

Dziennik Urzędowy C 181

Unii Europejskiej

Tom 51

Wydanie polskie

Informacje i zawiadomienia

18 lipca 2008

Powiadomienie nr

Spis treści

Strona

I *Rezolucje, zalecenia i opinie*

OPINIE

Europejski Inspektor Ochrony Danych

2008/C 181/01

Opinia Europejskiego Inspektora Ochrony Danych 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)

1

II *Informacje*

INFORMACJE INSTYTUCJI I ORGANÓW UNII EUROPEJSKIEJ

Komisja

2008/C 181/02

Zezwolenie na pomoc państwa w ramach przepisów zawartych w art. 87 i 88 Traktatu WE — Przypadki, względem których Komisja nie wnosi sprzeciwu

14

2008/C 181/03

Brak sprzeciwu wobec zgłoszonej koncentracji (Sprawa COMP/M.5162 — Avnet/Horizon) ⁽¹⁾

17

PL

IV *Zawiadomienia*

ZAWIADOMIENIA INSTYTUCJI I ORGANÓW UNII EUROPEJSKIEJ

Komisja

2008/C 181/04	Kursy walutowe euro	18
---------------	---------------------------	----

ZAWIADOMIENIA PAŃSTW CZŁONKOWSKICH

2008/C 181/05	Informacje przekazane przez państwa członkowskie, dotyczące pomocy państwa przyznanej na mocy rozporządzenia Komisji (WE) nr 1628/2006 w sprawie zastosowania art. 87 i 88 Traktatu WE do krajowej regionalnej pomocy inwestycyjnej ⁽¹⁾	19
2008/C 181/06	Informacje przekazane przez państwa członkowskie, dotyczące pomocy państwa przyznanej na mocy rozporządzenia Komisji (WE) nr 70/2001 w sprawie zastosowania art. 87 i 88 Traktatu WE w odniesieniu do pomocy państwa dla małych i średnich przedsiębiorstw ⁽¹⁾	20
2008/C 181/07	Informacje przekazane przez państwa członkowskie, dotyczące pomocy państwa przyznanej na mocy rozporządzenia Komisji (WE) nr 68/2001 w sprawie zastosowania art. 87 i 88 Traktatu WE do pomocy szkoleniowej ⁽¹⁾	22
2008/C 181/08	Informacje przekazane przez państwa członkowskie, dotyczące pomocy państwa przyznanej na mocy rozporządzenia Komisji (WE) nr 1628/2006 w sprawie zastosowania art. 87 i 88 Traktatu WE do krajowej regionalnej pomocy inwestycyjnej ⁽¹⁾	24

V *Ogłoszenia*

PROCEDURY ZWIĄZANE Z REALIZACJĄ WSPÓLNEJ POLITYKI HANDLOWEJ

Komisja

2008/C 181/09	Zawiadomienie o wszczęciu częściowego przeglądu okresowego środków antydumpingowych stosowanych względem przywozu łosia hodowlanego pochodzącego z Norwegii	25
---------------	---	----

PROCEDURY ZWIĄZANE Z REALIZACJĄ POLITYKI KONKURENCJI

Komisja

2008/C 181/10	Upřednie zgłoszenie koncentracji (Sprawa COMP/M.5231 — Bain Capital/D&M) — Sprawa kwalifikująca się do rozpatrzenia w ramach procedury uproszczonej ⁽¹⁾	28
---------------	--	----

⁽¹⁾ Tekst mający znaczenie dla EOG

(Ciąg dalszy na wewnętrznej tylnej stronie okładki)

<u>Powiadomienie nr</u>	Spis treści (ciąg dalszy)	Strona
2008/C 181/11	Zgłoszenie zamiaru koncentracji (Sprawa COMP/M.5227 — Robert Bosch/Samsung/JV) ⁽¹⁾	29
2008/C 181/12	Zgłoszenie zamiaru koncentracji (Sprawa COMP/M.5267 — Sun Capital/SCS Group) — Sprawa, która może kwalifikować się do rozpatrzenia w ramach procedury uproszczonej ⁽¹⁾	30

Sprostowania

2008/C 181/13	Sprostowanie do zaproszenia do składania wniosków dotyczących instrumentu LIFE+ na 2008 r. (<i>Dz.U. C 178 z 15.7.2008</i>)	31
---------------	---	----



⁽¹⁾ Tekst mający znaczenie dla EOG

I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych 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)

(2008/C 181/01)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

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

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

uwzględniając dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych ⁽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, w szczególności jego art. 41 ⁽³⁾,

uwzględniając wniosek o wydanie opinii zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001, otrzymany od Komisji Europejskiej w dniu 16 listopada 2007 r.,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. WPROWADZENIE

1. W dniu 13 listopada 2007 r. Komisja przyjęła wniosek dotyczący dyrektywy zmieniającej, m.in. dyrektywę 2002/58/WE dotyczącą przetwarzania danych i ochrony prywatności w sektorze łączności elektronicznej (dalej zwany „wnioskiem” lub „proponowanymi zmianami”). Obowiązująca wersja dyrektywy 2002/58/WE jest zwykle, również w niniejszej opinii, zwana dyrektywą o prywatności i łączności elektronicznej.

⁽¹⁾ Dz.U. L 281 z 23.11.1995, str. 31.

⁽²⁾ Dz.U. L 201 z 31.7.2002, str. 37.

⁽³⁾ Dz.U. L 8 z 12.1.2001, str. 1.

2. Wniosek ma na celu poprawienie ochrony prywatności osób fizycznych i ich danych osobowych w sektorze łączności elektronicznej. Dokonuje się tego nie poprzez nadanie zupełnie nowego kształtu obowiązującej dyrektywie o prywatności i łączności elektronicznej, lecz przez zaproponowanie doraźnych zmian, które służą przede wszystkim wzmocnieniu przepisów dotyczących bezpieczeństwa i poprawieniu mechanizmów ich egzekwowania.
3. Wniosek jest częścią szerszej zakrojonej reformy pięciu unijnych dyrektyw telekomunikacyjnych („pakietu telekomunikacyjnego”). Oprócz wniosków dotyczących przeglądu „pakietu telekomunikacyjnego” ⁽¹⁾ Komisja przyjęła również w tym samym czasie wniosek dotyczący rozporządzenia ustanawiającego Europejski Urząd ds. Rynku Łączności Elektronicznej ⁽²⁾.
4. Uwagi zawarte w niniejszej opinii ograniczają się do proponowanych zmian do dyrektywy o prywatności i łączności elektronicznej, chyba że takie proponowane zmiany odwołują się do pojęć lub przepisów zawartych we wnioskach dotyczących przeglądu pakietu telekomunikacyjnego. Niektóre z uwag zawartych w niniejszej opinii odnoszą się ponadto do przepisów dyrektywy o prywatności i łączności elektronicznej, które w myśl wniosku nie zostaną zmienione.
5. W niniejszej opinii poruszane są następujące kwestie: (i) zakres zastosowania dyrektywy o prywatności i łączności elektronicznej, w szczególności, usługi, których ma ona dotyczyć (proponowana zmiana do art. 3 ust. 1); (ii) powiadamianie o przypadkach naruszenia bezpieczeństwa (proponowana zmiana wprowadzająca art. 4 ust. 3 i ust. 4); (iii) przepisy dotyczące plików *cookie*, oprogramowania szpiegującego i podobnych urządzeń (proponowana zmiana w art. 5 ust. 3); (iv) występowanie na drogę sądową przez dostawców usług łączności elektronicznej i inne osoby prawne (proponowana zmiana wprowadzająca art. 13 ust. 6) oraz (v) usprawnienie egzekwowania przepisów (proponowana zmiana wprowadzająca art. 15a).

Zasięgnięcie opinii EIOD-a i szersze konsultacje publiczne

6. Komisja przesłała EIOD-owi wniosek w dniu 16 listopada 2007 r. EIOD sądzi, że przekazanie tego wniosku oznacza prośbę o doradzenie wspólnotowym instytucjom i organom, zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (zwanego dalej „rozporządzeniem (WE) nr 45/2001”).
7. Przed przyjęciem wniosku Komisja nieformalnie zwróciła się do EIOD-a o wydanie opinii na temat projektu wniosku; EIOD przychylnie odniósł się do tego działania, ponieważ dało mu to sposobność poczynienia pewnych sugestii dotyczących projektu wniosku, zanim został on przyjęty przez Komisję. EIOD cieszy się, że niektóre z tych sugestii zostały uwzględnione we wniosku.
8. Przyjęcie wniosku poprzedziły szeroko zakrojone konsultacje publiczne, praktyka ceniona przez EIOD-a. W czerwcu 2006 roku Komisja zapoczątkowała konsultacje publiczne w sprawie swojego komunikatu dotyczącego przeglądu pakietu telekomunikacyjnego, w którym Komisja przedstawiła swój pogląd na sytuację i przedstawiła propozycje zmian ⁽³⁾. Grupa Robocza ds. Ochrony Danych powołana na mocy art. 29 („GR 29”), której członkiem jest EIOD, skorzystała z tej sposobności, by w opinii przyjętej w dniu 26 września 2006 r. ⁽⁴⁾ wyrazić swoje poglądy na temat proponowanych zmian.

⁽¹⁾ Proponowane zmiany do dyrektyw telekomunikacyjnych są przedstawione w następujących wnioskach: (i) wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywy: 2002/21/WE w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej, 2002/19/WE w sprawie dostępu do sieci łączności elektronicznej oraz wzajemnych połączeń i 2002/20/WE w sprawie zezwoleń na udostępnienie sieci i usług łączności elektronicznej, 13 listopada 2007 r., COM(2007) 697 wersja ostateczna; (ii) wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników oraz dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy w dziedzinie ochrony konsumentów, 13 listopada 2007 r., COM(2007) 698 wersja ostateczna.

⁽²⁾ Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego Europejski Urząd ds. Rynku Łączności Elektronicznej, 13 listopada 2007 r., COM(2007) 699 wersja ostateczna.

⁽³⁾ Komunikat w sprawie ram regulacyjnych UE dotyczących sieci i usług łączności elektronicznej (SEC(2006) 816) przyjęty w dniu 29 czerwca 2006 r. Komunikatowi towarzyszył dokument roboczy służb Komisji — (COM(2006) 334 wersja ostateczna).

⁽⁴⁾ Opinia 8/2006 na temat przeglądu ram regulacyjnych dla łączności i usług elektronicznych, z naciskiem na dyrektywę o prywatności i łączności elektronicznej, przyjęta w dniu 26 września 2006 r.

Ogólna opinia EIOD-a

9. Ogólnie rzecz biorąc, EIOD pozytywnie postrzega wniosek. W pełni popiera cele, do osiągnięcia których dążyła Komisja, przyjmując wniosek zwiększający ochronę prywatności osób fizycznych i danych osobowych w sektorze łączności elektronicznej. Szczególne zadowolenie EIOD-a wzbudza propozycja istnienia systemu obowiązkowego powiadamiania o przypadkach naruszenia bezpieczeństwa (zmiana do art. 4 dyrektywy o prywatności i łączności elektronicznej, wprowadzająca ust. 3 i 4). Gdy dochodzi do naruszenia bezpieczeństwa danych, powiadamianie o tym fakcie wiąże się z wyraźnymi korzyściami, wzmacnia odpowiedzialność organizacji, sprawia, że firmy wdrażają rygorystyczne środki bezpieczeństwa i umożliwia stwierdzenie, przy użyciu jakich technologii najlepiej można chronić informacje. Poza tym daje poszkodowanym osobom fizycznym możliwość podjęcia kroków, które pozwolą im uchronić się przed kradzieżą tożsamości lub innym niezgodnym z prawem wykorzystaniem dotyczących ich informacji osobowych.
10. EIOD z zadowoleniem odnosi się do innych zmian zaproponowanych we wniosku, np. zadbania o to, by każda osoba prawna mająca uzasadniony interes mogła wystąpić na drogę sądową przeciwko osobom, które naruszają niektóre z przepisów dyrektywy o prywatności i łączności elektronicznej (zmiana do art. 13, wprowadzająca ust. 6). Pozytywnie należy również postrzegać wzmocnienie uprawnień do prowadzenia dochodzeń, którymi dysponują krajowe organy regulacyjne, ponieważ umożliwi im to ocenę, czy dany przypadek przetwarzania danych ma miejsce zgodnie z prawem, i pozwoli wskazać naruszenia (dodany art. 15a ust. 3). Posiadanie przez nie uprawnień do jak najszybszego powstrzymania niezgodnego z prawem przetwarzania danych osobowych i naruszeń prywatności, jest konieczne, by chronić prawa i swobody osób fizycznych. Z tego względu z dużym zadowoleniem przyjmuje się proponowany art. 15a ust. 2, który uznaje uprawnienia krajowych organów regulacyjnych do doprowadzenia do zaprzestania naruszeń, ponieważ umożliwi im on natychmiastowe powstrzymanie poważnych przypadków niezgodnego z prawem przetwarzania danych.
11. Podejście, którego wyrazem jest wniosek i większość proponowanych w nim zmian, jest zgodne z poglądami na temat planowanej polityki w zakresie ochrony danych, które przedstawione zostały we wcześniejszych opiniach EIOD-a, takich jak opinia w sprawie wdrażania dyrektywy o ochronie danych⁽¹⁾. Podejście opiera się m.in. na poglądzie, że choć nie są konieczne żadne nowe zasady ochrony danych, potrzeba bardziej precyzyjnych przepisów, by zaradzić problemom związanym z ochroną danych, które powstały wskutek pojawienia się nowych technologii, takich jak Internet, identyfikacja radiowa itp., a także narzędzi, które pomagają egzekwować i uczynić skutecznym ustawodawstwo w zakresie ochrony danych, takie jak narzędzie umożliwiające podmiotom prawnym wszczynanie działań, gdy nastąpiło naruszenie ochrony danych, lub zobowiązujące kontrolerów danych do powiadamiania o przypadkach naruszenia bezpieczeństwa.
12. Ogólnie rzecz biorąc, wniosek ma pozytywny wydźwięk, EIOD wyraża jednak żal, że nie idzie on tak daleko, jak byłoby to możliwe. Już bowiem od 2003 roku ze stosowania przepisów zawartych w dyrektywie o prywatności i łączności elektronicznej, a także z uważnej analizy przedmiotu możliwe było wysnucie wniosku, że niektórym z jej przepisów daleko do bycia klarownymi, co powoduje niepewność prawną i problemy z ich przestrzeganiem. Tak jest np. jeśli chodzi o stopień, w jakim wspomniana dyrektywa dotyczy półpublicznych dostawców usług łączności. Można było mieć nadzieję, że Komisja wykorzysta przegląd pakietu telekomunikacyjnego, a w szczególności przegląd dyrektywy o prywatności i łączności elektronicznej, by rozwiązać niektóre z tych wciąż istniejących problemów. Poza tym zajmując się nowymi kwestiami, jak choćby ustanowieniem systemu obowiązkowego powiadamiania o naruszeniach bezpieczeństwa, wniosek proponuje tylko częściowe rozwiązanie, gdyż w zakres organizacji zobowiązanych do powiadamiania o przypadkach naruszeń bezpieczeństwa nie zostały włączone podmioty, które przetwarzają wyjątkowo sensytywne dane, takie jak banki internetowe czy podmioty świadczące elektroniczne usługi opieki zdrowotnej. EIOD z żalem przyjmuje takie podejście.
13. EIOD wyraża nadzieję, że w procesie legislacyjnym prawodawca uwzględni uwagi i propozycje zawarte w niniejszej opinii, tak by zaradzić problemom, którymi nie zajmuje się wniosek Komisji.

⁽¹⁾ Opinia Europejskiego Inspektora Ochrony Danych 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, str. 1).

II. ANALIZA WNIOSKU

II.1. Zakres zastosowania dyrektywy o prywatności i łączności elektronicznej, w szczególności usługi, które są nim objęte

14. Zasadniczym zagadnieniem, jeśli chodzi o obecną dyrektywę o prywatności i łączności elektronicznej, jest zakres jej zastosowania. Wniosek zawiera pewne konstruktywne elementy pomocne w zdefiniowaniu i wyjaśnieniu zakresu dyrektywy, w szczególności w odniesieniu do usług nią objętych, które omówiono poniżej w części (i). Niestety, proponowane zmiany nie rozwiązują wszystkich istniejących problemów. Jak wspomniano w części (ii) poniżej, zmiany niestety nie mają na celu poszerzenia zakresu zastosowania dyrektywy na usługi łączności elektronicznej w sieciach prywatnych.
15. W art. 3 dyrektywy o prywatności i łączności elektronicznej podano opis usług, których ona dotyczy, innymi słowy usług, do których zastosowanie mają wymogi przedstawione w dyrektywie: „niniejszą dyrektywę stosuje się do przetwarzania danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności”.
16. Zatem dyrektywę tę stosuje się do usług świadczonych przez dostawców publicznie dostępnych usług łączności elektronicznej w sieciach publicznych (ang. „PPECS”). Definicja usługi PPECS podana została w art. 2 lit. c) dyrektywy ramowej ⁽¹⁾. Definicję publicznych sieci łączności podano w art. 2 lit. d) tej dyrektywy ramowej ⁽²⁾. Przykładami działań w ramach usługi PPECS są: dostarczanie dostępu do Internetu, przesyłanie informacji poprzez sieci elektroniczne, połączenia telefonii mobilnej i stacjonarnej itp.
- (i) *Proponowana zmiana w art. 3 dyrektywy o prywatności i łączności elektronicznej: „Usługi wchodzące w zakres zastosowania dyrektywy mają obejmować sieci łączności służące do zbierania danych i obsługi urządzeń identyfikacyjnych”*
17. Wniosek wprowadza zmianę w art. 3 dyrektywy o prywatności i łączności elektronicznej i precyzuje, że publiczne sieci łączności obejmują „publiczne sieci łączności służące do zbierania danych i obsługi urządzeń identyfikacyjnych”. W motywie 28 wyjaśniono, że rozwój urządzeń do zbierania informacji, w tym danych osobowych, wykorzystujących częstotliwości radiowe, w tym urządzeń do identyfikacji radiowej (RFID), musi podlegać dyrektywie o prywatności i łączności elektronicznej, jeśli urządzenia te są podłączone do publicznych sieci łączności elektronicznej lub korzystają z publicznie dostępnych usług łączności elektronicznej.
18. EIOD pozytywnie ocenia ten przepis, ponieważ wyjaśniono w nim, że pewne zastosowania urządzeń RFID wchodzą w zakres zastosowania dyrektywy o prywatności i łączności elektronicznej, a tym samym rozwiano pewne wątpliwości co do tej kwestii i ostatecznie usunięto przyczynę niewłaściwego rozumienia lub nieprawidłowej wykładni przepisów prawa.
19. Na mocy art. 3 dyrektywy o prywatności i łączności elektronicznej, w jego obecnym brzmieniu, pewne zastosowania urządzeń RFID są już objęte zakresem tej dyrektywy. Dzieje się tak z wielu łączących się ze sobą przyczyn. Po pierwsze, ponieważ stosowanie urządzeń RFID wchodzi w zakres definicji usług łączności elektronicznej. Po drugie, ponieważ odbywa się ono przy użyciu sieci łączności elektronicznej, jako że działanie tych urządzeń opiera się na systemie transmisji, który bezprzewodowo

⁽¹⁾ Dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (Dz.U. L 108 z 24.4.2002, str. 33). Ta dyrektywa ramowa określa, co należy rozumieć pod pojęciem usługi łączności elektronicznej, a mianowicie: (i) usługa łączności elektronicznej to usługa zwykle świadczona odpłatnie, która polega na przekazywaniu sygnałów w sieciach i obejmuje usługi telekomunikacyjne i usługi transmisyjne świadczone poprzez sieci; (ii) z definicji usług łączności elektronicznej wyłączone są usługi związane z zapewnianiem albo wykonywaniem kontroli treści przekazywanych przy wykorzystaniu sieci lub usług łączności elektronicznej; (iii) świadczenie usług oznacza ustanowienie, obsługę, kontrolowanie i udostępnianie sieci; (iv) usługi łączności elektronicznej nie obejmują usług społeczeństwa informacyjnego, za które w dyrektywie o handlu elektronicznym uznaje się usługi zwykle świadczone odpłatnie, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług.

⁽²⁾ „Publiczna sieć łączności” oznacza sieć łączności elektronicznej wykorzystywaną całkowicie lub częściowo do świadczenia publicznie dostępnych usług łączności elektronicznej.

przekazuje sygnały. I wreszcie, sieć ta może być zarówno publiczna, jak i prywatna. Jeśli jest publiczna, stosowanie urządzeń RFID zostanie uznane za „usługi, których dyrektywa dotyczy”, i tym samym wejdzie w zakres zastosowania dyrektywy o prywatności i łączności elektronicznej. Jednak proponowana zmiana usunie utrzymujące się wątpliwości co do tej kwestii i zagwarantuje większą pewność prawną.

20. Oczywiście, jak już wspomniano we wcześniejszej opinii EIOD-a na temat urządzeń RFID ⁽¹⁾, przepis ten nie wyklucza, że konieczne będzie wprowadzenie dodatkowych aktów prawnych w odniesieniu do tych urządzeń. Takie jednak środki należy przyjąć przy innej okazji, nie jako część omawianego wniosku.

(ii) *Potrzeba uwzględnienia usług łączności elektronicznej w sieciach prywatnych lub półprywatnych*

21. EIOD cieszy się z wyjaśnienia kwestii przedstawionej powyżej, żałuje jednak, że we wniosku nie zajęto się kwestią coraz mniej wyraźnej granicy między sieciami prywatnymi i publicznymi. EIOD wyraża też żal, że nie poszerzono zakresu definicji usług objętych dyrektywą o prywatności i łączności elektronicznej, by dotyczyła ona również prywatnych sieci. W swoim obecnym brzmieniu art. 3 ust. 1 dyrektywy o prywatności i łączności elektronicznej dotyczy wyłącznie *usług łączności elektronicznej w publicznych sieciach łączności*.
22. EIOD zauważa tendencję, że usługi coraz częściej stają się kombinacją usług prywatnych i publicznych. Weźmy choćby uniwersytety, które umożliwiają tysiącom swoich studentów korzystanie z Internetu i poczty elektronicznej. Oczywiście jest, że te półpubliczne (lub półprywatne) sieci mają możliwość naruszenia prywatności osób fizycznych, i dlatego tego typu usługi także powinny podlegać tym samym przepisom, które stosuje się do wyłącznie publicznych sieci. Ponadto prywatne sieci, jak sieci pracodawców umożliwiających pracownikom dostęp do Internetu, sieci hoteli i właścicieli mieszkań, których goście mogą korzystać z telefonu i poczty elektronicznej, a także sieci wykorzystywane przez kafejki internetowe mają wpływ na ochronę danych i prywatności ich użytkowników, z czego wynika, że również powinny zostać objęte zakresem zastosowania dyrektywy o prywatności i łączności elektronicznej.
23. W rzeczywistości w niektórych państwach członkowskich zapadały już orzeczenia stwierdzające, że usługi łączności elektronicznej świadczone w sieciach prywatnych podlegają tym samym wymogom co usługi w sieciach publicznych ⁽²⁾. Na mocy niemieckich przepisów organy ochrony danych uznały również, że umożliwianie pracownikom korzystania z prywatnego konta poczty elektronicznej w danym przedsiębiorstwie może spowodować, że przedsiębiorstwo to zostanie uznane za operatora publicznych usług telekomunikacyjnych, a zatem wejdzie w zakres przepisów dyrektywy o prywatności i łączności elektronicznej.
24. W skrócie — rosnące znaczenie mieszanych (prywatno-publicznych) i prywatnych sieci w codziennym życiu, a co za tym idzie rosnące zagrożenie dla danych osobowych i prywatności, uzasadnia potrzebę stosowania do takich usług tych samych zasad, które obowiązują publiczne usługi łączności elektronicznej. Z tego względu EIOD uważa, że dyrektywę należy zmienić tak, by zakresem jej zastosowania zostały objęte tego typu usługi prywatne; pogląd ten podziela grupa robocza ⁽³⁾.

II.2. Powiadamianie o przypadkach naruszenia bezpieczeństwa: zmiana do art. 4

25. Artykuł 4 dyrektywy o prywatności i łączności elektronicznej zmieniono, dodając dwa nowe ustępy (3 i 4), które wprowadzają obowiązek powiadamiania o przypadkach naruszenia bezpieczeństwa. Zgodnie z art. 4 ust. 3 dostawcy publicznie dostępnych usług łączności elektronicznej w sieciach publicznych są zobowiązani z jednej strony bez zbędnej zwłoki powiadamiać krajowe organy regulacyjne o każdym przypadku naruszenia bezpieczeństwa, które prowadzi do przypadkowego lub bezprawnego zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia lub dostępu do danych osobowych przekazywanych, przechowywanych lub przetwarzanych w inny sposób w związku ze świadczeniem publicznie dostępnych usług łączności (które to naruszenie jest ogólnie nazywane „narażeniem danych”); z drugiej strony dostawcy ci mają również obowiązek powiadomić swoich abonentów.

⁽¹⁾ Opinia Europejskiego Inspektora Ochrony Danych 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.

⁽²⁾ Na przykład w wyroku paryskiego Sądu Apelacyjnego, który zapadł 4 lutego 2005 r. w sprawie *BNP Paribas* przeciwko *World Press Online*, stwierdza się, że nie ma różnicy między dostawcami usługi internetowej, którzy komercyjnie oferują dostęp do Internetu, a pracodawcami, którzy umożliwiają dostęp do Internetu swojemu personelowi.

⁽³⁾ Opinia 8/2006 na temat przeglądu ram regulacyjnych dla łączności i usług elektronicznych, z naciskiem na dyrektywę o prywatności i łączności elektronicznej, przyjęta w dniu 26 września 2006 r.

Korzyści płynące z wprowadzenia takiego obowiązku

26. EIOD z zadowoleniem przyjmuje przepisy art. 4 ust. 3 i 4, które wprowadzają obowiązek powiadamiania o przypadkach naruszenia bezpieczeństwa. Powiadamianie o takich przypadkach ma pozytywne skutki, jeśli chodzi o ochronę danych osobowych i prywatności, co już przetestowano w Stanach Zjednoczonych, gdzie przepisy dotyczące powiadamiania o przypadkach naruszenia obowiązują już od wielu lat na poziomie poszczególnych stanów.
27. Po pierwsze, przepisy dotyczące powiadamiania o przypadkach naruszeń wpływają na zwiększenie odpowiedzialności dostawców PPECS za informacje, które zostały narażone. Na mocy regulacji dotyczących ochrony danych lub prywatności odpowiedzialność oznacza, że każda organizacja jest odpowiedzialna za informacje, które znajdują się pod jej opieką i kontrolą. Obowiązek powiadamiania jest równoznaczny z ponownym stwierdzeniem, że z jednej strony dane, które zostały narażone, były pod kontrolą danego dostawcy PPECS, a z drugiej strony że na organizacji tej ciąży odpowiedzialność za przedsięwzięcie niezbędnych działań w stosunku do takich danych.
28. Po drugie, istnienie obowiązku powiadamiania o naruszeniu bezpieczeństwa okazało się czynnikiem, który prowadzi do inwestycji w systemy bezpieczeństwa podejmowanych przez organizacje, które przetwarzają dane osobowe. Już sam wymóg publicznego powiadamiania o przypadkach naruszenia bezpieczeństwa powoduje, że organizacje stosują bardziej rygorystyczne normy bezpieczeństwa, służące ochronie informacji osobowych i zapobieganiu naruszeniom. Ponadto powiadamianie o przypadkach naruszenia bezpieczeństwa pomoże zidentyfikować i przeprowadzić wiarygodną analizę statystyczną dotyczącą najskuteczniejszych rozwiązań i mechanizmów w zakresie bezpieczeństwa. Przez długi czas brakowało twardych danych na temat przypadków niedostatecznego zabezpieczania danych i najstosowniejszych technologii służących ochronie informacji. Problem ten ma szansę zostać rozwiązany dzięki nałożeniu obowiązków w zakresie powiadamiania o przypadkach naruszenia bezpieczeństwa, jak to miało miejsce w przypadku amerykańskich ustaw o zgłaszaniu naruszeń bezpieczeństwa, ponieważ powiadamianie sprawi, że wiadomym stanie się, które technologie obciążone są większym ryzykiem naruszenia bezpieczeństwa danych ⁽¹⁾.
29. Poza tym powiadamianie o przypadkach naruszenia bezpieczeństwa sprawia, że osoby fizyczne są świadome ryzyka, gdy narażone zostały ich dane osobowe, i pomaga im podjąć konieczne działania, by ograniczyć takie ryzyko. Na przykład jeśli narażone zostały dane bankowe, osoba fizyczna, która została o tym poinformowana, może podjąć decyzję o zmianie danych odnoszących się do jej konta bankowego, by zapobiec przejęciu tych informacji i wykorzystaniu ich do celów niezgodnych z prawem (zwykle określanym mianem „kradzieży tożsamości”). Podsumowując — obowiązek ten zmniejsza prawdopodobieństwo, że dana osoba padnie ofiarą kradzieży tożsamości i może pomóc ofiarom w podjęciu działań niezbędnych do rozwiązywania problemów.

Niedostatki proponowanej zmiany

30. EIOD cieszy się, że w art. 4 ust. 3 i 4 wprowadza się system powiadamiania o przypadkach naruszenia bezpieczeństwa, opowiadałby się jednak za objęciem tymi przepisami także dostawców usług społeczeństwa informacyjnego. Oznaczałoby to, że banki internetowe, firmy internetowe i podmioty świadczące elektroniczne usługi opieki zdrowotnej zostałyby także objęte tym prawem ⁽²⁾.
31. Powody, dla których uzasadnione jest nałożenie na dostawców publicznie dostępnych usług łączności elektronicznej w sieciach publicznych wymogu powiadamiania o przypadkach naruszenia bezpieczeństwa, są prawdziwe również w przypadku innych organizacji, także przetwarzających masowe ilości danych osobowych, których ujawnienie byłoby dla podmiotów tych danych wyjątkowo szkodliwe. Dotyczy to banków internetowych, brokerów danych i innych dostawców internetowych, którzy przetwarzają dane sensytywne (w tym dane o zdrowiu, poglądach politycznych itd.). Narażenie informacji przechowywanych przez banki i przedsiębiorstwa internetowe, wśród których mogą być nie tylko numery kont bankowych, ale również dane karty kredytowej, może doprowadzić do kradzieży tożsamości, w którym to przypadku sprawą zasadniczą jest, by dane osoby były tego świadome i mogły podjąć niezbędne działania. W tym ostatnim przypadku (elektroniczne usługi zdrowotne), jeśli narażone zostaną informacje sensytywne, to nawet o ile dana osoba nie ucierpi finansowo, może doznać szkody pozaekonomicznej.

⁽¹⁾ Zob. sprawozdanie pt. „Security Economics and the Internal Market”, którego sporządzenie zleciła prof. Rossowi Andersonowi, Rainerowi Böhme, Richardowi Claytonowi i Tylerowi Moore Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA). Sprawozdanie jest dostępne pod adresem http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

⁽²⁾ Za usługi społeczeństwa informacyjnego w dyrektywie o handlu elektronicznym uznaje się usługi zwykle świadczone odpłatnie, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług.

32. Ponadto wymienione powyżej korzyści, których oczekuje się w związku z wprowadzeniem tego obowiązku, dzięki poszerzeniu jego zakresu nie będą się ograniczać tylko do jednego sektora działalności, czyli dostawców publicznie dostępnych usług łączności elektronicznej, ale obejmą ogół usług społeczeństwa informacyjnego. Nałożenie bowiem na usługi społeczeństwa informacyjnego, takie jak banki internetowe, obowiązku powiadamiania o przypadkach naruszenia bezpieczeństwa nie tylko zwiększy odpowiedzialność tych podmiotów, ale również zmotywuje je do wzmocnienia stosowanych środków bezpieczeństwa, a tym samym umożliwi im uniknięcie potencjalnych naruszeń bezpieczeństwa.
33. Istnieją inne precedensy, gdy dyrektywa o prywatności i łączności elektronicznej ma zastosowanie także do podmiotów innych niż dostawcy PPECS, jak choćby w przypadku art. 5 dotyczącego poufności komunikacji i art. 13 dotyczącego komunikatów niezamówionych (spam). Potwierdza to, że w przeszłości prawodawca podjął bardzo mądrą decyzję, by poszerzyć zakres zastosowania pewnych przepisów dyrektywy o prywatności i łączności elektronicznej, ponieważ uznał, że jest to celowe i konieczne. EIOD wyraża nadzieję, że w chwili obecnej prawodawca nie zawaha się przyjąć podobne, rozsądne i elastyczne podejście i rozszerzy zakres zastosowania art. 4 na dostawców usług społeczeństwa informacyjnego. W tym celu wystarczyłoby dodać do art. 4 ust. 3 wzmiankę o dostawcach usług społeczeństwa informacyjnego w brzmieniu: „W przypadku naruszenia bezpieczeństwa, prowadzącego do przypadkowego lub ... dostawca publicznie dostępnych usług łączności i dostawca usług społeczeństwa informacyjnego ... powiadamiają o takim naruszeniu zainteresowanego abonenta i krajowy organ regulacyjny”.
34. EIOD uważa wprowadzenie tego obowiązku i jego przestrzeganie zarówno przez dostawców PPECS, jak i dostawców usług społeczeństwa informacyjnego za pierwszy etap zmian, które ostatecznie można by stosować ogółem do wszystkich kontrolerów danych.

Konkretne ramy prawne dotyczące naruszeń bezpieczeństwa, którymi należy zająć się w procedurze komitetowej

35. Wniosek nie porusza pewnych kwestii związanych z obowiązkiem powiadamiania o przypadkach naruszenia bezpieczeństwa. Takimi kwestiami, którymi należy się zająć, są np. okoliczności powiadomienia, jego forma i stosowane procedury. Zamiast tego w art. 4 ust. 4 pozostawia się podejmowanie takich decyzji komitetowi działającemu w myśl procedury komitetowej⁽¹⁾, a mianowicie Komitetowi ds. łączności ustanowionemu w art. 22 dyrektywy ramowej, zgodnie z decyzją Rady z dnia 28 czerwca 1999 r. Dokładniej rzecz biorąc, środki takie byłyby przyjmowane zgodnie z art. 5 decyzji Rady z dnia 28 czerwca 1999 r., która ustanawia zasady procedury regulacyjnej w odniesieniu do „środków o ogólnym zasięgu mających na celu stosowanie istotnych przepisów aktów podstawowych”.
36. EIOD nie sprzeciwia się wyborowi, polegającemu na pozostawieniu wszystkich tych kwestii przepisom wykonawczym. Przyjęcie przepisów w procedurze komitetowej prawdopodobnie skróci procedurę legislacyjną. Procedura komitetowa pomoże również zapewnić harmonizację, będącą celem, do którego zdecydowanie należy dążyć.
37. Biorąc pod uwagę dużą liczbę kwestii, które trzeba będzie rozstrzygnąć w drodze przepisów wykonawczych, i znaczenie tych kwestii, które podkreślono poniżej, wydaje się, że należy się nimi zająć w jednym akcie prawnym, a nie każdej z nich poświęcać odrębny przepis, co doprowadziłoby do tego, że niektóre z tych kwestii wyjaśniałaby dyrektywa o prywatności i łączności elektronicznej, a inne — przepisy wykonawcze. Cieszyć zatem powinno podejście Komisji, chcącej pozostawić podjęcie tych decyzji przepisom wykonawczym, które będą przyjęte pod zasięgnięciem opinii EIOD-a, a także, miejmy nadzieję, innych podmiotów (zob. punkt poniżej).

Kwestie, które należy rozstrzygnąć w przepisach wykonawczych

38. Znaczenie środków wykonawczych docenia się zwłaszcza, jeśli można przewidzieć w miarę szczegółowo, jakie kwestie trzeba będzie rozstrzygnąć w przepisach wykonawczych. W środkach wykonawczych można bowiem ustalić normy przekazywania informacji. Na przykład można w nich sprecyzować, co stanowi naruszenie bezpieczeństwa, warunki, jakie muszą spełnić przekazywane osobom fizycznymi i organom informacje, termin przekazania informacji i powiadomienia.

⁽¹⁾ Procedury legislacyjne w WE, w które zaangażowane są komitety składające się z przedstawicieli rządów państw członkowskich na szczeblu urzędników państwowych.

39. EIOD uważa, że dyrektywa o prywatności i łączności elektronicznej, w szczególności jej art. 4, nie powinna zawierać żadnych wyjątków od obowiązku powiadomienia. Z tego względu EIOD wyraża zadowolenie z przyjętego przez Komisję podejścia, wyrażonego w art. 4, który wprowadza obowiązek powiadomienia i nie przewiduje od tego obowiązku żadnych wyjątków, pozwala jednak, by tę i inne kwestie rozstrzygały przepisy wykonawcze. Choć EIOD jest świadomy argumentów, które mogłyby uzasadniać wprowadzenie pewnych wyjątków od tego obowiązku, opowiada się za tym, by tę i inne kwestie szczegółowo rozstrzygnięto w przepisach wykonawczych, po przeprowadzeniu dogłębnej i kompleksowej debaty na temat wszystkich odpowiednich kwestii. Jak napisano powyżej, złożony charakter tych kwestii związany z obowiązkiem powiadomienia o przypadkach naruszenia bezpieczeństwa, w tym z zasadnością istnienia wyłączeń lub ograniczeń, wymaga ich traktowania w spójny sposób, tj. w jednym akcie prawnym, który jest poświęcony wyłącznie tym kwestiom.

Zasięgnięcie opinii EIOD-a i potrzeba poszerzenia konsultacji

40. Zważywszy na to, w jakim stopniu środki wykonawcze wpłyną na ochronę danych osobowych osób fizycznych, ważnym jest, by przed przyjęciem tych środków Komisja przeprowadziła odpowiednie konsultacje. Z tego powodu EIOD wyraża zadowolenie z art. 4 ust. 4 wniosku, w którym jednoznacznie stwierdza się, że przed przyjęciem środków wykonawczych Komisja zasięgnie opinii Europejskiego Inspektora Ochrony Danych. Środki takie będą nie tylko dotyczyć ochrony danych osobowych i prywatności osób fizycznych, ale również wywarą na nią poważny wpływ. Ważne jest zatem, by uzyskać opinię EIOD-a, zgodnie z wymogiem zawartym w art. 41 rozporządzenia (WE) nr 45/2001.
41. Poza koniecznością zasięgnięcia opinii EIOD-a zasadne może być wprowadzenie przepisu przewidującego, że planowane środki wykonawcze będą podlegać konsultacjom publicznym, które pozwolą uzyskać opinię społeczeństwa i będą zachętą do podzielenia się doświadczeniami wzorcowych rozwiązań w tej dziedzinie. Konsultacje takie będą nie tylko dla branży, ale także innych zainteresowanych stron, w tym innych organów ochrony danych i grupy roboczej art. 29, odpowiednim kanałem komunikacji, którym umożliwi im przedstawienie swoich poglądów. Potrzeba konsultacji publicznych nabiera jeszcze większego znaczenia, jeśli weźmiemy pod uwagę, że przepisy zostaną przyjęte w procedurze komitetowej, w której możliwość interwencji Parlamentu Europejskiego jest ograniczona.
42. EIOD zwraca uwagę, że w art. 4 ust. 4 wniosku przewiduje się, że przed przyjęciem przepisów wykonawczych Komisja zasięgnie również opinii Urzędu ds. Rynku Łączności Elektronicznej. W tym względzie EIOD docenia zasadę zasięgania opinii Urzędu ds. Rynku Łączności Elektronicznej, będącego spadkobiercą doświadczenia i wiedzy na temat kwestii sieci i bezpieczeństwa informacji, które zgromadziła Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA). Do czasu utworzenia Urzędu ds. Rynku Łączności Elektronicznej być może należałoby — jako rozwiązanie tymczasowe — przewidywać w proponowanej zmianie (art. 4 ust. 4) konsultacje z ENISA.

II.3. Przepis dotyczący plików *cookie*, oprogramowania szpiegującego i podobnych urządzeń: zmiana w art. 5 ust. 3

43. W art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej poruszono kwestię technologii, które umożliwiają dostęp do informacji i przechowywanie informacji w urządzeniu końcowym użytkownika za pośrednictwem sieci łączności elektronicznej. Przykładem zastosowania art. 5 ust. 3 jest korzystanie z plików *cookie* ⁽¹⁾. Innym przykładem jest wykorzystanie takich technologii, jak oprogramowanie szpiegujące i trojany (programy ukryte w wiadomościach lub innych, pozornie nieszkodliwych programach). Założenia takich technologii i ich cele bardzo się różnią, i o ile niektóre są dla użytkownika zupełnie nieszkodliwe czy nawet użyteczne, o tyle inne są wyraźnie szkodliwe i groźne.

⁽¹⁾ Pliki *cookie* są umieszczane przez dostawców usług społeczeństwa informacyjnego (strony internetowe) w urządzeniach końcowych użytkowników w różnych celach, również w celu rozpoznania użytkownika, gdy po raz kolejny odwiedza daną stronę internetową. W praktyce, gdy plik *cookie* jest przesyłany do użytkownika Internetu przez stronę internetową, komputerowi użytkownika jest nadawany niepowtarzalny numer (tzn. komputer, który otrzymał plik *cookie* od strony internetowej A, staje się „komputerem, w którym przechowywany jest plik *cookie* nr 111”). Strona internetowa zachowuje ten numer jako odniesienie. Jeśli użytkownik komputera, który otrzymał plik *cookie* nr 111, nie wykasuje tego pliku, to gdy po raz kolejny odwiedzi tę samą stronę internetową, będzie ona mogła zidentyfikować komputer jako ten, w którym przechowywany jest plik *cookie* nr 111. Z czego strona internetowa wyciąga oczywisty wniosek, że używając tego komputera odwiedzano ją już wcześniej. Mechanizm, który umożliwia stronie internetowej rozpoznanie komputera jako tego, z którego korzystano już przy wcześniejszych wizytach, jest prosty. Gdy komputer, z którego korzysta odwiedzający, przechowuje pliki *cookie*, takie jak *cookie* nr 111, i używany jest do odwiedzenia strony, która przy wcześniejszych odwiedzinach wygenerowała ten plik *cookie*, strona ta przeszuka twardego dysku tego komputera, by odnaleźć nr pliku *cookie*. Jeśli przeglądarka użytkownika odnajdzie plik *cookie* odpowiadający numerowi odniesienia zachowanemu na tej stronie internetowej, informuje tę stronę, że komputer przechowuje plik *cookie* nr 111.

44. W art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej przedstawiono warunki, które należy spełnić, gdy wykorzystuje się wspomniane powyżej technologie, by uzyskać dostęp informacji w urządzeniach końcowych użytkowników lub przechowywać je tam. Konkretniej mówiąc, zgodnie z art. 5 ust. 3: (i) użytkownikom Internetu należy przekazać jasne i wyczerpujące informacje zgodnie z dyrektywą 95/46/WE, m.in. na temat celów przetwarzania i (ii) użytkownicy Internetu muszą mieć możliwość niewyrażenia zgody na takie przetwarzanie, tj. powinni mieć do wyboru opcję, zgodnie z którą informacje uzyskane z ich urządzeń końcowych nie będą podlegać przetwarzaniu.

Korzyści płynące z proponowanej zmiany

45. Zakres zastosowania art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej w jego obecnym brzmieniu jest ograniczony do sytuacji, w których dostęp do informacji i przechowywanie informacji w urządzeniu końcowym użytkownika odbywa się za pośrednictwem sieci łączności elektronicznej. Obejmuje to sytuację opisaną powyżej, jeśli chodzi o korzystanie z plików *cookie*, a także z innych technologii, takich jak oprogramowanie szpiegujące dostarczane przez sieci łączności elektronicznej. Niejasne jest jednak, czy art. 5 ust. 3 dotyczy sytuacji, w których podobne technologie (pliki *cookie*, oprogramowanie szpiegujące itp.) są przekazywane za pośrednictwem oprogramowania dostarczanego przez zewnętrzne nośniki danych i ściągniętego na urządzenie końcowe użytkownika. Zważywszy, że zagrożenie dla prywatności istnieje bez względu na kanał łączności, ograniczenie zakresu zastosowania art. 5 ust. 3 do jednego kanału łączności jest rozwiązaniem niefortunnym.
46. Dlatego EIOD cieszy się z wprowadzenia zmiany do art. 5 ust. 3, która — dzięki usunięciu wzmianki o „elektronicznych sieciach łączności” — poszerza w istocie zakres zastosowania tego artykułu. W swej zmienionej wersji art. 5 ust. 3 obejmuje bowiem sytuacje, w których dostęp do informacji i ich przechowywanie w urządzeniu końcowym użytkownika odbywa się za pośrednictwem sieci łączności elektronicznej, ale także za pośrednictwem innych zewnętrznych nośników danych, takich jak płyty kompaktowe, CD-ROM-y, pamięci USB itd.

Techniczne przechowywanie danych w celu ułatwienia transmisji komunikatu

47. Ostatnie zdanie art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej zachowało swoje brzmienie w zmienionej postaci artykułu. W myśl tego zdania, konieczność przestrzegania wymogów określonych w art. 5 ust. 3 zdanie pierwsze „nie stanowi (to) przeszkody dla technicznego przechowywania danych ani dostępu do nich jedynie w celu wykonania lub ułatwienia transmisji komunikatu za pośrednictwem sieci łączności elektronicznej, lub gdy jest to szczególnie niezbędne w celu świadczenia usługi społeczeństwa informacyjnego ...”. A zatem obowiązkowe zasady określone w art. 5 ust. 3 (konieczność poinformowania i możliwość niewyrażenia zgody) nie mają zastosowania, gdy jedynym celem dostępu do urządzenia końcowego użytkownika lub przechowywanie informacji jest ułatwienie transmisji lub gdy jest to ściśle niezbędne, aby świadczyć usługi społeczeństwa informacyjnego zażądane przez tego użytkownika.
48. Dyrektywa nie podaje, kiedy jedynym celem dostępu lub przechowywania informacji jest ułatwienie transmisji lub dostarczenie informacji. Jedną z sytuacji, które bez wątpienia podlegałyby temu wyłączeniu, jest przyłączenie komputera do Internetu. Dzieje się tak, ponieważ aby przyłączyć komputer do Internetu konieczny jest adres IP ⁽¹⁾. Komputer użytkownika końcowego zostanie poproszony o podanie dostawcy usługi dostępu do Internetu pewnych informacji na swój temat, a w zamian dostawca ten przyzna mu adres IP. W tym przypadku informacje przechowywane w urządzeniu końcowym użytkownika zostaną przekazane dostawcy usługi dostępu do Internetu po to, aby użytkownik zyskał możliwość dostępu do Internetu. W tej sytuacji dostawca usługi dostępu do Internetu jest zwolniony zarówno z wymogu powiadomienia o gromadzeniu informacji, jak i z obowiązku zapewnienia prawa do odmowy, o ile gromadzenie informacji jest konieczne do świadczenia usługi.
49. Po podłączeniu do Internetu, jeśli użytkownik chce obejrzeć daną stronę internetową, musi wysłać zapytanie do serwera, na którym ta strona się znajduje. Ten ostatni odpowie, jeśli będzie wiedział, dokąd przesłać informacje, tj. jeśli zna adres IP użytkownika. Ze względu na sposób, w jaki przechowywany jest ten adres, oznacza to, że strona internetowa, którą użytkownik chce odwiedzić, będzie musiała ponownie uzyskać dostęp do informacji zgromadzonych w urządzeniu końcowym użytkownika Internetu. Taka wymiana oczywiście również podlegałaby wyłączeniu. I rzeczywiście, wydaje się, że te przypadki powinny znaleźć się poza zakresem zastosowania wymogów w art. 5 ust. 3.

⁽¹⁾ Adres IP (*Internet Protocol address*) to niepowtarzalny adres, którego używają niektóre urządzenia elektroniczne, by dokonać wzajemnej identyfikacji i komunikować się ze sobą w sieci komputerowej wykorzystującej standard IP (*Internet Protocol standard*) — mówiąc prościej, jest to adres komputera. Każde urządzenie podłączone do sieci — również routery, przełączniki, komputery, serwery infrastrukturalne (np. NTP, DNS, DHCP, SNMP itd.), drukarki, faksy internetowe i niektóre telefony — może mieć własny adres, który jest niepowtarzalny w ramach danej sieci. Niektóre adresy IP mają być niepowtarzalne w ramach całego Internetu, inne powinny być niepowtarzalne jedynie w ramach danego przedsiębiorstwa.

50. EIOD uważa za słuszne zwolnienie z wymogu powiadomienia i umożliwienia odmowy w sytuacjach przedstawionych powyżej, gdy techniczne przechowywanie i dostęp do urządzenia końcowego użytkownika jest *konieczne* jedynie po to, by przeprowadzić transmisję komunikatu przez sieć łączności elektronicznej. To samo odnosi się do sytuacji, w której techniczne przechowywanie lub dostęp jest ściśle konieczny, by świadczyć usługę społeczeństwa informacyjnego. EIOD nie widzi jednak potrzeby zwolnienia z obowiązku przekazania informacji i przyznania prawa do odmowy w sytuacjach, w których celem technicznego przechowywania czy dostępu jest tylko *ułatwienie* transmisji komunikatu. Na przykład w myśl ostatniego zdania omawianego artykułu podmiot danych nie może skorzystać z prawa do otrzymania informacji ani z prawa do niewyrażenia zgody na przetwarzanie swoich danych, jeśli plik *cookie* zbiera dane na temat jego preferencji językowych lub lokalizacji (np. Belgia, Chiny), ponieważ tego typu plik *cookie* można by przedstawić jako taki, którego celem jest ułatwienie transmisji komunikatu. EIOD jest świadomy, że na poziomie oprogramowania podmioty danych dysponują praktyczną możliwością niewyrażenia zgody na przechowywanie plików *cookie* lub możliwością jego modulowania. Nie stoi za tym jednak jednoznacznie żaden przepis prawny, który formalnie upoważniłby podmiot danych do obrony swoich praw w opisaney powyżej sytuacji.
51. Aby uniknąć takiego obrotu sprawy, EIOD sugeruje, by do ostatniej części art. 5 ust. 3 wprowadzić niewielką zmianę, która polega na wykreśleniu słów „lub ułatwiania” ze zdania: „nie stanowi to przeszkody dla technicznego przechowywania danych ani dostępu do nich jedynie w celu wykonania lub ułatwiania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej, lub gdy jest to szczególnie niezbędne w celu świadczenia usługi społeczeństwa informacyjnego ...”.

II.4. Występowanie na drogę sądową przez dostawców PPECS i podmioty prawne: dodanie ust. 6 do art. 13

52. Proponowany art. 13 ust. 6 przewiduje, że każda osoba fizyczna lub prawna mająca w tym uzasadniony interes, w szczególności dostawcy usług łączności elektronicznej chroniący swój interes gospodarczy, mogą podejmować kroki prawne, by walczyć z tymi, którzy naruszają art. 13 dyrektywy o prywatności i łączności elektronicznej. Artykuł ten dotyczy wysyłania niezamówionych komunikatów komercyjnych.
53. Proponowana zmiana umożliwi np. dostawcom usługi dostępu do Internetu uporanie się ze autorami spamu niewłaściwie wykorzystującymi ich sieci, pozywanie podmiotów podrabiających adresy nadawcy lub przejmujących kontrolę nad serwerami, by wykorzystywać je do wysyłania spamu itd.
54. Dyrektywa o prywatności i łączności elektronicznej nie mówiła jasno, czy dostawcom PPECS przysługuje prawo do podejmowania działań przeciwko autorom spamu, a dostawcy ci w odosobnionych przypadkach wnosili pozwy do sądu za naruszenie art. 13 wdrożonego przez przepisy państwa członkowskiego ⁽¹⁾. Przyznając, że powodem wejścia na drogę sądową może być dla dostawców usług łączności elektronicznej ochrona ich interesu gospodarczego, wniosek potwierdza, że dyrektywa o prywatności i łączności elektronicznej ma na celu nie tylko ochronę poszczególnych abonentów, ale również dostawców usług łączności elektronicznej.
55. EIOD wyraża zadowolenie, że wniosek dopuszcza, by dostawcy usług łączności elektronicznej w ochronie swojego interesu gospodarczego mogli występować na drogę sądową przeciwko autorom spamu. O ile nie zajądą wyjątkowe okoliczności, poszczególni abonenci nie mają środków na wszczęcie tego typu działań sądowych ani nic ich do tego zachęca. Z drugiej strony dostawcy usługi dostępu do Internetu i inni dostawcy PPECS dysponują zapleczem finansowym i technicznym, by dokładnie zbadać przypadki masowego wysyłania spamu i stwierdzić, kim są sprawcy, a zatem wydaje się słuszne, by przyznać im prawo występowania na drogę sądową przeciwko autorom spamu.
56. Zdaniem EIOD-a proponowana zmiana jest cenna o tyle, że pozwoliłaby również stowarzyszeniom konsumenckim i związkom zawodowym reprezentującym interesy konsumentów będących celem działań autorów spamu występowanie na drogę sądową w imieniu tych konsumentów. Jak stwierdzono powyżej, szkody wyrządzone podmiotowi danych, który był adresatem spamu, rozpatrywane indywidualnie, zwykle nie są same w sobie na tyle dotkliwe, by wszczynał on kroki sądowe. EIOD już zaproponował ten środek, by zaradzić naruszeniom prywatności i ochrony danych, gdy ogólnie

⁽¹⁾ Jednym z takich przypadków była sprawa korporacja Microsoft przeciwko Paul McDonald t/a Bizards UK (2006 All Er (D) 153).

wypowiadał się w swojej opinii w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych ⁽¹⁾. Zdaniem EIOD-a wniosek powinien być pójść dalej i zaproponować pozwy zbiorowe, umożliwiając grupom obywateli wspólnie wnosić spory sądowe w sprawach dotyczących ochrony danych osobowych. W przypadku spamu, gdy otrzymuje go spora liczba osób, grupy osób powinny móc połączyć siły i wnosić pozwy zbiorowe przeciwko autorom spamu.

57. EIOD ze szczególnym żalem przyjmuje fakt, że wniosek ogranicza prawo osób prawnych do wystąpienia na drogę sądową do sytuacji, w których nastąpiło naruszenie art. 13 dyrektywy, tj. sytuacji, w których pogwałcony został przepis dotyczący niechcianych wiadomości elektronicznych. W myśl proponowanej zmiany osoby prawne nie będą mogły wszczynać działań sądowych w przypadku naruszenia innych przepisów dyrektywy o prywatności i łączności elektronicznej. Na przykład, w swej obecnej postaci przepis ten nie pozwala osobie prawnej, np. stowarzyszeniu konsumenckiemu, wystąpić na drogę sądową przeciwko dostawcy usługi dostępu do Internetu, który ujawnił dane osobowe milionów konsumentów. Wykonywanie całej dyrektywy o prywatności i łączności elektronicznej, nie tylko danego artykułu, znacznie by się poprawiło, gdyby przepisowi art. 13 ust. 6 nadano ogólny charakter, by umożliwić osobom prawnym podejmowanie działań sądowych w przypadku naruszenia któregośkolwiek przepisu tej dyrektywy.
58. Aby zaradzić temu problemowi, EIOD proponuje, by przekształcić art. 13 ust. 6 w odrębny artykuł (art. 14). Ponadto brzmienie art. 13 ust. 6 należałoby nieznacznie zmodyfikować: zamiast „na podstawie niniejszego artykułu” powinno być „na podstawie niniejszej dyrektywy”.

II.5. Wzmocnienie przepisów dotyczących egzekwowania: dodany art. 15a

59. Dyrektywa o prywatności i łączności elektronicznej nie zawiera jednoznacznych przepisów dotyczących egzekwowania. Zamiast tego, zawiera ona odniesienie do części dyrektywy o ochronie danych ⁽²⁾ poświęconej egzekwowaniu. EIOD z zadowoleniem przyjmuje nowy art. 15a wniosku, w którym jednoznacznie wyjaśnione są kwestie dotyczące egzekwowania na mocy tej dyrektywy.
60. Po pierwsze, EIOD zwraca uwagę, że skuteczna strategia egzekwowania w tej dziedzinie zakłada, zgodnie z wymogiem zawartym w art. 15a ust. 3, że organy krajowe mają uprawnienia do prowadzenia dochodzeń koniecznych do zgromadzenia niezbędnych informacji. Bardzo często dowód naruszenia przepisów dyrektywy o prywatności i łączności elektronicznej będzie miał postać elektroniczną i może być przechowywany w różnych komputerach i urządzeniach lub sieciach. Z tego względu ważne jest, by agencje odpowiedzialne za egzekwowanie prawa mogły uzyskiwać nakaz przeszukania, dający im prawo do wejścia, przeszukania i zajęcia.
61. Po drugie, EIOD szczególnie przychylnie przyjmuje proponowaną zmianę, tzn. art. 15a ust. 2, zgodnie z którym krajowe organy regulacyjne muszą dysponować uprawnieniami do wydania nakazu, tj. do doprowadzenia do zaprzestania naruszeń, i uprawnieniami i zasobami niezbędnymi do prowadzenia dochodzeń. Krajowe organy regulacyjne, także krajowe organy ochrony danych, powinny dysponować uprawnieniami do wydawania nakazu sądowego zmuszającego sprawców do zaprzestania działalności, która narusza dyrektywę o prywatności i łączności elektronicznej. Nakaz lub uprawnienie, by nakazać zaprzestanie naruszania przepisów jest użytecznym narzędziem w przypadku uporczywego postępowania, które narusza prawa osób fizycznych. Nakazy będą bardzo użyteczne, by powstrzymać przypadki nieprzestrzegania dyrektywy o prywatności i łączności elektronicznej, np. naruszania art. 13 dotyczącego niezamówionych komunikatów komercyjnych, które to naruszenie z natury rzeczy jest postępowaniem uporczywym.
62. Po trzecie, wniosek umożliwia Komisji wprowadzenie technicznych środków wykonawczych, które pozwolą zapewnić skuteczną współpracę transgraniczną przy egzekwowaniu przepisów krajowych (proponowany art. 15a ust. 4). Dotychczas współpraca ta obejmuje porozumienie, ustanowione z inicjatywy Komisji, w sprawie opracowania wspólnej procedury rozpatrywania transgranicznych skarg dotyczących spamu.

⁽¹⁾ Opinia Europejskiego Inspektora Ochrony Danych 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, str. 1).

⁽²⁾ 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.

63. EIOD uważa, że jeśli pomagając swojemu odpowiednikowi w innym kraju organ regulacyjny będzie miał przepisy po swojej stronie, niewątpliwie pomoże to egzekwować przepisy w sytuacjach transgranicznych. Zatem właściwe jest, by wniosek umożliwił Komisji stworzenie warunków do zapewnienia współpracy transgranicznej, w tym procedur dzielenia się informacjami.

III. WNIOSKI I ZALECENIA

64. EIOD całkowicie popiera wniosek. Proponowane zmiany poprawiają ochronę prywatności i danych osobowych osób fizycznych w sektorze łączności elektronicznej, a proces ten przebiega z wyczuciem, bez nieuzasadnionego i zbędnego obciążania organizacji. Ścisłej mówiąc, EIOD uważa, że większość proponowanych zmian nie wymaga modyfikacji, ponieważ dobrze odpowiadają one zamierzonemu celowi. W pkt 69 poniżej przedstawiono zmiany, co do których EIOD wyraża nadzieję, że nie ulegną modyfikacji.
65. Choć EIOD ogólnie bardzo pozytywnie ocenia wniosek, uważa, że niektóre z zaproponowanych w nim zmian należy poprawić, tak by dopilnować, że faktycznie zapewniają one odpowiednią ochronę danych osobowych i prywatności osób fizycznych. Odnosi się to w szczególności do przepisów dotyczących powiadamiania o przypadkach naruszenia bezpieczeństwa oraz przepisów mówiących o występowaniu na drogę sądową przez dostawców usług łączności elektronicznej w związku z pogwałceniem przepisów o niezamówionych komunikatach komercyjnych. Ponadto EIOD wyraża żal, że we wniosku nie poruszono pewnych kwestii, które nie są też dokładnie wyjaśnione w obowiązującej dyrektywie o prywatności i łączności elektronicznej; nie skorzystano tym samym ze sposobności, jaką daje ten przegląd, by zaradzić nierozwiązanym problemom.
66. Aby rozwiązać oba problemy, czyli kwestie niedostatecznie wyjaśnione we wniosku i wcale w nim nieporuszone, w niniejszej opinii zaproponowano pewne zmiany redakcyjne. W pkt 67 i 68 podsumowano te problemy i zaproponowano konkretne sformułowania. EIOD apeluje do prawodawcy o ich uwzględnienie w trakcie procesu legislacyjnego.
67. Zmiany zawarte we wniosku, w przypadku których EIOD zdecydowanie opowiada się za modyfikacją, to:

- (i) **Powiadamianie o przypadkach naruszenia bezpieczeństwa:** W obecnym brzmieniu proponowana zmiana, dodająca art. 4 ust. 4, ma zastosowanie do dostawców publicznie dostępnych usług łączności elektronicznej w sieciach publicznych (dostawcy usługi dostępu do Internetu, operatorzy sieci), którzy mają obowiązek powiadamiać krajowe organy regulacyjne i swoich klientów o przypadkach naruszenia bezpieczeństwa. EIOD w pełni popiera istnienie takiego obowiązku. Uważa jednak, że obowiązek ten powinien dotyczyć również dostawców usług społeczeństwa informacyjnego, którzy często przetwarzają sensytywne dane osobowe. Tak więc banki internetowe, dostawcy elektronicznych usług zdrowotnych i wszystkie pozostałe firmy internetowe także musieliby się wywiązywać z tego obowiązku.

W tym celu EIOD proponuje, by dodać do art. 4 ust. 3 wzmiankę o dostawcach usług społeczeństwa informacyjnego w brzmieniu: „W przypadku naruszenia bezpieczeństwa, prowadzącego do przypadkowego lub ... dostawca publicznie dostępnych usług łączności i dostawca usług społeczeństwa informacyjnego ... powiadamiają o takim naruszeniu zainteresowanego abonenta i krajowy organ regulacyjny”.

- (ii) **Występowanie na drogę sądową przez dostawców publicznie dostępnych usług łączności elektronicznej w sieciach publicznych:** W obecnym brzmieniu proponowana zmiana, dodająca art. 13 ust. 6, przewiduje, że aby zwalczać przypadki naruszenia art. 13 dyrektywy o prywatności i łączności elektronicznej, który zajmuje się kwestią spamu, środki cywilnoprawne może podejmować każda osoba fizyczna lub prawna, w szczególności dostawcy usług łączności elektronicznej. EIOD wyraża zadowolenie z tego przepisu. Nie może jednak zrozumieć, dlaczego to nowe uprawnienie ma się ograniczać do przypadków naruszenia art. 13. EIOD proponuje, aby osoby prawne miały prawo występować na drogę sądową w przypadku naruszenia któregośkolwiek z przepisów dyrektywy o prywatności i łączności elektronicznej.

Aby osiągnąć zamierzony skutek, EIOD proponuje, by art. 13 ust. 6 został przekształcony w odrębny artykuł (art. 14). Ponadto brzmienie art. 13 ust. 6 należałoby nieznacznie zmodyfikować: zamiast „na podstawie niniejszego artykułu” powinno być „na podstawie niniejszej dyrektywy”.

68. Zakres zastosowania dyrektywy o prywatności i łączności elektronicznej, który jest obecnie ograniczony do dostawców publicznych sieci łączności elektronicznej, pozostaje jednym z najbardziej niepokojących problemów, których wniosek nie rozwiązuje. Zdaniem EIOD-a dyrektywa o prywatności i łączności elektronicznej powinna zostać zmieniona tak, by jej stosowanie obowiązywało dostawców usług łączności elektronicznej również w sieciach mieszanych (publiczno-prywatnych) i prywatnych.
69. EIOD stoi zdecydowanie na stanowisku, że poniższe zmiany nie powinny ulec modyfikacji:
- (i) **Identyfikacja radiowa:** Proponowana zmiana w art. 3, zgodnie z którą sieci łączności elektronicznej obejmują również „publiczne sieci łączności służące do zbierania danych i obsługi urządzeń identyfikacyjnych”, jest w pełni zadowalająca. Przepis ten ma bardzo pozytywny wymiar, ponieważ wyjaśnia, że pewne zastosowania identyfikacji radiowej muszą być zgodne z dyrektywą o prywatności i łączności elektronicznej, i tym samym zmniejsza niepewność prawną w tym względzie.
 - (ii) **Pliki cookie/oprogramowanie szpiegujące:** Należy cieszyć się z proponowanej zmiany w art. 5 ust. 3, ponieważ dzięki niej obowiązek poinformowania danego użytkownika i dania mu możliwości niewyrażenia zgody na przechowywanie plików *cookie*/oprogramowania szpiegującego w jego urządzeniu końcowym będzie istniał również wtedy, gdy takie pliki/oprogramowanie są przekazywane za pośrednictwem zewnętrznych nośników danych, takich jak CD-ROM-y czy pamięci USB. EIOD sugeruje jednak, by do ostatniej części art. 5 ust. 3 wprowadzić niewielką zmianę, która polega na wykreśleniu słów „lub ułatwiania” ze zdania.
 - (iii) **Wybór procedury komitetowej z zasięgnięciem opinii EIOD-a oraz warunki/ograniczenia obowiązku powiadamiania:** Proponowana zmiana, w której dodaje się art. 4 ust. 4 dotyczący powiadamiania o przypadkach naruszenia bezpieczeństwa, pozostawia komitetowi — po zasięgnięciu opinii EIOD-a — decyzję w sprawie złożonych kwestii dotyczących okoliczności/formy/procedur systemu powiadamiania o przypadkach naruszenia bezpieczeństwa. EIOD wyraża zdecydowane poparcie dla takiego ujednoliconego podejścia. Przepisy dotyczące powiadamiania o przypadkach naruszenia bezpieczeństwa są same w sobie tematem, którym należy się zająć, po dogłębnej dyskusji i analizie.

Z tą sprawą wiąże się apel do niektórych podmiotów o zaproponowanie, w jakich sytuacjach nie istniałby obowiązek powiadamiania o przypadkach naruszenia bezpieczeństwa zgodnie z art. 4 ust. 4. EIOD stanowczo sprzeciwia się takiemu podejściu. Opowiada się raczej za tym, by zagadnienie ogólnego obowiązku powiadomienia, sposobów powiadamiania czy tego, w jakich okolicznościach treść powiadomienia mogłaby zostać skrócona lub ograniczona, było przedmiotem całościowej analizy poprzedzonej rzeczową dyskusją.
 - (iv) **Egzekwowanie:** Proponowana zmiana dotycząca dodania art. 15a zawiera wiele pomocnych elementów, które należy zachować, ponieważ przyczynią się one do faktycznego przestrzegania przepisów; elementy te to m.in. wzmocnienie uprawnień do prowadzenia dochodzeń, którymi dysponują krajowe organy regulacyjne (art. 15a ust. 3), oraz przyznanie krajowym organom regulacyjnym uprawnienia do nakazania zaprzestania naruszeń.

Sporządzono w Brukseli, dnia 10 kwietnia 2008 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych

II

(Informacje)

INFORMACJE INSTYTUCJI I ORGANÓW UNII EUROPEJSKIEJ

KOMISJA

Zezwolenie na pomoc państwa w ramach przepisów zawartych w art. 87 i 88 Traktatu WE**Przypadki, względem których Komisja nie wnosi sprzeciwu**

(2008/C 181/02)

Data przyjęcia decyzji	15.10.2007
Numer pomocy	N 204/06 i N 605/06
Państwo członkowskie	Hiszpania
Region	Extremadura, Andalucía, Canarias, Castilla y León, Cataluña, Galicia, Baleares, Castilla la Mancha, Asturias y Valencia
Nazwa środka pomocy	Ayudas para compensar los daños causados por los incendios (verano 2005)
Podstawa prawna	Real Decreto-Ley n° 11/2005, de 22 de julio Real Decreto n° 949/2005, de 29 de julio Real Decreto n° 609/2006, de 19 de mayo
Rodzaj środka pomocy	Program pomocy
Cel pomocy	Rekompensata szkód w produkcji rolnej na skutek pożarów
Forma pomocy	Dotacja bezpośrednia, subwencjonowanie odsetek, korzyści podatkowe
Budżet	4 mln EUR Linia budżetowa wynosząca 20 mln EUR na subwencjonowanie odsetek
Intensywność pomocy	Do 100 % szkód
Czas trwania pomocy	Do zakończenia wypłacania pomocy
Sektory gospodarki	Rolnictwo (sektory zwierząt gospodarskich i pszczelarski)
Nazwa i adres organu przyznającego pomoc	Entidad Estatal de Seguros Agrarios Ministerio de Agricultura, Pesca y Alimentación C/ Miguel Ángel n° 25, 5ª planta E-28010 Madrid

Inne informacje	Korzyści podatkowe nie stanowią pomocy państwa w rozumieniu obwieszczenia Komisji w sprawie stosowania reguł pomocy publicznej do środków związanych z bezpośrednim opodatkowaniem działalności gospodarczej (Dz.U. C 384 z 10.12.1998, str. 3)
-----------------	---

Tekst decyzji w autentycznej wersji językowej, z którego usunięto wszystkie informacje o charakterze poufnym, można znaleźć na stronie:

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

Data przyjęcia decyzji	5.12.2007
Numer pomocy	N 327/07
Państwo członkowskie	Hiszpania
Region	—
Nazwa środka pomocy (i/lub nazwa podmiotu otrzymującego pomoc)	Ayudas para la reparación de daños causados por los incendios ocurridos durante el año 2006 en diferentes regiones españolas
Podstawa prawna	Orden APA/1446/2007, de 16 de mayo, por la que se dictan disposiciones para el desarrollo del Real Decreto nº 86/2007, de 26 de enero, por el que se declara, para incendios acaecidos en diversas Comunidades Autónomas, la aplicación de las disposiciones contenidas en el Real Decreto-Ley nº 8/2006, de 28 de agosto, por el que se aprueban medidas urgentes en materia de incendios forestales en la Comunidad Autónoma de Galicia
Rodzaj środka pomocy	Program pomocy
Cel pomocy	Odszkodowanie za szkody poniesione w wyniku pożarów w 2006 r. w gospodarstwach rolnych, hodowlanych i pasiekach znajdujących się w kilku prowincjach Wysp Kanaryjskich (wyspa El Hierro), Estremadury (Caceres), Kastylii-La Manchy (Toledo), Aragonii, (Huesca) i Galicji (Lugo)
Forma pomocy	Dotacja bezpośrednia
Budżet	800 000 EUR
Intensywność pomocy	Maksymalnie 100 %
Czas trwania pomocy	Pomoc doraźna
Sektory gospodarki	Rolnictwo
Nazwa i adres organu przyznającego pomoc	Entidad Estatal de Seguros Agrarios Ministerio de Agricultura, Pesca y Alimentación C/ Miguel Ángel nº 23, 5ª planta E-28010 Madrid
Inne informacje	—

Tekst decyzji w autentycznej wersji językowej, z którego usunięto wszystkie informacje o charakterze poufnym, można znaleźć na stronie:

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

Data przyjęcia decyzji	14.11.2007
Numer pomocy	N 346/07
Państwo członkowskie	Zjednoczone Królestwo
Region	England
Nazwa środka pomocy (i/lub nazwa podmiotu otrzymującego pomoc)	Woodland Management Grant for Access
Podstawa prawna	The Forestry Act 1979
Rodzaj środka pomocy	Program pomocy
Cel pomocy	Leśnictwo
Forma pomocy	Dotacja
Budżet	Roczna kwota: 300 000 GBP (około 440 000 EUR) Całkowita kwota: 2,10 mln GBP (około 3,08 mln EUR)
Intensywność pomocy	Maksymalnie 70 %
Czas trwania pomocy	Data decyzji Komisji do dnia 31 grudnia 2013 r.
Sektory gospodarki	Leśnictwo
Nazwa i adres organu przyznającego pomoc	Forestry Commission England Great Eastern House Tenison Rd Cambridge CB1 2DU United Kingdom
Inne informacje	—

Tekst decyzji w autentycznej wersji językowej, z którego usunięto wszystkie informacje o charakterze poufnym, można znaleźć na stronie:

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

Brak sprzeciwu wobec zgłoszonej koncentracji
(Sprawa COMP/M.5162 — Avnet/Horizon)

(Tekst mający znaczenie dla EOG)

(2008/C 181/03)

W dniu 26 czerwca 2008 r. Komisja podjęła decyzję o nie sprzeciwianiu się wyżej wymienionej koncentracji oraz uznaniu jej za zgodną z regułami wspólnego rynku. Powyższa decyzja zostaje wydana na mocy art. 6 ust. 1 lit. b) rozporządzenia Rady (WE) nr 139/2004. Pełny tekst decyzji jest dostępny wyłącznie w języku angielskim i będzie opublikowany po uprzednim usunięciu ewentualnych tajemnic handlowych przedsiębiorstw. Tekst decyzji będzie dostępny:

- na stronie internetowej: Europa — Dyrekcja Generalna do spraw Konkurencji (<http://ec.europa.eu/comm/competition/mergers/cases/>). Strona ta została wyposażona w różnorodne opcje wyszukiwania, takie jak spis firm, numerów spraw, dat oraz spis sektorów przemysłowych, które mogą być pomocne w znalezieniu poszczególnych decyzji w sprawach połączeń,
 - w formie elektronicznej na stronie internetowej EUR-Lex, pod numerem dokumentu 32008M5162. EUR-Lex pozwala na dostęp on-line do dokumentacji prawa Europejskiego (<http://eur-lex.europa.eu>).
-

IV

(Zawiadomienia)

ZAWIADOMIENIA INSTYTUCJI I ORGANÓW UNII
EUROPEJSKIEJ

KOMISJA

Kursy walutowe euro ⁽¹⁾

17 lipca 2008 r.

(2008/C 181/04)

1 euro =

Waluta			Kurs wymiany			Waluta			Kurs wymiany		
USD	Dolar amerykański		1,5849			TRY	Lir turecki		1,9109		
JPY	Jen		167,43			AUD	Dolar australijski		1,6246		
DKK	Korona duńska		7,4588			CAD	Dolar kanadyjski		1,5860		
GBP	Funt szterling		0,79140			HKD	Dolar hong kong		12,3581		
SEK	Korona szwedzka		9,4778			NZD	Dolar nowozelandzki		2,0661		
CHF	Frank szwajcarski		1,6145			SGD	Dolar singapurski		2,1414		
ISK	Korona islandzka		122,11			KRW	Won		1 603,13		
NOK	Korona norweska		8,0640			ZAR	Rand		11,9765		
BGN	Lew		1,9558			CNY	Juan renminbi		10,8111		
CZK	Korona czeska		23,142			HRK	Kuna chorwacka		7,2271		
EEK	Korona estońska		15,6466			IDR	Rupia indonezyjska		14 498,67		
HUF	Forint węgierski		230,13			MYR	Ringgit malezyjski		5,1232		
LTL	Lit litewski		3,4528			PHP	Peso filipińskie		70,631		
LVL	Łat łotewski		0,7027			RUB	Rubel rosyjski		36,8300		
PLN	Złoty polski		3,2235			THB	Bat tajlandzki		52,985		
RON	Lej rumuński		3,5620			BRL	Real		2,5190		
SKK	Korona słowacka		30,318			MXN	Peso meksykańskie		16,2001		

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

ZAWIADOMIENIA PAŃSTW CZŁONKOWSKICH

Informacje przekazane przez państwa członkowskie, dotyczące pomocy państwa przyznanej na mocy rozporządzenia Komisji (WE) nr 1628/2006 w sprawie zastosowania art. 87 i 88 Traktatu WE do krajowej regionalnej pomocy inwestycyjnej

(Tekst mający znaczenie dla EOG)

(2008/C 181/05)

Numer pomocy	XR 37/08
Państwo członkowskie	Francja
Region	Corse 87(3)c
Nazwa programu pomocy lub nazwa przedsiębiorstwa otrzymującego uzupełniającą pomoc <i>ad hoc</i>	Mesures fiscales d'aide à l'investissement en Corse: crédit d'impôt et exonération de taxe professionnelle
Podstawa prawna	Articles 244 <i>quater</i> E et 1466 C du code général des impôts
Rodzaj środka pomocy	Program pomocy
Roczne wydatki planowane w ramach programu pomocy	43 mln EUR
Maksymalna intensywność pomocy	15 %
	Zgodnie z art. 4 rozporządzenia
Data realizacji	1.1.2007
Czas trwania	31.12.2012
Sektory gospodarki	—
	NACE A, D (sine DA 15.2, DF 23.1, DF 24.7, DJ 27.1, DJ 27.2, DJ 27.3, DM 34, DM 35.1), DM 35.1 A, E, F, G, GA 50.2, GA 52.7, H, I, J, JA 65.2, JA 67, K, KA 72, KA 72.5, KA 74, M, N, O, O92
Nazwa i adres organu przyznającego pomoc	Ministère de l'économie, des finances et de l'emploi 139, rue de Bercy F-75012 Paris
Adres internetowy publikacji programu pomocy	http://www.legifrance.gouv.fr/./affichCode.do?cidTexte=LEGITEXT000006069577
Inne informacje	—

Informacje przekazane przez państwa członkowskie, dotyczące pomocy państwa przyznanej na mocy rozporządzenia Komisji (WE) nr 70/2001 w sprawie zastosowania art. 87 i 88 Traktatu WE w odniesieniu do pomocy państwa dla małych i średnich przedsiębiorstw

(Tekst mający znaczenie dla EOG)

(2008/C 181/06)

Numer pomocy	XS 87/08
Państwo członkowskie	Polska
Region	Centralny PL 12
Nazwa programu pomocy lub nazwa podmiotu otrzymującego pomoc indywidualną	Przedsiębiorstwo produkcyjno handlowo usługowe Bomet
Podstawa prawna	Ustawa z dnia 8 października 2004 r. o zasadach finansowania nauki art. 10, Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego Dz.U. nr 221 z 14 listopada 2007 r. § 3 ust. 1, umowa nr II-189/P-218/2008
Rodzaj środka pomocy	<i>Ad hoc</i>
Budżet	Roczne wydatki planowane w ramach programu pomocy: — Całkowita kwota pomocy przewidziana w ramach programu: 66 487,86 EUR
Maksymalna intensywność pomocy	Zgodnie z artykułem 4 ust. 2–6 i art. 5 rozporządzenia
Data realizacji	18.3.2008
Czas trwania	18.3.2008
Cel pomocy	Małe i średnie przedsiębiorstwa
Sektory gospodarki	Wszystkie sektory kwalifikujące się do pomocy dla MŚP
Nazwa i adres organu przyznającego pomoc	Ministerstwo Nauki i Szkolnictwa Wyższego ul. Wspólna 1/3 PL-00-529 Warszawa

Numer pomocy	XS 88/08
Państwo członkowskie	Polska
Region	Północny PL 63
Nazwa programu pomocy lub nazwa podmiotu otrzymującego pomoc indywidualną	Remprodex Sp. z o.o.
Podstawa prawna	Ustawa z dnia 8 października 2004 r. o zasadach finansowania nauki art. 10, Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego Dz.U. nr 221 z 14 listopada 2007 r. § 3 ust. 1, umowa nr II-188/P-208/2008
Rodzaj środka pomocy	<i>Ad hoc</i>
Budżet	Roczne wydatki planowane w ramach programu pomocy: — Całkowita kwota pomocy przewidziana w ramach programu: 0,10951177 mln EUR

Maksymalna intensywność pomocy	Zgodnie z artykułem 4 ust. 2–6 i art. 5 rozporządzenia
Data realizacji	13.2.2008
Czas trwania	13.2.2008
Cel pomocy	Małe i średnie przedsiębiorstwa
Sektory gospodarki	Wszystkie sektory kwalifikujące się do pomocy dla MŚP
Nazwa i adres organu przyznającego pomoc	Ministerstwo Nauki i Szkolnictwa Wyższego ul. Wspólna 1/3 PL-00-529 Warszawa

Informacje przekazane przez państwa członkowskie, dotyczące pomocy państwa przyznanej na mocy rozporządzenia Komisji (WE) nr 68/2001 w sprawie zastosowania art. 87 i 88 Traktatu WE do pomocy szkoleniowej

(Tekst mający znaczenie dla EOG)

(2008/C 181/07)

Numer pomocy	XT 49/08
Państwo członkowskie	Republika Czeska
Region	Regiony soudržnosti NUTS II Střední Čechy, Jihozápad, Severozápad, Severovýchod, Jihovýchod, Střední Morava, Moravskoslezsko
Nazwa programu pomocy lub nazwa podmiotu otrzymującego pomoc indywidualną	Operační program Podnikání a inovace 2007–2013. Podprogram Inovace – školení
Podstawa prawna	Zákon č. 47/2002 Sb., o podpoře malého a středního podnikání. Zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů
Rodzaj środka pomocy	Program pomocy
Budżet	Roczne wydatki planowane w ramach programu pomocy: 45 mln CZK Całkowita kwota pomocy przewidziana w ramach programu: —
Maksymalna intensywność pomocy	Zgodnie z art. 4 ust. 2–7 rozporządzenia
Data realizacji	1.6.2007
Czas trwania	31.12.2008
Cel pomocy	Szkolenia specjalistyczne
Sektory gospodarki	Produkcja sprzętu transportowego Inny sektor związany z produkcją Inne usługi
Nazwa i adres organu przyznającego pomoc	Ministerstvo průmyslu a obchodu Na Františku 32 CZ-110 15 Praha

Numer pomocy	XT 52/08
Państwo członkowskie	Polska
Region	PL 421 — Podregion szczeciński
Nazwa programu pomocy lub nazwa podmiotu otrzymującego pomoc indywidualną	Wojewódzka Handlowa Spółdzielnia Inwalidów ZPCH
Podstawa prawna	Art. 30, 31 ustawy z dnia 20 kwietnia 2004 r. o Narodowym Planie Rozwoju (Dz.U. nr 116, poz. 1206). Rozporządzenie Ministra Gospodarki i Pracy z dnia 21 września 2004 r. w sprawie przyjęcia Uzupełnienia programu operacyjnego — Program Inicjatywy Wspólnotowej EQUAL dla Polski 2004–2006 (Dz.U. nr 214, poz. 2172). Umowa szkoleniowa nr SZCZECIN/WHSI/4/2007 z dnia 7 grudnia 2007 r.

Rodzaj środka pomocy	<i>Ad hoc</i>
Budżet	Roczne wydatki planowane w ramach programu pomocy: — Całkowita kwota pomocy przewidziana w ramach programu: 508,9 EUR
Maksymalna intensywność pomocy	Zgodnie z art. 4 ust. 2–7 rozporządzenia
Data realizacji	7.12.2007
Czas trwania	14.12.2007
Cel pomocy	Szkolenia ogólne
Sektory gospodarki	Wszystkie sektory kwalifikujące się do pomocy szkoleniowej
Nazwa i adres organu przyznającego pomoc	Zachodniopomorska Szkoła Biznesu Żołnierska 53 PL-71-210 Szczecin

Numer pomocy	XT 53/08
Państwo członkowskie	Polska
Region	PL 421 — Podregion szczeciński
Nazwa programu pomocy lub nazwa podmiotu otrzymującego pomoc indywidualną	Wojewódzka Handlowa Spółdzielnia Inwalidów ZPCH
Podstawa prawna	Art. 30, 31 ustawy z dnia 20 kwietnia 2004 r. o Narodowym Planie Rozwoju (Dz.U. nr 116, poz. 1206). Rozporządzenie Ministra Gospodarki i Pracy z dnia 21 września 2004 r. w sprawie przyjęcia Uzupełnienia programu operacyjnego — Program Inicjatywy Wspólnotowej EQUAL dla Polski 2004–2006 (Dz.U. nr 214, poz. 2172). Umowa szkoleniowa nr SZCZECIN/WHSI/2/2007 z dnia 5 listopada 2007 r.
Rodzaj środka pomocy	<i>Ad hoc</i>
Budżet	Roczne wydatki planowane w ramach programu pomocy: — Całkowita kwota pomocy przewidziana w ramach programu: 586,64 EUR
Maksymalna intensywność pomocy	Zgodnie z art. 4 ust. 2–7 rozporządzenia
Data realizacji	5.11.2007
Czas trwania	16.11.2007
Cel pomocy	Szkolenia ogólne
Sektory gospodarki	Wszystkie sektory kwalifikujące się do pomocy szkoleniowej
Nazwa i adres organu przyznającego pomoc	Zachodniopomorska Szkoła Biznesu Żołnierska 53 PL-71-210 Szczecin

Informacje przekazane przez państwa członkowskie, dotyczące pomocy państwa przyznanej na mocy rozporządzenia Komisji (WE) nr 1628/2006 w sprawie zastosowania art. 87 i 88 Traktatu WE do krajowej regionalnej pomocy inwestycyjnej

(Tekst mający znaczenie dla EOG)

(2008/C 181/08)

Numer pomocy	XR 10/08
Państwo członkowskie	Malta
Region	Malta
Nazwa programu pomocy lub nazwa przedsiębiorstwa otrzymującego uzupełniającą pomoc <i>ad hoc</i>	Investment Aid Scheme
Podstawa prawna	Investment Aid Regulations
Rodzaj środka pomocy	Program pomocy
Roczne wydatki planowane w ramach programu pomocy	13 mln MTL
Maksymalna intensywność pomocy	30 %
	Zgodnie z art. 4 rozporządzenia
Data realizacji	1.1.2008
Czas trwania	31.12.2013
Sektory gospodarki	Pomoc ograniczona do konkretnych sektorów
	NACE D, K072, K0731, K07482, K07486, M0803, N0851, O0921
Nazwa i adres organu przyznającego pomoc	Malta Enterprise Enterprise Centre San Gwann SGN 3000 Malta
Adres internetowy publikacji programu pomocy	www.maltaenterprise.com
Inne informacje	—

V

(Ogłoszenia)

PROCEDURY ZWIĄZANE Z REALIZACJĄ WSPÓLNEJ POLITYKI HANDLOWEJ

KOMISJA

Zawiadomienie o wszczęciu częściowego przeglądu okresowego środków antydumpingowych stosowanych względem przywozu łososia hodowlanego pochodzącego z Norwegii

(2008/C 181/09)

Komisja z własnej inicjatywy podjęła decyzję o wszczęciu częściowego przeglądu okresowego zgodnie z art. 11 ust. 3 rozporządzenia Rady (WE) nr 384/96 z 22 grudnia 1995 r. w sprawie ochrony przed dumpin-gowym przywozem z krajów niebędących członkami Wspólnoty Europejskiej ⁽¹⁾ („rozporządzenie podsta-wowe”). Przegląd ten ogranicza się do zbadania zakresu produktu w celu wyjaśnienia, czy środki dotyczące łososia hodowlanego obejmują niektóre typy produktów.

1. Produkt

Produktem objętym przeglądem jest łosoś hodowlany (inny niż dziki), filetowy lub niefiletowy, świeży, schłodzony lub mrożony, pochodzący z Norwegii („produkt objęty postępowaniem”), obecnie objęty kodami CN ex 0302 12 00, ex 0303 11 00, ex 0303 19 00, ex 0303 22 00, ex 0304 19 13 i ex 0304 29 13. Powyższe kody CN podane są jedynie w celach informacyjnych.

2. Obowiązujące środki

Obecnie obowiązującymi środkami są ostateczne cła antydumpingowe nałożone rozporządzeniem Rady (WE) nr 85/2006 z dnia 17 stycznia 2006 r. na przywóz łososia hodowlanego pochodzącego z Norwegii ⁽²⁾.

3. Podstawy dokonania przeglądu

Sąd administracyjny w Tallinnie zwrócił się do Europejskiego Trybunału Sprawiedliwości o orzeczenie w trybie prejudycjalnym, czy mrożone kręgosłupy (ości z mięsem rybnym) łososia objęte są kodami Taric wymienionymi w art. 1 rozporządzenia (WE) nr 85/2006 nakładającego ostateczne cło antydumpingowe na przywóz łososia hodowlanego pochodzącego z Norwegii oraz jakie konsekwencje dla środków antydumpin-gowych ma ta klasyfikacja. Artykuł 1 powyższego rozporządzenia nakłada środki na różnych poziomach w zależności od formy produktu objętego postępowaniem. Jedną z takich form jest „inny łosoś hodowlany (w tym patroszony, bez głowy), świeży, schłodzony lub mrożony”. Komisja z własnej inicjatywy podjęła decyzję, że zakres produktu podlegającego środkom antydumpingowym powinien zostać wyjaśniony w odniesieniu do wspomnianej powyżej formy (w tym tych samych kręgosłupów, świeżych lub schłodzonych), tak by było jasne, czy mrożone kręgosłupy łososia objęte są definicją przedmiotowego produktu.

⁽¹⁾ Dz.U. L 56 z 6.3.1996, str. 1. Rozporządzenie ostatnio zmienione rozporządzeniem (WE) nr 2117/2005 (Dz.U. L 340 z 23.12.2005, str. 17).

⁽²⁾ Dz.U. L 15 z 20.1.2006, str. 1.

Należy zatem dokonać przeglądu sprawy w odniesieniu do zakresu definicji produktu, a decyzja go dotycząca może mieć skutek wsteczny od daty nałożenia odpowiednich środków. Wszystkie podmioty gospodarcze, a w szczególności importerów, wzywa się do przedstawienia opinii dotyczących powyższej kwestii oraz do przedłożenia dowodów potwierdzających te opinie.

4. Procedura

Po konsultacji z Komitetem Doradczym i ustaleniu, że istnieją wystarczające dowody uzasadniające wszczęcie częściowego przeglądu okresowego, Komisja niniejszym wszczyna przegląd zgodnie z art. 11 ust. 3 rozporządzenia podstawowego, ograniczony do zbadania zakresu produktu.

a) Kwestionariusze

W celu uzyskania informacji uznanych za niezbędne dla dochodzenia Komisja prześle kwestionariusze do przemysłu wspólnotowego, do innych znanych producentów wspólnotowych, do znanych importerów, do znanych użytkowników, do znanych producentów eksportujących w Norwegii i do władz tego kraju. Wymienione informacje i dowody je potwierdzające powinny wpłynąć do Komisji w terminie określonym w pkt 5 lit. a).

b) Gromadzenie informacji i przeprowadzanie przesłuchań

Wszystkie zainteresowane strony niniejszym wzywa się do przedstawienia opinii, do przedłożenia informacji, w tym także informacji innych niż odpowiedzi udzielone na pytania zawarte w kwestionariuszu, oraz do dostarczenia dowodów potwierdzających zgłaszane fakty. Wymienione informacje i dowody je potwierdzające powinny wpłynąć do Komisji w terminie określonym w pkt 5 lit. a).

Ponadto Komisja może przesłuchiwać zainteresowane strony, pod warunkiem że wystąpiły one z wnioskiem o przesłuchanie, wskazując szczególne powody, dla których powinny zostać wysłuchane. Wniosek taki należy złożyć w terminie określonym w pkt 5 lit. b).

5. Terminy

a) Dla stron zgłaszających się, udzielających odpowiedzi na pytania zawarte w kwestionariuszu i przedkładających inne informacje

Wszystkie zainteresowane strony, jeżeli ich wnioski mają być uwzględnione podczas dochodzenia, muszą zgłosić się do Komisji, przedstawić swoje opinie i przedłożyć odpowiedzi na pytania zawarte w kwestionariuszu lub przedstawić wszelkie inne informacje w terminie 40 dni od daty opublikowania niniejszego zawiadomienia w *Dzienniku Urzędowym Unii Europejskiej*, o ile nie wskazano inaczej. Należy zwrócić uwagę na fakt, iż korzystanie z większości praw proceduralnych ustanowionych w rozporządzeniu podstawowym jest uwarunkowane zgłoszeniem się przez stronę w wyżej wymienionym terminie.

b) Przesłuchania

Wszystkie zainteresowane strony mogą również składać wnioski o przesłuchanie przez Komisję w takim samym terminie 40 dni.

6. Oświadczenia pisemne, odpowiedzi na pytania zawarte w kwestionariuszu i korespondencja

Wszelkie oświadczenia i wnioski przedkładane przez zainteresowane strony należy składać na piśmie (nie w formie elektronicznej, chyba że ustalono inaczej); należy w nich wskazać nazwę, adres, adres e-mail, numery telefonu i faksu lub teleksu zainteresowanej strony. Wszelkie oświadczenia pisemne, łącznie z informacjami wymaganymi w niniejszym zawiadomieniu, odpowiedzi na pytania zawarte w kwestionariuszu i korespondencję dostarczaną przez zainteresowane strony na zasadzie poufności należy oznakować „*Limited*” ⁽¹⁾ oraz, zgodnie z art. 19 ust. 2 rozporządzenia podstawowego, dołączyć do nich wersję bez klauzuli poufności, oznakowaną „*Do wglądu zainteresowanych stron*”.

⁽¹⁾ Oznacza to, że dokument przeznaczony jest jedynie do użytku wewnętrznego. Jest on chroniony zgodnie z art. 4 rozporządzenia (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 (Dz.U. L 145 z 31.5.2001, str. 43). Jest to dokument poufny zgodnie z art. 19 rozporządzenia podstawowego i art. 6 Porozumienia WTO o stosowaniu artykułu VI GATT z 1994 r. (porozumienie antydumpingowe).

Adres Komisji do celów korespondencji:

European Commission
Directorate General for Trade
Directorate H
Office: J-79 4/23
B-1049 Brussels
Faks: (32-2) 295 65 05

7. Brak współpracy

W przypadkach, w których zainteresowana strona odmawia dostępu do niezbędnych informacji, nie dostarcza ich w określonych terminach albo znacznie utrudnia dochodzenie, istnieje możliwość dokonania ustaleń tymczasowych lub końcowych, potwierdzających lub zaprzeczających, na podstawie dostępnych faktów, zgodnie z art. 18 rozporządzenia podstawowego.

W przypadku ustalenia, że zainteresowana strona dostarczyła nieprawdziwe lub wprowadzające w błąd informacje, informacje te nie są brane pod uwagę, a ustalenia mogą być dokonywane na podstawie dostępnych faktów, zgodnie z art. 18 rozporządzenia podstawowego. Jeżeli zainteresowana strona nie współpracuje lub współpracuje jedynie częściowo i z tego względu ustalenia opierają się na dostępnych faktach zgodnie z art. 18 rozporządzenia podstawowego, wynik może być mniej korzystny dla wymienionej strony niż w przypadku, gdyby strona ta współpracowała.

8. Harmonogram dochodzenia

Dochodzenie zostanie zamknięte, zgodnie z art. 11 ust. 5 rozporządzenia podstawowego, w terminie 15 miesięcy począwszy od daty opublikowania niniejszego zawiadomienia w *Dzienniku Urzędowym Unii Europejskiej*.

9. Inne przeglądy okresowe zgodnie z art. 11 ust. 3 rozporządzenia podstawowego

Zakres bieżącego przeglądu przedstawiono w pkt 3 powyżej. Wszystkie strony pragnące złożyć wniosek o przeprowadzenie przeglądu na innej podstawie mogą to uczynić zgodnie z przepisami art. 11 ust. 3 rozporządzenia podstawowego.

Bieżący przegląd zakresu produktu nie ma wpływu na okres stosowania aktualnie obowiązujących środków antydumpingowych.

10. Przetwarzanie danych osobowych

Należy zauważyć, iż wszelkie dane osobowe zgromadzone podczas niniejszego dochodzenia będą traktowane 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 ⁽¹⁾.

11. Rzecznik praw stron

Należy również zauważyć, że w przypadku napotkania przez zainteresowane strony problemów związanych z korzystaniem z prawa do obrony strony te mogą wystąpić o interwencję urzędnika DG ds. Handlu pełniącego rolę rzecznika praw stron. Pośredniczy on w kontaktach między zainteresowanymi stronami i służbami Komisji, zapewniając, w stosownych przypadkach, mediację w kwestiach proceduralnych związanych z ochroną interesów stron podczas postępowania, w szczególności w odniesieniu do spraw dotyczących dostępu do akt, poufności, przedłużenia terminów oraz rozpatrywania pisemnych lub ustnych oświadczeń lub uwag. Dodatkowe informacje i dane kontaktowe zainteresowane strony mogą uzyskać na stronach internetowych rzecznika praw stron w DG ds. Handlu (<http://ec.europa.eu/trade>).

⁽¹⁾ Dz.U. L 8 z 12.1.2001, str. 1.

PROCEDURY ZWIĄZANE Z REALIZACJĄ POLITYKI KONKURENCJI

KOMISJA

Uprzednie zgłoszenie koncentracji

(Sprawa COMP/M.5231 — Bain Capital/D&M)

Sprawa kwalifikująca się do rozpatrzenia w ramach procedury uproszczonej

(Tekst mający znaczenie dla EOG)

(2008/C 181/10)

1. W dniu 9 lipca 2008 r. do Komisji wpłynęło zgłoszenie planowanej koncentracji, dokonane na podstawie art. 4 rozporządzenia Rady (WE) nr 139/2004 ⁽¹⁾, zgodnie z którym przedsiębiorstwo Bain Capital Investors LLC (USA) nabywa kontrolę nad całością przedsiębiorstwa D&M Holdings Inc. (Japonia) w rozumieniu art. 3 ust. 1 lit. b) wymienionego rozporządzenia w drodze publicznej oferty przejęcia.

2. Dziedziny działalności gospodarczej zainteresowanych przedsiębiorstw są następujące:

- przedsiębiorstwo Bain Capital Investors LLC: inwestycje typu private equity,
- przedsiębiorstwo D&M Holdings Inc.: projektowanie, produkcja, marketing i dystrybucja elektronicznego sprzętu audio-wizualnego.

3. Po wstępnej analizie Komisja uznała, zastrzegając sobie jednocześnie prawo do ostatecznej decyzji w tej kwestii, iż zgłoszona transakcja może wchodzić w zakres zastosowania rozporządzenia (WE) nr 139/2004. Należy zauważyć, iż zgodnie z obwieszczeniem Komisji w sprawie procedury uproszczonej stosowanej do niektórych koncentracji w rozumieniu rozporządzenia Rady (WE) nr 139/2004 ⁽²⁾, sprawa ta kwalifikuje się do rozpatrzenia w ramach procedury określonej w tym obwieszczeniu.

4. Komisja zaprasza zainteresowane strony trzecie do przedłożenia jej ewentualnych uwag o planowanej koncentracji.

Spostrzeżenia te muszą dotrzeć do Komisji nie później niż w ciągu 10 dni od daty niniejszej publikacji. Mogą one zostać nadesłane Komisji za pomocą faksu (nr faksu: (32-2) 296 43 01 lub 296 72 44) lub listownie, z zaznaczonym numerem referencyjnym: COMP/M.5231 — Bain Capital/D&M, na adres:

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

⁽¹⁾ Dz.U. L 24 z 29.1.2004, str. 1.

⁽²⁾ Dz.U. C 56 z 5.3.2005, str. 32.

Zgłoszenie zamiaru koncentracji
(Sprawa COMP/M.5227 — Robert Bosch/Samsung/JV)

(Tekst mający znaczenie dla EOG)

(2008/C 181/11)

1. W dniu 10 lipca 2008 r. zgodnie z art. 4 rozporządzenia Rady (WE) nr 139/2004 ⁽¹⁾, Komisja otrzymała zgłoszenie planowanej koncentracji, w wyniku której przedsiębiorstwa Robert Bosch GmbH („Bosch”, Niemcy) oraz Samsung SDI Co. Ltd („Samsung SDI”, Korea Południowa) przejmują w rozumieniu art. 3 ust. 1 lit. b) rozporządzenia Rady wspólną kontrolę nad przedsiębiorstwem SB LiMotive Ltd („SB LiMotive”, Korea Południowa) w drodze zakupu udziałów w nowo utworzonej spółce joint venture.

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

- w przypadku przedsiębiorstwa Bosch: technologie w przemyśle motoryzacyjnym, technologia przemysłowa, technologia budowlana, artykuły konsumpcyjne,
- w przypadku przedsiębiorstwa Samsung SDI: wyświetlacze do monitorów, telefonów komórkowych i innych urządzeń przenośnych, akumulatory do telefonów komórkowych, laptopów, aparatów fotograficznych i kamer wideo,
- w przypadku przedsiębiorstwa SB LiMotive: opracowywanie, produkcja i sprzedaż systemów akumulatorów litowo-jonowych stosowanych w pojazdach elektrycznych hybrydowych i innych pojazdach elektrycznych.

3. Po wstępnej analizie Komisja uznała, że zgłoszona koncentracja może wchodzić w zakres rozporządzenia (WE) nr 139/2004. 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 przysyłać do Komisji faksem (nr faksu: (32-2) 296 43 01 lub 296 72 44) lub listownie, podając numer referencyjny: COMP/M.5227 — Robert Bosch/Samsung/JV, na poniższy adres Dyrekcji Generalnej ds. Konkurencji Komisji Europejskiej:

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

⁽¹⁾ Dz.U. L 24 z 29.1.2004, str. 1.

Zgłoszenie zamiaru koncentracji**(Sprawa COMP/M.5267 — Sun Capital/SCS Group)****Sprawa, która może kwalifikować się do rozpatrzenia w ramach procedury uproszczonej****(Tekst mający znaczenie dla EOG)**

(2008/C 181/12)

1. W dniu 9 lipca 2008 r. zgodnie z art. 4 rozporządzenia Rady (WE) nr 139/2004 ⁽¹⁾, Komisja otrzymała zgłoszenie planowanej koncentracji, w wyniku której przedsiębiorstwo Sun Capital Partners V, L.P. („Sun Capital”, Stany Zjednoczone) przejmuje w rozumieniu art. 3 ust. 1 lit. b) rozporządzenia Rady kontrolę nad operacyjnymi elementami przedsiębiorstwa SCS Upholstery plc („SCS Group”, Zjednoczone Królestwo), tj. nad Share & Sons Ltd w drodze zakupu akcji.

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

— w przypadku Sun Capital: inwestycje na niepublicznym rynku kapitałowym,

— w przypadku SCS Group: wyspecjalizowany sprzedawca detaliczny mebli tapicerowanych w Zjednoczonym Królestwie.

3. Po wstępnej analizie Komisja uznała, że zgłoszona koncentracja może wchodzić w zakres rozporządzenia (WE) nr 139/2004. 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 Rady (WE) nr 139/2004 ⁽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 przysyłać do Komisji faksem (nr faksu: (32-2) 296 43 01 lub 296 72 44) lub listownie, podając numer referencyjny: COMP/M.5267 — Sun Capital/SCS Group, na poniższy adres Dyrekcji Generalnej ds. Konkurencji Komisji Europejskiej:

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

⁽¹⁾ Dz.U. L 24 z 29.1.2004, str. 1.

⁽²⁾ Dz.U. C 56 z 5.3.2005, str. 32.

SPROSTOWANIA**Sprostowanie do zaproszenia do składania wniosków dotyczących instrumentu LIFE+ na 2008 r.**

(Dziennik Urzędowy Unii Europejskiej C 178 z dnia 15 lipca 2008 r.)

(2008/C 181/13)

Strona 23, termin zgłoszeń:

zamiast: „21 października 2008 r.”,

powinno być: „21 listopada 2008”.
