być może trzeba będzie zaproponować, EIOD zaleca zapewnienie zasady wyrażania zgody w punkcie sprzedaży, zgodnie z którą wszystkie etykiety RFID dołączone do produktów konsumenckich byłyby dezaktywowane domyślnie w punkcie sprzedaży. Określenie przez Komisję konkretnej technologii, która ma zostać wykorzystana, może nie być konieczne ani właściwe. Natomiast w prawie UE należy ustanowić obowiązek prawny uzyskania zgody co do aktywowania etykiet, pozostawiając operatorom możliwość decydowania, w jaki sposób mają spełnić ten wymóg.

V.4. Dalsze kwestie do rozważenia: zarządzanie Internetem przedmiotów

67. Informacje wytworzone przez etykiety RFID – na przykład informacje o produkcie – mogą być połączone w globalną sieć infrastruktury komunikacyjnej. Jest ona zwykle nazywana „Internetem przedmiotów”. Kwestie dotyczące ochrony danych/prywatności powstają, ponieważ przedmioty świata rzeczywistego mogą być identyfikowane poprzez etykiety RFID, które oprócz informacji o produkcie mogą zawierać dane osobowe.
68. Istnieje wiele otwartych pytań co do tego, kto będzie zarządzał przechowywaniem informacji związanych z obiektami opatrzonymi etykietami. Jak będzie to zorganizowane? Kto będzie miał dostęp do tych informacji? W czerwcu 2009 r. Komisja przyjęła komunikat w sprawie Internetu przedmiotów⁽³⁾, w którym jednoznacznie określono potencjalne problemy tego zjawiska związane z ochroną danych i prywatności.

⁽¹⁾ Komunikat Komisji z dnia 15.3.2007 r. 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 wersja ostateczna).

⁽²⁾ Zalecenie Komisji z dnia 12.5.2009 r. w sprawie wdrażania zasad ochrony prywatności i ochrony danych w zastosowaniach wspieranych identyfikacją radiową (C(2009) 3200 wersja ostateczna).

⁽³⁾ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie Internetu przedmiotów – plan działań dla Europy, 18.6.2009 r., (COM(2009) 278 wersja ostateczna).

69. EIOD pragnie podkreślić niektóre z tych kwestii podniesionych przez Komisję, które – jego zdaniem – zasługują na bliższą uwagę w miarę rozwoju Internetu przedmiotów. Po pierwsze, potrzeba zdecentralizowanej architektury może ułatwić wykonalność i odpowiedzialność w zakresie ram prawnych UE. Po drugie, w możliwie szerokim zakresie powinno być chronione prawo osób fizycznych do niepodlegania śledzeniu. Innymi słowy, przypadki, w których osoby fizyczne są śledzone przy pomocy etykiet RFID bez wyrażenia na to zgody, powinny być bardzo ograniczone. Taka zgoda powinna być jednoznaczna. Zazwyczaj nazywa się to „milczeniem czipów” i prawem do pozostawienia w spokoju. Ponadto przy projektowaniu Internetu przedmiotów zasada poszanowania prywatności od samego początku powinna być zasadą naczelną. Na przykład wymagałoby to projektowania konkretnych zastosowań RFID, które posiadają wbudowane mechanizmy przekazujące użytkownikom kontrolę, z domyślnymi ustawieniami prywatności.

70. EIOD oczekuje, że będzie proszony o opinię, gdy Komisja będzie wprowadzać działania przewidziane w komunikacie, szczególnie w odniesieniu do projektu komunikatu w sprawie poszanowania prywatności i zaufania we wszechobecnym społeczeństwie informacyjnym.

VI. PORTALE SPOŁECZNOŚCIOWE I POTRZEBA DOMYŚLNYCH USTAWIEŃ PRYWATNOŚCI

71. Portale społecznościowe są „hitem miesiąca”. Wydaje się, że pod względem popularności przewyższają wiadomości e-mail. Łączą one ludzi z innymi osobami o podobnych zainteresowaniach lub aktywności. Ludzie mogą posiadać własne profile internetowe i wymieniać pliki multimedialne, takie jak: filmy wideo, zdjęcia, muzykę, a także profile kariery zawodowej.

72. Młodzież szybko przyjęła portale społecznościowe i tendencja ta utrzymuje się. W ciągu ostatnich kilku lat spadła średnia wieku użytkowników Internetu w Europie: 9–10-latkowie obecnie łączą się z Internetem kilka razy w tygodniu; 12–14-latkowie codziennie, często spędzają w sieci od jednej do trzech godzin.

VI.1. Portale społecznościowe a obowiązujące ramy prawne dotyczące ochrony danych i prywatności

73. Rozwój portali społecznościowych umożliwił użytkownikom przesyłanie do Internetu informacji o sobie i o osobach trzecich. Czyniąc to, zdaniem grupy roboczej art. 29⁽¹⁾, użytkownicy Internetu działają jako

administratorzy danych, zgodnie z art. 2 lit. d) dyrektywy o ochronie danych, w odniesieniu do danych, które przesyłają⁽²⁾. Jednakże w większości przypadków takie przetwarzanie objęte jest wyjątkiem dotyczącym domowego charakteru przetwarzania danych wynikającym z art. 3 ust. 2 dyrektywy. Jednocześnie portale społecznościowe uznawane są za administratorów danych o tyle, o ile zapewniają środki do przetwarzania danych użytkownika i wszystkie podstawowe usługi związane z zarządzaniem przez użytkownika (np. rejestracja i usuwanie kont).

74. W kategoriach prawnych oznacza to, że użytkownicy Internetu i portale społecznościowe wspólnie ponoszą odpowiedzialność za przetwarzanie danych osobowych jako „administratorzy danych” w rozumieniu art. 2 lit. d) dyrektywy, aczkolwiek w różnym stopniu i przy zastosowaniu różnych obowiązków.

75. Zatem użytkownicy powinni wiedzieć i rozumieć, że poprzez przetwarzanie danych osobowych własnych oraz innych osób podlegają przepisom prawodawstwa UE dotyczącego ochrony danych, które wymaga m.in. uzyskania świadomej zgody osób, których informacje są przesyłane, oraz zapewnienia tym osobom prawa do sprostowania, sprzeciwu itd. Podobnie portale społecznościowe muszą m.in. wdrożyć odpowiednie techniczne i organizacyjne środki zapobiegające nieuprawnionemu przetwarzaniu, biorąc pod uwagę zagrożenia związane z przetwarzaniem danych i ich charakterem. To z kolei oznacza, że portale społecznościowe powinny zapewnić przyjazne dla użytkownika ustawienia domyślne, w tym ustawienia ograniczające dostęp do profilu użytkownika do jego własnych, samodzielnie wybranych kontaktów. Ustawienia powinny również wymagać wyrażenia zgody przez użytkownika zanim jakikolwiek profil zostanie udostępniony osobom trzecim, a profile o ograniczonym dostępie nie powinny być znajdowane przez wyszukiwarki wewnętrzne.

76. Niestety istnieje różnica pomiędzy wymogami prawnymi a faktyczną zgodnością. Podczas gdy, w sensie prawnym, użytkownicy Internetu są uważani za administratorów danych i są związani ramami prawnymi UE w zakresie ochrony danych i prywatności, w rzeczywistości często nie są świadomi tej roli. Ogólnie mówiąc, mają bardzo małą wiedzę o tym, że przetwarzają dane osobowe oraz że z publikowaniem takich informacji wiążą się zagrożenia dla prywatności i ochrony danych. Szczególnie młodzież umieszcza w Internecie treści, lekceważąc konsekwencje dla siebie i innych osób, np. w kontekście późniejszych zapisów do instytucji edukacyjnych lub starania się o pracę.

⁽¹⁾ Zob. opinia grupy roboczej art. 29 WP 168 w sprawie portali społecznościowych, przyjęta w dniu 12 czerwca 2009 r.

⁽²⁾ „Administrator danych” oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych; jeżeli cele i sposoby przetwarzania danych są określone w przepisach ustawowych i wykonawczych lub przepisach wspólnotowych, administrator danych może być powoływany lub kryteria jego powołania mogą być ustalane przez ustawodawstwo krajowe lub wspólnotowe.

77. Jednocześnie operatorzy portali społecznościowych często wybierają wstępnie ustawienia domyślne w oparciu o opcję rezygnowania, ułatwiając w ten sposób ujawnianie danych osobowych. Niektórzy umożliwiają domyślne udostępnianie profili wyszukiwarkom. W związku z tym powstaje pytanie, czy osoby fizyczne rzeczywiście wyraziły zgodę na ujawnienie danych, jak również czy portale społecznościowe działają zgodnie z art. 17 dyrektywy (opisanym powyżej), wymagającym od nich wdrożenia odpowiednich technicznych i organizacyjnych środków zapobiegających nieuprawnionemu przetwarzaniu.

VI.2. Zagrożenia powodowane przez portale społecznościowe i sugerowane przeciwdziałanie tym zagrożeniom

78. Wynikiem powyżej opisanych zagadnień jest wzrost zagrożenia dla prywatności i ochrony danych osób fizycznych. Naraża to użytkowników Internetu i osoby, których dane przesłano, na jawne naruszenie ich prywatności i ochrony danych.

79. W tym kontekście kwestią, którą Komisja powinna się zająć, jest co należy i można zrobić, aby rozwiązać ten problem. Niniejsza opinia nie zawiera wyczerpującej odpowiedzi na to pytanie, ale przedstawia kilka sugestii do dalszego rozważenia.

Investowanie w edukację użytkowników Internetu

80. Pierwszą sugestią jest inwestowanie w edukację użytkowników. Pod tym względem instytucje UE i organy krajowe powinny zainwestować w edukowanie i poszerzanie wiedzy w zakresie zagrożeń, jakie stanowią strony internetowe portali społecznościowych. Na przykład DG ds. Społeczeństwa Informacyjnego i Mediów uruchomiła program Bezpieczniejszy Internet, który ma na celu zwiększenie roli dzieci i młodzieży oraz ich ochronę poprzez na przykład działania poszerzające wiedzę⁽¹⁾. Niedawno instytucje UE rozpoczęły kampanię „Pomyśl, zanim napiszesz”, aby poszerzyć wiedzę na temat zagrożeń wynikających z udostępniania nieznanymi danymi osobowych.

81. EIOD zachęca Komisję do dalszego wspierania tego typu działań. Jednakże sami operatorzy portali społecznościowych również powinni odgrywać aktywną rolę, ponieważ mają prawny i społeczny obowiązek edukowania użytkowników w zakresie korzystania z ich usług w sposób bezpieczny i przyjazny dla prywatności.

82. Jak opisano powyżej, publikując informacje na portalach społecznościowych, można je domyślnie udostępnić na kilka różnych sposobów. Na przykład informacje mogą zostać ogólnie udostępnione, w tym wyszukiwarkom internetowym, które mogą je indeksować, zapewniając w ten sposób bezpośredni odnośnik do tych informacji.

Z drugiej strony udostępnianie informacji może być ograniczone do „wybranych przyjaciół” lub mogą być one zupełnie prywatne. Oczywiście zezwolenia dotyczące profilu i stosowana terminologia różnią się w zależności od portalu.

83. Jednakże, jak w skrócie przedstawiono powyżej, bardzo niewielu użytkowników serwisów społecznościowych wie, jak kontrolować dostęp do publikowanych informacji, a co dopiero jak zmienić domyślne ustawienia prywatności. Ustawienia prywatności zwykle pozostają niezmiennione, ponieważ użytkownicy nie zdają sobie sprawy ze skutków niezmienniania tych ustawień lub nie wiedzą, jak to zrobić. Dlatego też najczęściej brak zmiany ustawień prywatności nie oznacza, że osoby fizyczne podjęły świadomą decyzję o zezwoleniu na udostępnianie informacji. W tym kontekście jest szczególnie ważne, aby osoby trzecie, takie jak wyszukiwarki, nie przekazywały odnośników do poszczególnych profili zgodnie z założeniem, że użytkownicy domyślnie zezwolili (bez zmiany ustawień prywatności) na udostępnianie informacji bez ograniczeń.

84. Chociaż edukacja użytkowników może pomóc w rozwiązaniu tego problemu, sama w sobie nie wystarczy. Według zaleceń grupy roboczej art. 29 zawartych w jej opinii w sprawie portali społecznościowych dostawcy usług portali społecznościowych powinni oferować przyjazne dla prywatności, bezpłatne domyślne ustawienia prywatności. Dzięki temu użytkownicy byłiby bardziej świadomi swoich działań i mieli możliwość podejmowania lepszych decyzji co do tego, czy chcą udostępniać informacje i komu.

Rola samoregulacji

85. Komisja zawarła porozumienie z dwudziestoma dostawcami usług portali społecznościowych, które znane jest jako „Zasady bezpieczniejszego korzystania z portali społecznościowych dla UE”⁽²⁾. Celem porozumienia jest poprawienie bezpieczeństwa nieletnich w czasie korzystania ze stron portali społecznościowych w Europie. Zasady te obejmują wiele wymogów wywodzących się ze stosowania wyżej opisanych ram prawnych dotyczących ochrony danych. Obejmują one na przykład wymóg zwiększenia roli użytkowników poprzez narzędzia i technologie w celu zagwarantowania, że mogą oni kontrolować wykorzystywanie i rozpowszechnianie swoich danych osobowych. Obejmuje to również potrzebę zapewnienia domyślnych ustawień prywatności.

86. Na początku stycznia 2010 r. Komisja udostępniła wnioski ze sprawozdania oceniającego wdrażanie tych zasad⁽³⁾. Zaniepokojenie EIOD budzi fakt, że sprawozdanie wykazuje, iż podjęto pewne kroki, natomiast wielu innych nie zrealizowano. Na przykład sprawozdanie ujawniło problemy w zakresie przekazywania informacji o środkach i narzędziach bezpieczeństwa dostępnych na

⁽¹⁾ Informacje na temat tego programu dostępne są pod adresem: http://ec.europa.eu/information_society/activities/sip/index_en.htm

⁽²⁾ Zasady te dostępne są pod adresem: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

⁽³⁾ Sprawozdanie na temat oceny wdrożenia zasad bezpieczniejszych portali społecznościowych w UE, dostępne pod adresem: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

stronach internetowych. Wykazano w nim również, że mniej niż połowa sygnatariuszy porozumienia ogranicza dostęp do profili nieletnich wyłącznie do ich przyjaciół.

Potrzeba obowiązkowego domyślnego ustawienia prywatności

87. W tym kontekście najważniejszą kwestią jest to, czy dodatkowe środki o charakterze politycznym są konieczne do zagwarantowania, że portale społecznościowe skonfiguruje swoje usługi z zastosowaniem domyślnego ustawienia prywatności. Kwestię tę poruszyła była komisarz ds. społeczeństwa informacyjnego i mediów Viviane Reding, która zwróciła uwagę, że prawodawstwo może być niezbędne ⁽¹⁾. Podobnie Europejski Komitet Ekonomiczno-Społeczny stwierdził, że oprócz samoregulacji należy prawnie narzucić minimalne normy ochrony ⁽²⁾.

88. Jak zauważono powyżej, obowiązek nałożony na dostawców usług portali społecznościowych co do wprowadzenia domyślnych ustawień prywatności można pośrednio wywieść z art. 17 dyrektywy o ochronie danych ⁽³⁾, który zobowiązuje administratorów danych do wdrożenia odpowiednich środków technicznych i organizacyjnych („zarówno przy opracowywaniu systemu przetwarzania danych, jak i podczas samego ich przetwarzania”), aby utrzymać bezpieczeństwo i zapobiec nieuprawnionemu przetwarzaniu, biorąc pod uwagę zagrożenia wynikające z przetwarzania danych oraz charakter danych.

89. Jednakże artykuł ten jest zbyt ogólny i pozbawiony szczególności, również w tym kontekście. Nie stwierdza się w nim wyraźnie, co rozumie się przez odpowiednie środki techniczne i organizacyjne w kontekście portali społecznościowych. Obecna sytuacja wiąże się zatem z niepewnością prawną, które powoduje problemy, zarówno dla organów regulacyjnych, jak i osób fizycznych, których prywatność i dane osobowe nie są w pełni chronione.

90. W świetle powyższego EIOD zaleca Komisji przygotowanie prawodawstwa, które obejmowałoby, jako minimum, nadrzędny wymóg dotyczący obowiązkowych ustawień prywatności, połączony z bardziej szczegółowymi wymogami w zakresie:

- a) zapewnienia ustawień ograniczających dostęp do profilu użytkownika do jego własnych, samodzielnie wybranych kontaktów. Ustawienia powinny również wymagać wyrażenia zgody przez użytkownika zanim jakikolwiek profil zostanie udostępniony osobom trzecim;

⁽¹⁾ Viviane Reding, członek Komisji Europejskiej odpowiedzialna za społeczeństwo informacyjne i media, „Pomyśl, zanim napiszesz! Jak sprawić, aby portale społecznościowe były bezpieczniejsze dla dzieci i nastolatków?” (Think before you post! How to make social networking sites safer for children and teenagers?), Dzień Bezpiecznego Internetu, Strasburg, dnia 9 lutego 2010 r.

⁽²⁾ Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie wpływu portali społecznościowych na obywateli/konsumentów, dnia 4 listopada 2009 r.

⁽³⁾ Omówiony również w pkt 33 niniejszego dokumentu.

- b) zagwarantowania, że profile o ograniczonym dostępie nie mogą być znajdowane przez wyszukiwarki wewnętrzne/zewnętrzne.

91. Oprócz zapewnienia obowiązkowych domyślnych ustawień prywatności pozostaje pytanie, czy dodatkowe, szczególne środki ochrony danych i inne środki (na przykład dotyczące ochrony nieletnich) również byłyby odpowiednie. Wiąże się z nim ogólniejsza kwestia, czy właściwe byłoby utworzenie szczegółowych ram prawnych dla tych rodzajów usług, które oprócz przewidywania obowiązkowych ustawień prywatności regulowałyby inne aspekty. EIOD prosi Komisję o wzięcie tej kwestii pod rozwagę.

VII. DOMYŚLNE USTAWIENIA PRYMATNOŚCI W PRZEGLĄDARKACH W CELU ZAGWARANTOWANIA ŚWIADOMEJ ZGODY NA OTRZYMYWANIE REKLAM

92. Dostawcy reklamy internetowej wykorzystują pliki cookie oraz inne narzędzia do monitorowania zachowania indywidualnych użytkowników w czasie ich surfowania po Internecie w celu katalogowania ich zainteresowań i tworzenia profili. Informacje te są następnie wykorzystywane do wysyłania im ukierunkowanych reklam ⁽⁴⁾.

VII.1. Pozostałe wyzwania i zagrożenia w obecnych ramach prawnych dotyczących ochrony danych/prywatności

93. Przetwarzanie to jest objęte dyrektywą o ochronie danych (gdy dotyczy danych osobowych) oraz art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. Artykuł ten wyraźnie wymaga informowania użytkownika o gromadzeniu na jego komputerze lub innym urządzeniu takich narzędzi jak pliki cookie itd. i zapewnieniu mu możliwości zareagowania na to poprzez wyrażenie zgody lub odmowę ⁽⁵⁾.

94. Do chwili obecnej dostawcy reklamy internetowej polegali na ustawieniach wyszukiwarki i polityce prywatności, żeby informować użytkowników oraz umożliwić im wyrażenie zgody na otrzymywanie plików cookie lub odmowę tej zgody. Wyjaśniali w polityce prywatności

⁽⁴⁾ Śledzące pliki cookie (tzw. ciasteczka) to małe pliki tekstowe zawierające niepowtarzalny identyfikator. Zwykle reklamodawcy internetowi (a także operatorzy lub wydawcy stron internetowych) umieszczają pliki cookie na dyskach twardych odwiedzających, w szczególności w przeglądarkach użytkowników Internetu, gdy odwiedzający po raz pierwszy wejdą na stronę internetową zawierającą reklamy będące częścią ich sieci. Plik cookie umożliwia reklamodawcy internetowemu rozpoznanie odwiedzającego, który ponownie odwiedzi daną stronę internetową lub każdą inną stronę w ramach sieci reklamowej. Takie powtarzające się odwiedziny umożliwią reklamodawcy internetowemu opracowanie profilu odwiedzającego.

⁽⁵⁾ Artykuł 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej niedawno zmieniono w celu zwiększenia ochrony przed przechwyceniem komunikacji użytkowników za pośrednictwem np. oprogramowania szpiegującego i plików cookie przechowywanych na komputerze użytkownika lub innym urządzeniu. Na mocy nowej dyrektywy użytkownicy powinni mieć zapewnione lepsze informacje i łatwiejsze sposoby kontrolowania tego, czy chcą, aby pliki cookie były przechowywane na ich terminalach.

wydawców, w jaki sposób można zrezygnować z otrzymywania wszystkich plików cookie lub przyjmować je w poszczególnych przypadkach. W ten sposób zamierzali spełniać obowiązek oferowania użytkownikom prawa od odrzucenia plików cookie.

95. Podczas gdy metoda ta (poprzez przeglądarkę internetową) rzeczywiście może skutecznie zapewnić wyrażanie świadomej zgody, rzeczywistość jest zupełnie inna. Na ogół użytkownicy nie mają podstawowej wiedzy na temat gromadzenia danych, a tym bardziej od osób trzecich, wartości takich danych, ich wykorzystania, sposobu działania tej technologii, a szczególnie jak i gdzie można z plików cookie zrezygnować. Kroki, jakie użytkownik musi wykonać, aby zrezygnować z otrzymywania plików cookie, wydają się nie tylko skomplikowane, ale również nadmierne (najpierw musi ustawić przeglądarkę, aby akceptowała pliki cookie, a następnie skorzystać z opcji rezygnowania).
96. Wskutek tego w praktyce bardzo niewiele osób korzysta z opcji rezygnowania, nie dlatego, że podjęły świadomą decyzję o akceptowaniu reklamy behawioralnej, ale raczej dlatego, że nie zdają sobie sprawy z tego, iż poprzez niekorzystanie z tej opcji w rzeczywistości akceptują otrzymywanie plików cookie.
97. Dlatego też chociaż w sensie prawnym art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej zapewnia skuteczną ochronę prawną, w praktyce uznaje się, że użytkownicy Internetu wyrażają zgodę na objęcie monitorowaniem dla celów wysyłania reklamy behawioralnej, podczas gdy w rzeczywistości w wielu, jeżeli nie w większości przypadków, są całkowicie nieświadomi, że takie monitorowanie ma miejsce.
98. Grupa robocza art. 29 przygotowuje przydatną opinię mającą na celu wyjaśnienie wymogów prawnych dotyczących prezentowania reklamy behawioralnej. Jednakże interpretacja może nie być sama w sobie wystarczająca do rozwiązania tego problemu i być może Unia Europejska będzie musiała podjąć dodatkowe działania.

VII.2. Potrzeba dalszych działań, w szczególności przewidujących obowiązkowe domyślne ustawienia prywatności

99. Jak opisano powyżej, przeglądarki internetowe zwykle pozwalają na pewien poziom kontroli nad pewnymi rodzajami plików cookie. Obecnie ustawienia domyślne większości przeglądarek internetowych akceptują wszystkie pliki cookie. Innymi słowy, domyślnie przeglądarki internetowe są ustawione na akceptowanie wszystkich plików cookie, niezależnie od ich celu. Jedynie gdy użytkownik zmieni ustawienia swojej przeglądarki internetowej, żeby odrzucała pliki cookie, co – jak opisano powyżej – robi bardzo niewiele osób, nie będzie otrzymywać plików cookie. Ponadto w trakcie pierwszej instalacji lub aktualizacji programu przeglądarki nie istnieje żaden kreator ustawień prywatności.
100. Sposobem zaradzenia powyższemu problemowi byłoby wyposażenie przeglądarek w domyślne ustawienia prywatności. Innymi słowy, przeglądarki posiadałyby ustawienie „nie akceptuj plików cookie osób trzecich”. Aby uzupełnić

to rozwiązanie i zwiększyć jego skuteczność, wyszukiwarka powinna żądać od użytkownika przejścia przez kreator ustawień prywatności przy pierwszej instalacji lub aktualizacji przeglądarki. Potrzebne są bardziej szczegółowe i przejrzyste informacje na temat rodzajów plików cookie oraz przydatności niektórych z nich. Użytkownicy chcący być monitorowani w celu otrzymywania reklamy będą należycie informowani i będą musieli zmienić ustawienia przeglądarki. Zapewniłoby im to większą kontrolę nad swoimi danymi osobowymi i prywatnością. Zdaniem EIOD byłby to efektywny sposób poszanowania i zapewnienia zgody użytkownika ⁽¹⁾.

101. Biorąc pod uwagę z jednej strony powszechny charakter problemu, czyli liczbę użytkowników Internetu, którzy są obecnie monitorowani w oparciu o iluzoryczną zgodę, a z drugiej skalę interesu, potrzeba dodatkowych zabezpieczeń staje się poważniejsza. Wdrożenie zasady poszanowania prywatności od samego początku w aplikacjach przeglądarek internetowych mogłoby spowodować zasadniczą zmianę, dając osobom fizycznym kontrolę nad praktykami gromadzenia danych wykorzystywanymi w celach reklamowych.
102. Z tych powodów EIOD nalega, aby Komisja rozważyła środki ustawodawcze wymagające obowiązkowego domyślnego ustawienia prywatności w przeglądarkach oraz udzielania istotnych informacji.

VIII. INNE ZASADY MAJĄCE NA CELU OCHRONĘ PRYWATNOŚCI OSÓB FIZYCZNYCH/OCHRONĘ DANYCH

103. Chociaż zasada poszanowania prywatności od samego początku ma duże możliwości poprawienia ochrony danych osobowych osób fizycznych i ich prywatności, konieczne jest opracowanie i wdrożenia do prawodawstwa zasad uzupełniających w celu zapewnienia zaufania konsumentów do TIK. W tym kontekście EIOD zwraca uwagę na zasadę odpowiedzialności i ukończenie procesu tworzenia obowiązkowych ram dotyczących naruszenia bezpieczeństwa, które mają zastosowanie we wszystkich sektorach.

VIII.1. Zasada odpowiedzialności w celu zapewnienia zgodności z zasadą poszanowania prywatności od samego początku

104. W dokumencie grupy roboczej art. 29 pt. „Przyszłość prywatności” ⁽²⁾ zaleca się włączenie zasady odpowiedzialności do dyrektywy o ochronie danych. Zasada ta jest

⁽¹⁾ Jednocześnie EIOD zdaje sobie sprawę, że nie rozwiązałoby to całkowicie problemu, ponieważ istnieją pliki cookie, które nie mogą być kontrolowane za pośrednictwem przeglądarki, np. pliki Flash cookie. Z tego względu twórcy przeglądarek musieliby domyślnie włączyć opcje kontroli Flash do opcji kontroli plików cookie przy udostępnianiu nowych przeglądarek.

⁽²⁾ Opinia grupy roboczej art. 29 WP 168 „Przyszłość prywatności. Wspólny wkład w konsultacje Komisji Europejskiej w sprawie ram prawnych dotyczących podstawowego prawa do ochrony danych osobowych” (The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data), przyjęta w dniu 1 grudnia 2009 r.

obecna w niektórych międzynarodowych instrumentach dotyczących ochrony danych⁽¹⁾. Wymaga od organizacji wdrożenia procedur dostosowujących ją do istniejącego prawodawstwa, a także ustalenia metod oceniania i wykazywania zgodności z prawem i innymi obowiązującymi instrumentami.

105. EIOD w pełni popiera zalecenie grupy roboczej art. 29. Uważa, że zasada ta będzie miała duże znaczenie dla ułatwienia skutecznego stosowania zasad i zobowiązań dotyczących ochrony danych. Zasada odpowiedzialności będzie wymagała od administratorów danych wykazania, że wprowadzili mechanizm niezbędny do zapewnienia zgodności z obowiązującymi przepisami w zakresie ochrony danych. Prawdopodobnie przyczyni się to do skutecznego wdrożenia zasady poszanowania prywatności od samego początku w TIK, ponieważ jest to szczególnie stosowny element pod względem wykazywania odpowiedzialności.
106. Do pomiaru i wykazania odpowiedzialności administratorzy danych mogliby wykorzystać wewnętrzne procedury i osoby trzecie, które mogą przeprowadzić audyt lub inne rodzaje kontroli i weryfikacji, co może skutkować przyznaniem odznaczeń lub nagród. W tym kontekście EIOD zaleca Komisji rozważenie, czy – oprócz ogólnej zasady odpowiedzialności – przydatny może być wymóg prawny dotyczący określonych środków związanych z odpowiedzialnością, takich jak konieczność dokonywania oceny skutków w zakresie ochrony danych i prywatności oraz okoliczności takiej oceny.

VIII.2. Naruszenie bezpieczeństwa: ukończenie procesu tworzenia ram prawnych

107. Zeszlóroczne poprawki do dyrektywy o prywatności i łączności elektronicznej wprowadziły wymóg zgłaszania przypadków naruszenia danych osobom, których te dane dotyczą, oraz właściwym organom. Naruszenie danych jest ogólnie definiowane jako każde naruszenie prowadzące do zniszczenia, utraty, ujawnienia itd. danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych w związku z usługą. Powiadomienie osób fizycznych będzie konieczne, jeżeli naruszenie danych może wywrzeć niekorzystny wpływ na ich dane osobowe lub prywatność. Może to mieć miejsce w przypadku gdy naruszenie może doprowadzić do kradzieży tożsamości lub poważnego upokorzenia lub szkody dla reputacji. Powiadomienie właściwych organów będzie wymagane w przypadku każdego naruszenia danych, niezależnie od tego, czy istnieje zagrożenie dla osób fizycznych.

Stosowanie obowiązków związanych z naruszeniem bezpieczeństwa we wszystkich sektorach

108. Niestety obowiązek ten stosuje się wyłącznie do dostawców publicznie dostępnych usług łączności elektronicznej, takich jak: spółki telekomunikacyjne, dostawcy usług dostępu do Internetu, dostawców usług poczty elektronicznej itd. EIOD zaleca Komisji przedstawienie wniosków w sprawie naruszenia bezpieczeństwa mających

zastosowanie do wszystkich sektorów. Jeśli chodzi o treść takich ram, EIOD uważa, że ramy prawne dotyczące naruszenia bezpieczeństwa przyjęte w dyrektywie o prywatności i łączności elektronicznej stanowią złoty środek między ochroną praw osób fizycznych, w tym praw do ochrony danych i do prywatności, a obowiązkami nałożonymi na podmioty objęte dyrektywą. Jednocześnie są to ramy posiadające prawdziwą siłę, ponieważ są wspierane konstruktywnymi przepisami wykonawczymi, które zapewniają organom wystarczające uprawnienia do prowadzenia dochodzeń i nakładania kar w przypadku niezgodności.

109. EIOD zaleca zatem Komisji przyjęcie wniosku ustawodawczego stosującego te ramy do wszystkich sektorów, z właściwymi poprawkami, jeśli to konieczne. Ponadto zapewniłoby to stosowanie takich samych norm i procedur we wszystkich sektorach.

Ukończenie procesu tworzenia ram prawnych przewidzianych w dyrektywie o prywatności i łączności elektronicznej poprzez procedurę komitetową

110. Zmieniona dyrektywa o prywatności i łączności elektronicznej upoważnia Komisję do przyjęcia technicznych środków wykonawczych, tj. szczegółowych środków dotyczących powiadamiania o naruszeniach bezpieczeństwa, w drodze procedury komitetowej⁽²⁾. To upoważnienie jest uzasadnione koniecznością zapewnienia spójnego wdrożenia i stosowania ram prawnych dotyczących naruszenia bezpieczeństwa. Spójne wdrożenie ma na celu zagwarantowanie, że osoby fizyczne w całej Wspólnocie korzystają z równie wysokiego poziomu ochrony i że właściwe podmioty nie są obciążone różnymi wymogami co do powiadamiania.
111. Dyrektywę o prywatności i łączności elektronicznej przyjęto w listopadzie 2009 r. Wydaje się, że nie istnieje żaden powód uzasadniający opóźnienie rozpoczęcia prac nad przyjęciem technicznych środków wykonawczych. EIOD zorganizował dwa seminaria, które miały na celu wymianę i zbieranie doświadczeń w zakresie powiadamiania o naruszeniu danych. Z przyjemnością podzieli się wynikami tych działań i oczekuje współpracy z Komisją oraz innymi zainteresowanymi stronami nad dostosowaniem ogólnych ram prawnych w zakresie naruszenia danych.
112. EIOD zaleca Komisji szybkie podjęcie koniecznych kroków. Przed przyjęciem technicznych środków wykonawczych Komisja musi przeprowadzić szeroko zakrojone konsultacje, w tym z udziałem Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji, EIOD i grupy roboczej art. 29. Ponadto konsultacjami muszą zostać objęte także inne właściwe zainteresowane strony, szczególnie w celu poinformowania ich o najlepszych technicznych i gospodarczych środkach wykonawczych.

⁽¹⁾ Wytoczne OECD z 1980 r. w sprawie ochrony prywatności i transgranicznego przepływu danych osobowych; deklaracja madrycka o prywatności w sprawie globalnych norm w zakresie prywatności na całym świecie, dnia 3 listopada 2009 r.

⁽²⁾ Procedura komitetowa polega na przyjęciu technicznych środków wykonawczych za pośrednictwem komitetu przedstawicieli państw członkowskich, któremu przewodniczy Komisja. W przypadku dyrektywy o prywatności i łączności elektronicznej ma zastosowanie tzw. procedura regulacyjna połączona z kontrolą, co oznacza, że Parlament Europejski i Rada mogą wyrazić sprzeciw wobec środków zaproponowanych przez Komisję. Zob. http://europa.eu/scadplus/glossary/comitology_en.htm

IX. WNIOSKI

113. Ustalono, że zaufanie, a raczej jego brak, jest podstawowym zagadnieniem w powstawaniu i skutecznym wprowadzaniu technologii informacyjno-komunikacyjnych. Jeżeli ludzie nie ufają TIK, technologie te prawdopodobnie nie odniosą sukcesu. Zaufanie do TIK zależy od różnych czynników – najważniejszym jest zagwarantowanie, że te technologie nie ograniczają podstawowych praw osób fizycznych do prywatności i ochrony danych osobowych.
114. W celu dalszego wzmocnienia ram prawnych dotyczących ochrony danych/prywatności, które to zasady pozostają całkowicie uzasadnione w społeczeństwie informacyjnym, EIOD proponuje, aby Komisja wprowadziła poszanowanie prywatności od samego początku na różnych szczeblach prawa i formułowania zasad polityki.
115. Zaleca Komisji cztery następujące kierunki działania:
- a) zaproponowanie włączenia ogólnego przepisu o poszanowaniu prywatności od samego początku do ram prawnych dotyczących ochrony danych. Przepis ten powinien być neutralny technologicznie, a zgodność z nim powinna być obowiązkowa na różnych etapach;
 - b) rozwinięcie tego ogólnego przepisu w przepisach szczegółowych, gdy w różnych sektorach zaproponowane będą szczegółowe instrumenty prawne. Te przepisy szczegółowe już mogłyby zostać włączone do instrumentów prawnych; na podstawie art. 17 dyrektywy o ochronie danych (oraz innych istniejących przepisów);
 - c) uwzględnienie poszanowania prywatności od samego początku jako naczelnej zasady europejskiej agendy cyfrowej;
 - d) wprowadzenie poszanowania prywatności od samego początku jako zasady w innych inicjatywach UE (głównie o charakterze nieustawodawczym).
116. W trzech wyznaczonych obszarach TIK EIOD zaleca Komisji dokonanie oceny potrzeby przedstawienia wniosków w sprawie wdrożenia zasady poszanowania prywatności od samego początku w określony sposób:
- a) w odniesieniu do RFID – zaproponowanie środków ustawodawczych regulujących podstawowe kwestie wykorzystywania RFID na wypadek gdyby nie powiodło się skuteczne wdrożenie istniejących ram prawnych poprzez samoregulację. W szczególności należy uwzględnić zasadę wyrażania zgody w punkcie sprzedaży, zgodnie z którą wszystkie etykiety RFID dołączone do produktów konsumenckich byłyby domyślnie dezaktywowane w punkcie sprzedaży;
 - b) w odniesieniu do portali społecznościowych – przygotowanie prawodawstwa, które obejmowałoby, jako minimum, nadrzędny wymóg dotyczący obowiązkowych ustawień prywatności, połączony z bardziej szczegółowymi wymogami w zakresie ograniczenia dostępu do profili użytkowników do własnych, samodzielnie wybranych kontaktów użytkownika, a także zagwarantowania, że profile o ograniczonym dostępie nie mogą być znajdowane przez wyszukiwarki wewnętrzne/zewnętrzne;
 - c) w odniesieniu do reklamy ukierunkowanej – rozważenie przepisów przewidujących w ustawieniach przeglądark domyślne odrzucanie plików cookie osób trzecich i wymaganie od użytkownika skorzystania z kreatora ustawień prywatności przy pierwszej instalacji lub aktualizacji przeglądarki.
117. Ponadto EIOD zaleca Komisji:
- a) rozważenie wdrożenia zasady odpowiedzialności w istniejącej dyrektywie o ochronie danych; oraz
 - b) opracowanie ram zasad i procedur wdrażania przepisów dyrektywy o ochronie prywatności i łączności elektronicznej dotyczących powiadamiania o naruszeniu bezpieczeństwa, a także rozszerzenia ich zakresu stosowania na wszystkich administratorów danych.
- Sporządzono w Brukseli dnia 18 marca 2010 r.
- Peter HUSTINX
Europejski Inspektor Ochrony Danych

Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie zużytego sprzętu elektrycznego i elektronicznego (WEEE)

(2010/C 280/02)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16,

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, w szczególności jej art. 17,

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,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ

I. WPROWADZENIE

1. W dniu 3 grudnia 2008 r. Komisja przyjęła wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie zużytego sprzętu elektrycznego i elektronicznego (WEEE) (zwany dalej „wnioskiem”) ⁽¹⁾. Wniosek ma na celu przekształcenie dyrektywy 2002/96/WE w sprawie zużytego sprzętu elektrotechnicznego i elektronicznego (WEEE) przyjętej w dniu 27 stycznia 2003 r. (zwanej dalej „dyrektywą”) ⁽²⁾ bez zmiany przyczyn lub czynników napędowych związanych ze zbieraniem i recyklingiem WEEE.
2. Nie skonsultowano się z EIOD zgodnie z wymogami art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 ⁽³⁾. Działając w własnej inicjatywy, EIOD przyjął zatem obecną opinię w oparciu o art. 41 ust. 2 tego rozporządzenia. EIOD zaleca włączenie odniesienia do niniejszej opinii w preambułę wniosku.

3. EIOD zdaje sobie sprawę, że niniejsza porada ma miejsce na późnym etapie procesu legislacyjnego, niemniej jednak uważa wydanie niniejszej opinii za stosowne i przydatne, ponieważ we wniosku poruszono znaczące kwestie ochrony danych nieuwzględnione w jego tekście. Celem niniejszej opinii nie jest zmiana głównego i dominującego celu i treści wniosku, którego „istotą” ⁽⁴⁾ pozostaje ochrona środowiska, a przywołanie dodatkowego wymiaru, który staje się coraz ważniejszy dla naszego społeczeństwa informacyjnego ⁽⁵⁾.
4. Zdając sobie sprawę z ograniczonego zakresu procedury przekształcenia, EIOD niemniej jednak nalega, aby ustawodawca uwzględnił te zalecenia zgodnie z art. 8 porozumienia międzyinstytucjonalnego w sprawie procedury przekształcania (które przewiduje możliwość zmiany przepisów niezmienionych) ⁽⁶⁾.

II. KONTEKST I PODSTAWA WNIOSKU ORAZ JEGO ZNACZENIE DLA OCHRONY DANYCH

5. Wniosek ma na celu uaktualnienie istniejącej dyrektywy dotyczącej unieszkodliwiania, ponownego użycia i recyklingu WEEE. Do powstania wniosku, zgodnie z tym, co przewidziano w art. 17 ust. 5 dyrektywy, doprowadziły problemy techniczne, prawne i administracyjne występujące w ciągu pierwszych lat wykonania tej dyrektywy.
6. Sprzęt elektryczny i elektroniczny (EEE) stanowi dużą grupę produktów, która obejmuje różne rodzaje nośników mogących przechowywać dane osobowe, takich jak sprzęt informatyczny i telekomunikacyjny (np. komputery osobiste, laptopy, terminale komunikacji elektronicznej). W obecnym kontekście technologicznym i gospodarczym sprzęt ten charakteryzuje się coraz szybszym cyklem innowacyjnym oraz – z uwagi na konwergencję technologiczną

⁽¹⁾ COM(2008) 810 wersja ostateczna.

⁽²⁾ Dz.U. L 37 z 13.2.2003, s. 24.

⁽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⁾ Zob. Trybunał Sprawiedliwości, 23.2.1999, sprawa C-42/97 Parlament Europejski przeciwko Radzie Unii Europejskiej, [1999] Zb.Orz. s. I-869, pkt 43.

⁽⁵⁾ Zob. także m.in. Trybunał Sprawiedliwości, 30.1.2001, sprawa C-36/98 Królestwo Hiszpanii przeciwko Radzie Unii Europejskiej, [1999] Zb.Orz. s. I-779, pkt 59: „W przypadku gdy analiza wspólnotowego aktu prawnego wykaże, że omawiany akt ma dwa cele lub dwa elementy składowe, a jeden z tych aspektów można zidentyfikować jako główny lub dominujący, podczas gdy drugi ma jedynie charakter pomocniczy, wówczas ten akt prawny powinien zostać oparty na jednej podstawie prawnej, a mianowicie na tej, która wymagana jest z racji głównego lub dominującego celu lub takiego elementu składowego”.

⁽⁶⁾ Porozumienie międzyinstytucjonalne z dnia 28 listopada 2001 r. w sprawie bardziej uporządkowanego wykorzystania techniki przekształcania aktów prawnych, Dz.U. C 77 z 28.3.2002, s. 1.

- dostępnością urzędzeń wielofunkcyjnych. Rozwój elektronicznych nośników informacji szybko przyspiesza, szczególnie pod względem ich pojemności i rozmiaru, i dlatego siły rynkowe powodują, że obrót EEE (zawierającym duże ilości danych osobowych, często szczególnie chronionych) ulega podobnemu przyspieszeniu. W rezultacie nie tylko WEEE „jest uważany za najszybciej rosnący strumień odpadów w UE”⁽⁷⁾, ale również – w przypadku jego niewłaściwego unieszkodliwienia – istnieje oczywiście większe ryzyko utraty i rozpowszechnienia danych osobowych przechowywanych na danym rodzaju EEE.
7. Przez długi czas polityka Unii Europejskiej w dziedzinie ochrony środowiska i zrównoważonego rozwoju miała na celu ograniczanie marnowania zasobów naturalnych i wprowadzanie środków zapobiegających zanieczyszczeniu.
8. Ramy te obejmują unieszkodliwianie, ponowne użycie i recykling WEEE. Środki te dążą do zapobiegania unieszkodliwianiu sprzętu elektrycznego i elektronicznego razem z odpadami mieszanymi, nakładając na producentów obowiązek zapewnienia unieszkodliwiania w sposób określony w dyrektywie.
9. Wśród różnych środków przewidzianych w dyrektywie należy w szczególności zwrócić uwagę na te, które mają na celu *ponowne użycie* (tj. każdą czynność, w której wyniku WEEE lub ich części składowych używa się w tym samym celu, dla jakiego były przewidziane, w tym dalsze użycie urządzeń lub ich części składowych, które zwrócono do punktów zbiórki, dystrybutorów, zakładów recyklingu lub wytwórców), *recykling* (tj. ponowne przetworzenie odpadów w procesie produkcji do pierwotnego celu lub do innych celów) oraz znalezienie innych form odzyskania WEEE, aby ograniczyć ilość unieszkodliwianych odpadów (zob. art. 1 i 3 lit. d) i e) dyrektywy).
10. Działania te, w szczególności ponowne użycie i recykling WEEE, zwłaszcza sprzętu informatycznego i telekomunikacyjnego, mogą stanowić ryzyko, i to większe niż w przeszłości, że podmioty prowadzące zbiórkę WEEE lub sprzedające i kupujące urządzenia używane lub pochodzące z recyklingu mogą zdać sobie sprawę z danych osobowych przechowywanych na tych urządzeniach. Dane te często mogą być szczególnie chronione lub dotyczyć dużej liczby osób fizycznych.
11. Z tego względu EIOD uważa, że wszystkim zainteresowanym stronom (użytkownikom i producentom EEE) należy jak najszybciej uświadomić zagrożenia dla danych osobowych, szczególnie na końcowym etapie cyklu życia EEE. Mimo że na tym etapie EEE ma mniejszą wartość
- gospodarczą, prawdopodobnie zawiera duże ilości danych osobowych, a zatem może mieć dużą wartość „rzeczywistą” dla osoby, której dane dotyczą, lub innych osób.

III. ANALIZA WNIOSKU

III.1. Stosowanie dyrektywy 95/46/WE

12. EIOD nie ma żadnych uwag w odniesieniu do ogólnego celu omawianego wniosku i w pełni popiera podjętą inicjatywę, która ma na celu ulepszenie przyjaznej dla środowiska polityki w dziedzinie WEEE.
13. Wniosek i dyrektywa koncentrują się jednak wyłącznie na zagrożeniach dla środowiska, jakie wiążą się z unieszkodliwianiem WEEE. Wniosek nie uwzględnia innych dodatkowych zagrożeń dla osób fizycznych lub organizacji, które mogą być wynikiem operacji unieszkodliwiania, ponownego użycia lub recyklingu WEEE, a w szczególności zagrożeń związanych z prawdopodobieństwem niewłaściwego uzyskania, ujawnienia lub rozpowszechnienia danych osobowych przechowywanych na WEEE.
14. Należy zauważyć, że dyrektywa 95/46/WE⁽⁸⁾ stosuje się do „każdej operacji lub zestawu operacji dokonywanych na danych osobowych”, w tym ich „usuwania lub niszczenia” (art. 2 lit. b). Unieszkodliwianie EEE może obejmować operacje przetwarzania danych. Z tego względu wniosek i wspomniana dyrektywa częściowo się pokrywają, a zatem zasady ochrony danych mogą w takiej sytuacji stosować się do działań objętych wnioskiem.

III.2. Unieszkodliwianie WEEE a środki bezpieczeństwa

15. EIOD chce zwrócić uwagę na znaczące zagrożenia, które mogą mieć wpływ na osoby fizyczne i organizacje działające jako „administratorzy danych”⁽⁹⁾, gdy WEEE, w szczególności sprzęt informatyczny i telekomunikacyjny, zawiera w trakcie unieszkodliwiania dane osobowe dotyczące użytkowników tych urządzeń lub stron trzecich. Bezprawny dostęp do takich danych osobowych, które czasami obejmują szczególne kategorie danych ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane osobowe dotyczące stanu zdrowia lub życia seksualnego (tak zwane „dane szczególnie chronione”)⁽¹⁰⁾, lub ich ujawnienie rzeczywistości mogą wpłynąć na prywatność i godność osób, których dane te dotyczą, jak również na inne uzasadnione interesy tych osób fizycznych/organizacji (np. gospodarcze).

⁽⁷⁾ Zob. dokument roboczy służb Komisji towarzyszący wnioskowi dotyczącemu dyrektywy Parlamentu Europejskiego i Rady w sprawie zużytego sprzętu elektrycznego i elektronicznego (WEEE) (wersja przekształcona). Ocena skutków z 3.12.2008 (COM(2008) 810 wersja ostateczna) SEC(2008) 2933, s. 17.

⁽⁸⁾ 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.

⁽⁹⁾ Zob. definicja „administratora danych” w art. 2 lit. d) dyrektywy 95/46/WE.

⁽¹⁰⁾ Zob. art. 8 dyrektywy 95/46/WE.

16. Ogólnie rzecz biorąc, EIOD uważa za konieczne podkreślenie znaczenia przyjęcia stosownych środków bezpieczeństwa na każdym etapie (od początku do końca) przetwarzania danych osobowych, co wielokrotnie stwierdził w innych opiniach⁽¹¹⁾. Ma to *a fortiori* zastosowanie na szczególnie wrażliwym etapie, gdy administrator danych zamierza unieszkodliwić urządzenia zawierające dane osobowe.
17. Stosowanie środków bezpieczeństwa jest często warunkiem wstępnym mającym na celu skuteczne zagwarantowanie prawa do ochrony danych osobowych.
18. Dlatego też sprzeczne z logiką byłoby obowiązkowe wprowadzenie (czasem kosztownych) środków bezpieczeństwa do zwykłych operacji przetwarzania danych osobowych (jak w stosownych przypadkach przewiduje art. 17 dyrektywy 95/46/WE⁽¹²⁾), a następnie pominięcie uwzględnienia wprowadzenia odpowiednich zabezpieczeń w odniesieniu do unieszkodliwiania WEEE.
19. Podobnie sprzeczne z logiką byłoby podkreślenie znaczenia kwestii bezpieczeństwa danych poprzez wprowadzenie wymogu powiadamiania o naruszeniu danych na mocy art. 2 dyrektywy 2009/136/WE⁽¹³⁾, a następnie niezapewnienie żadnych gwarancji ani zabezpieczeń w trakcie unieszkodliwiania WEEE, jak również w przypadku ponownego użycia lub recyklingu WEEE.
20. EIOD z przykrością stwierdza, że wniosek nie uwzględnia potencjalnie szkodliwego wpływu unieszkodliwiania WEEE na ochronę danych osobowych przechowywanych na sprzęcie „używanym”.
21. Ten aspekt nie jest również brany pod uwagę w ocenie wpływu dokonanej przez Komisję⁽¹⁴⁾, chociaż doświadczenie pokazało, że niepodjęcie właściwych środków bezpieczeństwa w przypadku unieszkodliwiania WEEE może zagrażać ochronie danych osobowych⁽¹⁵⁾. Ze względu na złożoność kwestii związanych z tym problemem (na przykład ogromną liczbę różnych zasadnych metod, technologii i zainteresowanych stron w cyklu unieszkodliwiania WEEE) EIOD uważa, że stosowne byłoby dokonanie „oceny wpływu na prywatność i ochronę danych” w odniesieniu do procesów związanych z unieszkodliwianiem WEEE.
22. Niemniej jednak EIOD zdecydowanie zaleca opracowanie „najlepszych dostępnych technik” odnośnie do prywatności, ochrony danych i bezpieczeństwa w tej dziedzinie.
23. Kolejnym dowodem jest fakt, że w trakcie konsultacji społecznych poprzedzających przekształcenie dyrektywy, zainteresowane strony, w szczególności przedsiębiorstwa z sektora technologii informacyjnych i łączności elektronicznej, od czasu do czasu podnosiły kwestie dotyczące bezpieczeństwa i ochrony danych osobowych⁽¹⁶⁾.
24. Warto także podkreślić, że niektóre krajowe organy ochrony danych opublikowały wytyczne w celu zminimalizowania zagrożeń, które mogą wynikać z niepodjęcia koniecznych środków bezpieczeństwa, szczególnie w zakresie unieszkodliwiania materiałów, do których stosuje się dyrektywa⁽¹⁷⁾.

⁽¹⁵⁾ Zob. np. dostępny w Internecie artykuł BBC „Children’s files on eBay computer” z dnia 4 maja 2007 r., w którym odnotowano, że na aukcji na portalu eBay sprzedano komputer zawierający dane osobowe na temat opieki zastępczej i adopcji dzieci (http://news.bbc.co.uk/2/hi/uk_news/england/6627265.stm); zob. także dostępny w Internecie artykuł BBC „Bank customer data sold on eBay” z dnia 26 sierpnia 2008 r., w którym odnotowano, że na aukcji na portalu eBay sprzedano dysk twardy zawierający dane osobowe pochodzące z banku posiadającego milion klientów (http://news.bbc.co.uk/2/hi/uk_news/7581540.stm).

⁽¹⁶⁾ Zob. HP, Stakeholder Consultation on the Review of Directive 2002/96/EC of the European Parliament and of the Council on Waste Electrical and Electronic Equipment (WEEE), s. 7–8; DELL (projekt uwagi), WEEE Review Policy Options of the stakeholder consultation on the review of directive 2002/96/EC of the European Parliament and of the Council on Waste Electrical And Electronic Equipment (WEEE), s. 2, pkt 1.1. i 4, pkt 1.3. (3.6.2008); Royal Philips Electronics Position and Proposal, Stakeholder consultation on the Revision of the WEEE Directive, s. 12 (5.6.2008) (http://circa.europa.eu/Public/irc/env/weee_2008_review/library). Zob. także WEEE Consultation Response, Summary of responses and Government response to fourth consultation on implementation of Directives 2002/96/EC and 2003/108/EC on Waste Electrical and Electronic Equipment, grudzień 2006 r., s. 30: „Ochrona i bezpieczeństwo danych. Niektóre przedsiębiorstwa gospodarujące odpadami chciałyby, aby wydano pewne wytyczne dotyczące ochrony i bezpieczeństwa danych, szczególnie w świetle faktu, że przedsiębiorstwa te będą dokonywać obróbki danych szczególnie chronionych” (<http://www.berr.gov.uk/files/file35961.pdf>).

⁽¹⁷⁾ Landesbeauftragter für Datenschutz und Informationsfreiheit Bremen, Entwicklung eines Konzeptes zur Löschung und Datenträgervernichtung durch Behörden und Unternehmen, dnia 16 maja 2007 r. (<http://www.datenschutz-bremen.de/rtf/datenloeschung.rtf>); Garante per la protezione dei dati personali, Electrical and Electronic Waste and Data Protection, dnia 13 października 2008 r. (<http://www.garanteprivacy.it/garante/doc.jsp?ID=1583482>), wspomniane także w dwunastym sprawozdaniu rocznym grupy roboczej art. 29 ds. ochrony danych, dnia 16 czerwca 2009 r., s. 57; zob. także zalecenia Międzynarodowej Grupy Roboczej ds. Ochrony Danych w Telekomunikacji, Recommendation on Data Protection and E-Waste, Sofia, 12–13.3.2009 (<http://www.datenschutz-berlin.de/attachments/650/675.38.14.pdf?1264671551>).

⁽¹¹⁾ Zob. opinia EIOD w sprawie agencji do spraw zarządzania operacyjnego wielkoskalowymi systemami informatycznymi (Dz.U. C 70 z 19.3.2010, s. 13), pkt 46 i 47; opinia w sprawie wniosku dotyczącego dyrektywy w sprawie stosowania praw pacjenta w transgranicznej opiece zdrowotnej (Dz.U. C 128 z 6.6.2009, s. 20), pkt 27–31.

⁽¹²⁾ Zob. art. 3 tejże dyrektywy.

⁽¹³⁾ Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów, Dz.U. L 337 z 18.12.2009, s. 11.

⁽¹⁴⁾ Dokument roboczy służb Komisji towarzyszący wnioskowi dotyczącemu dyrektywy Parlamentu Europejskiego i Rady w sprawie użytego sprzętu elektrycznego i elektronicznego (WEEE) (wersja przekształcona), SEC(2008) 2933 z 3.12.2008; zob. jednak Uniwersytet Narodów Zjednoczonych, 2008 Review of Directive 2002/96/EC on Waste Electrical and Electronic Equipment (WEEE), Komisja Europejska, Belgia, 2007 r., s. 273 (http://ec.europa.eu/environment/waste/weee/pdf/final_rep_unu.pdf); „Data security is also an issue — removing personal data from a hard-drive” (Ważną kwestią jest również bezpieczeństwo danych – usuwanie danych osobowych z dysku twardego).

25. EIOD powtarza, że dyrektywa 95/46/WE ma zastosowanie na etapie unieszkodliwiania WEEE zawierającego dane osobowe. Z tego względu administratorzy danych – w szczególności wykorzystujący urządzenia informatyczne i komunikacyjne – są zobowiązani do spełniania swoich obowiązków dotyczących bezpieczeństwa, aby zapobiec niedozwolonemu ujawnieniu lub rozpowszechnieniu danych osobowych. W tym celu oraz aby uniknąć pociągnięcia do odpowiedzialności za naruszenie środków bezpieczeństwa administratorzy danych w sektorze publicznym lub prywatnym powinni – przy współpracy z inspektorami ochrony danych (tam, gdzie są obecni) – przyjąć właściwą politykę unieszkodliwiania WEEE zawierającego dane osobowe.

26. Jeżeli administratorzy danych unieszkodliwiający EEE nie posiadają potrzebnych umiejętności lub technicznej wiedzy eksperckiej, aby usunąć dane osobowe, o których mowa, mogą powierzyć to zadanie uprawnionym przetwarzającym (np. centrom pomocy, producentom sprzętu i dystrybutorom) na warunkach przewidzianych w art. 17 ust. 2, 3 i 4 dyrektywy 95/46/WE. Z kolei przetwarzający poświadczą przeprowadzenie operacji, o których mowa, lub je wykonają.

27. Z powyższych względów EIOD dochodzi do wniosku, że przekształcenie dyrektywy powinno obejmować dodanie zasad ochrony danych do przepisów mających na celu ochronę środowiska.

28. EIOD zaleca zatem Radzie i Parlamentowi Europejskiemu włączenie do obecnego wniosku przepisu szczegółowego stwierdzającego, że dyrektywa stosuje się do unieszkodliwiania WEEE bez uszczerbku dla przepisów dyrektywy 95/46/WE.

III.3. Ponowne użycie lub recykling WEEE a środki bezpieczeństwa

29. Ze względu na fakt, że podmioty odpowiedzialne za czynności unieszkodliwiania znajdują się w sytuacji umożliwiającej podjęcie niezależnej decyzji co do danych przechowywanych na EEE, można by te podmioty uważać za „administratorów danych”⁽¹⁸⁾. Dlatego też muszą one przyjąć wewnętrzne procedury w celu uniknięcia niepotrzebnych operacji przetwarzania jakichkolwiek danych osobowych przechowywanych na WEEE, a mianowicie operacji innych

⁽¹⁸⁾ „Pojęcie administratora danych jest (...) funkcjonalne w tym sensie, że ma na celu przydzielanie obowiązków tam, gdzie występuje faktyczny wpływ, a zatem opiera się raczej na analizie *okoliczności faktycznych* niż na analizie formalnej”: zob. grupa robocza art. 29 ds. ochrony danych, WP 169, Opinia 1/2010 w sprawie pojęć „administrator danych” i „przetwarzający”, przyjęta dnia 16 lutego 2010 r.

niż te, które są całkowicie niezbędne do potwierdzenia skutecznego usunięcia danych znajdujących się na tym sprzęcie.

30. Ponadto nie mogą zezwolić nieupoważnionym osobom fizycznym na uzyskanie wiedzy o danych przechowywanych na EEE lub ich przetwarzanie. Większe ryzyko niewłaściwego ujawnienia lub rozpowszechnienia danych osobowych oraz konieczność zapobieżenia nieupoważnionemu dostępowi do danych osobowych występują szczególnie, gdy nośniki informacji są poddane recyklingowi lub ponownie użyte i tym samym ponownie wprowadzone na rynek.

31. Z tego względu EIOD zaleca Radzie i Parlamentowi Europejskiemu włączenie do obecnego wniosku przepisu szczegółowego zakazującego wprowadzania do obrotu używanych urządzeń, wobec których wcześniej nie zastosowano odpowiednich środków bezpieczeństwa zgodnie z najnowocześniejszymi normami technicznymi (na przykład wielokrotnego nadpisywania) w celu usunięcia wszelkich danych osobowych, jakie mogą zawierać.

III.4. Poszanowanie prywatności i bezpieczeństwa od samego początku

32. Nadchodzące ramy prawne dotyczące e-odpadów powinny nie tylko zawierać przepis szczegółowy odnoszący się do szerszej „zasady ekoprojektu” sprzętu (zob. art. 4 wniosku w sprawie „projektu produktu”), ale również – jak stwierdzono w innych opiniach EIOD⁽¹⁹⁾ – przepis odnoszący się do zasady „poszanowania prywatności od samego początku”⁽²⁰⁾ lub, co dokładniej dotyczy tej dziedziny, „bezpieczeństwa od samego początku”⁽²¹⁾. Prywatność i ochrona danych powinny być uwzględniane, o ile to możliwe, w projekcie sprzętu elektrycznego lub elektronicznego „w sposób domyślny”, aby umożliwić użytkownikom usunięcie – w prosty sposób i bezpłatnie – danych osobowych, które mogą być obecne na urządzeniach w przypadku ich unieszkodliwiania⁽²²⁾.

⁽¹⁹⁾ Zob. np. The EDPS and EU Research and Technological Development. Policy paper, dnia 28 kwietnia 2008 r., s. 2; opinia EIOD w sprawie inteligentnych systemów transportowych (Dz.U. C 47 z 25.2.2010, s. 6); opinia EIOD w sprawie nadzoru nad bezpieczeństwem farmakoterapii (Dz.U. C 229 z 23.9.2009, s. 19).

⁽²⁰⁾ Argument przemawiający za szerokim stosowaniem tej zasady – zob. grupa robocza art. 29 ds. ochrony danych – Working Party on Police and Justice, The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, dokument przyjęty w dniu 1 grudnia 2009 r., s. 3 i 12; zob. także zalecenie Komisji w sprawie wdrażania zasad ochrony prywatności i ochrony danych w zastosowaniach wspieranych identyfikacją radiową, C(2009) 3200 wersja ostateczna, s. 8.

⁽²¹⁾ Zob. komunikat Komisji „Europejski program badań i innowacji w dziedzinie bezpieczeństwa” – wstępne stanowisko Komisji w sprawie głównych ustaleń i zaleceń europejskiego forum badań i innowacji w dziedzinie bezpieczeństwa (ESRIF), COM(2009) 691 wersja ostateczna, s. 6 i 14.

⁽²²⁾ Zob. także EIOD, opinia z dnia 18 marca 2010 r. w sprawie wspierania zaufania w społeczeństwie informacyjnym poprzez działania na rzecz ochrony danych i prywatności.

33. To podejście jest wyraźnie popierane w art. 3 ust. 3 lit. c) dyrektywy 1999/5/WE⁽²³⁾ w sprawie urządzeń radiowych i końcowych urządzeń telekomunikacyjnych oraz w art. 14 ust. 3 dyrektywy 2002/58/WE⁽²⁴⁾.
34. Producenci powinni zatem „wbudowywać” środki ochrony prywatności i bezpieczeństwa poprzez rozwiązania technologiczne⁽²⁵⁾. W tych ramach należy również promować i wspierać inicjatywy mające na celu informowanie zainteresowanych stron o potrzebie usunięcia wszelkich danych osobowych przed unieszkodliwieniem WEEE (w tym producentów, którzy w tym celu udostępniają bezpłatne oprogramowanie)⁽²⁶⁾.

IV. WNIOSKI

35. 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 unieszkodliwianiem WEEE na zasadzie konsultacji na dostatecznie wczesnym etapie przed opracowaniem odpowiednich środków.
36. Biorąc jednak pod uwagę kontekst, w którym dane osobowe są przetwarzane, EIOD zaleca, aby wniosek zawierał przepisy szczególne:

- stwierdzające, że dyrektywę WEEE stosuje się bez uszczerbku dla przepisów dyrektywy 95/46/WE,
- zakazujące wprowadzania do obrotu używanych urządzeń, wobec których wcześniej nie zastosowano odpowiednich środków bezpieczeństwa zgodnie z najnowocześniejszymi normami technicznymi w celu usunięcia wszelkich danych osobowych, jakie mogą zawierać,

— odnoszące się do zasady „poszanowania prywatności od samego początku” lub „bezpieczeństwa od samego początku”: prywatność i ochrona danych powinny być uwzględniane, o ile to możliwe, w projekcie sprzętu elektrycznego lub elektronicznego „w sposób domyślny”, aby umożliwić użytkownikom usunięcie – w prosty sposób i bezpłatnie – danych osobowych, które mogą być obecne na urządzeniach w przypadku ich unieszkodliwiania.

37. EIOD zdecydowanie zaleca zatem, aby zgodnie z dyrektywą 95/46/WE wprowadzić we wniosku następujące zmiany:

— motyw (11): „Ponadto niniejszą dyrektywę należy stosować bez uszczerbku dla przepisów dotyczących ochrony danych, w szczególności dyrektywy 95/46/WE. Ponieważ sprzęt elektryczny i elektroniczny (EEE) jest dużą grupą produktów, która obejmuje różne rodzaje nośników mogących przechowywać dane osobowe (takie jak sprzęt informatyczny i telekomunikacyjny), związane z nimi czynności unieszkodliwiania, w szczególności ponowne użycie i recykling, mogą stanowić zagrożenie nieupoważnionym dostępem do danych osobowych przechowywanych na WEEE. Dlatego też w miarę możliwości środki ochrony prywatności i bezpieczeństwa danych powinny być domyślnie włączone w projekt sprzętu elektrycznego i elektronicznego umożliwiającego przechowywanie danych osobowych, aby umożliwić użytkownikom usunięcie – w prosty sposób i bezpłatnie – wszelkich takich danych obecnych w czasie unieszkodliwiania.”,

⁽²³⁾ Artykuł 3 ust. 3 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 (Dz.U. L 91 z 7.4.1999, s. 10): „(...) Komisja może zdecydować, że aparatura należąca do niektórych klas sprzętu lub aparatura określonego typu ma być tak skonstruowana, aby (...) miała wbudowane systemy zabezpieczające w celu zapewnienia ochrony danych osobowych i prywatności użytkownika lub subskrybenta”.

⁽²⁴⁾ „W miarę potrzeb, możliwe jest przyjęcie środków w celu zapewnienia, że terminal jest skonstruowany w sposób zgodny z prawem użytkowników do ochrony i kontroli używania ich danych osobowych, zgodnie z dyrektywą 1999/5/WE i decyzją Rady 87/95/EWG z dnia 22 grudnia 1986 r. w sprawie normalizacji w dziedzinie technologii informatycznych i telekomunikacji”. Zob. także motyw 46 teże dyrektywy, wspomniany w przypisie 13.

⁽²⁵⁾ Argument przemawiający za tą perspektywą polityki – zob. także V. Reding, Keynote Speech at the Data Protection Day, dnia 28 stycznia 2010 r., Parlament Europejski, Bruksela, SPEECH/10/16: „Przedsiębiorstwa muszą wykorzystywać swoją siłę innowacji do poprawienia ochrony prywatności i danych osobowych od samego początku cyklu rozwoju. Poszanowanie prywatności od samego początku to zasada leżąca w interesie zarówno obywateli, jak i przedsiębiorstw. Poszanowanie prywatności od samego początku doprowadzi do lepszej ochrony osób fizycznych, a także do zwiększenia zaufania do nowych usług i produktów, co z kolei będzie miało pozytywny wpływ na gospodarkę. Widziałam pewne zachęcające przykłady, lecz bardzo wiele pozostaje do zrobienia”.

⁽²⁶⁾ Zob. np. Kanadyjska Królewska Policja Konna, B2-002 — IT Media Overwrite and Secure Erase Products (05/2009), <http://www.rcmp-grc.gc.ca/ts-st/pubs/it-ti-sec/index-eng.htm>

— artykuł 2 ust. 3: „Niniejszą dyrektywę stosuje się bez uszczerbku dla przepisów dotyczących ochrony danych, w szczególności dyrektywy 95/46/WE.”.

38. Ponadto EIOD uważa, że należy wziąć pod uwagę wprowadzenie następujących zmian:

— artykuł 4 ust. 2: „Państwa członkowskie wspierają środki promujące projektowanie i produkcję sprzętu elektrycznego i elektronicznego, który ułatwia usuwanie wszelkich danych osobowych zawartych na EEE w czasie jego unieszkodliwiania”,

— artykuł 8 ust. 7: „Państwa członkowskie gwarantują, że jakiegokolwiek zebrany WEEE zawierający dane osobowe, który podlega obróbce w celu recyklingu lub ponownego użycia, nie jest wprowadzany do obiegu, dopóki dane te nie zostaną usunięte z wykorzystaniem najlepszych dostępnych technik.”,

-
- artykuł 14 ust. 6.: „Państwa członkowskie mogą wymagać, aby użytkownicy EEE zawierającego dane osobowe otrzymywali od producentów lub dystrybutorów, np. w instrukcji użytkowania lub w punkcie sprzedaży, informacje odnoszące się do konieczności usunięcia danych osobowych, które mogą być przechowywane na EEE przed jego unieszkodliwieniem”.

Sporządzono w Brukseli dnia 14 kwietnia 2010 r.

Peter HUSTINX
Europejski Inspektor Ochrony Danych

II

(Komunikaty)

KOMUNIKATY INSTYTUCJI, ORGANÓW I JEDNOSTEK ORGANIZACYJNYCH
UNII EUROPEJSKIEJ

KOMISJA EUROPEJSKA

Zatwierdzenie pomocy państwa zgodnie z art. 107 i 108 TFUE

Sprawy, w których Komisja nie wnosi zastrzeżeń

(Tekst mający znaczenie dla EOG, z wyjątkiem działań wchodzących w zakres załącznika I do Traktatu)

(2010/C 280/03)

Data przyjęcia decyzji	6.7.2010
Numer środka pomocy państwa	N 42/10
Państwo członkowskie	Finlandia
Region	—
Nazwa (i/lub nazwa beneficjenta)	Tuki maataloustuotannon lopettamiseen
Podstawa prawna	Laki maatalouden harjoittamisesta luopumisen tukemisesta (612/2006), sellaisena kuin se on viimeksi muutettuna lailla (1787/2009); Valtioneuvoston asetus maatalouden harjoittamisesta luopumisen tukemisesta (25/2007).
Rodzaj środka pomocy	Wsparcie z tytułu przejścia na wcześniejszą emeryturę
Cel pomocy	Rozwój sektorowy
Forma pomocy	Dotacja bezpośrednia
Budżet	184 mln EUR
Intensywność pomocy	Zmienna
Czas trwania	1.1.2011–31.12.2014
Sektory gospodarki	Podstawowa produkcja rolna
Nazwa i adres organu przyznającego pomoc	Maa- ja metsätalousministeriö PL 30 FI-00023 Valtioneuvosto Helsinki SUOMI/FINLAND
Inne informacje	—

Oryginalny tekst decyzji, z którego usunięto wszystkie informacje poufne, znajduje się na stronie:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_pl.htm

Data przyjęcia decyzji	20.7.2010
Numer środka pomocy państwa	N 131/10
Państwo członkowskie	Bułgaria
Region	—
Nazwa (i/lub nazwa beneficjenta)	Държавна помощ за компенсирани на загуби, понесени от селскостопанските производители в напълно опустошени райони вследствие на природни бедствия или неблагоприятни климатични условия (нотификация на изменение)
Podstawa prawna	Чл. 12, ал. 1, т. 2 и чл. 12, ал. 2, т. 1, буква „а“ от Закона за подпомагане на земеделските производители, ДВ 58/98 Указания за предоставяне на държавна помощ за компенсирани на загуби в следствие на природни бедствия и неблагоприятни климатични условия
Rodzaj środka pomocy	Program pomocy
Cel pomocy	Pomoc z tytułu niekorzystnych warunków pogodowych, klęsk żywiołowych lub zdarzeń nadzwyczajnych
Forma pomocy	Dotacja bezpośrednia
Budżet	Budżet całkowity: 600 BGN (w mln)
Intensywność pomocy	80 %
Czas trwania	Do dnia 31.12.2013
Sektory gospodarki	Rolnictwo
Nazwa i adres organu przyznającego pomoc	Държавен фонд „Земеделие“ Бул. „Цар Борис III“ № 136 1618 София/Sofia БЪЛГАРИЯ/BULGARIA
Inne informacje	—

Oryginalny tekst decyzji, z którego usunięto wszystkie informacje poufne, znajduje się na stronie:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_pl.htm

Data przyjęcia decyzji	9.7.2010
Numer środka pomocy państwa	N 133/10
Państwo członkowskie	Włochy
Region	Provincia autonoma di Bolzano
Nazwa (i/lub nazwa beneficjenta)	Disciplina degli aiuti regionali in materia di foreste
Podstawa prawna	Legge Provinciale del 21.10.1996 «Ordinamento Forestale» decreto del Presidente della Giunta provinciale 31 luglio 2000, n. 29 Regolamento all'ordinamento forestale 2000; Programma di sviluppo rurale 2007-2013, misure 111, 122, 123 settore Foreste, 125 Settore Foreste, 226, 227
Rodzaj środka pomocy	Program pomocy
Cel pomocy	Pomoc przeznaczona dla sektora leśnictwa
Forma pomocy	Dotacja bezpośrednia

Budżet	Łączna maksymalna kwota: 30 milionów EUR
Intensywność pomocy	Do 100 % kosztów kwalifikowalnych
Czas trwania	Na lata 2010–2013
Sektory gospodarki	Sektor leśnictwa
Nazwa i adres organu przyznającego pomoc	Provincia Autonoma di Bolzano Ripartizione Foreste Ufficio economia montana Via Brennero 6 39100 Bolzano BZ ITALIA
Inne informacje	—

Oryginalny tekst decyzji, z którego usunięto wszystkie informacje poufne, znajduje się na stronie:
http://ec.europa.eu/community_law/state_aids/state_aids_texts_pl.htm

Data przyjęcia decyzji	4.6.2010
Numer środka pomocy państwa	N 148/10
Państwo członkowskie	Włochy
Region	Provincia autonoma di Trento
Nazwa (i/lub nazwa beneficjenta)	Ricostituzione del potenziale forestale e interventi preventivi
Podstawa prawna	Piano di sviluppo rurale della Provincia autonoma di Trento 2007-2013 (Misura 226)
Rodzaj środka pomocy	Program pomocy
Cel pomocy	Pomoc dla sektora leśnictwa
Forma pomocy	Dotacja bezpośrednia
Budżet	Maksymalne roczne wydatki: 3,25 mln EUR Łączna maksymalna kwota: 13 mln EUR
Intensywność pomocy	Do 100 % kosztów kwalifikowalnych
Czas trwania	Do 31.12.2013
Sektory gospodarki	Sektor leśnictwa
Nazwa i adres organu przyznającego pomoc	Provincia autonoma di Trento Piazza Dante 5 38122 Trento TN ITALIA
Inne informacje	—

Oryginalny tekst decyzji, z którego usunięto wszystkie informacje poufne, znajduje się na stronie:
http://ec.europa.eu/community_law/state_aids/state_aids_texts_pl.htm

Data przyjęcia decyzji	17.6.2010
Numer środka pomocy państwa	N 209/10
Państwo członkowskie	Francja
Region	Departamenty Charente-Maritime, Vendée i Gironde
Nazwa (i/lub nazwa beneficjenta)	Aides aux exploitants agricoles victimes des inondations marines causées par la tempête Xynthia du 28 février 2010.
Podstawa prawna	<ul style="list-style-type: none"> — Articles L 361-1 et s. du code rural (le budget nécessaire aux aides d'État affectées à ce dispositif sera prélevé sur le fonds national de garantie des calamités agricoles). — Articles 1511-2 à 1511-6 du code général des collectivités territoriales et L 3231-2 et suivants pour les aides des collectivités territoriales. — Arrêté interministériel du 1^{er} mars 2010 de reconnaissance de catastrophe naturelle. — Arrêté interministériel du 11 mars 2010 de reconnaissance de catastrophe naturelle.
Rodzaj środka pomocy	Program pomocy
Cel pomocy	Pomoc mająca na celu rekompensatę szkód w zakresie produkcji rolnej.
Forma pomocy	Dotacja bezpośrednia
Budżet	Maksymalnie 43 000 000 EUR
Intensywność pomocy	Maksymalnie 60 %
Czas trwania	4 lata
Sektory gospodarki	Rolnictwo
Nazwa i adres organu przyznającego pomoc	Ministère de l'alimentation, de l'agriculture et de la pêche 78 rue de Varenne 75349 Paris 07 SP FRANCE
Inne informacje	—

Oryginalny tekst decyzji, z którego usunięto wszystkie informacje poufne, znajduje się na stronie:
http://ec.europa.eu/community_law/state_aids/state_aids_texts_pl.htm

Zatwierdzenie pomocy państwa zgodnie z art. 107 i 108 TFUE**Sprawy, w których Komisja nie wnosi zastrzeżeń**

(Tekst mający znaczenie dla EOG, z wyjątkiem działań wchodzących w zakres załącznika I do Traktatu)

(2010/C 280/04)

Data przyjęcia decyzji	16.7.2010
Numer środka pomocy państwa	N 414/09
Państwo członkowskie	Francja
Region	—
Nazwa (i/lub nazwa beneficjenta)	Aides de l'Agence de l'eau Artois-Picardie aux engagements agro-environnementaux dans le bassin Artois Picardie (EAEAP)
Podstawa prawna	Loi n° 2006-1772 du 30 décembre 2006 sur l'eau et les milieux aquatiques (JORF n° 303 du 31 décembre 2006). Proposition de dispositif pour des aides agro-environnementales de l'agence de l'eau Artois-Picardie.
Rodzaj środka pomocy	Program pomocy
Cel pomocy	Pomoc na działania rolno-środowiskowe
Forma pomocy	Dotacja bezpośrednia
Budżet	Roczne wydatki: 21,33 mln EUR Ogólna kwota: 64 mln EUR
Intensywność pomocy	Maksymalnie 100 % kosztów kwalifikowalnych
Czas trwania	Lata 2010–2012
Sektory gospodarki	Sektor rolny
Nazwa i adres organu przyznającego pomoc	Agence de l'eau Artois-Picardie 200 rue Marceline BP 818 59508 Douai FRANCE
Inne informacje	—

Oryginalny tekst decyzji, z którego usunięto wszystkie informacje poufne, znajduje się na stronie:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_pl.htm

Data przyjęcia decyzji	3.2.2010
Numer środka pomocy państwa	N 582/09
Państwo członkowskie	Włochy
Region	Sardaigne
Nazwa (i/lub nazwa beneficjenta)	Ristrutturazione dell'azienda «Cooperativa viticoltori della Planargia»

Podstawa prawna	Legge regionale 19 gennaio 1998, n. 4 «Interventi a favore di aziende agricole in difficoltà» Legge regionale 29 maggio 2007, n. 2 «Legge finanziaria 2007» — articolo. 21 Decreto dell'Assessore n. 2532/DecA/105 del 13.10.2009
Rodzaj środka pomocy	Pomoc indywidualna
Cel pomocy	Restrukturyzacja zagrożonego przedsiębiorstwa
Forma pomocy	Dotacja bezpośrednia
Budżet	294 540 EUR
Intensywność pomocy	75 %
Czas trwania	Od dnia zatwierdzenia pomocy przez Komisję
Sektory gospodarki	Rolnictwo (sektor wina)
Nazwa i adres organu przyznającego pomoc	Assessorato dell'agricoltura e riforma agro-pastorale Via Pessagno 4 09126 Cagliari CA ITALIA
Inne informacje	—

Oryginalny tekst decyzji, z którego usunięto wszystkie informacje poufne, znajduje się na stronie:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_pl.htm

Data przyjęcia decyzji	20.7.2010
Numer środka pomocy państwa	NN 26/10
Państwo członkowskie	Republika Czeska
Region	—
Nazwa (i/lub nazwa beneficjenta)	Vrácení části spotřební daně na pohonné hmoty spotřebované při zemědělské produkci (změna režimu podpory č. N 678/07)
Podstawa prawna	Zákon č. 353/2003 Sb., o spotřebních daních, ve znění pozdějších předpisů Vyhláška 48/2008 Sb., o způsobu výpočtu nároku na vrácení spotřební daně zaplacené v cenách některých minerálních olejů spotřebovaných v zemědělské prvovýrobě
Rodzaj środka pomocy	Program pomocy
Cel pomocy	Pomoc związana ze zwolnieniem z podatków na mocy dyrektywy 2003/96/WE
Forma pomocy	Ulga podatkowa
Budżet	Łącznie: 6 800 mln CZK (około 272 mln EUR) Rocznie: 1 700 mln CZK (około 68 mln EUR)
Intensywność pomocy	60 % kosztów kwalifikowalnych
Czas trwania	Do dnia 31 grudnia 2013 r.

Sektory gospodarki	Sektor rolnictwa
Nazwa i adres organu przyznającego pomoc	Ministerstvo zemědělství Těšnov 17 117 05 Praha 1 ČESKÁ REPUBLIKA
Inne informacje	—

Oryginalny tekst decyzji, z którego usunięto wszystkie informacje poufne, znajduje się na stronie:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_pl.htm

Data przyjęcia decyzji	16.7.2010
Numer środka pomocy państwa	N 213/10
Państwo członkowskie	Estonia
Region	—
Nazwa (i/lub nazwa beneficjenta)	Eesti maaelu arengukava 2007–2013 meede 2.7 „Natura 2000 toetus erametsamaale”
Podstawa prawna	Eesti maaelu arengukava 2007–2013, peatükk 5.3.2.2; Põllumajandusministri 11.3.2010. aasta määrus nr 26 „Natura 2000 alal asuva erametsamaa kohta antava toetuse saamise nõuded, toetuse taotlemise ja taotluse menetlemise täpsem kord”; Euroopa Liidu ühise põllumajanduspoliitika rakendamise seadus
Rodzaj środka pomocy	Pomoc na rzecz sektora leśnictwa
Cel pomocy	Leśnictwo
Forma pomocy	Dotacja bezpośrednia
Budżet	Budżet całkowity w wysokości 326 mln EEK (około 20,8 mln EUR)
Intensywność pomocy	Do 100 % kosztów kwalifikowalnych.
Czas trwania	Począwszy od daty podjęcia decyzji przez Komisję do dnia 31 grudnia 2013 r.
Sektory gospodarki	Leśnictwo
Nazwa i adres organu przyznającego pomoc	Põllumajanduse Registrate ja Informatsiooni Amet Narva 3 51009 Tartu EESTI/ESTONIA
Inne informacje	—

Oryginalny tekst decyzji, z którego usunięto wszystkie informacje poufne, znajduje się na stronie:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_pl.htm

Zatwierdzenie pomocy państwa zgodnie z art. 107 i 108 TFUE**Sprawy, w których Komisja nie wnosi zastrzeżeń**

(Tekst mający znaczenie dla EOG, z wyjątkiem działań wchodzących w zakres załącznika I do Traktatu)

(2010/C 280/05)

Data przyjęcia decyzji	12.8.2010
Numer środka pomocy państwa	N 83/10
Państwo członkowskie	Włochy
Region	Sardegna
Nazwa (i/lub nazwa beneficjenta)	Aiuto alla ristrutturazione a favore dell'Unione Pastori Società Cooperativa Agricola, registrata nella Z.I Taccu — Nurri Cagliari
Podstawa prawna	Legge regionale 19 gennaio 1998 «Interventi a favore delle aziende agricole in difficoltà» Articolo 21 della legge regionale 29 maggio 2007, n. 2 Decreto regionale n. 343/DecA/7 del 4 febbraio 2010
Rodzaj środka pomocy	Pomoc indywidualna
Cel pomocy	Restrukturyzacja średniego przedsiębiorstwa
Forma pomocy	Dotacja bezpośrednia
Budżet	1 mln EUR
Intensywność pomocy	33,3 % całkowitych kosztów restrukturyzacji (3 mln EUR)
Czas trwania	Pomoc <i>ad hoc</i>
Sektory gospodarki	Rolnictwo
Nazwa i adres organu przyznającego pomoc	Regione Autonoma Sardegna Assessorato dell'Agricoltura Via Pessagno 4 09125 Cagliari CA ITALIA
Inne informacje	—

Oryginalny tekst decyzji, z którego usunięto wszystkie informacje poufne, znajduje się na stronie:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_pl.htm

Zatwierdzenie pomocy państwa zgodnie z art. 107 i 108 TFUE

Sprawy, w których Komisja nie wnosi zastrzeżeń

(Tekst mający znaczenie dla EOG, z wyjątkiem działań wchodzących w zakres załącznika I do Traktatu)

(2010/C 280/06)

Data przyjęcia decyzji	7.4.2010
Numer środka pomocy państwa	N 716/09
Państwo członkowskie	Grecja
Region	Περιοχές που επλήγησαν από τις πυρκαγιές του 2009
Nazwa (i/lub nazwa beneficjenta)	Πρόγραμμα κρατικών οικονομικών ενισχύσεων για την αντιστάθμιση ζημιών από πυρκαγιές έτους 2009
Podstawa prawna	Σχέδιο ΚΥΑ για τη λήψη μέτρων υπέρ των παραγωγών της χώρας των οποίων οι γεωργοκτηνοτροφικές τους εκμεταλλεύσεις ζημιώθηκαν από πυρκαγιές κατά το έτος 2009
Rodzaj środka pomocy	Odszkodowania z tytułu strat poniesionych w zakresie środków produkcji rolnej z powodu zdarzenia nadzwyczajnego
Cel pomocy	Zdarzenia nadzwyczajne
Forma pomocy	Dotacja bezpośrednia
Budżet	Budżet całkowity 8 000 000 EUR
Intensywność pomocy	Prawo do otrzymania pomocy przysługiwać będzie producentom, którzy ponieśli straty przekraczające minimalny próg wynoszący 30 %. Intensywność pomocy zależna będzie od charakteru obiektu, którego dotyczy strata, i wyniesie od 50 % do 80 %
Czas trwania	Od daty zatwierdzenia programu do dnia 31 grudnia 2013 r.
Sektory gospodarki	Sektor rolnictwa
Nazwa i adres organu przyznającego pomoc	α. Υπουργείο Αγροτικής Ανάπτυξης και Τροφίμων Αχαρνών 2 101 76 Αθήνα/Athens ΕΛΛΑΔΑ/GREECE β. ΕΛΓΑ Μεσογείων 45 115 10 Αθήνα/Athens ΕΛΛΑΔΑ/GREECE
Inne informacje	—

Oryginalny tekst decyzji, z którego usunięto wszystkie informacje poufne, znajduje się na stronie:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_pl.htm

IV

(Informacje)

INFORMACJE INSTYTUCJI, ORGANÓW I JEDNOSTEK ORGANIZACYJNYCH
UNII EUROPEJSKIEJ

KOMISJA EUROPEJSKA

Kursy walutowe euro ⁽¹⁾

15 października 2010 r.

(2010/C 280/07)

1 euro =

Waluta	Kurs wymiany	Waluta	Kurs wymiany		
USD	Dolar amerykański	1,4089	AUD	Dolar australijski	1,4142
JPY	Jen	114,28	CAD	Dolar kanadyjski	1,4165
DKK	Korona duńska	7,4564	HKD	Dolar hong kong	10,9300
GBP	Funt szterling	0,87750	NZD	Dolar nowozelandzki	1,8565
SEK	Korona szwedzka	9,2230	SGD	Dolar singapurski	1,8244
CHF	Frank szwajcarski	1,3423	KRW	Won	1 564,64
ISK	Korona islandzka		ZAR	Rand	9,5833
NOK	Korona norweska	8,0925	CNY	Yuan renminbi	9,3568
BGN	Lew	1,9558	HRK	Kuna chorwacka	7,3355
CZK	Korona czeska	24,515	IDR	Rupia indonezyjska	12 530,82
EEK	Korona estońska	15,6466	MYR	Ringgit malezyjski	4,3443
HUF	Forint węgierski	274,18	PHP	Peso filipińskie	60,847
LTL	Lit litewski	3,4528	RUB	Rubel rosyjski	42,5650
LVL	Łat łotewski	0,7097	THB	Bat tajlandzki	42,015
PLN	Złoty polski	3,9050	BRL	Real	2,3369
RON	Lej rumuński	4,2765	MXN	Peso meksykańskie	17,4580
TRY	Lir turecki	1,9808	INR	Rupia indyjska	62,1320

⁽¹⁾ Źródło: referencyjny kurs wymiany walut opublikowany przez ECB.

DECYZJA KOMISJI

z dnia 14 października 2010 r.

powołująca ponownie CARS 21 – grupę wysokiego szczebla ds. konkurencyjności i zrównoważonego rozwoju przemysłu motoryzacyjnego w Unii Europejskiej

(2010/C 280/08)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

a także mając na uwadze, co następuje:

- (1) Artykułem 173 Traktatu nałożono na Unię Europejską i państwa członkowskie zadanie zapewnienia warunków niezbędnych dla konkurencyjności przemysłu unijnego. Artykuł 191 TFUE stanowi, że unijna polityka w dziedzinie środowiska naturalnego przyczynia się do promowania środków mających na celu zachowanie, ochronę i poprawę jakości środowiska naturalnego oraz zwalczanie zmian klimatu.
- (2) W ramach procesu CARS 21 („Competitive Automotive Regulatory System for the 21st century” (konkurencyjny system prawny dla przemysłu motoryzacyjnego w XXI w.)), zapoczątkowanego w 2005 r. jako element polityki przemysłowej Komisji, opracowano zalecenia dotyczące krótko-, średnio- i długoterminowej polityki w dziedzinie ram prawnych dla przemysłu motoryzacyjnego Unii Europejskiej, która zwiększa światową konkurencyjność i zatrudnienie, zapewniając przy tym dalszy postęp w obszarze bezpieczeństwa i oddziaływania na środowisko naturalne za cenę przystępną dla konsumentów.
- (3) W komunikacie „EUROPA 2020 – strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu”⁽¹⁾ Komisja przedstawiła propozycje modernizacji sektora transportu i zmniejszenia jego udziału w emisji związków węgla oraz promowania nowych technologii, w tym samochodów o napędzie elektrycznym. Celem projektu przewodniego „Polityka przemysłowa w erze globalizacji” jest polityka przemysłowa, która stwarza najlepsze warunki dla utrzymania i rozwoju silnej, konkurencyjnej i zróżnicowanej bazy przemysłowej w Europie, a zarazem propaguje zrównoważony rozwój, wspierając przejście sektorów wytwórczych do efektywniejszego korzystania z energii i zasobów. Projekt przewodni „Europa efektywnie korzystająca z zasobów” ma zachęcać do stosowania różnych środków w zakresie infrastruktury, takich jak infrastruktura sieci mobilności elektrycznej czy inteligentne zarządzanie ruchem, a przede wszystkim promować nowe technologie, w tym samochody o napędzie elektrycznym i hybrydowym.
- (4) W komunikacie Komisji „Europejska strategia na rzecz ekologicznie czystych i energooszczędnych pojazdów”⁽²⁾ określono krótko- i długoterminowe cele wspierania badań i innowacji, poszukiwania nowych rozwiązań

w zakresie wytwarzania i dystrybucji energii, pobudzania zatrudnienia oraz zachęcania konsumentów do kupowania pojazdów ekologicznych.

- (5) W związku z tym konieczne jest ustanowienie grupy ekspertów w dziedzinie konkurencyjności i zrównoważonego rozwoju przemysłu motoryzacyjnego Unii Europejskiej, w oparciu o proces CARS 21, oraz określenie zadań i struktury tej grupy.
- (6) Grupa ta powinna pomóc w ustaleniu, jakie polityki i środki, na poziomie Unii Europejskiej, krajowym oraz innych podmiotów, wspierają konkurencyjność i zrównoważony rozwój przemysłu motoryzacyjnego Unii Europejskiej.
- (7) W skład grupy powinni wejść przedstawiciele Parlamentu Europejskiego, Komisji, państw członkowskich oraz właściwych podmiotów reprezentujących przemysł i społeczeństwo obywatelskie, w szczególności konsumentów, związki zawodowe i organizacje pozarządowe.
- (8) Bez uszczerbku dla przepisów Komisji dotyczących bezpieczeństwa, określonych w załączniku do decyzji Komisji 2001/844/WE, EWWiS, Euratom z dnia 29 listopada 2001 r. zmieniającej jej regulamin wewnętrzny⁽³⁾, należy określić zasady dotyczące ujawniania informacji przez członków grupy.
- (9) Wszelkie dane osobowe powinny być przetwarzane zgodnie z rozporządzeniem (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⁽⁴⁾.
- (10) Należy ustalić okres stosowania niniejszej decyzji. W odpowiednim czasie Komisja rozważy celowość przedłużenia tego okresu,

STANOWI, CO NASTĘPUJE:

Artykuł 1

Grupa

Niniejszym powołuje się ponownie grupę wysokiego szczebla ds. konkurencyjności i zrównoważonego rozwoju przemysłu motoryzacyjnego w Unii Europejskiej, dalej zwaną „grupą”, która wcześniej działała na nieformalnych zasadach pod nazwą „Competitive Automotive Regulatory System for the 21st century” (konkurencyjny system prawny dla przemysłu motoryzacyjnego w XXI w.).

⁽¹⁾ COM(2010) 2020.⁽²⁾ COM(2010) 186.⁽³⁾ Dz.U. L 317 z 3.12.2001, s. 1.⁽⁴⁾ Dz.U. L 8 z 12.1.2001, s. 1.

Artykuł 2

Zadania

Do zadań grupy należy:

- 1) wspieranie Komisji w kwestiach związanych z konkurencyjnością i zrównoważonym rozwojem przemysłu motoryzacyjnego;
- 2) przeprowadzenie analizy ekonomicznej i statystycznej czynników napędzających zmiany strukturalne w przemyśle motoryzacyjnym, jak również innych czynników wpływających na konkurencyjną pozycję unijnego przemysłu motoryzacyjnego;
- 3) wspieranie Komisji w realizacji polityki określonej w strategii EUROPA 2020, projekcie przewodnim dotyczącym Europy efektywnie korzystającej z zasobów, projekcie przewodnim polityki przemysłowej w erze globalizacji oraz komunikacji na temat ekologicznie czystych i energooszczędnych pojazdów COM(2010) 186, w celu zachowania konkurencyjnego i zrównoważonego przemysłu motoryzacyjnego Unii Europejskiej;
- 4) działanie na rzecz zapewnienia płynnych i zrównoważonych przekształceń gospodarczych i społecznych, poprzez aktywne przewidywanie procesów restrukturyzacyjnych i potrzeb w zakresie umiejętności i kwalifikacji oraz zarządzanie nimi, z uwzględnieniem osiągnięć „Europejskiego partnerstwa na rzecz przewidywania zmian w sektorze motoryzacyjnym”;
- 5) sformułowanie zestawu sektorowych zaleceń dotyczących polityki skierowanych do decydentów politycznych na poziomie unijnym i krajowym, a także do przemysłu oraz organizacji społeczeństwa obywatelskiego;
- 6) opracowywanie zasad dobrego postępowania w celu promowania przejrzystości w relacjach handlowych i stosunkach umownych między stronami porozumień pionowych w sektorze motoryzacyjnym;
- 7) służenie radą w określonych aspektach wdrażania strategii Komisji EUROPA 2020 dotyczącej inteligentnego, zrównoważonego i sprzyjającego włączeniu społecznemu wzrostu gospodarczego.

Artykuł 3

Skład i powoływanie

1. W skład grupy wchodzi nie więcej niż 40 członków.
2. Członkowie grupy są powoływani jako osoby prywatne. Każdy członek grupy mianuje swojego przedstawiciela do stałej podgrupy przygotowawczej, zwanej dalej „podgrupą przygotowawczą”.
3. Członkowie grupy są wyznaczani przez Komisję spośród podmiotów wysokiego szczebla posiadających kompetencje i obowiązki w dziedzinach związanych z konkurencyjnością i zrównoważonym rozwojem przemysłu motoryzacyjnego UE. Skład grupy odzwierciedla proporcjonalną reprezentację różnych podmiotów. W skład grupy wchodzi przedstawiciele Parlamentu Europejskiego, Komisji, państw członkowskich oraz uczestników łańcucha wartości przemysłu, związków zawodowych i społeczeństwa obywatelskiego (organizacji pozarządowych i konsumentów).

4. Okres kadencji członków wynosi dwa lata. Pełnią oni swoje funkcje do czasu ich zastąpienia lub do upływu ich kadencji. Kadencja jest odnawialna.

5. Członkowie, którzy utracą zdolność wnoszenia należytego wkładu w prace grupy, złożą rezygnację lub nie spełniają warunków określonych w art. 339 Traktatu, mogą zostać zastąpieni na okres, jaki pozostaje do upływu ich kadencji.

6. Nazwiska członków grupy powołanych jako osoby prywatne są publikowane w rejestrze grup ekspertów Komisji i podobnych zespołów, dalej zwanym „rejestrem”.

7. Dane osobowe są gromadzone, przetwarzane i publikowane zgodnie z rozporządzeniem (WE) nr 45/2001.

Artykuł 4

Funkcjonowanie grupy

1. Grupie przewodniczy przedstawiciel Komisji.
2. Podgrupa przygotowawcza przygotowuje posiedzenia, dokumenty przedstawiające stanowiska oraz proponowane przez grupę zalecenia dotyczące działań i środków politycznych; w tym celu podgrupa współpracuje ściśle z właściwymi służbami Komisji.
3. W porozumieniu ze służbami Komisji grupa może powoływać oprócz podgrupy przygotowawczej także grupy robocze celem zbadania szczegółowych kwestii związanych z zadaniami grupy, zgodnie z zakresem obowiązków ustalonym przez grupę. Grupy robocze są rozwiązywane po wypełnieniu swoich zadań.
4. W trybie doraźnym przedstawiciel Komisji może zaprosić do udziału w pracach grupy lub podgrupy zewnętrznych ekspertów lub obserwatorów posiadających określone kompetencje w dziedzinie, którą zajmuje się grupa lub grupa robocza. Ponadto przedstawiciel Komisji może nadawać osobom fizycznym i organizacjom status obserwatora zgodnie z przepisem 8 ust. 3 zasad horyzontalnych dotyczących grup ekspertów, agencji UE i krajów przystępujących.

5. Członkowie grup eksperckich i ich przedstawiciele oraz zaproszeni eksperci i obserwatorzy podlegają wymogom zachowania tajemnicy zawodowej określonym w traktatach i ich przepisach wykonawczych, a także przestrzegają przepisów Komisji dotyczących bezpieczeństwa w zakresie ochrony informacji niejawnych UE, określonych w załączniku do decyzji Komisji 2001/844/WE, EWWiS, Euratom. W przypadku nieprzebrzegania powyższych zobowiązań Komisja może podjąć wszelkie stosowne środki.

6. Jeżeli Komisja uzna, że informacje uzyskane w wyniku uczestnictwa w obradach grupy, grup *ad hoc* lub podgrup dotyczą spraw poufnych, wówczas nie mogą one być ujawniane.

7. Posiedzenia grupy, podgrupy przygotowawczej i grup roboczych odbywają się w siedzibie Komisji. Komisja zapewnia grupie obsługę sekretariatu. W posiedzeniach grupy, podgrupy przygotowawczej i grup roboczych uczestniczyć mogą zainteresowani ich pracami inni urzędnicy Komisji.

8. Grupa przyjmuje swój regulamin wewnętrzny na podstawie standardowego regulaminu przyjętego przez Komisję ⁽¹⁾.

9. Komisja publikuje stosowne informacje na temat działalności grupy w rejestrze lub na specjalnej stronie internetowej dostępnej poprzez link umieszczony w rejestrze. Sprawozdanie końcowe jest publikowane możliwie najszybciej po końcowym spotkaniu grupy.

Artykuł 5

Koszty posiedzeń

1. Osoby uczestniczące w pracach grupy nie otrzymują wynagrodzenia za świadczone usługi.
2. Wydatki na podróże służbowe i koszty utrzymania ponoszone przez osoby uczestniczące w pracach grupy są zwracane przez Komisję zgodnie z przepisami obowiązującymi w Komisji.

3. Zwrot kosztów odbywa się w granicach dostępnych środków przyznanych w ramach rocznej procedury przydziału zasobów.

Artykuł 6

Stosowanie

Niniejszą decyzję stosuje się do dnia 14 października 2012 r.

Sporządzono w Brukseli dnia 14 października 2010 r.

W imieniu Komisji
Antonio TAJANI
Wiceprzewodniczący

⁽¹⁾ Dz.U. L 55/61 z 5.3.2010, s. 61.

V

(Ogłoszenia)

POSTĘPOWANIA ZWIĄZANE Z REALIZACJĄ POLITYKI KONKURENCJI

KOMISJA EUROPEJSKA

Zgłoszenie zamiaru koncentracji
(Sprawa COMP/M.5927 – BASF/Cognis)
(Tekst mający znaczenie dla EOG)
(2010/C 280/09)

1. W dniu 8 października 2010 r., zgodnie z art. 4 rozporządzenia Rady (WE) nr 139/2004 ⁽¹⁾, Komisja otrzymała zgłoszenie planowanej koncentracji, w wyniku której przedsiębiorstwo BASF SE („BASF”, Niemcy) przejmuje w rozumieniu art. 3 ust. 1 lit. b) rozporządzenia w sprawie kontroli łączenia przedsiębiorstw wyłączną kontrolę nad przedsiębiorstwem Cognis GmbH („Cognis”, Niemcy) w drodze zakupu udziałów.
2. Przedmiotem działalności gospodarczej przedsiębiorstw biorących udział w koncentracji jest:
 - w przypadku przedsiębiorstwa BASF: chemikalia, tworzywa sztuczne, środki uszlachetniające, rozwiązania w zakresie rolnictwa oraz w innych specjalistycznych sektorach, działalność w sektorze ropy naftowej i gazu,
 - w przypadku przedsiębiorstwa Cognis: specjalistyczne produkty chemiczne oraz składniki odżywcze.
3. Po wstępnej analizie Komisja uznała, że zgłoszona koncentracja może wchodzić w zakres rozporządzenia WE w sprawie kontroli łączenia przedsiębiorstw. Jednocześnie Komisja zastrzega sobie prawo do podjęcia ostatecznej decyzji w tej kwestii.
4. Komisja zwraca się do zainteresowanych osób trzecich o zgłaszanie ewentualnych uwag na temat planowanej koncentracji.

Komisja musi otrzymać takie uwagi w nieprzekraczalnym terminie dziesięciu dni od daty niniejszej publikacji. Można je przesyłać do Komisji faksem (+32 22964301), pocztą elektroniczną na adres: COMP-MERGER-REGISTRY@ec.europa.eu lub listownie, podając numer referencyjny: COMP/M.5927 – BASF/Cognis, na poniższy adres Dyrekcji Generalnej ds. Konkurencji Komisji Europejskiej:

European Commission
Directorate-General for Competition
Merger Registry
J-70
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

⁽¹⁾ Dz.U. L 24 z 29.1.2004, s. 1 („rozporządzenie WE w sprawie kontroli łączenia przedsiębiorstw”).

Zgłoszenie zamiaru koncentracji**(Sprawa COMP/M.5982 – CVCII/Advance Properties/Huvepharma)****Sprawa, która może kwalifikować się do rozpatrzenia w ramach procedury uproszczonej****(Tekst mający znaczenie dla EOG)**

(2010/C 280/10)

1. W dniu 8 października 2010 r., zgodnie z art. 4 rozporządzenia Rady (WE) nr 139/2004 ⁽¹⁾ i po odesłaniu sprawy zgodnie z art. 4 ust. 5 tego rozporządzenia, Komisja otrzymała zgłoszenie planowanej koncentracji, w wyniku której przedsiębiorstwo Citigroup Venture Capital International Investment G.P. Limited („CVCII”, Jersey), kontrolowane przez przedsiębiorstwo Citigroup, Inc. (Stany Zjednoczone) oraz przedsiębiorstwo Advance Properties OOD („Advance Properties”, Bułgaria) przejmują, w rozumieniu art. 3 ust. 1 lit. b) rozporządzenia w sprawie kontroli łączenia przedsiębiorstw, wspólną kontrolę nad przedsiębiorstwem Huvepharma AD („Huvepharma”, Bułgaria), będącym obecnie pod wyłączną kontrolą przedsiębiorstwa Advance Properties, w drodze zakupu akcji/udziałów.

2. Przedmiotem działalności gospodarczej przedsiębiorstw biorących udział w koncentracji jest:

- w przypadku Citigroup: usługi finansowe, w tym usługi bankowe, brokerskie oraz zarządzanie funduszami *private equity*,
- w przypadku Advance Properties: inwestycje w sektorze farmaceutycznym, nieruchomości, energetycznym oraz w żegludze,
- w przypadku Huvepharma: produkty farmaceutyczne, szczególnie produkty w zakresie zdrowia zwierząt oraz produkty żywieniowe.

3. Po wstępnej analizie Komisja uznała, że zgłoszona koncentracja może wchodzić w zakres rozporządzenia WE w sprawie kontroli łączenia przedsiębiorstw. Jednocześnie Komisja zastrzega sobie prawo do podjęcia ostatecznej decyzji w tej kwestii. Należy zauważyć, iż zgodnie z obwieszczeniem Komisji w sprawie uproszczonej procedury stosowanej do niektórych koncentracji na mocy rozporządzenia WE w sprawie kontroli łączenia przedsiębiorstw ⁽²⁾, sprawa ta może kwalifikować się do rozpatrzenia w ramach procedury określonej w tym obwieszczeniu.

4. Komisja zwraca się do zainteresowanych osób trzecich o zgłaszanie ewentualnych uwag na temat planowanej koncentracji.

Komisja musi otrzymać takie uwagi w nieprzekraczalnym terminie dziesięciu dni od daty niniejszej publikacji. Można je przesyłać do Komisji faksem (+32 22964301), pocztą elektroniczną na adres: COMP-MERGER-REGISTRY@ec.europa.eu lub listownie, podając numer referencyjny: COMP/M.5982 – CVCII/Advance Properties/Huvepharma, na poniższy adres Dyrekcji Generalnej ds. Konkurencji Komisji Europejskiej:

European Commission
Directorate-General for Competition
Merger Registry
J-70
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

⁽¹⁾ Dz.U. L 24 z 29.1.2004, s. 1 („rozporządzenie WE w sprawie kontroli łączenia przedsiębiorstw”).

⁽²⁾ Dz.U. C 56 z 5.3.2005, s. 32 („obwieszczenie Komisji w sprawie uproszczonej procedury”).

Komunikat Ministra Gospodarki Królestwa Niderlandów wydany na podstawie art. 3 ust. 2 dyrektywy 94/22/WE Parlamentu Europejskiego i Rady w sprawie warunków udzielania i korzystania z zezwoleń na poszukiwanie, badanie i produkcję węglowodorów

(2010/C 280/11)

Minister Gospodarki informuje, że złożono wniosek o zezwolenie na poszukiwanie węglowodorów na obszarze oznaczonym jako część segmentu P18 na mapie stanowiącej załącznik 3 do rozporządzenia o górnictwie (Dziennik Urzędowy Królestwa Niderlandów (*Staatscourant*) 2002, nr 245), zwanym dalej segmentem P18b.

Zgodnie z dyrektywą wymienioną w tytule oraz art. 15 ustawy o górnictwie (Dziennik Ustaw (*Staatsblad*) 2002, nr 542) Minister Gospodarki zaprasza niniejszym zainteresowane strony do składania konkurencyjnych wniosków o zezwolenie na poszukiwanie węglowodorów w segmencie P18b szelfu kontynentalnego należącego do Królestwa Niderlandów.

Segment P18b wyznaczają równoleżniki pomiędzy parami punktów A–B i H–I, południki między parami punktów B–C, G–H i A–I, ortodromy pomiędzy parami punktów C–D i E–F, łuk okręgu 1 pomiędzy punktami D i E oraz łuk okręgu 2 pomiędzy punktami F i G.

Współrzędne tych punktów to:

Punkt	°	'	" E	°	'	" N
A	3	40	0,000	52	10	0,000
B	3	47	0,000	52	10	0,000
C	3	47	0,000	52	4	21,072
D	3	47	16,385	52	4	16,801
E	3	51	32,620	52	6	15,485
F	3	51	40,829	52	6	37,449
G	4	0	0,000	52	4	48,172
H	4	0	0,000	52	0	0,000
I	3	40	0,000	52	0	0,000

Środkiem łuku okręgu 1 są współrzędne 3° 54' 0,000" E oraz 52° 1' 30,000" N, a jego promień wynosi 5 mil morskich.

Środkiem łuku okręgu 2 są współrzędne 3° 53' 34,000" E oraz 52° 1' 46,000" N, a jego promień wynosi 5 mil morskich.

Położenie wyżej wymienionych punktów wyrażone jest we współrzędnych geograficznych obliczonych zgodnie z europejskim systemem pozycjonowania.

Powierzchnia segmentu P18b wynosi 313,2 km².

Organem upoważnionym do wydawania zezwoleń jest Minister Gospodarki. Kryteria, warunki i wymagania, o których mowa w art. 5 ust. 1 i 2 oraz art. 6 ust. 2 wyżej wymienionej dyrektywy, określa ustawa o górnictwie (Dziennik Ustaw (*Staatsblad*) 2002, nr 542).

Wnioski można składać przez 13 tygodni od daty opublikowania niniejszego zaproszenia w *Dzienniku Urzędowym Unii Europejskiej*. Wnioski należy przysyłać na adres:

De Minister van Economische Zaken
ter attentie van J. C. De Groot, directeur Energiemarkt
ALP/562
Bezuidenhoutseweg 30
Postbus 20101
2500 EJ Den Haag
NEDERLAND

Wnioski, które wpłyną po upływie powyższego terminu, nie będą rozpatrywane.

Decyzja w sprawie wniosków zostanie podjęta w ciągu 12 miesięcy od upływu wspomnianego terminu.

Dodatkowych informacji udziela pan E.J. Hoppel, pod numerem telefonu +31 703797088.

SPROSTOWANIA

Sprostowanie do publikacji wniosku o uznanie określenia tradycyjnego, o którym mowa w art. 33 rozporządzenia Komisji (WE) nr 607/2009

(Dziennik Urzędowy Unii Europejskiej C 275 z dnia 12 października 2010 r.)

(2010/C 280/12)

Strony 11, 13 i 15, skreśla się wyrażenie „Właściwy organ państwa członkowskiego”.

Sprostowania

2010/C 280/12

Sprostowanie do publikacji wniosku o uznanie określenia tradycyjnego, o którym mowa w art. 33 rozporządzenia Komisji (WE) nr 607/2009 (Dz.U. C 275 z 12.10.2010) 39



CENY PRENUMERATY w 2010 r. (bez VAT, włącznie z normalną opłatą za dostawę przesyłki)

Dziennik Urzędowy UE, serie L i C, wyłącznie wersja papierowa	w 22 językach urzędowych UE	1 100 EUR/rok
Dziennik Urzędowy UE, serie L i C, wersja papierowa + roczne wydanie CD-ROM	w 22 językach urzędowych UE	1 200 EUR/rok
Dziennik Urzędowy UE, seria L, wyłącznie wersja papierowa	w 22 językach urzędowych UE	770 EUR/rok
Dziennik Urzędowy UE, serie L i C, miesięczne wydanie CD-ROM (komplet)	w 22 językach urzędowych UE	400 EUR/rok
Suplement do Dziennika Urzędowego (seria S) – Ogłoszenia o przetargach, CD-ROM dwa razy w tygodniu	wielojęzyczny: w 23 językach urzędowych UE	300 EUR/rok
Dziennik Urzędowy UE, seria C – Konkursy	w językach, których dotyczy konkurs	50 EUR/rok

Prenumerata *Dziennika Urzędowego Unii Europejskiej*, który jest wydawany w językach urzędowych Unii, dostępna jest w 22 wersjach językowych. Dziennik Urzędowy składa się z dwóch serii – L (Legislacja) oraz C (Informacje i zawiadomienia).

Dla każdej wersji językowej jest otwierana osobna prenumerata.

Zgodnie z rozporządzeniem Rady (WE) nr 920/2005, opublikowanym w Dzienniku Urzędowym L 156 z dnia 18 czerwca 2005 r., instytucje Unii Europejskiej nie mają obowiązku sporządzania wszystkich aktów prawnych w języku irlandzkim ani publikowania ich w tym języku. W związku z tym irlandzkie wydania Dziennika Urzędowego sprzedawane są osobno.

Prenumerata Suplementu do Dziennika Urzędowego (seria S – Ogłoszenia o przetargach) obejmuje wszystkie 23 wersje językowe na pojedynczym CD-ROM-ie.

Na żądanie prenumeratorzy *Dziennika Urzędowego Unii Europejskiej* mogą otrzymać różne załączniki do Dziennika Urzędowego. Prenumeratory informowani są o publikacji załączników poprzez zawiadomienia dołączane do *Dziennika Urzędowego Unii Europejskiej*.

Format CD-ROM zostanie w ciągu roku 2010 zastąpiony formatem DVD.

Sprzedaż i prenumerata

Prenumeratę różnych odpłatnych publikacji wydawanych okresowo, na przykład prenumeratę *Dziennika Urzędowego Unii Europejskiej*, można zamówić u naszych dystrybutorów handlowych. Wykaz dystrybutorów handlowych znajduje się na stronie internetowej:

http://publications.europa.eu/others/agents/index_pl.htm

Portal EUR-Lex (<http://eur-lex.europa.eu>) zapewnia bezpośredni i bezpłatny dostęp do prawodawstwa Unii Europejskiej. EUR-Lex umożliwia dostęp do *Dziennika Urzędowego Unii Europejskiej* oraz traktatów, aktów prawnych, orzecznictwa oraz aktów przygotowawczych.

Dodatkowe informacje o Unii Europejskiej znajdują się na stronie: <http://europa.eu>

