



**00350/09/PL
WP 159**

**Opinia 1/2009 w sprawie wniosków zmieniających dyrektywę 2002/58/WE o
prywatności
i łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)**

przyjęta w dniu 10 lutego 2009 r.

Grupa robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określa art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (Sądownictwo Cywilne, Prawa i Obywatelstwo) Dyrekcji Generalnej ds. Sprawiedliwości, Wolności i Bezpieczeństwa Komisji Europejskiej, B-1049 Bruksela, Belgia, Biuro nr LX-46 01/06.

Strona internetowa: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Spis treści

1.	Informacje podstawowe	3
2.	Zgłaszanie przypadków naruszenia ochrony danych osobowych.....	4
2.1.	Spostrzeżenia.....	4
2.2.	Zwolnienia z obowiązku powiadomienia.....	6
3.	Dane o ruchu	7
3.1.	Przetwarzanie danych o ruchu dla celów bezpieczeństwa	7
4.	Adresy IP.....	8
5.	Informacje organów ochrony danych.....	9
6.	Komunikaty niezamówione.....	9
7.	Ustawienia przeglądarki	10
8.	Kroki prawne podejmowane przez osoby fizyczne i prawne.....	11
9.	Inne kwestie.....	11
10.	Wniosek.....	12

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

powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.¹,

uwzględniając art. 29, art. 30 ust. 1 lit. a) i art. 30 ust. 3 tej dyrektywy oraz art. 15 ust. 3 dyrektywy nr 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r.,

uwzględniając art. 255 Traktatu WE i rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji,

uwzględniając swój regulamin wewnętrzny,

PRZYJMUJE NINIEJSZĄ OPINIĘ:

1. INFORMACJE PODSTAWOWE

W dniu 13 listopada 2007 r. Komisja przyjęła wniosek dotyczący dyrektywy („wniosek”) zmieniającej dyrektywę 2002/58/WE (dyrektywę o prywatności i łączności elektronicznej) dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz dyrektywę 2002/21/WE (dyrektywę ramową).

W pierwszym czytaniu w dniu 24 września 2008 r. Parlament Europejski przyjął poprawki do wniosku („poprawki Parlamentu”), do których uwagi Komisji Europejskiej przedstawiono 6 listopada 2008 r. w dokumencie COM(2008) 723 wersja ostateczna („uwagi Komisji”).

Następnie, w dniu 27 listopada 2008 r. Rada Unii Europejskiej osiągnęła porozumienie polityczne („porozumienie Rady”).

Grupa robocza powołana na mocy art. 29 pragnie przedstawić swoje uwagi na temat poprawek Parlamentu, uwag Komisji oraz porozumienia Rady.

Grupa robocza pragnie przypomnieć, że przyjęła już dwie opinie w sprawie wniosków zmieniających unijne ramy prawne w zakresie sieci i usług łączności elektronicznej (opinia 8/2006 przyjęta w dniu 26 września 2006 r.² oraz opinia 2/2008 w dniu 15 maja 2008 r.³).

Mimo że grupa robocza wyraża zadowolenie, że niektóre z jej wcześniejszych zaleceń zostały wzięte pod uwagę, pragnie podkreślić kilka głównych obaw związanych z kwestiami podniesionymi po pierwszym czytaniu w Parlamencie i Radzie; grupa robocza nie powtarza wszystkich uwag przedstawionych we wcześniejszych opiniach, które nie straciły na znaczeniu.

¹ Dziennik Urzędowy nr L 281 z 23.11.1995, s. 31,

http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

² http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_pl.pdf

³ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_pl.pdf

2. ZGŁASZANIE PRZYPADKÓW NARUSZENIA OCHRONY DANYCH OSOBOWYCH

2.1. Spostrzeżenia

Grupa robocza w pełni popiera zaproponowane wzmocnienie art. 4 dyrektywy o prywatności i łączności elektronicznej przez wprowadzenie obowiązku powiadamiania o przypadkach naruszenia bezpieczeństwa przez dostawców publicznie dostępnych usług łączności. Powiadomienia o naruszeniach bezpieczeństwa mogą stać się ważnym narzędziem organów ochrony danych służącym do zwiększenia skoncentrowania i skuteczności w egzekwowaniu obowiązku podejmowania stosownych środków bezpieczeństwa przez dostawców usług.

Zasadniczo grupa robocza zaleca przyjęcie następującego podejścia do kwestii powiadomień o naruszeniach danych osobowych:

- powiadamianie właściwego krajowego organu regulacyjnego w każdym przypadku wystąpienia ryzyka negatywnych skutków⁴ dla prywatności osób fizycznych i ochrony danych;
- ważne jest, aby w przypadkach, gdy naruszenie bezpieczeństwa może doprowadzić do wystąpienia negatywnych skutków⁵ dla prywatności osób fizycznych i ochrony danych, użytkownicy, których to dotyczy, byli o tym niezwłocznie informowani przez dostawców usług, niezależnie od możliwości opublikowania informacji na temat naruszenia przez właściwy krajowy organ regulacyjny oraz zmuszenia dostawcy usług do ujawnienia informacji na temat naruszenia;
- każdy dostawca usług powinien prowadzić rejestr⁶ wszystkich naruszeń bezpieczeństwa danych osobowych.

Grupa robocza zauważyła również, że każda z trzech grup poprawek (Parlamentu, Komisji i Rady) przyjmuje diametralnie inne podejście do kwestii bezpieczeństwa oraz naruszeń bezpieczeństwa danych osobowych, szczególnie pod względem:

- zakresu zobowiązania (który rozszerza się na usługi społeczeństwa informacyjnego w poprawkach Parlamentu, a w uwagach Rady i Komisji ogranicza się do publicznie dostępnych usług łączności elektronicznej); grupa robocza stanowczo popiera rozszerzenie zakresu zobowiązania na usługi społeczeństwa informacyjnego;
- podmiotu uprawnionego do podejmowania decyzji o powiadomieniu osób fizycznych (zdaniem Parlamentu i Komisji jest to właściwy organ, natomiast w opinii Rady – dostawca usług);

⁴ Ryzyko negatywnych skutków należy oceniać przy uwzględnieniu takich elementów, jak dane, których dotyczy naruszenie bezpieczeństwa, ich charakter, skutki naruszenia dla osoby prywatnej, na przykład kradzież tożsamości, straty finansowe, straty gospodarcze lub utrata możliwości zatrudnienia, bądź połączenie wymienionych lub zbliżonych okoliczności. Jakościowe i ilościowe kryteria oceny wpływu negatywnych skutków należy szczegółowo określić w toku procedury komitetowej, pamiętając przy tym, że nie należy zasypywać władz drobnymi sprawami ani wzbudzać niepotrzebnego niepokoju wśród osób prywatnych.

⁵ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_pl.pdf

⁶ Format rejestru powinien być ustandaryzowany, aby właściwy krajowy organ regulacyjny mógł przeprowadzić jego kontrolę.

- rodzajów zgłaszanych naruszeń (wszystkie naruszenia zgodnie z wnioskiem Parlamentu i uwagami Komisji, natomiast wyłącznie poważne naruszenia zgodnie z porozumieniem Rady);
- oraz powiadamianych osób (abonentów lub osób fizycznych w propozycjach Parlamentu i Komisji, lecz tylko abonentów zdaniem Rady).

Zakres powiadomienia: usługi społeczeństwa informacyjnego

Grupa robocza stanowczo popiera poprawki Parlamentu 187/rev i 184. **Rozszerzenie powiadomień o naruszeniach bezpieczeństwa danych osobowych na usługi społeczeństwa informacyjnego jest konieczne ze względu na coraz większą rolę tych usług w codziennym życiu obywateli europejskich** oraz ze względu na rosnącą ilość danych osobowych przetwarzanych w ramach tych usług. Transakcje internetowe, w tym między innymi dostęp do usług bankowych, dane medyczne sektora prywatnego oraz zakupy internetowe to tylko kilka przykładowych usług, które mogą być narażone na naruszenia danych osobowych stwarzające poważne zagrożenie dla znacznej liczby obywateli europejskich. Ograniczenie zakresu tych obowiązków do publicznie dostępnych usług łączności elektronicznej dotyczyłoby jedynie bardzo ograniczonej liczby zainteresowanych stron, a tym samym poważnie ograniczyłoby skuteczność powiadomień o naruszeniach bezpieczeństwa danych osobowych jako środka ochrony osób fizycznych przed takim ryzykiem, jak kradzież tożsamości, straty finansowe, straty gospodarcze lub utrata możliwości zatrudnienia, czy też szkody fizyczne.

Dlatego też grupa robocza głęboko żałuje, że wniosek ten nie uzyskał poparcia Komisji i Rady, a także przypomina, że niektóre przepisy dyrektywy o prywatności i łączności elektronicznej już teraz mają zastosowanie w szerszym zakresie, niż jedynie w odniesieniu do usług łączności elektronicznej⁷.

Odpowiedzialność i kryteria powiadomienia

Za ocenę ryzyka, jakie stwarza naruszenie danych osobowych, powinni odpowiadać odnośni dostawcy usług; zgodnie z zasadami oceny ustanowionymi przez władze, mają oni najlepsze możliwości niezwłocznego ustalenia, czy należy powiadomić osoby, których dotyczą naruszenia. **Niezależnie od obowiązku powiadomienia właściwych krajowych organów regulacyjnych o wszystkich naruszeniach w przypadku ryzyka negatywnych skutków, dostawcy usług powinni ustalić, czy wymagane jest powiadomienie abonentów lub osób fizycznych. Aby zapewnić opinii publicznej dostęp do dokładnych i istotnych informacji, właściwe krajowe organy regulacyjne, jeżeli uznają to za stosowne, mogą zdecydować o podaniu naruszenia do publicznej wiadomości, a także zmusić dostawcę usług do ujawnienia informacji o naruszeniu.**

⁷ Niektóre przepisy dyrektywy o prywatności i łączności elektronicznej, takie jak art. 5 ust. 3 (pliki typu cookie i programy typu spyware) i art. 13 (komunikaty niezamówione) są już teraz przepisami ogólnymi, które stosuje się nie tylko w odniesieniu do usług łączności elektronicznej.

Możliwe rozszerzenie poza wąski zakres publicznie dostępnych usług łączności elektronicznej przewiduje się również w innych sytuacjach, ponieważ Komisja zaproponowała rozszerzenie zakresu stosowania art. 5 ust. 3 tak, aby obejmował przypadki, w których „cookies” i programy typu spyware są przenoszone za pośrednictwem takich mediów, jak płyty CD lub nośniki USB, które nie zaliczają się do publicznie dostępnych usług łączności elektronicznej.

Ponieważ powiadomień dokonuje dostawca usługi, **ważne jest, aby dyrektywa wprowadzała zabezpieczenia przed ukrywaniem naruszeń**, aby ocena naruszenia była przeprowadzana prawidłowo i aby osoby fizyczne były powiadamiane w stosownych przypadkach.

Większość przypadków będzie zgłaszana władzom, tak by były one w stanie nadzorować proces powiadamiania osób fizycznych przez dostawców usług. Format powiadomienia powinien być ujednolicony na szczeblu Unii Europejskiej i powinien zawierać obiektywne, jasne kryteria ułatwiające ocenę wpływu negatywnych skutków spowodowanych naruszeniem bezpieczeństwa. Ponadto właściwy organ regulacyjny powinien zweryfikować poprawność przeprowadzenia oceny naruszenia przez dostawcę usługi oraz ustalić, czy po naruszeniu danych osobowych podjęto odpowiednie środki. **Aby zapobiec ukrywaniu naruszeń, ważne jest, aby dyrektywa nadawała właściwemu krajowemu organowi regulacyjnemu prawo do nakładania sankcji finansowych (kar)⁸ w przypadku niepowiadomienia lub nieprawidłowego powiadomienia osób fizycznych lub krajowego organu regulacyjnego o naruszenia danych osobowych przez dostawcę usług.**

Rodzaje naruszeń zgłaszanych osobom fizycznym: pojęcie negatywnych skutków

Grupa robocza z zadowoleniem przyjmuje wprowadzenie nowej definicji „naruszenia danych osobowych” w art. 2⁹, zaproponowanej w uwagach Komisji¹⁰.

Grupa robocza zauważyła jednak, że w trzech propozycjach użyto różnych sformułowań na określenie w jakich sytuacjach o naruszeniach należy powiadamiać podmioty danych. W związku z powyższym grupa robocza zaleca powiadamianie przedmiotów danych o naruszeniach bezpieczeństwa wówczas, gdy mogą one doprowadzić do negatywnych skutków dla prywatności osób fizycznych i ochrony danych. Przydatne przykłady w tym względzie przedstawiono w motywie 29 porozumienia Rady.

Osoby, które można powiadamiać

Grupa robocza z zadowoleniem przyjęła odniesienia do „abonentów lub osób fizycznych”, „zagrożonych użytkowników ” oraz „właściwego organu krajowego” zawarte w motywie 29 poprawek Parlamentu¹¹. Porozumienie Rady ogranicza powiadomienia do „abonentów”, zgodnie z czym o pewnych naruszeniach danych osobowych opisane w opinii 2/2008 nie zostaną powiadomione osoby, których one dotyczą.

2.2. Zwolnienia z obowiązku powiadomienia

Grupa robocza przyznaje, że powiadomienia o naruszeniach powinny zawierać informacje na temat okoliczności naruszenia, w tym m.in. informacje o tym, czy dane osobowe były zabezpieczone przy pomocy kodowania; informacje te są niezbędne dla właściwego krajowego organu regulacyjnego w przypadku naruszenia, aby mógł on ustalić, jakie ewentualne działania należy podjąć wraz z dostawcą usług.

⁸ Grupa robocza przyjmuje do wiadomości, że przepis taki został zaproponowany przez Parlament, Komisję i Radę w nowym art. 15a ust. 1.

⁹ Zob. uwagi Komisji w sprawie poprawek Parlamentu 187/rev i 184.

¹⁰ Niezależnie od powyższego pojęcie „naruszenia danych osobowych” ma charakter ogólny i nie powinno ograniczać się do danych przetwarzanych w związku ze świadczeniem publicznie dostępnych usług łączności elektronicznej; powinno ono obejmować również co najmniej usługi społeczeństwa informacyjnego.

¹¹ Zob. poprawka 183.

Grupa Robocza sprzeciwia się jednak zwolnieniu z obowiązku powiadamiania¹² w przypadku, gdy dostawcy usług wdrożyli „odpowiednie technologiczne środki ochrony oraz [...] środki te zostały zastosowane do danych, których dotyczyło naruszenie bezpieczeństwa”. Przepis ten znacząco zmniejszyłby jakość i przydatność informacji przekazywanych osobom, których to dotyczy. Osoby, których dotyczy naruszenia bezpieczeństwa danych osobowych mogą podejmować stosowne kroki mające na celu ograniczenie grożącego im ryzyka jedynie wówczas, gdy zostaną o tym odpowiednio powiadomione. Dlatego grupa robocza podkreśla znaczenie formatu powiadomienia oraz oceny ryzyka dla ustalenia, czy osoby fizyczne powinny zostać powiadomione, niezależnie od środków technicznych podjętych w rzeczywistości w celu ochrony ich danych.

3. DANE O RUCHU

3.1. Przetwarzanie danych o ruchu dla celów bezpieczeństwa

W nowym art. 6 ust. 6a Parlament, Rada oraz Komisja proponują utworzenie nowego zwolnienia w dyrektywie o prywatności i łączności elektronicznej, które umożliwiłoby przetwarzanie danych o ruchu dla celów bezpieczeństwa.

Grupa robocza ma świadomość, że „dostawcy usług bezpieczeństwa” stosują zabezpieczenia¹³ (takie jak oprogramowanie antywirusowe lub antyspamowe, zapory sieciowe czy systemy wykrywania intruzów), które mogą wymagać przetwarzania danych o ruchu w celu ochrony danych osobowych użytkowników i zabezpieczenia samej usługi. Niezależnie od powyższego grupa robocza obawia się, że obecne brzmienie może usankcjonować wykorzystanie na szeroką skalę technologii wnikliwej analizy pakietów¹⁴, zarówno w sieci, jak i w urządzeniach przeznaczonych dla użytkowników końcowych, takich jak urządzenia ADSL, mimo że obecne prawodawstwo już teraz szczegółowo określa przypadki, w których dane o ruchu mogą być przetwarzane dla celów bezpieczeństwa.

Istotnie, podstawy prawne dopuszczające przetwarzanie danych o ruchu przez publicznie dostępne usługi łączności elektronicznej oraz przetwarzanie danych osobowych przez administratorów danych zostały określone w art. 6 dyrektywy o prywatności i łączności elektronicznej oraz w art. 7 i 17 dyrektywy o ochronie danych. Dopuszczalny zakres przetwarzania danych osobowych uzasadniony interesami administratora danych został określony szczegółowo w art. 7 lit. f) dyrektywy o ochronie danych; nie może on jednak przeważać nad interesami podmiotów danych w zakresie podstawowych praw i wolności. Artykuł 17 dyrektywy o ochronie danych wymaga także, aby administrator danych „wprowadził odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub dostępem, (...) jak również przed wszelkimi innymi nielegalnymi formami przetwarzania”. Przyjęte środki muszą być również proporcjonalne do ryzyka stwarzanego przez przetwarzanie oraz charakteru danych podlegających ochronie.

Grupa robocza podkreśla również, że zakres poprawki Parlamentu 180 został objaśniony w uwagach Komisji. **Grupa robocza pragnie zaznaczyć, że zapis zaproponowany przez Komisję stanowi ponad wszelką wątpliwość, że przetwarzanie danych o ruchu wchodzi**

¹² Zob. motyw 29 poprawek Parlamentu (poprawka 122) oraz motywy 29 i 32 porozumienia Rady.

¹³ W urządzeniach końcowych użytkowników lub w sieci.

¹⁴ Głęboka inspekcja pakietów (ang. *deep packet inspection*) umożliwia bardzo inwazyjne śledzenie i monitorowanie zachowań użytkowników.

w zakres stosowania dyrektywy o ochronie danych. Dlatego też dostawcy usług bezpieczeństwa zobowiązani są powiadomić krajowe organy ochrony danych zawsze wtedy, gdy to konieczne, a także zapewnić możliwość egzekwowania swoich praw przez osoby fizyczne.

Grupa robocza pragnie również przypomnieć, że dane o ruchu są już przetwarzane dla celów bezpieczeństwa przez państwa członkowskie, w których przyjęto środki specjalne zgodnie z art. 15 ust. 1 dyrektywy o prywatności i łączności elektronicznej, który umożliwia państwom członkowskim przyjęcie środków prawnych znoszących zasadę usunięcia danych o ruchu lub uczynienia ich anonimowymi¹⁵, gdy nie są już potrzebne do celów transmisji komunikatu, aby zapobiec niedozwolonemu wykorzystywaniu systemów łączności elektronicznej.

Z wymienionych powyżej względów **wniosek dotyczący nowego art. 6 ust. 6a nie jest konieczny.**

4. ADRESY IP

Parlament i Komisja proponują wprowadzenie nowego motywu (27a) dotyczącego adresów IP¹⁶.

Grupa robocza z zadowoleniem przyjmuje brzmienie zaproponowane w uwagach Komisji, w zakresie w jakim odwołuje się ono konkretnie do pracy grupy roboczej. Grupa robocza nie popiera jednak propozycji wyraźnego poruszania tej kwestii w dyrektywie.

W tym względzie Grupa Robocza pragnie **ponownie podkreślić swoją wcześniejszą opinię¹⁷, że poza przypadkiem, gdy dostawca usług** „może stwierdzić z całkowitą pewnością, że dane dotyczą użytkowników niemożliwych do zidentyfikowania, musi on ze względów bezpieczeństwa traktować wszystkie informacje związane z adresem IP jako dane osobowe”.

W większości przypadków adresy IP dotyczą osób, które można zidentyfikować. Możliwość zidentyfikowania oznacza, że istnieje możliwość identyfikacji osoby przez dostawcę dostępu do Internetu lub w inny sposób, przy jednoczesnym wykorzystaniu dodatkowych identyfikatorów, takich jak pliki typu cookie lub przy współpracy z usługami internetowymi, w ramach których podmiot danych identyfikuje się jawnie lub niejawnie.

Motyw 26 dyrektywy o ochronie danych wyraźnie stanowi, że w celu ustalenia, czy daną osobę można zidentyfikować, „należy wziąć pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba w celu zidentyfikowania”.

Definicja danych osobowych zawarta w dyrektywie o ochronie danych odnosi się do danych „dotyczących” osoby, a adresy IP są powszechnie stosowane w celu rozróżnienia pomiędzy użytkownikami, którzy powinni zostać traktowani w odmienny sposób, na przykład w kontekście reklamy ukierunkowanej lub tworzenia profilu.

Mimo że grupa robocza jest gotowa wspierać Komisję w pracach nad adresami IP zasugerowanych przez Parlament¹⁸, zgadza się z Komisją, że materialny przepis dyrektywy nie jest najbardziej odpowiednim sposobem poruszania tego problemu, oraz że obowiązek

¹⁵ Ustanowioną w art. 6 ust. 1.

¹⁶ Poprawka Parlamentu 185.

¹⁷ Opinia 4/2007 w sprawie pojęcia danych osobowych oraz Opinia w sprawie kwestii ochrony danych w wyszukiwarkach internetowych.

¹⁸ Poprawki 139 i 186/rev.

składania sprawozdań odnoszący się do „celów nieobjętych niniejszą dyrektywą” nie jest odpowiedni.

5. INFORMACJE ORGANÓW OCHRONY DANYCH.

W pierwszym czytaniu Parlament przyjął poprawkę 136 do art. 15 dyrektywy o prywatności i łączności elektronicznej, która została następnie zmieniona w uwagach Komisji. Zaproponowana zmiana nakładałaby na wszystkich dostawców usług i sieci telekomunikacyjnych oraz na wszystkich dostawców usług społeczeństwa informacyjnego obowiązek zgłaszania właściwemu organowi ochrony danych wszelkich wniosków „otrzymanych zgodnie z ust. 1”¹⁹ oraz obowiązek badania każdego powiadomienia przez dany organ i składania sprawozdania właściwym organom sądowym, jeżeli uzna on, że naruszono odnośne przepisy prawa krajowego.

Wnioskowane zgłaszanie stanowi przydatne uzupełnienie służące większej przejrzystości i kontroli przez organy regulacyjne. Jednak mimo że przepis ten znacząco wzmocniłby potencjał organów ochrony danych w zakresie nadzoru i egzekwowania prawa, przyczyniając się tym samym do lepszego stosowania zgodnego z prawem dostępu do informacji, stanowiłby również obciążenie administracyjne zarówno dla zaangażowanych przedsiębiorstw, jak i organów ochrony danych. W tym względzie grupa robocza odczuwa zaniepokojenie koniecznością monitorowania rosnącej liczby wniosków organów sądowych²⁰ oraz nowymi obowiązkami organów ochrony danych obejmującymi kontrolę każdego postępowania sądowego, które wymagają znacznego wzrostu zasobów finansowych i ludzkich tych organów.

Dlatego też **grupa robocza zgłasza wniosek, aby sprawozdania tego typu składać raz do roku. Mogłyby one zawierać informacje na temat procedur wewnętrznych wykorzystywanych w odpowiedzi na wnioski o dostęp do danych osobowych użytkowników, liczby otrzymanych wniosków, przywołanego uzasadnienia prawnego oraz napotkanych problemów, jeżeli takie wystąpiły.** Bardzo ważne jest również, by obowiązek składania sprawozdań był ujednolicony i opisany szczegółowo na poziomie UE.

6. KOMUNIKATY NIEZAMÓWIONE

Poprawka Parlamentu 131 zawiera wyjaśnienie, że wiadomości multimedialne MMS i podobne technologie są objęte definicją „poczty elektronicznej” w art. 2 lit. h).

Po pierwsze, grupa robocza pragnie zauważyć, że motyw 40 dyrektywy o prywatności i łączności elektronicznej wyjaśnia już, że wiadomości SMS są objęte definicją poczty elektronicznej²¹.

¹⁹ Który opisuje obowiązki w zakresie zatrzymywania danych sformułowane w dyrektywie o zatrzymywaniu danych (2006/24/WE).

²⁰ Wielu operatorów telekomunikacyjnych otrzymuje kilkaset wniosków dziennie.

²¹ Zdefiniowanej w art. 2 lit. h) dyrektywy o prywatności i łączności elektronicznej.

Po drugie, konieczne jest dostosowanie art. 13 ust. 1 do powstających technologii, zgodnie z zasadą określoną w motywie 4²². Aktualne brzmienie art. 13 ust. 1 zakłada, że dana osoba jest już przyłączona do sieci, w której komunikat (na przykład rozmowa telefoniczna lub poczta elektroniczna) jest przekazywany. Nie obejmuje natomiast przypadków, w których namawiano użytkowników do przyłączenia się do sieci służącej jedynie reklamie. Typowym przykładem mogą być aplikacje Bluetooth wykorzystywane w marketingu.

W związku z powyższym grupa robocza z zadowoleniem powitała objaśnienia przedstawione w uwagach Komisji odnośnie do zakresu art. 13 dotyczących głównie użycia słowa „komunikat” oraz nowego motywu odnoszącego się do „podobnych technologii”. Gwarantuje to wymóg uprzedniej zgody w przypadku aplikacji Bluetooth wykorzystywanych w marketingu, tym samym uwzględniając spostrzeżenia grupy roboczej przedstawione w opinii 2/2008 w sprawie „konieczności ochrony użytkowników bezprzewodowych odbiorników medialnych krótkiego zasięgu przed komunikatami niezamówionymi określonymi w art. 13”. Wyraźne odniesienie do technologii Bluetooth można zawrzeć również w motywie 40.

Po trzecie, grupa robocza przywołuje spostrzeżenie przedstawione w opinii 2/2008 dotyczące użycia pojęcia „abonent” w art. 13 i z zadowoleniem przyjmuje brzmienie zaproponowane z porozumieniem Rady.

Wniosek Rady dotyczący zmiany art. 13 ust. 2 przez dodanie wyrażenia „w chwili gromadzenia tych danych kontaktowych” jest bardzo przydatny, ponieważ dostarcza jednoznacznych informacji na temat momentu, w którym użytkownicy mają możliwość sprzeciwienia się wykorzystywaniu ich elektronicznych danych kontaktowych do celów marketingu bezpośredniego.

7. USTAWIENIA PRZEGLĄDARKI

Grupa robocza stanowczo sprzeciwia się przyjęciu przez Parlament poprawki 128, zgodnie z którą domyślne ustawienia przeglądarki stanowiłyby środek wyrażenia uprzedniej zgody. Mimo że poprawka ta została uwzględniona w uwagach Komisji i porozumieniu Rady, grupa robocza pragnie zgłosić swoje uwagi na ten temat.

Poza formalnym problemem związanym z tworzeniem w dyrektywie języka odnoszącego się do specyficznej technologii, grupa robocza jest zaniepokojona zawężeniem definicji zgody i wynikającym z tego brakiem przejrzystości.

Większość przeglądarek wykorzystuje ustawienia domyślne, które nie umożliwiają powiadamiania użytkowników o próbach przechwytywania danych lub dostępu do ich urządzeń końcowych. W związku z powyższym domyślne ustawienia przeglądarek powinny sprzyjać zachowaniu prywatności, nie mogą jednak stanowić środka do pozyskiwania dobrowolnej, konkretnej i świadomej zgody użytkowników wymaganej na mocy art. 2 lit. h) dyrektywy o ochronie danych.

W odniesieniu do plików typu cookie grupa robocza jest zdania, że kontroler plików typu cookie powinien powiadamiać o nich swoich użytkowników w oświadczeniu o ochronie

²² Który stanowi, że dyrektywa o prywatności i łączności elektronicznej „musi zostać dostosowana do rozwoju rynków i technologii w usługach łączności elektronicznej, aby zapewnić równy poziom ochrony danych osobowych i prywatności użytkownikom dostępnych publicznie usług łączności elektronicznej, bez względu na zastosowane technologie”.

prywatności i nie może opierać się na (domyślnych) ustawieniach przeglądarki. Także wybrane brzmienie nie ogranicza się do bieżącej kwestii plików typu cookie, lecz obejmuje również wszelkie nowe technologie, które mogłyby zostać użyte w celu śledzenia zachowań użytkowników korzystających ze swoich przeglądarek.

8. KROKI PRAWNE PODEJMOWANE PRZEZ OSOBY FIZYCZNE I PRAWNE

Grupa robocza popiera wniosek Parlamentu²³ o wprowadzenie w art. 13 ust. 6 możliwości „podjęcia działań prawnych przez każdą osobę fizyczną i prawną w przypadku, jeżeli odczuła negatywne skutki naruszenia przepisów prawa krajowego przyjętych zgodnie z dyrektywą o prywatności i łączności elektronicznej”.

Przepis ten bez wątpienia wzmocni prawa użytkowników i przyczyni się do rozwoju lepszych praktyk w zakresie bezpieczeństwa wśród przedstawicieli branży.

9. INNE KWESTIE

Grupa robocza z zadowoleniem przyjmuje fakt, że:

- ustawodawca ma zamiar karać praktyki polegające na wyludzaniu poufnych informacji osobistych (ang. *phising*)²⁴;
- Komisja i Rada wzięły pod uwagę²⁵ wniosek grupy roboczej o przeprowadzanie z nią konsultacji w toku procedury komitetowej określonej w art. 4 ust. 4;
- że została ona uwzględniona w procesie konsultacji określonym w art. 15a ust. 4;
- że będzie konsultowana w toku przygotowywania sprawozdania ze stosowania zmienionej dyrektywy o prywatności i łączności elektronicznej²⁶;
- że Komisja, Rada i Parlament pragną wyjaśnić, iż dyrektywa o prywatności i łączności elektronicznej znajduje zastosowanie do powstających technologii, takich jak RFID²⁷ czy NFC, które opierają się na bezstykowych urządzeniach identyfikacyjnych wykorzystujących częstotliwości radiowe.

²³ Poprawka nr 133.

²⁴ Zob. poprawka Parlamentu 132.

²⁵ W komentarzu Komisji do poprawki 127 Parlamentu.

²⁶ Zob. poprawki Parlamentu 139 i 186/rev.

²⁷ Artykuł 3 i motyw 28.

10. WNIOSEK

Grupa robocza powołana na mocy art. 29 wzywa prawodawców europejskich do rozważenia przede wszystkim, poza innymi kwestiami naświetlonymi w niniejszej opinii, możliwości rozszerzenia zakresu obowiązku zgłaszania przypadków naruszenia bezpieczeństwa danych osobowych na usługi społeczeństwa informacyjnego, ze względu na ich wpływ na ochronę danych osobowych wszystkich obywateli europejskich.

Sporządzono w Brukseli dnia 10 lutego 2009 r.

W imieniu grupy roboczej
Przewodniczący
Alex TÜRK