ISSN 1725-5228

Dziennik Urzędowy C 279
Unii Europejskiej

Wydanie polskie

Tom 54
23 września 2011

Informacje i zawiadomienia

Powiadomienie nr | Spis treści | Strona

I *Rezolucje, zalecenia i opinie*

OPINIE

Europejski Inspektor Ochrony Danych

2011/C 279/01 Opinia Europejskiego Inspektora Ochrony Danych na temat sprawozdania z oceny Komisji dla Rady i Parlamentu Europejskiego w sprawie dyrektywy w sprawie zatrzymywania danych (dyrektywa 2006/24/WE) 1

2011/C 279/02 Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (WE) nr 1073/1999 dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) i uchylającego rozporządzenie (Euratom) nr 1074/1999 11

2011/C 279/03 Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie integralności i przejrzystości rynku energii 20

II *Komunikaty*

KOMUNIKATY INSTYTUCJI, ORGANÓW I JEDNOSTEK ORGANIZACYJNYCH UNII EUROPEJSKIEJ

Komisja Europejska

2011/C 279/04 Brak sprzeciwu wobec zgłoszonej koncentracji (Sprawa COMP/M.6349 – Motherson/Cross Industries/Peguform/Wethje) [1] 28

PL

Cena: 3 EUR

[1] Tekst mający znaczenie dla EOG

(Ciąg dalszy na następnej stronie)

Powiadomienie nr | Spis treści (ciąg dalszy) | Strona

2011/C 279/05 Brak sprzeciwu wobec zgłoszonej koncentracji (Sprawa COMP/M.6218 – Ineos/Tessenderlo Group S-PVC Assets) [1] 28

IV *Informacje*

INFORMACJE INSTYTUCJI, ORGANÓW I JEDNOSTEK ORGANIZACYJNYCH UNII EUROPEJSKIEJ

Komisja Europejska

2011/C 279/06 Kursy walutowe euro 29

V *Ogłoszenia*

POSTĘPOWANIA ADMINISTRACYJNE

Komisja Europejska

2011/C 279/07 MEDIA 2007 – Rozwój, dystrybucja, promocja i szkolenia – Zaproszenie do składania wniosków – EACEA/21/11 – Wspieranie rozwoju projektów produkcji filmów fabularnych, filmow dokumentalnych i filmów animowanych w ramach schematu „Projekty pojedyncze" oraz „Pakiety projektów" I i II etap 30

2011/C 279/08 MEDIA 2007 – Rozwój, dystrybucja, promocja i szkolenia – Zaproszenie do składania wniosków – EACEA/22/11 – Wspieranie rozwoju projektów interaktywnych online i offline 33

POSTĘPOWANIA ZWIĄZANE Z REALIZACJĄ POLITYKI KONKURENCJI

Komisja Europejska

2011/C 279/09 Zgłoszenie zamiaru koncentracji (Sprawa COMP/M.6348 – Arla Foods/Allgäuland) [1] 36

2011/C 279/10 Zgłoszenie zamiaru koncentracji (Sprawa COMP/M.6392 – Gores/Mexx) – Sprawa, która może kwalifikować się do rozpatrzenia w ramach procedury uproszczonej [1] 37

PL

[1] Tekst mający znaczenie dla EOG

I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych na temat sprawozdania z oceny Komisji dla Rady i Parlamentu Europejskiego w sprawie dyrektywy w sprawie zatrzymywania danych (dyrektywa 2006/24/WE)

(2011/C 279/01)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

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

uwzględniając Kartę praw podstawowych Unii Europejskiej, a w szczególności art. 7 i 8,

uwzględniając dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych ([1]),

uwzględniając dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej ([2]),

uwzględniając rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych ([3]), a w szczególności art. 41,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. **WPROWADZENIE**

I.1. **Publikacja sprawozdania**

1. W dniu 18 kwietnia 2011 r. Komisja przedstawiła swoje sprawozdanie z oceny na temat dyrektywy w sprawie zatrzymywania danych (zwane dalej „sprawozdaniem z oceny") ([4]). Sprawozdanie zostało przesłane do wiadomości EIOD tego samego dnia. Z powodów określonych w części I.2 poniżej, EIOD wydaje niniejszą opinię z własnej inicjatywy, zgodnie z art. 41 rozporządzenia (WE) nr 45/2001.

2. Przed przyjęciem komunikatu EIOD miał możliwość przekazania nieformalnych uwag. EIOD wyraża zadowolenie, że wiele z tych uwag zostało uwzględnionych przez Komisję przy pracy nad ostateczną wersją dokumentu.

3. Komisja opracowała sprawozdanie z oceny w celu spełnienia obowiązku wynikającego z art. 14 dyrektywy w sprawie zatrzymywania danych, związanego z oceną stosowania dyrektywy, oraz jego wpływu na podmioty gospodarcze i konsumentów, aby stwierdzić, czy konieczna jest zmiana przepisów dyrektywy ([5]). EIOD z zadowoleniem stwierdza, iż mimo że nie jest to ściśle wymagane zgodnie z art. 14, Komisja uwzględniła również w sprawozdaniu „implikacje dyrektywy dla praw podstawowych, w świetle krytyki, którą podnoszono ogólnie w odniesieniu do zatrzymywania danych" ([6]).

I.2. **Przyczyny i cel niniejszej opinii EIOD**

4. Dyrektywa w sprawie zatrzymywania danych stanowiła odpowiedź UE na pilne wyzwania związane z bezpieczeństwem po zamachach terrorystycznych w Madrycie w 2004 r. i Londynie w 2005 r. Pomimo zgodnego z prawem celu ustanowienia mechanizmu zatrzymywania danych, pojawiły się głosy krytyczne w związku z olbrzymim wpływem, jaki środek miał na prywatność obywateli.

5. Obowiązek zatrzymywania danych zgodnie z dyrektywą w sprawie zatrzymywania danych pozwala właściwym władzom krajowym prześledzenie połączeń telefonicznych i internetowych wszystkich osób w UE za każdym razem, kiedy korzystają z telefonu lub Internetu, w okresie do dwóch lat.

([1]) Dz.U. L 281 z 23.11.1995, s. 31.
([2]) Dz.U. L 201 z 31.7.2002, s. 37, zmieniona dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r., Dz.U. L 337 z 18.12.2009, s. 11.
([3]) Dz.U. L 8 z 12.1.2001, s. 1.
([4]) COM(2011) 225 wersja ostateczna.
([5]) Dyrektywa w sprawie zatrzymywania danych (dyrektywa 2006/24/WE) została przyjęta w dniu 15 marca 2006 r. i opublikowana w Dz.U. L 105 z 13.4.2006, s. 54. Termin wydania raportu określono na dzień 15 września 2010 r., zob. art. 14 ust. 1 dyrektywy w sprawie zatrzymywania danych.
([6]) Zob. s. 1 sprawozdania z oceny.

6. Zatrzymywanie danych telekomunikacyjnych stanowi w jasny sposób ingerencję w prawo do poszanowania prywatności zainteresowanych osób zgodnie z art. 8 Europejskiej Konwencji Praw Człowieka (zwanej dalej „Konwencją") oraz art. 7 Karty praw podstawowych UE.

7. Europejski Trybunał Praw Człowieka wielokrotnie stwierdzał, że „samo zatrzymywanie danych dotyczących prywatnego życia poszczególnych osób stanowi ingerencję w rozumieniu art. 8 [Konwencji]" ([7]). W szczególności w odniesieniu do danych telefonicznych Europejski Trybunał Praw Człowieka stwierdził, że „ujawnianie tych informacji policji bez zgody abonenta stanowi […] ingerencję w prawo gwarantowane przez art. 8 [Konwencji]" ([8]).

8. Z art. 8 ust. 2 Konwencji i art. 52 ust. 1 Karty praw podstawowych UE wynika, że ingerencja może być uzasadniona, o ile stanowi tak prawo, służy to uzasadnionemu celowi oraz jest niezbędne w społeczeństwie demokratycznym do osiągnięcia celu zgodnego z prawem.

9. EIOD potwierdza, że dostępność pewnych danych dotyczących ruchu i lokalizacji może być kluczowa dla organów wymiaru sprawiedliwości w zwalczaniu terroryzmu i innych poważnych przestępstw. Równocześnie jednak EIOD wielokrotnie wyrażał wątpliwości, co do uzasadnienia zatrzymywania danych na taką skalę w świetle prawa do poszanowania prywatności i ochrony danych ([9]). Te wątpliwości podziela wiele organizacji społeczeństwa obywatelskiego ([10]).

10. EIOD z bliska przyglądał się na różne sposoby opracowywaniu, wdrażaniu i ocenie dyrektywy od 2005 r. W 2005 r. EIOD wydał krytyczną opinię po tym, jak Komisja opublikowała swój wniosek w sprawie dyrektywy ([11]). Po przyjęciu dyrektywy EIOD został członkiem grupy ekspertów ds. zachowywania danych, o której mowa w motywie 14 dyrektywy w sprawie zatrzymywania danych ([12]). Ponadto EIOD uczestniczy w pracach grupy roboczej powołanej na mocy art. 29, która opublikowała wiele dokumentów w tej sprawie, ostatnio w lipcu 2010 r. – sprawozdanie na temat stosowania dyrektywy w praktyce ([13]). EIOD działał również w charakterze interwenienta w sprawie przed Europejskim Trybunałem Sprawiedliwości, w której podnoszono kwestię ważności dyrektywy ([14]).

11. Nie można przeceniać znaczenia sprawozdania z oceny i procesu oceny ([15]). Dyrektywa w sprawie zatrzymywania danych stanowi doskonały przykład środka UE mającego na celu zapewnienie dostępności danych generowanych i przetwarzanych w kontekście komunikacji elektronicznej do egzekwowania prawa. Ponieważ środek istnieje już od kilku lat, ocena jego praktycznego stosowania powinna wykazać niezbędność i proporcjonalność środka w świetle prawa do poszanowania prywatności i ochrony danych. W tym kontekście EIOD nazwał ocenę „chwilą prawdy" dla dyrektywy w sprawie zatrzymywania danych ([16]).

12. Obecny proces oceny ma również implikacje dla innych instrumentów regulujących zarządzanie informacjami, w tym przetwarzanie olbrzymich ilości danych osobowych w obszarze wolności, bezpieczeństwa i sprawiedliwości. W komunikacie z 2010 r. Komisja stwierdziła, że mechanizmy oceny różnych instrumentów wskazują na duże zróżnicowanie ([17]). EIOD jest zdania, że obecną procedurę oceny należy wykorzystać do ustalenia standardu oceny innych instrumentów UE i zapewnienia pozostawienia wyłącznie w pełni uzasadnionych środków.

13. W związku z tym EIOD pragnie podzielić się w upublicznionej opinii uwagami w sprawie ustaleń przedstawionych w sprawozdaniu z oceny. Dzieje się to na wczesnym etapie procesu w celu wniesienia rzeczywistego i konstruktywnego wkładu w przyszłe dyskusje, prawdopodobnie w kontekście nowego wniosku legislacyjnego, o którym mowa w sprawozdaniu z oceny Komisji ([18]).

I.3. **Struktura opinii**

14. W niniejszej opinii zostanie przeanalizowana i omówiona treść sprawozdania z oceny z punktu widzenia poszanowania prywatności i ochrony danych. Analiza skupi się na tym, czy obecna dyrektywa w sprawie zatrzymywania danych spełnia wymagania określone przez te dwa prawa podstawowe. Obejmuje to analizę tego, czy konieczność zatrzymywania danych regulowana w dyrektywie została wystarczająco wykazana.

15. Niniejsza opinia zorganizowana jest w następujący sposób: część II zawiera opis najważniejszych przepisów dyrektywy

([7]) Zob. np. Europejska Konwencja Praw Człowieka, wyrok z dnia 4 grudnia 2008 r. w sprawie *S. i Marper* v. *UK*, 30562/04 i 30566/04, pkt 67.

([8]) Zob. Europejska Konwencja Praw Człowieka, wyrok z dnia 2 sierpnia 1984 r. w sprawie *Malone* v. *UK*, A-82, pkt 84.

([9]) Zob. opinia EIOD z dnia 26 września 2005 r., Dz.U. C 298 z 29.11.2005, s. 1. Podczas konferencji zorganizowanej przez Komisję w grudniu 2010 r. EIOD odniósł się do instrumentu jako do „najsilniej ingerującego instrumentu kiedykolwiek przyjętego przez UE, jeśli chodzi o zakres i liczbę osób, których dotyczy", zob. wystąpienie z dnia 3 grudnia 2010 r., które znajduje się na stronie internetowej EIOD (http://www.edps.europa.eu) w zakładce „Publications" >> „Speeches & Articles" >> „2010".

([10]) Te wątpliwości podziela wiele organizacji społeczeństwa obywatelskiego (http://www.vorratsdatenspeicherung.de/images/DRletter_Malmstroem.pdf).

([11]) Zob. opinia EIOD, o której mowa w przypisie 9.

([12]) Zob. również decyzję Komisji z dnia 25 marca 2008 r., Dz.U. L 111 z 23.4.2008, s. 11.

([13]) Zob. grupa robocza 172 z dnia 13 lipca 2010 r., sprawozdanie 1/2010 w sprawie drugiego wspólnego egzekwowania.

([14]) Zob. ETS, wyrok z dnia 10 lutego 2009 r. w sprawie *Irlandia* przeciwko *Parlamentowi i Radzie*, C-301/06. W tej sprawie zob. również pkt 29 poniżej.

([15]) EIOD już podkreślał w swojej opinii z 2005 r. znaczenie obowiązku dokonania oceny instrumentu (zob. przypis 9, pkt 72–73).

([16]) Zob. wystąpienie z dnia 3 grudnia 2010 r., o którym mowa w przypisie 9.

([17]) COM(2010) 385 z dnia 20 lipca 2010 r., Przegląd zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, s. 24. W sprawie tego komunikatu zob. opinię EIOD z dnia 30 września 2010 r., która znajduje się na stronie internetowej EIOD (http://www.edps.europa.eu) w zakładce „Consultation" >> „Opinions" >> „2010".

([18]) Zob. s. 32 sprawozdania z oceny.

w sprawie zatrzymywania danych oraz jej związków z dyrektywą 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dalej: „dyrektywa o prywatności i łączności elektronicznej") ([19]). W części III krótko zostaną przedstawione zmiany wprowadzone przez traktat lizboński, gdyż odnoszą się one w szczególności do bieżącej sprawy i mają bezpośrednie konsekwencje dla sposobu, w jaki należy postrzegać, oceniać i – ewentualnie – zmieniać przepisy UE w sprawie zatrzymywania danych. Najdłuższa część opinii, część IV, zawiera analizę ważności dyrektywy w sprawie zatrzymywania danych w świetle prawa do poszanowania prywatności i ochrony danych oraz z myślą o ustaleniach przedstawionych w sprawozdaniu z oceny. W części V omówione zostaną możliwe dalsze działania. Opinię kończą wnioski zawarte w części VI.

II. **PRZEPISY UE W ZAKRESIE ZATRZYMYWANIA DANYCH**

16. W kontekście niniejszej opinii zatrzymywanie danych odnosi się do obowiązku nałożonego na dostawców powszechnie dostępnych usług komunikacji elektronicznej lub publicznych sieci komunikacyjnych do zatrzymywania danych dotyczących ruchu i danych, a także powiązanych danych niezbędnych do zidentyfikowania abonenta lub użytkownika, przez określony okres. Obowiązek ten wprowadza dyrektywa w sprawie zatrzymywania danych, w której w art. 5 ust. 1 określono kategorie zatrzymywanych danych. Zgodnie z art. 6 dyrektywy w sprawie zatrzymywania danych państwa członkowskie gwarantują, że dane są zatrzymywane na okresy nie krótsze niż sześć miesięcy oraz nie dłuższe niż dwa lata od daty połączenia.

17. Dane są zatrzymywane, o ile dane te są generowane lub przetwarzane przez dostawców w procesie dostarczania przedmiotowych usług łączności. Obejmuje to również dane związane z nieskutecznymi próbami połączenia. Zgodnie z dyrektywą (art. 5 ust. 1) nie można zatrzymywać żadnych danych ujawniających treść komunikacji.

18. Dane są zatrzymywane w celu zapewnienia ich dostępności do celu „dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego" (art. 1 ust. 1).

19. Dyrektywa w sprawie zatrzymywania danych nie zawiera dalszych przepisów w sprawie warunków, na jakich właściwe władze krajowe mogą mieć dostęp do zatrzymywanych danych. Leży to w gestii państw członkowskich i wykracza poza zakres dyrektywy. W art. 4 dyrektywy podkreślono, że przepisy krajowe powinny być zgodne z wymogami niezbędności i proporcjonalności, określonymi w szczególności w Konwencji.

20. Dyrektywa w sprawie zatrzymywania danych jest ściśle powiązana z dyrektywą o prywatności elektronicznej. Dyrektywa ta, uszczegółowiająca i uzupełniająca ogólną dyrektywę w sprawie ochrony danych 95/46/WE, określa, że państwa członkowskie zapewniają poufność łączności i powiązanych danych o ruchu ([20]). Dyrektywa o prywatności elektronicznej wymaga, by dane o ruchu i lokalizacji wygenerowane w wyniku korzystania z usług komunikacji elektronicznej były usuwane lub uczynione anonimowymi, gdy nie będą już potrzebne do celów przesyłu w ramach komunikacji, chyba że są one niezbędne w celu naliczania opłat i tylko tak długo, jak będzie to niezbędne ([21]). Niektóre dane mogą być przetwarzane przez okres niezbędny do świadczenia usług o wartości dodanej, pod warunkiem uzyskania zgody.

21. Na podstawie art. 15 ust. 1 dyrektywy o prywatności elektronicznej państwa członkowskie mają możliwość przyjmowania środków prawnych ograniczających zakres wspomnianych wyżej zobowiązań, jeżeli „takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (np. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych […]". Ta kwestia zatrzymywania danych jest przywołana *explicite* w art. 15 ust. 1 dyrektywy o prywatności elektronicznej. Państwa członkowskie mogą „uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas" uzasadnione we wspomniany sposób.

22. Dyrektywa w sprawie zatrzymywania danych miała na celu dostosowanie inicjatyw państw członkowskich na mocy art. 15 ust. 1 w zakresie zatrzymywania danych do celów dochodzenia, wykrywania i ścigania poważnych przestępstw. Należy podkreślić, że dyrektywa w sprawie zatrzymywania danych stanowi wyjątek od ogólnego obowiązku wynikającego z dyrektywy o prywatności elektronicznej, zgodnie z którym dane należy usunąć, gdy nie są już potrzebne ([22]).

23. Wraz z przyjęciem dyrektywy w sprawie zatrzymywania danych dodano dodatkowy ustęp 1a w art. 15 dyrektywy o prywatności elektronicznej, w którym stwierdza się, że art. 15 ust. 1 nie ma zastosowania do danych, które w sposób szczególny na mocy dyrektywy w sprawie zatrzymywania danych mają być zatrzymywane do celów określonych w art. 1 ust. 1 tej dyrektywy.

24. W sprawozdaniu z oceny stwierdzono, że art. 15 ust. 1 i art. 15 ust. 1b są stosowane przez niektóre państwa członkowskie w celu wykorzystania danych zatrzymywanych na mocy dyrektywy o zatrzymywaniu danych również do innych celów, co zostanie dalej omówione w części IV.3 poniżej ([23]). EIOD odniósł się do tej kwestii jako do „luki prawnej" w przepisach, która uniemożliwia osiągnięcie celu dyrektywy w sprawie zatrzymywania danych, którym jest stworzenie takich samych warunków działania dla całego sektora ([24]).

([19]) Porównaj: przypis 2.

([20]) Zob. art. 5 dyrektywy o prywatności elektronicznej.

([21]) Zob. art. 6 dyrektywy o prywatności elektronicznej.

([22]) Zob. również grupa robocza 29 w sprawozdaniu z dnia 13 lipca 2010 r., o którym mowa w przypisie 13, s. 1.

([23]) Zob. s. 4 sprawozdania z oceny. Zob. również w tym kontekście motyw 12 dyrektywy w sprawie zatrzymywania danych.

([24]) Zob. wystąpienie z dnia 3 grudnia 2010 r., o którym mowa w przypisie 9, s. 4.

III. **PO LIZBONIE ZMIENIŁ SIĘ OGÓLNY KONTEKST PRAWNY UE**

25. Ogólny kontekst prawny UE w odniesieniu do dyrektywy w sprawie zatrzymywania danych zmienił się w znaczący sposób z wejściem w życie traktatu lizbońskiego. Istotną zmianą było zniesienie struktury opartej na filarach, która ustanawiała różne procedury legislacyjne i mechanizmy przeglądu dla różnych obszarów kompetencji UE.

26. Wcześniejsza struktura oparta na filarach wywoływała dyskusje dotyczące właściwej podstawy prawnej instrumentu UE, jeżeli dana kwestia leżała w kompetencjach UE należących do różnych filarów. Wybór podstawy prawnej nie był bez znaczenia, ponieważ prowadził do różnych procedur legislacyjnych w odniesieniu do, przykładowo, wymogu głosowania w Radzie (większość kwalifikowana lub jednomyślność) lub udziału Parlamentu Europejskiego.

27. Dyskusje te odnosiły się ściśle do zatrzymywania danych. Ponieważ celem dyrektywy w sprawie zatrzymywania danych była harmonizacja obowiązków dla operatorów i tym samym wyeliminowanie przeszkód dla rynku wewnętrznego, podstawę prawną można było znaleźć w art. 95 poprzedniego Traktatu WE (stary pierwszy filar). Do kwestii można jednak było podejść od strony egzekwowania prawa, argumentując, że celem przechowywania danych było zwalczanie poważnych przestępstw w ramach współpracy policyjnej i sądowej w sprawach karnych zgodnie ze starym Traktatem UE (poprzednio trzeci filar) ([25]).

28. Ostatecznie dyrektywa w sprawie zatrzymywania danych została przyjęta w oparciu o art. 95 poprzedniego Traktatu WE, regulując jedynie obowiązki operatorów. Dyrektywa nie określała zasad dostępu ani wykorzystywania zatrzymywanych danych przez wymiar sprawiedliwości.

29. Ważność dyrektywy po jej przyjęciu była badana przez Trybunał Sprawiedliwości. Twierdzono, że dyrektywę należało oprzeć na trzecim filarze zamiast na pierwszym, ponieważ cel, dla którego dane miały być zatrzymywane (dochodzenie, wykrywanie oraz ściganie poważnych przestępstw), leżał w zakresie kompetencji UE w ramach trzeciego filaru ([26]). Ponieważ jednak działania właściwych organów *explicite* znalazły się poza zakresem dyrektywy, Trybunał Sprawiedliwości stwierdził, że dyrektywa słusznie oparta jest na Traktacie WE ([27]).

30. Od początku EIOD twierdził, że jeżeli UE przyjęłaby instrument w sprawie zatrzymywania danych, powinien on regulować obowiązek operatorów, a także dostęp i przyszłe wykorzystanie danych przez organy wymiaru sprawiedliwości. W opinii z 2005 r. w sprawie wniosku Komisji EIOD podkreślał, że dostęp i dalsze wykorzystanie danych przez właściwe władze krajowe stanowiły kluczową i niemożliwą do wyodrębnienia część przedmiotowej kwestii ([28]).

31. Negatywny wpływ uregulowania przez UE jedynie połowy kwestii potwierdza przedmiotowe sprawozdanie z oceny, co zostanie rozwinięte w dalszej części opinii. Komisja stwierdza, że różnice w prawie krajowym w zakresie dostępu i dalszego wykorzystania przez właściwe władze krajowe doprowadziły do „znacznych trudności" dla operatorów ([29]).

32. Wraz ze zniesieniem struktury opartej na filarach po wejściu w życie traktatu lizbońskiego w TFUE dwa przedmiotowe obszary kompetencji UE zostały połączone, co pozwala na przyjmowanie przepisów prawa UE w oparciu o tę samą procedurę legislacyjną. Ten nowy kontekst umożliwia przyjęcie nowego wspólnego instrumentu w sprawie zatrzymywania danych, regulującego obowiązki operatorów oraz warunki dostępu i dalszego wykorzystania przez organy wymiaru sprawiedliwości. Prawo do poszanowania prywatności i ochrony danych, jak wyjaśniono w części IV.3 poniżej, wymaga uregulowania tej kwestii w całości, o ile rozważany byłby zmieniony środek UE w sprawie zatrzymywania danych.

33. Traktat lizboński nie tylko zniósł strukturę opartą na filarach, ale również nadał Karcie praw podstawowych, dotychczas niewiążącej, zawierającej prawo do poszanowania prywatności i ochrony danych w art. 7 i 8, taką samą wartość prawną jak traktatom ([30]). Podmiotowe prawo do ochrony danych zostało również zawarte w art. 16 TFUE, tworząc odrębną podstawę prawną dla instrumentów UE o ochronie danych osobowych.

34. Ochrona praw podstawowych od dawna stanowi podstawę polityki UE, a traktat lizboński doprowadził do jeszcze silniejszego zaangażowania w poszanowanie tych praw w kontekście UE. Zmiany wynikające z traktatu lizbońskiego zachęciły Komisję w październiku 2010 r. do ogłoszenia promowania „kultury praw podstawowych" na wszystkich etapach procesu legislacyjnego oraz do stwierdzenia, że postanowienia Karty praw podstawowych UE „powinny przyświecać […] politykom Unii" ([31]). EIOD jest zdania, że obecny proces oceny stanowi dla Komisji doskonałą okazję potwierdzenia zaangażowania w realizację tego zobowiązania.

([25]) Pierwszy wniosek w sprawie zasad zatrzymywania danych w UE (decyzja ramowa) opierał się na poprzednim Traktacie UE i został wniesiony przez Irlandię, Francję Szwecję i Zjednoczone Królestwo. Zob. dokument Rady 8958/04 z dnia 28 kwietnia 2004 r. Po tym wniosku powstał wniosek Komisji oparty na Traktacie WE. Zob. COM(2005) 438 z dnia 21 września 2005 r.

([26]) Argument ten opierał się na wyroku Trybunału Sprawiedliwości w „sprawach PNR", zob. ETS, wyrok z dnia 30 maja 2006 r. w sprawie *Parlament* przeciwko *Radzie i Komisji,* C-317/05 i C-318/04.

([27]) Zob. ETS, wyrok z dnia 10 lutego 2009 r. w sprawie *Irlandia* przeciwko *Parlamentowi i Radzie,* C-301/06, pkt 82–83.

([28]) Zob. opinię z 2005 r., pkt 80. Zob. również w tej kwestii część IV.3 niniejszej opinii.

([29]) Zob. s. 31 sprawozdania z oceny.

([30]) Zob. art. 6 ust. 1 TUE.

([31]) COM(2010) 573 z dnia 19 października 2010 r., Strategia skutecznego wprowadzania w życie Karty praw podstawowych przez Unię Europejską, s. 4.

IV. **CZY DYREKTYWA W SPRAWIE ZATRZYMYWANIA DANYCH SPEŁNIA WYMOGI DOTYCZĄCE POSZANOWANIA PRYWATNOŚCI I OCHRONY DANYCH?**

35. Sprawozdanie z oceny wskazuje na pewne słabości obecnej dyrektywy w sprawie zatrzymywania informacji. Przedstawione informacje wskazują, że dyrektywa nie osiągnęła swojego głównego celu, jakim jest harmonizacja ustawodawstw krajowych dotyczących zatrzymywania danych. Komisja zauważa, że istnieją „znaczące" różnice w transpozycji przepisów w obszarze ograniczenia celu, dostępu do danych, okresów zatrzymywania, ochrony danych, bezpieczeństwa danych i danych statystycznych ([32]). Według Komisji różnice wynikają częściowo z różnorodności wprowadzonej *explicite* przez dyrektywę. Komisja stwierdza jednak, że nawet poza tą kwestią „różnice w krajowym stosowaniu zatrzymywania danych stanowią poważną trudność dla operatorów" oraz „sektorowi nadal brakuje pewności prawnej" ([33]). Oczywiste jest, że taki brak harmonizacji działa na niekorzyść wszystkich zainteresowanych stron: obywateli, przedsiębiorców oraz organów wymiaru sprawiedliwości.

36. Z punktu widzenia poszanowania prywatności i ochrony danych sprawozdanie z oceny uzasadnia wniosek, że dyrektywa w sprawie zatrzymywania danych nie spełnia wymogów wypływających z prawa do poszanowania prywatności i ochrony danych. Istnieje wiele braków: konieczność zatrzymywania danych zgodnie z dyrektywą w sprawie zatrzymywania danych nie została wystarczająco wykazana, zatrzymywanie danych mogło być regulowane w sposób mniej ingerujący w prywatność, a dyrektywie w sprawie zatrzymywania danych brakuje przewidywalności. Te trzy kwestie zostaną omówione bardziej szczegółowo poniżej.

IV.1. **Konieczność zatrzymywania danych, o której mowa w dyrektywie w sprawie zatrzymywania danych, nie została wystarczająco wykazana**

37. Ingerencja w prawo do poszanowania prywatności i ochrony danych jest dopuszczalna jedynie wówczas, jeżeli środek jest niezbędny do osiągnięcia zgodnego z prawem celu. Konieczność zatrzymywania danych jako środek egzekwowania prawa stale jest przedmiotem dyskusji ([34]). We wniosku w sprawie dyrektywy stwierdzono, że ograniczenie prawa do poszanowania prywatności i ochrony danych jest „proporcjonalne i niezbędne do osiągnięcia ogólnie uznanych celów, jakimi są zapobieganie i zwalczanie przestępczości i terroryzmu" ([35]). W opinii z 2005 r. EIOD wskazywał jednak, że to stwierdzenie go nie przekonuje, gdyż niezbędne są dalsze dowody ([36]). Tym niemniej bez dostarczenia żadnych dodatkowych dowodów w motywie 9 dyrektywy w sprawie zatrzymywania danych stwierdzono, że „zatrzymywanie danych okazało się niezbędnym i skutecznym narzędziem egzekwowania prawa […] w niektórych państwach członkowskich".

38. W związku z brakiem wystarczających dowodów EIOD stwierdził, że dyrektywa w sprawie zatrzymywania danych była wyłącznie oparta na założeniu, że tak rozwinięte zatrzymywanie danych, jak przewiduje dyrektywa w sprawie zatrzymywania danych, stanowiło środek konieczny ([37]). EIOD zwrócił się więc do Komisji i do państw członkowskich o wykorzystanie sprawozdania z oceny do przedstawienia dodatkowych dowodów potwierdzających, że założenie konieczności środka zatrzymywania danych i sposób jego uregulowania w dyrektywie w sprawie zatrzymywania danych jest właściwy.

39. W tej kwestii Komisja stwierdza w sprawozdaniu z oceny, że „większość państw członkowskich przyjmuje stanowisko, że przepisy UE w sprawie zatrzymywania danych pozostają konieczne jako narzędzie egzekwowania prawa, ochrony ofiar i systemów wymiaru sprawiedliwości". Zatrzymywanie danych opisywane jest również jako odgrywające „bardzo ważną rolę" w dochodzeniach w sprawach karnych oraz jako „cenne, a w niektórych sprawach niezbędne". Stwierdza się również, że bez zatrzymywania danych niektóre sprawy karne „mogłyby nigdy nie zostać rozwiązane" ([38]). Komisja stwierdza, że UE powinna w związku z tym „wspierać i regulować zatrzymywanie danych jako środek bezpieczeństwa" ([39]).

40. Wątpliwe jest jednak, czy Komisja może też stwierdzić, że większość państw członkowskich uznaje zatrzymywanie danych za narzędzie konieczne. Nie wskazuje się, które państwa członkowskie tworzą większość, którą w UE 27 państw członkowskich powinno stanowić co najmniej 14 z nich, by można było mówić o większości państw członkowskich. W rozdziale 5, na którym oparte są wnioski, konkretne odwołania dotyczą co najwyżej dziewięciu państw członkowskich ([40]).

41. Ponadto wydaje się, że Komisja opiera się przede wszystkim na stwierdzeniach państw członkowskich dotyczących tego, czy zatrzymywanie danych jest narzędziem niezbędnym do egzekwowania prawa. Stwierdzenia te wskazują jednak, czy poszczególne państwa członkowskie chcą mieć przepisy w sprawie zatrzymywania danych, ale nie mogą jako takie stwierdzić zapotrzebowania na zatrzymywanie danych jako środka egzekwowania prawa, wspieranego i regulowanego przez UE. Stwierdzenia o konieczności wymagają poparcia wystarczającymi dowodami.

42. Wykazanie konieczności środka ingerującego w prywatność nie jest na pewno łatwym zadaniem. W szczególności nie jest to łatwe dla Komisji, która w dużej mierze uzależniona jest od informacji dostarczonych przez państwa członkowskie.

43. Jeżeli środek już istnieje, tak jak dyrektywa w sprawie zatrzymywania danych, i zebrano już doświadczenie praktyczne, powinny istnieć wystarczające informacje

([32]) Zob. s. 31 sprawozdania z oceny.
([33]) Zob. s. 31 sprawozdania z oceny.
([34]) Zob. opinia EIOD z 2005 r. Zob. również pismo z dnia 22 czerwca 2010 r. od dużej grupy organizacji społeczeństwa obywatelskiego, o którym mowa w przypisie 10.
([35]) COM(2005) 438 z dnia 21 września 2005 r., s. 3.
([36]) Zob. opinia z 2005 r., pkt 17–22.
([37]) Zob. wystąpienie z dnia 3 grudnia 2010 r., o którym mowa w przypisie 9.
([38]) Wszystkie cytaty ze s. 23 lub s. 31 sprawozdania z oceny.
([39]) Zob. s. 31 sprawozdania z oceny.
([40]) Republika Czeska, Niemcy, Irlandia, Węgry, Niderlandy, Polska, Słowenia, Finlandia i Zjednoczone Królestwo.

jakościowe i ilościowe pozwalające na ocenę, czy środek rzeczywiście działa oraz czy porównywalne wyniki można by było osiągnąć bez tego instrumentu lub za pomocą środka alternatywnego, mniej ingerującego w prywatność. Takie informacje powinny stanowić niezbywalny dowód i pokazywać związek pomiędzy wykorzystaniem a wynikiem ([41]). Ponieważ dotyczy to dyrektywy UE, informacje powinny przedstawiać praktykę co najmniej większości państw członkowskich UE.

44. Po uważnej analizie EIOD uważa, że mimo iż Komisja włożyła znaczne wysiłki w zebranie informacji od rządów państw członkowskich, informacje ilościowe i jakościowe dostarczone przez państwa członkowskie nie są wystarczające, by potwierdzić konieczność zatrzymywania danych w sposób określony w dyrektywie w sprawie zatrzymywania danych. Przedstawiono ciekawe przykłady zastosowań, jest jednak zbyt wiele braków w przedstawionych w sprawozdaniu informacjach, by móc wyciągnąć ogólne wnioski o konieczności instrumentu. Ponadto nadal należy dokładniej przeanalizować alternatywne środki. Te dwie kwestie zostaną omówione bardziej szczegółowo poniżej.

Informacje ilościowe i jakościowe przedstawione w sprawozdaniu z oceny

45. W odniesieniu do aspektu ilościowego informacje statystyczne przedstawiono przede wszystkim w rozdziale 5 i w załączniku do sprawozdania z oceny, brakuje jednak kluczowych informacji. Na przykład przedstawione dane nie wskazują celów, do których dane były potrzebne. Ponadto dane liczbowe nie pokazują, czy wszystkie dane, co do których wnoszono o dostęp, były danymi przechowywanymi w wyniku obowiązku prawnego zatrzymywania danych, czy były to dane przechowywane do celów komercyjnych. Nie ma również informacji o wynikach wykorzystania danych. W kontekście wyciągania wniosków problematyczna jest również kwestia niepełnej porównywalności informacji z różnych państw członkowskich, a w wielu przypadkach wykresy pokazują jedynie dziewięć państw członkowskich.

46. Przykłady jakościowe zawarte w sprawozdaniu służą lepszemu zobrazowaniu ważnej roli, jaką odegrały zatrzymywane dane w konkretnych sytuacjach oraz potencjalnych korzyści płynących z systemu zatrzymywania danych. Nie we wszystkich przypadkach jest jednak jasne, czy wykorzystanie zatrzymywanych danych było jedynym sposobem rozwiązania sprawy danego przestępstwa.

47. Niektóre przykłady ilustrują niezbędność środka polegającego na zatrzymywaniu danych do zwalczania cyberprzestępczości. W tej kwestii należy zauważyć, że główny międzynarodowy instrument w tym zakresie – Konwencja Rady Europy w sprawie cyberprzestępczości – nie przewiduje zatrzymywania danych jako środka zwalczania cyberprzestępczości, a odwołuje się jedynie do zachowywania danych jako narzędzia śledczego ([42]).

48. Komisja wydaje się przywiązywać dużą wagę do przykładów przedstawionych przez państwa członkowskie, w których zatrzymywane dane były wykorzystywane do wykluczenia podejrzanych o przestępstwo i do sprawdzania alibi ([43]). Mimo że są to ciekawe przykłady wykorzystywania danych przez wymiar sprawiedliwości, nie można ich wykorzystywać jako potwierdzenia potrzeby zatrzymywania danych. Argument ten należy wykorzystywać ostrożnie, ponieważ może zostać źle zrozumiany, sugerując, że zatrzymywanie danych jest niezbędne do udowodnienia niewinności obywateli, co trudno byłoby pogodzić z domniemaniem niewinności.

49. Sprawozdanie z oceny zawiera jedynie krótką informację na temat wartości zatrzymywania danych w powiązaniu z rozwiązaniami technologicznymi, a w szczególności wykorzystaniem przedpłaconych kart SIM ([44]). EIOD podkreśla, że większa ilość informacji ilościowych i jakościowych dotyczących nowych technologii nieobjętych dyrektywą (na przykład VoIP i sieci społecznościowe) pomogłaby dokonać oceny skuteczności dyrektywy.

50. Sprawozdanie z oceny jest ograniczone, ponieważ skupiono się w nim przede wszystkim na danych ilościowych i jakościowych dostarczonych przez państwa członkowskie, które wdrożyły dyrektywę w sprawie zatrzymywania danych. Ciekawe byłoby jednak przyjrzeć się, czy pomiędzy tymi państwami członkowskimi a państwami, które nie wdrożyły dyrektywy, pojawiły się znaczące różnice. W szczególności w odniesieniu do tych państw członkowskich, w których unieważniono przepisy wykonujące (Republika Czeska, Niemcy i Rumunia), ciekawe byłoby sprawdzenie, czy są jakiekolwiek dowody na sukces lub niepowodzenie dochodzeń przed unieważnieniem lub po nim.

51. Komisja przyznaje, że dane statystyczne i przykłady zawarte w sprawozdaniu z oceny są „w niektórych aspektach ograniczone", ale stwierdza jednak, że dowody potwierdzają „bardzo istotną rolę zatrzymywanych danych w śledztwach w sprawach karnych" ([45]).

52. EIOD jest zdania, że Komisja powinna być bardziej krytyczna wobec państw członkowskich. Jak wyjaśniono, same deklaracje polityczne niektórych państw członkowskich w sprawie potrzeby takiego środka nie mogą uzasadniać działania UE. Komisja powinna była naciskać na państwa członkowskie, by dostarczyły wystarczających dowodów potwierdzających konieczność środka. Według EIOD Komisja powinna była przynajmniej uzależnić swoje poparcie dla środka bezpieczeństwa w postaci zatrzymywania danych (zob. s. 31 sprawozdania z oceny) od dostarczenia przez państwa członkowskie dodatkowych dowodów podczas oceny wpływu.

Środki alternatywne

53. Konieczność zatrzymywania danych w sposób określony w dyrektywie w sprawie zatrzymywania danych zależy również od tego, czy istnieje środek mniej ingerujący w prywatność prowadzący do porównywalnych wyników. Zostało to potwierdzone przez Trybunał Sprawiedliwości w wyroku w sprawie *Schecke* w listopadzie 2010 r.,

([41]) W kwestii konieczności i proporcjonalności zob. również opinię EIOD z dnia 25 marca 2011 r. w sprawie wniosku UE PNR, która znajduje się na stronie internetowej EIOD (http://www.edps.europa.eu) w zakładce „Consultation" >> „Opinions" >> „2011".

([42]) Zob. s. 5 sprawozdania z oceny.

([43]) Zob. s. 24 sprawozdania z oceny.

([44]) Zob. s. 25 sprawozdania z oceny.

([45]) Zob. s. 31 sprawozdania z oceny.

w którym Trybunał stwierdził nieważność przepisów UE dotyczących publikacji nazwisk beneficjentów funduszy rolniczych ([46]). Jedną z przyczyn unieważnienia był fakt, że Rada i Komisja nie rozważyły alternatywnych środków, które byłyby spójne z celem publikacji, a równocześnie powodowałyby mniej ingerencji w prawo do poszanowania prywatności i ochrony danych zainteresowanych osób ([47]).

54. Najważniejsza alternatywa pojawiająca się w dyskusjach wokół dyrektywy w sprawie zatrzymywania danych to metoda zachowywania danych („szybkie zamrożenie" i „szybkie zamrożenie plus") ([48]). Polega ona na czasowym zabezpieczeniu, czyli „zamrożeniu", niektórych danych dotyczących ruchu telekomunikacyjnego i lokalizacji, wyłącznie w odniesieniu do konkretnych osób podejrzanych o działalność przestępczą, a które to dane mogą być dalej udostępnione organom wymiaru sprawiedliwości na mocy zezwolenia sądu.

55. W sprawozdaniu z oceny zachowywanie danych jest wspomniane w kontekście wspomnianej już Konwencji w sprawie cyberprzestępczości, ale jest uznane za niewłaściwe, ponieważ „nie gwarantuje zdolności do ustalenia ścieżek dowodowych przed nakazem zachowania oraz nie pozwala prowadzić dochodzenia, jeżeli nie jest znany cel, a także nie pozwala na zbieranie dowodów o ruchach np. ofiar lub świadków przestępstwa" ([49]).

56. EIOD przyznaje, że jeżeli zamiast szerokiego systemu zatrzymywania danych wykorzystywany jest system zachowywania danych, dostępnych jest mniej informacji. Jednak to właśnie z powodu bardziej ukierunkowanego charakteru zachowywanie danych stanowi instrument mniej ingerujący w prywatność, jeśli chodzi o skalę i liczbę osób, których dotyka. Ocena powinna skupić się nie tylko na dostępnych danych, ale też na różnych wynikach uzyskiwanych z obu systemów. EIOD jest zdania, że uzasadniona i niezbędna jest bardziej pogłębiona analiza tego środka. Mogłoby to zostać wykonane podczas oceny wpływu w najbliższych miesiącach.

57. W tej kwestii niefortunne jest stwierdzenie we wnioskach sprawozdania, że Komisja zobowiązuje się do przeanalizowania, czy – a jeżeli tak, to w jaki sposób – podejście UE do zachowywania danych mogłoby uzupełnić (czyli nie zastąpić) zatrzymywanie danych ([50]). Możliwość połączenia jednego z systemów zatrzymywania danych z gwarancjami proceduralnymi dotyczącymi różnych sposobów zachowywania danych rzeczywiście wymaga dalszej analizy. EIOD zaleca jednak, by Komisja podczas oceny wpływu rozważyła również, czy system zachowywania danych lub inny alternatywny środek mógłby w całości lub w części zastąpić obecny system zatrzymywania danych.

([46]) ETS, wyrok z dnia 9 listopada 2010 r. w sprawie *Volker und Markus Schecke*, C-92/09 i C-93/09.
([47]) ETS, wyrok w sprawie *Schecke*, pkt 81.
([48]) „Szybkie zamrożenie" dotyczy „zamrożenia" danych dotyczących ruchu i lokalizacji w odniesieniu do konkretnego podejrzanego od dnia zezwolenia sądu. „Szybie zamrożenie plus" również obejmuje „zamrożenie" danych już będących w posiadaniu operatorów do celów naliczania opłat i przesyłu.
([49]) Zob. s. 5 sprawozdania z oceny.
([50]) Zob. s. 32 sprawozdania z oceny.

IV.2. **Zatrzymywanie danych zgodnie z dyrektywą w sprawie zatrzymywania danych jednoznacznie wykracza poza to, co niezbędne**

58. Według EIOD informacje w sprawozdaniu z oceny nie zawierają wystarczającego potwierdzenia konieczności istnienia środka zatrzymywania danych w postaci przyjętej w dyrektywie w sprawie zatrzymywania danych. Sprawozdanie z oceny pozwala jednak na stwierdzenie, że dyrektywa w sprawie zatrzymywania danych reguluje zatrzymywanie danych w sposób wykraczający poza to, co niezbędne, lub co najmniej nie zapewnia niewykorzystywania zatrzymywania danych w taki sposób. W tej kwestii można podkreślić cztery elementy.

59. Po pierwsze, niejasny cel środka i szerokie pojęcie „właściwych władz krajowych" prowadzi do wykorzystania zatrzymywanych danych w zdecydowanie zbyt szerokim zakresie celów i przez zdecydowanie zbyt wiele organów. Ponadto brakuje konsekwencji w obostrzeniach i warunkach dostępu do danych. Na przykład do uzyskania dostępu nie we wszystkich państwach członkowskich konieczne jest uzyskanie wcześniejszego zatwierdzenia przez organy sądowe lub inne niezależne organy.

60. Po drugie, maksymalny okres zatrzymywania wynoszący dwa lata wydaje się wykraczać poza to, co konieczne. Dane statystyczne z wielu państw członkowskich w sprawozdaniu z oceny wskazują, że zdecydowana większość wniosków o dostęp dotyczy danych z ostatnich sześciu miesięcy: jest to 86 % ([51]). Ponadto szesnaście państw członkowskich w swoich przepisach zdecydowało się na okres zatrzymywania wynoszący jeden rok lub krótszy ([52]). To wyraźnie sugeruje, że maksymalny okres wynoszący dwa lata zdecydowanie wykracza poza to, co uznano za niezbędne w większości państw członkowskich.

61. Ponadto brak ustalonego wspólnego okresu zatrzymywania dla wszystkich państw członkowskich spowodował przyjęcie rozbieżnych przepisów krajowych, co może rodzić komplikacje, gdyż nie zawsze jest jasne, które prawo krajowe – zarówno w odniesieniu do zatrzymywania danych, jak i do ochrony danych – ma zastosowanie, jeżeli operatorzy przechowują dane w państwie członkowskim innym niż to, w którym dane są zbierane.

62. Po trzecie, poziom bezpieczeństwa nie jest wystarczająco zharmonizowany. Jeden z głównych wniosków grupy roboczej powołanej na mocy art. 29 zawartego w jej sprawozdaniu z lipca 2010 r. jest taki, że istnieje duża różnorodność środków bezpieczeństwa istniejących w poszczególnych państwach członkowskich. Komisja wydaje się uważać, że środki bezpieczeństwa w obecnej dyrektywie są wystarczające, ponieważ „nie ma konkretnych przykładów poważnego łamania prywatności" ([53]). Wydaje się jednak, że Komisja zwróciła się o informacje w tej kwestii wyłącznie do rządów państw członkowskich. W celu dokonania oceny przydatności obecnych przepisów i środków bezpieczeństwa potrzebne są szersze konsultacje

([51]) Zob. s. 22 sprawozdania z oceny. 12 % dotyczy danych z okresu sprzed 6 do 12 miesięcy, a 2 % – danych starszych niż rok.
([52]) Zob. s. 14 sprawozdania z oceny.
([53]) Zob. s. 30 sprawozdania z oceny.

i bardziej konkretne zbadanie przypadków nadużyć. Mimo że w tym kontekście nie mówi się o konkretnych przypadkach złamania zasad bezpieczeństwa, przypadki łamania bezpieczeństwa danych i skandale w obszarze danych przesyłowych i komunikacji elektronicznej w niektórych państwach członkowskich stanowią również czytelne ostrzeżenia. Do kwestii tej nie można podchodzić lekko, gdyż bezpieczeństwo zatrzymywanych danych ma kluczowe znaczenie dla samego systemu zatrzymywania danych, ponieważ zapewnia ona przestrzeganie wszystkich innych obostrzeń ([54]).

63. Po czwarte, ze sprawozdania nie wynika jasno, czy wszystkie kategorie zatrzymywanych danych rzeczywiście są niezbędne. Rozróżnia się tylko w sposób ogólny dane telefoniczne i internetowe. Niektóre państwa członkowskie zdecydowały się na wprowadzenie krótszego okresu zatrzymywania w odniesieniu do danych internetowych ([55]). Nie można jednak wyciągnąć z tego ogólnych wniosków.

IV.3. **Dyrektywie w sprawie zatrzymywania danych brakuje przewidywalności**

64. Kolejna słabość dyrektywy w sprawie zatrzymywania danych dotyczy jej braku przewidywalności. Wymóg przewidywalności wynika z ogólnego wymogu określonego w art. 8 ust. 2 Konwencji oraz art. 52 ust. 1 Karty praw podstawowych UE, zgodnie z którymi ingerencja powinna być określona w przepisach. Według Europejskiego Trybunału Praw Człowieka oznacza to, że środek powinien mieć podstawę prawną i być spójny z zasadą praworządności. Oznacza to, że prawo jest odpowiednio dostępne i przewidywalne ([56]). Trybunał Sprawiedliwości podkreślił w wyroku w sprawie *Österreichischer Rundfunk*, że przepisy należy formułować wystarczająco precyzyjnie, by obywatele mogli odpowiednio dostosować swoje postępowanie ([57]). Przepisy muszą wskazywać wystarczająco jasno zakres swobody właściwych władz i sposób jej wykonywania ([58]).

65. Również w liście sprawdzającej określonej w komunikacie Komisji w sprawie Karty praw podstawowych UE jedno z pytań, na które należy odpowiedzieć, dotyczy tego, czy wszelkie ograniczenie praw podstawowych jest sformułowane „w sposób jasny i przewidywalny" ([59]). W komunikacie poświęconym przeglądowi zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości Komisja stwierdziła również, że obywatele „mają prawo wiedzieć, które z ich danych osobowych są przetwarzane i wymieniane, przez kogo i z jakiego powodu" ([60]).

66. W przypadku dyrektywy UE odpowiedzialność za zgodność z prawami podstawowymi, w tym z wymogiem przewidywalności, leży przede wszystkim w gestii państw członkowskich wdrażających dyrektywę do swojego prawa krajowego. Powszechnie znany jest wymóg, zgodnie z którym taka implementacja musi być zgodna z prawami podstawowymi ([61]).

67. Również w sprawozdaniu z oceny Komisja podkreśla, że dyrektywa „jako taka nie gwarantuje, że zatrzymywane dane są przechowywane, pozyskiwane i wykorzystywane z pełnym poszanowaniem prawa do prywatności i ochrony danych osobowych". Powołuje się na „odpowiedzialność państw członkowskich za zapewnienie przestrzegania tych praw" ([62]).

68. EIOD jest jednak zdania, że sama dyrektywa powinna w pewnym zakresie również spełniać wymóg przewidywalności. Reformułując wyrok Trybunału Sprawiedliwości w sprawie *Lindqvist*, systemowi określanemu w dyrektywie nie powinno „brakować przewidywalności" ([63]). Dotyczy to w szczególności środka UE, na mocy którego państwa członkowskie ingerują na szeroką skalę w prawo do prywatności i ochronę danych obywateli. EIOD jest zdania, że UE odpowiada za zapewnienie co najmniej jasnego określenia celu i tego, kto może uzyskać dostęp do danych oraz na jakich warunkach.

69. Takie stanowisko potwierdza nowy kontekst prawny wynikający z traktatu lizbońskiego, który, jak wyjaśniono, zwiększa kompetencje UE w zakresie współpracy policyjnej i sądowej w sprawach karnych i ustanawia silniejsze zobowiązanie UE do przestrzegania praw podstawowych.

70. EIOD pragnie przypomnieć, że wymóg określonego celu i wynikający z tego zakaz przetwarzania danych w sposób niezgodny z tym celem („zasada ograniczenia celu") mają podstawowe znaczenie dla ochrony danych osobowych, co potwierdza art. 8 Karty praw podstawowych UE ([64]).

71. Sprawozdanie z oceny pokazuje, że wybór pozostawienia państwom członkowskim precyzyjnego zdefiniowania, czym jest „poważne przestępstwo", a w konsekwencji, co należy uznać za „właściwe władze", doprowadził do wykorzystywania danych do wielu różnych celów ([65]).

72. Komisja stwierdza, że „większość państw członkowskich dokonujących transpozycji zgodnie z przepisami krajowymi umożliwia dostęp i wykorzystanie zatrzymywanych danych do celów wykraczających poza te określone w dyrektywie, w tym do ogólnego zapobiegania i zwalczania przestępczości oraz w sytuacjach zagrożenia życia" ([66]). Państwa członkowskie wykorzystają „lukę prawną" wynikającą z art. 15 ust. 1 dyrektywy o prywatności elektronicznej ([67]). Komisja uważa, że ta sytuacja może nie zapewniać

([54]) Zob. również w tej kwestii opinię EIOD z 2005 r., pkt 29–37. Zob. również wystąpienie zastępcy inspektora z dnia 4 maja 2011 r., które znajduje się na stronie internetowej EIOD (http://www.edps.europa.eu) w zakładce „Publications" >> „Speeches & Articles" >> „2011".
([55]) Zob. s. 14 sprawozdania z oceny.
([56]) Zob. Europejski Trybunał Praw Człowieka, wyrok w sprawie *S. i Marper*, o którym mowa w przypisie 7, pkt 151.
([57]) ETS, dnia 20 maja 2003 r., wyrok w sprawie *Österreichischer Rundfunk*, C-465/00, pkt 77 oraz Europejski Trybunał Praw Człowieka, wyrok w sprawie *S. i Marper*, o którym mowa w przypisie 7, pkt 95.
([58]) Zob. Europejski Trybunał Praw Człowieka, wyrok w sprawie *Malone*, o którym mowa w przypisie 8, pkt 66–68.
([59]) COM(2010) 573, o którym mowa w przypisie 31, s. 5.
([60]) COM(2010) 385, o którym mowa w przypisie 17, s. 3.
([61]) Zob. np. ETS, wyrok z dnia 6 listopada 2003 r. w sprawie *Lindqvist*, pkt 87.
([62]) Zob. s. 31 sprawozdania z oceny.
([63]) ETS, wyrok w sprawie *Lindqvist*, pkt 84.
([64]) Zob. również art. 6 dyrektywy 95/46/WE.
([65]) Zob. s. 8 sprawozdania z oceny.
([66]) Zob. s. 8 sprawozdania z oceny.
([67]) Zgodnie z omówieniem w pkt 24 powyżej.

wystarczającej „przewidywalności stanowiącej wymóg dla wszystkich środków prawnych ograniczających prawo do prywatności" ([68]).

73. W tych okolicznościach nie można stwierdzić, że sama dyrektywa w sprawie zatrzymywania danych, czytana w szczególności w połączeniu z dyrektywą o prywatności elektronicznej, zapewnia jasność niezbędną do spełnienia zasady przewidywalności na poziomie UE.

V. **ROZWIĄZANIA NA PRZYSZŁOŚĆ: NALEŻY ROZWAŻYĆ WSZYSTKIE OPCJE**

74. Analiza w poprzednich częściach uzasadnia wniosek, że dyrektywa w sprawie zatrzymywania danych nie spełnia wymogów ustalonych w prawie do poszanowania prywatności i ochrony danych. Jest więc oczywiste, że dyrektywa w sprawie zatrzymywania danych nie może dalej istnieć w obecnej formie. W związku z tym Komisja słusznie proponuje przegląd obecnych ram dla zatrzymywania danych ([69]).

75. Przed zaproponowaniem jednak zmienionej wersji dyrektywy:

a) Komisja powinna, podczas oceny wpływu, zaangażować się w zebranie większej liczby dowodów praktycznych z państw członkowskich, w celu wykazania niezbędności zatrzymywania danych jako środka w ramach prawa UE;

b) jeżeli większość państw członkowskich uważa, że zatrzymywanie danych jest konieczne, państwa te powinny dostarczyć Komisji dowody ilościowe i jakościowe, które to potwierdzą;

c) państwa członkowskie, które sprzeciwiają się takiemu środkowi zatrzymywania danych, powinny dostarczyć Komisji informacje umożliwiające dokonanie szerszej oceny tej kwestii.

76. W ocenie wpływu należałoby dodatkowo przeanalizować, czy alternatywne, mniej ingerujące w prywatność środki mogłyby prowadzić w przeszłości lub obecnie do porównywalnych wyników. Komisja powinna podjąć w tej kwestii inicjatywę, korzystając w razie potrzeby z zewnętrznego wsparcia ekspertów.

77. EIOD z radością przyjmuje fakt, że Komisja ogłosiła konsultacje obejmujące wszystkie zainteresowane strony podczas oceny wpływu ([70]). W związku z tym EIOD zachęca Komisję do znalezienia sposobów bezpośrednio angażujących obywateli w to zadanie.

78. Należy podkreślić, że ocena konieczności i analiza alternatywnych, mniej ingerujących w prywatność środków, może zostać przeprowadzona w uczciwy sposób wyłącznie wówczas, jeżeli wszystkie opcje dla przyszłej dyrektywy pozostaną otwarte. W związku z tym Komisja wydaje się wykluczać możliwość uchylenia dyrektywy, albo jako takiej, albo w połączeniu z wnioskiem w sprawie alternatywnego, bardziej ukierunkowanego środka UE. EIOD zwraca się więc do Komisji o poważne rozważenie również tych opcji w ocenie wpływu.

79. Przyszła dyrektywa w sprawie zatrzymywania danych może być rozważana wyłącznie w przypadku porozumienia, że potrzebne są przepisy UE z perspektywy rynku wewnętrznego oraz współpracy w sprawach karnych i sądowych oraz jeżeli, podczas oceny wpływu, można by wystarczająco wykazać konieczność zatrzymywania danych, popieraną i regulowaną przez UE, co obejmuje uważne przeanalizowanie środków alternatywnych.

80. EIOD nie podważa dużej wartości zatrzymywanych danych dla celów egzekwowania prawa oraz kluczowego znaczenia, jakie mogą one odegrać w konkretnych przypadkach. Podobnie jak niemiecki Bundesverfassungsgericht EIOD nie wyklucza, że dobrze zdefiniowany obowiązek zatrzymywania danych telekomunikacyjnych mógłby być uzasadniony w niektórych, bardzo ograniczonych, okolicznościach ([71]).

81. Każdy przyszły instrument UE w zakresie zatrzymywania danych powinien więc spełniać następujące podstawowe wymogi:

— być zrozumiały i w pełni harmonizować przepisy w zakresie obowiązku zatrzymywania danych oraz w sprawie dostępu i przyszłego wykorzystywania danych przez właściwe władze,

— być wyczerpujący, co oznacza, że ma jasny i precyzyjny cel oraz likwiduje lukę prawną, która istnieje w związku z art. 15 ust. 1 dyrektywy o prywatności elektronicznej,

— być proporcjonalny i nie wykraczać poza niezbędny zakres (zob. w tej kwestii uwagi zawarte w części IV.2 powyżej).

82. EIOD oczywiście szczegółowo przeanalizuje każdy przyszły wniosek w sprawie zatrzymywania danych w świetle tych podstawowych warunków.

VI. **WNIOSKI**

83. EIOD z zadowoleniem stwierdza, iż mimo że nie jest to ściśle wymagane zgodnie z art. 14 dyrektywy w sprawie zatrzymywania danych, Komisja uwzględniła również w sprawozdaniu z oceny implikacje dyrektywy dla praw podstawowych.

84. Sprawozdanie z oceny wskazuje, że dyrektywa nie osiągnęła swojego głównego celu, jakim jest harmonizacja ustawodawstw krajowych dotyczących zatrzymywania danych. Taki brak harmonizacji działa na niekorzyść wszystkich zainteresowanych stron: obywateli, przedsiębiorców oraz organów egzekwowania prawa.

85. Na podstawie sprawozdania z oceny można wnioskować, że dyrektywa w sprawie zatrzymywania danych nie spełnia wymogów wynikających z prawa do poszanowania prywatności i ochrony danych z następujących powodów:

— konieczność zatrzymywania danych, o której mowa w dyrektywie w sprawie zatrzymywania danych, nie została wystarczająco wykazana,

— zatrzymywanie danych mogłoby być regulowane w sposób mniej ingerujący w prywatność,

([68]) Zob. s. 9 i s. 15 sprawozdania z oceny.
([69]) Zob. s. 32–33 sprawozdania z oceny.
([70]) Zob. s. 32–33 sprawozdania z oceny.
([71]) Zob. Bundesverfasssungsgericht, 1 BvR 256/08.

— dyrektywie w sprawie zatrzymywania danych brakuje przewidywalności.

86. EIOD zwraca się do Komisji o poważne rozważenie wszystkich możliwości w ocenie wpływu, w tym możliwości samego uchylenia dyrektywy, albo jej uchylenia z wnioskiem w sprawie alternatywnego, bardziej ukierunkowanego środka UE.

87. Przyszła dyrektywa w sprawie zatrzymywania danych powinna być rozważana wyłącznie w przypadku porozumienia, że potrzebne są przepisy UE z perspektywy rynku wewnętrznego oraz współpracy w sprawach karnych i sądowych oraz jeżeli, podczas oceny wpływu, można by wystarczająco wykazać konieczność zatrzymywania danych, popieraną i regulowaną przez UE, co obejmuje uważne przeanalizowanie środków alternatywnych. Taki instrument powinien spełniać poniższe podstawowe wymagania:

— być zrozumiały i w pełni harmonizować przepisy w zakresie obowiązku zatrzymywania danych oraz w sprawie dostępu i przyszłego wykorzystywania danych przez właściwe władze,

— być wyczerpujący, co oznacza, że ma jasny i precyzyjny cel oraz likwiduje lukę prawną, która istnieje w związku z art. 15 ust. 1 dyrektywy o prywatności elektronicznej,

— być proporcjonalny i nie wykraczać poza niezbędny zakres.

Sporządzono w Brukseli dnia 31 maja 2011 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych

Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (WE) nr 1073/1999 dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) i uchylającego rozporządzenie (Euratom) nr 1074/1999

(2011/C 279/02)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

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

uwzględniając Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 7 i 8,

uwzględniając dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych ([1]),

uwzględniając 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 ([2]), w szczególności jego art. 41 ust. 2,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

1. **WPROWADZENIE**

1. W dniu 17 marca 2011 r. Komisja przyjęła wniosek w sprawie rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (WE) nr 1073/1999 dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) i uchylającego rozporządzenie (Euratom) nr 1074/1999 (zwany dalej „wnioskiem").

1.1. **Konsultacje z EIOD**

2. Wniosek został przesłany przez Radę do EIOD w dniu 8 kwietnia 2011 r. EIOD interpretuje to jako wezwanie do doradzenia wspólnotowym instytucjom i organom, jak przewiduje art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 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 (dalej zwanego „rozporządzeniem (WE) nr 45/2001"). EIOD z zadowoleniem przyjmuje wyraźne odniesienie do tej konsultacji w preambule do wniosku.

3. Celem wniosku jest zmiana art. 1–14 oraz skreślenie art. 15 rozporządzenia (WE) nr 1073/1999. Rozporządzenie (Euratom) nr 1074/1999 z dnia 25 maja 1999 r. dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) ma zostać uchylone.

4. Wcześniej ([3]), przed przyjęciem wniosku, Komisja umożliwiła EIOD przekazanie nieformalnych uwag. EIOD z zadowoleniem przyjmuje jawność procesu, co pomogło udoskonalić tekst z punktu widzenia ochrony danych na wczesnym etapie. Niektóre z tych uwag rzeczywiście zostały uwzględnione we wniosku.

5. Ten nowy tekst jest wynikiem długiego procesu przeglądu. W 2006 r. Komisja wystąpiła z wnioskiem w sprawie zmiany rozporządzenia (WE) nr 1073/1999. Głównym celem wniosku legislacyjnego było „osiągnięcie poprawy efektywności operacyjnej i usprawnienie zarządzania Urzędem".

6. Ten wcześniejszy wniosek był przedmiotem dyskusji w Radzie i Parlamencie Europejskim w ramach procedury współdecyzji. W kwietniu 2007 r. EIOD wydał opinię zawierającą szereg uwag służących zwiększeniu spójności tekstu wniosku z zasadami ochrony danych ustanowionymi w rozporządzeniu (WE) nr 45/2001 ([4]). W dniu 20 listopada 2008 r. ([5]) Parlament przyjął w pierwszym czytaniu rezolucję obejmującą około stu poprawek do wniosku.

7. Na wniosek prezydencji czeskiej w Radzie (trwającej od stycznia do czerwca 2009 r.) w lipcu 2010 r. Komisja przedstawiła Parlamentowi Europejskiemu i Radzie zmieniony dokument analityczny na temat reformy Europejskiego Urzędu ds. Zwalczania Nadużyć Finansowych. W październiku 2010 r. Parlament Europejski z zadowoleniem przyjął dokument analityczny i zwrócił się do Komisji o ponowne zainicjowanie procedury ustawodawczej. W dniu 6 grudnia 2010 r. Rada przyjęła

([1]) Dz.U. L 281 z 23.11.1995, s. 31.
([2]) Dz.U. L 8 z 12.1.2001, s. 1.
([3]) W styczniu 2011 r.
([4]) Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (WE) nr 1073/1999 dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF), Dz.U. C 91 z 26.4.2007, s. 1.
([5]) Rezolucja legislacyjna Parlamentu Europejskiego z dnia 20 listopada 2008 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (WE) nr 1073/1999 dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF), P6_TA-PROV(2008) 553.

konkluzje w sprawie dokumentu analitycznego przedstawionego przez Komisję. Komitet Nadzoru OLAF wniósł wkład do dyskusji, przedstawiając opinie na temat dokumentu analitycznego oraz przestrzegania praw podstawowych i gwarancji proceduralnych w dochodzeniach prowadzonych przez OLAF. Komisja przedstawiła następnie nowy wniosek.

1.2. **Znaczenie wniosku i zalecenia EIOD**

8. Wniosek zawiera przepisy, które mają duży wpływ na prawa osób fizycznych. OLAF będzie w dalszym ciągu gromadzić i przetwarzać dane szczególnie chronione odnoszące się do informacji dotyczących ewentualnych wykroczeń, wykroczeń wyroków w sprawach karnych, jak również informacji, które mogłyby posłużyć do pozbawienia danych osób prawa, korzyści lub wykluczenia z umowy – w takim stopniu, w jakim informacje te stanowią szczególne zagrożenie dla praw i wolności osób, których dotyczą dane. Podstawowe prawo do ochrony danych osobowych jest istotne nie tylko samo w sobie, ale jest również ściśle powiązane z innymi prawami podstawowymi, takimi jak niedyskryminacja i sprawiedliwość proceduralna, z uwzględnieniem prawa do obrony w dochodzeniach OLAF. Poszanowanie sprawiedliwości proceduralnej wpływa na wiarygodność dowodów i powinno być postrzegane przez OLAF jako priorytet umożliwiający zwiększenie zakresu jego odpowiedzialności. Niezbędne jest zatem zapewnienie należytego zagwarantowania przestrzegania przez OLAF praw podstawowych, w tym prawa do ochrony danych i prywatności osób wynikającego z tych praw, podczas przeprowadzania dochodzeń.

1.3. **Główne elementy wniosku**

9. Celem wniosku jest poprawa wydajności, skuteczności i rozliczalności OLAF, przy jednoczesnym zagwarantowaniu niezależności dochodzeniowej Urzędu. Wspomniany cel zostanie osiągnięty głównie poprzez: (i) zacieśnienie współpracy oraz szerszą wymianę informacji z innymi instytucjami, urzędami, organami i agencjami UE, jak również z państwami członkowskimi; (ii) dostosowanie podejścia *de minimis* ([6]) do dochodzeń; (iii) wzmocnienie gwarancji proceduralnych dla osób objętych dochodzeniami OLAF; (iv) przyznanie OLAF uprawnień do przyjmowania ustaleń administracyjnych w celu ułatwienia wymiany informacji z Europolem, Eurojustem, właściwymi organami państw trzecich oraz organizacjami międzynarodowymi; a także (v) sprecyzowanie roli Komitetu Nadzoru polegającej na monitorowaniu.

10. EIOD popiera cele proponowanych zmian i w tym zakresie z zadowoleniem przyjmuje wniosek. EIOD w szczególności docenia wprowadzenie nowego art. 7 lit. a), który dotyczy gwarancji proceduralnych przysługujących osobom fizycznym. W odniesieniu do praw osób fizycznych do ochrony ich danych osobowych i prywatności EIOD uważa, że generalnie wniosek zawiera ulepszenia w stosunku do obecnej sytuacji. Jednym z takich ulepszeń, przyjmowanych z zadowoleniem przez EIOD, jest przede wszystkim wyraźne uznanie znaczenia praw osób, których dane dotyczą, zgodnie z art. 11 i 12 rozporządzenia (WE) nr 45/2001 ([7]).

11. Pomimo ogólnego dobrego wrażenia EIOD uważa jednak, że z punktu widzenia ochrony danych osobowych wniosek mógłby zostać jeszcze bardziej ulepszony w sposób nie zagrażający celom, jakie ma realizować. W szczególności EIOD zwraca uwagę na to, że ze względu na brak spójności w odniesieniu do niektórych aspektów wniosek może być uznany za *lex specialis* regulujące przetwarzanie danych osobowych zgromadzonych w ramach dochodzeń OLAF, które miałoby pierwszeństwo przed stosowaniem ogólnych ram ochrony danych zawartych w rozporządzeniu (WE) nr 45/2001. Istnieje zatem ryzyko, że standardy ochrony danych zawarte we wniosku mogą być interpretowane *ex contrario* jako niższe niż standardy zawarte w rozporządzeniu, przy czym nie jest to wyraźnie uzasadnione ani w samym wniosku, ani w uzasadnieniu.

12. W celu uniknięcia takiego rezultatu dalsze części tekstu zawierają analizę wniosku, która z jednej strony stanowi opis jego usterek, a z drugiej sugeruje konkretne sposoby ich zlikwidowania. Zakres zastosowania niniejszej analizy jest ograniczony do przepisów mających bezpośredni wpływ na ochronę danych osobowych, w szczególności art. 1 ust. 8, 9, 10, 11 i 12, w myśl których dodaje się lub zmienia art. 7a, 7b, 8, 9, 10 i 10a.

2. **ANALIZA WNIOSKU**

2.1. **Kontekst ogólny**

13. OLAF został utworzony w 1999 r. ([8]) w celu ochrony interesów finansowych UE i pieniędzy podatników przed nadużyciami finansowymi, korupcją i wszelką inną bezprawną działalnością. Urząd należy do Komisji, ale jest od niej niezależny. OLAF prowadzi dochodzenia, które mogą być zewnętrzne ([9]) (w szczególności dochodzenia, które mogą mieć miejsce w państwach członkowskich lub państwach trzecich) i wewnętrzne ([10]) (dochodzenia w ramach instytucji, organów, urzędów i agencji UE), w celu zwalczania nadużyć finansowanych i nielegalnej działalności, które mogą szkodzić interesom finansowym Unii Europejskiej.

14. Ponadto OLAF może również (i) przekazywać krajowym właściwym organom informacje ujawnione podczas dochodzeń zewnętrznych Urzędu; (ii) przekazywać krajowym

([6]) Tzn. OLAF powinien zdefiniować swoje priorytety w zakresie dochodzeń i skoncentrować się na nich w celu skutecznego wykorzystania zasobów.

([7]) Zob. wniosek, nowy art. 7 lit. a) i art. 8 ust. 4.

([8]) Decyzja Komisji 1999/352/WE z dnia 28 kwietnia 1999 r. ustanawiająca Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF), Dz.U. L 136 z 31.5.1999, s. 20. Zob. również rozporządzenie (WE) nr 1073/1999 Parlamentu Europejskiego i Rady z dnia 25 maja 1999 r. dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF), Dz.U. L 136 z 31.5.1999, s. 1.

([9]) Zob. art. 3, rozporządzenie (WE) nr 1073/1999.

([10]) Zob. art. 1 i 4, rozporządzenie (WE) nr 1073/1999.

organom sądowniczym informacje wykryte podczas dochodzeń wewnętrznych w sprawach, które mogą prowadzić do postępowania karnego oraz (iii) przekazywać zainteresowanym instytucjom, organom, urzędom lub agencjom informacje uzyskane podczas dochodzeń wewnętrznych ([11]).

15. OLAF może również ściśle współpracować z Eurojustem ([12]) i Europolem ([13]) w celu realizowania swojego statutowego obowiązku zwalczania nadużyć finansowych, korupcji i wszelkiej innej działalności, która może mieć wpływ na interesy finansowe Unii. W tym kontekście Europol ([14]) i Eurojust ([15]) mogą wymieniać się informacjami operacyjnymi, strategicznymi i technicznymi, w tym danymi osobowymi, z Urzędem.

16. Na mocy rozporządzenia (WE) nr 1073/1999 OLAF może również prowadzić dochodzenia w państwach trzecich zgodnie z różnymi obwiązującymi umowami o współpracy między Unią Europejską a takimi państwami trzecimi. Działalność oszukańcza przynosząca szkodę budżetowi Unii może również odbywać się poza terytorium Unii Europejskiej, na przykład w odniesieniu do pomocy zagranicznej przyznanej przez Unię Europejską krajom rozwijającym się, krajom kandydującym lub innym krajom-beneficjentom lub w odniesieniu do naruszeń przepisów prawa celnego. W celu efektywnego wykrywania i zwalczania takich naruszeń OLAF musi zatem przeprowadzać inspekcje i kontrole na miejscu również w państwach trzecich. Znaczenie współpracy międzynarodowej, a tym samym również wymiany danych, ilustruje fakt, iż obecnie Unia Europejska posiada ponad 50 porozumień wzajemnej pomocy administracyjnej w sprawach celnych, w tym z dużymi partnerami handlowymi, takimi jak Chiny, Stany Zjednoczone Ameryki, Japonia, Turcja, Federacja Rosyjska oraz Indie.

17. Wdrażanie przepisów rozporządzenia (WE) nr 45/2001 w działalności OLAF było przedmiotem wielu interwencji EIOD w ostatnich latach. W odniesieniu do celu wniosku (dochodzenia OLAF) należy zwrócić uwagę na opinię z dnia 23 czerwca 2006 r. w sprawie powiadamiania o kontroli wstępnej w odniesieniu do dochodzeń wewnętrznych OLAF ([16]), opinię z dnia 4 października 2007 r. w sprawie pięciu powiadomień o kontroli wstępnej w odniesieniu do dochodzeń zewnętrznych ([17]) oraz opinię z dnia 19 lipca 2007 r. w sprawie powiadamiania o kontroli wstępnej w odniesieniu do regularnego monitorowania realizacji funkcji dochodzeniowej ([18]), która dotyczy działalności Komitetu Nadzoru.

2.2. **Prywatność i ocena skutków**

18. Ani wniosek, ani załączone do wniosku uzasadnienie nie zawierają odniesienia do wpływu wniosku na zasady ochrony danych. Brakuje w nich również odniesień do oceny skutków w zakresie prywatności i ochrony danych. Wyjaśnienie, w jaki sposób rozwiązano kwestię wpływu na ochronę danych, z pewnością zwiększyłoby przejrzystość ogólnej oceny wniosku. EIOD z zaskoczeniem przyjmuje fakt, że w uzasadnieniu zupełnie nie uwzględniono rozdziału poświęconego wynikom konsultacji z zainteresowanymi stronami oraz ocenom skutków.

2.3. **Zastosowanie rozporządzenia (WE) nr 45/2001**

19. Jak wspomniano w poprzedniej opinii w sprawie wniosku z 2006 r. ([19]), EIOD z zadowoleniem przyjmuje uznanie we wniosku, że rozporządzenie (WE) nr 45/2001 ma zastosowanie do wszystkich działań związanych z przetwarzaniem danych prowadzonych przez OLAF. W szczególności

([11]) Zob. art. 10, rozporządzenie (WE) nr 1073/1999.

([12]) Eurojust został powołany do życia decyzją Rady 2002/187/WSiSW (zmienioną następnie decyzją Rady 2003/659/WSiSW oraz decyzją Rady 2009/426/WSiSW z dnia 16 grudnia 2008 r. w sprawie wzmocnienia Eurojustu) jako organ Unii Europejskiej posiadający osobowość prawną, mający stymulować i polepszać koordynację działań i współpracę między właściwymi organami sądowymi państw członkowskich. W szczególności art. 26 ust. 4 tej decyzji stanowi, że „OLAF może wspomagać prace Eurojustu przy koordynowaniu postępowań karnych dotyczących ochrony interesów finansowych Wspólnot Europejskich z inicjatywy Eurojustu lub na wniosek OLAF-u, w przypadku gdy zainteresowane właściwe organy krajowe nie sprzeciwiają się temu udziałowi". W 2008 r. Eurojust i OLAF zawarły porozumienie administracyjne (Praktyczne porozumienie w sprawie zasad współpracy między Eurojustem a OLAF z dnia 24 września 2008 r.), którego celem jest zacieśnianie współpracy między obydwoma podmiotami i które zawiera przepis szczegółowy dotyczący przekazywania danych osobowych.

([13]) Europol to Europejski Urząd Policji, którego celem jest poprawa efektywności i współpracy właściwych organów w państwach członkowskich w zakresie zapobiegania terroryzmowi, nielegalnemu handlowi narkotykami i innym formom poważnej przestępczości zorganizowanej oraz zwalczania tych zjawisk. Artykuł 22 decyzji Rady z dnia 6 kwietnia 2009 r. ustanawiającej Europejski Urząd Policji (Europol) (2009/371/WSiSW) stanowi, że „W zakresie, w jakim jest to istotne dla wykonywania jego zadań, Europol może ustanawiać i utrzymywać współpracę z […] Europejskim Urzędem ds. Zwalczania Nadużyć Finansowych (OLAF)". We wspomnianym artykule przewiduje się również, że Europol może, przed wejściem w życie porozumień lub uzgodnień roboczych z różnymi podmiotami UE, do współpracy z którymi został wezwany, „bezpośrednio uzyskać i wykorzystywać informacje, w tym dane osobowe, pochodzące od podmiotów […] w zakresie, w jakim jest to niezbędne do właściwego wykonywania jego obowiązków, i może […] bezpośrednio przekazywać informacje, w tym dane osobowe, do tych podmiotów w zakresie, w jakim jest to niezbędne do właściwego wykonywania obowiązków odbiorcy".

([14]) Zob. art. 22 decyzji Rady z dnia 6 kwietnia 2009 r. ustanawiającej Europejski Urząd Policji (Europol) (2009/371/WSiSW), Dz.U. L 121 z 15.5.2009, s. 37.

([15]) Zob. art. 1 ust. 26 decyzji Rady 2009/426/WSiSW z dnia 16 grudnia 2008 r. w sprawie wzmocnienia Eurojustu i w sprawie zmiany decyzji 2002/187/WSiSW.

([16]) Sprawa 2005-418, dostępna na stronie: http://www.edps.europa.eu

([17]) Sprawy 2007-47, 2007-48, 2007-49, 2007-50, 2007-72, dostępne na stronie: http://www.edps.europa.eu

([18]) Sprawa 2007-73, dostępna na stronie: http://www.edps.europa.eu

([19]) Opinia EIOD w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (WE) nr 1073/1999 dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF), Dz.U. C 91 z 26.4.2007, s. 1.

w nowym art. 8 ust. 4 ([20]) wyraźnie zaznaczono rolę rozporządzenia w kontekście różnych działań OLAF. Jest to aktualizacja tekstu rozporządzenia (WE) nr 1073/1999, w którym jedynie wspomniano o dyrektywie 95/46/WE jako punkcie odniesienia w zakresie obowiązków ochrony danych.

20. W ostatnim zdaniu art. 8 ust. 4 wprowadza się realizację obowiązku wyznaczenia inspektora ochrony danych: „Urząd powołuje inspektora ochrony danych zgodnie z art. 24 rozporządzenia (WE) nr 45/2001". Także wprowadzenie tego zapisu, który formalizuje rzeczywiste powołanie inspektora ochrony danych OLAF, EIOD przyjmuje z zadowoleniem.

21. EIOD obawia się jednak, że wdrożenie standardów ochrony danych w proponowanym tekście nie jest w pełni zgodne z wymaganiami rozporządzenia, co może wzbudzać wątpliwości odnośnie do spójności tekstu. Ten aspekt zostanie szczegółowo omówiony poniżej.

3. UWAGI SZCZEGÓŁOWE

3.1. OLAF a poszanowanie praw podstawowych, w tym zasad ochrony danych

22. Dochodzenia OLAF mogą mieć poważne skutki dla poszanowania praw podstawowych osób fizycznych. Jak wskazał Trybunał Sprawiedliwości w wyroku w sprawie *Kadi* ([21]), wspomniane prawa są chronione przez wspólnotowy porządek prawny. Ściślej rzecz ujmując, w wyroku w sprawie *Schecke* ([22]) Trybunał, w odniesieniu do Karty praw podstawowych Unii Europejskiej („Karta") ([23]), w szczególności jej art. 8 i 52, podkreśla, że jakiekolwiek ograniczenie prawa do ochrony danych osobowych może być uzasadnione wyłącznie wówczas, jeśli zostało przewidziane w przepisach prawa, istota takiego prawa zostaje zachowana i ograniczenie podlega zasadzie proporcjonalności i spełnia cele ogólnego interesu Unii Europejskiej. EIOD przywiązuje dużą wagę do poszanowania praw podstawowych w obszarze działalności OLAF.

23. W motywie 13 wniosku wyjaśnia się, że poszanowanie praw podstawowych osób objętych dochodzeniem, w szczególności przy przekazywaniu informacji o dochodzeniach w toku, powinno być zawsze zagwarantowane. W dalszej części motywu podkreśla się konieczność przestrzegania poufności dochodzeń, przynależnych praw osób objętych dochodzeniem, przepisów krajowych mających zastosowanie w postępowaniach sądowych i wreszcie przepisów Unii w sprawie ochrony danych. Wskazuje się, że wymiana informacji powinna podlegać zasadom proporcjonalności i ograniczonego dostępu.

24. W motywie tym najwyraźniej wprowadza się ograniczenie zastosowania praw podstawowych zarówno w zakresie podmiotowym (ograniczenie do osób objętych dochodzeniem), jak i w zakresie przedmiotowym (ograniczenie do wymiany informacji). Mogłoby to doprowadzić do niewłaściwej interpretacji tekstu, zgodnie z którą prawa podstawowe w obszarze działalności OLAF byłyby stosowane w sposób „ograniczający" ([24]).

25. EIOD sugeruje zatem zmodyfikowanie tekstu motywu w celu uniknięcia ewentualnych błędnych interpretacji: w motywie zaznaczono, że poszanowanie praw podstawowych „osób objętych dochodzeniem" powinno być zawsze zagwarantowane. Jednak w związku z tym, że OLAF zajmuje się nie tylko osobami objętymi dochodzeniem („podejrzanymi"), ale również informatorami (osobami przekazującymi informacje na temat potencjalnej lub zaistniałej sprawy), osobami zgłaszającymi przypadki naruszenia ([25]) (osoby w ramach instytucji UE, które zgłaszają do OLAF fakty związane z potencjalną lub zaistniałą sprawą) i świadkami, w przepisie należy bardziej ogólnie zdefiniować kategorie „osób", którym przysługują prawa podstawowe.

26. Ponadto motyw 13 dotyczy poszanowania praw podstawowych w szczególności w kontekście „wymiany informacji". W motywie zaznacza się, że poza poszanowaniem praw podstawowych i przestrzeganiem poufności, „(i)nformacje przekazane lub uzyskane w trakcie dochodzeń powinny być traktowane zgodnie z przepisami Unii w sprawie ochrony danych". Zdanie w tym miejscu może być mylące i należy je umieścić w oddzielnym motywie, aby było jasne, że przestrzeganie przepisów w zakresie ochrony danych jest oddzielnym i niezależnym obowiązkiem, a nie tylko obowiązkiem powiązanym z wymianą danych.

([20]) „Urząd przetwarza tylko takie dane osobowe, jakie są mu niezbędne do wypełnienia zadań na podstawie niniejszego rozporządzenia. Takie przetwarzanie danych osobowych odbywa się zgodnie z rozporządzeniem (WE) nr 45/2001 i obejmuje przekazywanie stosownych informacji osobom, których dotyczą dane, wymagane przepisami art. 11 i 12 tego rozporządzenia. Takie informacje nie mogą być przekazywane osobom innym niż te, których funkcje w instytucjach Unii lub w państwach członkowskich wymagają ich znajomości, ani być wykorzystywane do innych celów niż zwalczanie nadużyć finansowych, korupcji i wszelkiej innej nielegalnej działalności. (…)".

([21]) Wyrok z dnia 3 września 2008 r. w sprawach połączonych C-402/05 P i C-415/05 P, Kadi przeciwko Radzie Unii Europejskiej i Komisji Wspólnot Europejskich, pkt 283, „[…] prawa podstawowe stanowią integralną część ogólnych zasad prawa, nad których przestrzeganiem czuwa Trybunał. W tym zakresie Trybunał opiera się na tradycjach konstytucyjnych, wspólnych państwom członkowskim, oraz na wskazówkach zaczerpniętych z umów międzynarodowych dotyczących ochrony praw człowieka, przy których tworzeniu państwa członkowskie współpracowały lub do których przystąpiły. EKPC ma tutaj znaczenie szczególne". Zob. również pkt 304.

([22]) Wyrok z dnia 9 listopada 2010 r. w sprawach połączonych C-92/09 i C-93/09, *Volker und Markus Schecke*, pkt 44 i nast.

([23]) Po wejściu w życie traktatu lizbońskiego EKPC ma zastosowanie do wszystkich obszarów działalności Unii Europejskiej.

([24]) Zob. również ust. 36 poniżej.

([25]) Zob. opinia w sprawie powiadamiania o kontroli wstępnej przez inspektora danych osobowych Europejskiego Urzędu ds. Zwalczania Nadużyć Finansowych (OLAF) w sprawie dochodzeń wewnętrznych OLAF, dnia 23 czerwca 2006 r., sprawa 2005/0418, dostępna na stronie: http://www.edps.europa.eu

27. EIOD z zadowoleniem przyjmuje fakt, że art. 7a jest poświęcony gwarancjom proceduralnym w trakcie dochodzeń. Ten nowy przepis jest zgodny z celem wniosku polegającym na zwiększeniu rozliczalności OLAF. Artykuł zawiera również odniesienie do Karty, która zawiera przepisy istotne z punktu widzenia dochodzeń OLAF, mianowicie art. 8 („Ochrona danych osobowych") oraz cały tytuł VI („Wymiar sprawiedliwości").

28. W art. 7a ust. 1 wniosku nakłada się na Urząd wymóg poszukiwania zarówno dowodów obciążających, jak i odciążających osobę objętą dochodzeniem, oraz przypomina się o obowiązku prowadzenia dochodzeń w sposób obiektywny i bezstronny. Wspomniane zasady mają pozytywny wpływ na zasadę „jakości danych" ([26]) ustanowioną w art. 4 rozporządzenia (WE) nr 45/2001 w zakresie, w jakim wymaga się, aby dane były prawidłowe, zgodne z obiektywną rzeczywistością, kompletne i aktualne. EIOD z zadowoleniem przyjmuje zatem dodanie tego ustępu.

Prawo do informacji, prawo dostępu i prawo do sprostowania

29. Przedstawione poniżej ustępy art. 7a dotyczą różnych etapów dochodzeń prowadzonych przez OLAF. Etapy te można podsumować w następujący sposób: (i) przesłuchiwanie świadków lub zainteresowanych osób (art. 7a ust. 2); (ii) ustalenie, że dana osoba jest objęta prowadzonymi dochodzeniami (art. 7a ust. 3); (iii) przedstawienie wniosków z dochodzenia odnoszących się imiennie do tej osoby (art. 7a ust. 4).

30. EIOD zauważa, że o obowiązku przekazania informacji zgodnie z art. 11 i 12 rozporządzenia (WE) nr 45/2001 wspomina się (wyłącznie) w związku z etapem (iii) powyżej. EIOD z zadowoleniem stwierdza, że we wniosku uwzględniono zalecenia EIOD przedstawione w opinii z 2006 r. ([27]).

31. Tego rodzaju selektywne wskazanie praw osób, których dotyczą dane, w odniesieniu do pojedynczego etapu procedury może jednak zostać zinterpretowane w taki sposób, że osobie, której dotyczą dane (świadkowi lub zainteresowanej osobie), nie powinno się udzielać takich samych informacji w przypadku, gdy zostanie ona wezwana na przesłuchanie, lub gdy pracownik otrzyma informację o tym, że taka osoba może być objęta zakresem prowadzonego dochodzenia. Ze względu na jasność prawną EIOD sugeruje, by w odniesieniu do wszystkich trzech sytuacji wskazanych w pkt (i), (ii) i (iii) powyżej dodać odniesienia do odpowiednich artykułów. Jeżeli jednak informacje, o których mowa w art. 11 lub 12 rozporządzenia (WE) nr 45/2001, zostały przekazane osobie, której dotyczą dane, ponowne przekazywanie tych samych informacji na dalszych etapach nie będzie konieczne.

32. Ponadto w tekście nie wprowadza się żadnego uściślenia w odniesieniu do prawa dostępu i prawa do sprostowania przysługującego osobie, której dotyczą dane, zgodnie z przepisami art. 13 i 14 rozporządzenia (WE) nr 45/2001. Prawa te podlegają ochronie na mocy art. 8 ust. 2 Karty i w związku z tym zajmują szczególne miejsce pośród praw przysługujących osobie, której dotyczą dane. EIOD zwrócił się już ([28]) o dodanie wyraźniejszego uściślenia w sprawie prawa dostępu i prawa do sprostowania przysługującego osobie, której dotyczą dane, w celu uniknięcia ryzyka związanego z możliwością zinterpretowania tekstu jako wprowadzającego szczególną „obniżoną normę" w ramach systemu ochrony danych dla osób objętych dochodzeniami prowadzonymi przez OLAF. EIOD z przykrością stwierdza, że elementy te nie zostały uwzględnione we wniosku.

33. EIOD pragnie również zwrócić uwagę na możliwość ograniczenia prawa do informacji, dostępu i sprostowania w określonych przypadkach, zgodnie z przepisami art. 20 rozporządzenia (WE) nr 45/2001. W związku z tym przestrzeganie zasad ochrony danych przez OLAF może iść w parze z koniecznością zachowania poufności prowadzonych przez niego dochodzeń. Kwestia ta zostanie omówiona szerzej w poniższych punktach.

Poufność dochodzenia i prawa osoby, której dotyczą dane

34. EIOD zasadniczo uznaje, że pełniona przez OLAF rola organu dochodzeniowego wymaga zdolności do ochrony poufności prowadzonych dochodzeń w celu skutecznego zwalczania nadużyć finansowych i nielegalnej działalności, co stanowi podstawowy aspekt jego działalności. EIOD zwraca jednak uwagę na fakt, że uprawnienie to wywiera wpływ na niektóre prawa osób, których dotyczą dane, i że w rozporządzeniu (WE) nr 45/2001 ustanowiono szczególne warunki, w których takie prawa mogą podlegać ograniczeniu w omawianym kontekście (art. 20).

35. Zgodnie z przepisami art. 20 rozporządzenia (WE) nr 45/2001 prawa przyznane na mocy art. 4 (jakość danych) oraz art. 11 do 17 (informacje, które należy przedstawić, prawo dostępu, prawo do sprostowania, zablokowania, skasowania, prawo do powiadomienia osób trzecich) może zostać ograniczone na okres niezbędny do tego, aby chronić między innymi: „a) zapobieganie, dochodzenie, wykrywanie i karanie przestępstw" lub „b) ważny interes ekonomiczny lub finansowy państwa członkowskiego lub Wspólnot Europejskich" oraz „e) funkcje kontrolne, inspekcyjne […] związane nawet sporadycznie z wykonywaniem władzy publicznej w przypadkach wymienionych w lit. a) i b) powyżej". Ten sam artykuł stanowi, że osoba, której dotyczą dane, powinna zostać poinformowana o podstawowych powodach zastosowania takiego ograniczenia, a także o możliwości odwołania się do EIOD (art. 20 ust. 3). Ponadto art. 20 ust. 5 stanowi, że dostarczenie informacji tego rodzaju może zostać odłożone na tak długo, aby taka informacja nie pozbawiła efektu ograniczenia nałożonego przez ust. 1.

([26]) Porównaj: przypis 25.

([27]) Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (WE) nr 1073/1999 dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF), Dz.U. C 91 z 26.4.2007, s. 1, pkt 14 i nast.

([28]) W swojej opinii z 2006 r., zob. przypis 19 powyżej.

36. Tekst wniosku zasadniczo wprowadza wyjątki od obowiązku przestrzegania praw przysługujących osobom, których dotyczą dane, ze względu na konieczność zapewnienia poufności prowadzonych dochodzeń. Artykuł 7a ust. 4 stanowi, że „Nie naruszając przepisów art. 4 ust. 6 i art. 6 ust. 5" ([29]) nie można wyciągać wniosków odnoszących się imiennie do osoby objętej dochodzeniem „po zakończeniu dochodzenia, bez umożliwienia jej ustosunkowania się do dotyczących jej faktów na piśmie lub w czasie przesłuchania […] i przekazania jej informacji wymaganych przepisami art. 11 i 12 rozporządzenia (WE) nr 45/2001". W związku z tym tekst zdaje się sugerować, że w przypadkach przewidzianych w art. 4 ust. 6 i art. 6 ust. 5 prawo do bycia wysłuchanym i prawo do informacji przysługujące osobie, której dotyczą dane, może podlegać ograniczeniu.

37. Wniosek stanowi również, że w przypadkach, w których jest to konieczne dla zachowania poufności dochodzenia i które wiążą się z zastosowaniem środków dochodzeniowych będących w kompetencji krajowego organu sądowego, dyrektor generalny OLAF może zadecydować o odroczeniu obowiązku wezwania osoby objętej dochodzeniem do wyrażenia swojego stanowiska. Tekst nie wskazuje, czy w tym kontekście również udzielenie informacji, których przedstawienie jest wymagane zgodnie z przepisami art. 11 i 12 rozporządzenia (WE) nr 45/2001, powinno zostać odroczone.

38. Zawarte w tekście sformułowanie jest niejasne. Po pierwsze, związek między możliwymi ograniczeniami praw osoby objętej dochodzeniem w związku z wnioskami odnoszącymi się do niej imiennie a rodzajem informacji, które OLAF powinien przekazać odpowiedniemu organowi UE w ramach bieżącego dochodzenia, jest niejasny. Po drugie, nie wskazano jednoznacznie, które kategorie praw osoby, której dotyczą dane, mogą podlegać potencjalnemu ograniczeniu. Po trzecie, przepisy artykułu nie wprowadzają koniecznego zabezpieczenia przewidzianego w art. 20 ust. 3 rozporządzenia (WE) nr 45/2001.

39. W rezultacie osoby fizyczne mogą w niektórych przypadkach otrzymać wnioski z dochodzenia nie wiedząc o tym, że były objęte takim dochodzeniem, i nie uzyskując żadnych informacji dotyczących powodów, dla których przysługujące im zgodnie z przepisami art. 11 i 12 rozporządzenia (WE) nr 45/2001 prawo do bycia wysłuchanym i prawo do informacji zostało ograniczone.

40. Jeżeli przepisy art. 20 ust. 3 i ust. 5 rozporządzenia (WE) nr 45/2001 byłyby w pełni przestrzegane, sytuacja ta nie byłaby jako taka sprzeczna z przepisami rozporządzenia. Jednak brak wyraźnego odniesienia do artykułów rozporządzenia w tekście nie wydaje się być zgodny z zawartym we wniosku celem polegającym na wzmocnieniu gwarancji procesowych w odniesieniu do osób objętych dochodzeniami prowadzonymi przez OLAF oraz zwiększeniu rozliczalności OLAF.

41. W związku z tym EIOD sugeruje, aby informacje dotyczące potencjalnego ograniczenia praw osoby, której dotyczą dane, w rozumieniu art. 20 rozporządzenia (WE) nr 45/2001, zostały wyraźnie wprowadzone. Ponadto w tekście należy wspomnieć o zabezpieczeniach proceduralnych przewidzianych w art. 20 ust. 3, a także o możliwym wyjątku przewidzianym w art. 20 ust. 5. Stworzenie takiego jasnego przepisu zwiększyłoby pewność prawa osób, których dotyczą dane, oraz wpłynęłoby na poprawę rozliczalności OLAF.

42. Podsumowując, w celu ustanowienia wyraźnie określonego zestawu praw przysługujących osobie, której dotyczą dane, oraz w celu wprowadzenia możliwych wyjątków związanych z koniecznością zapewnienia poufności prowadzonych dochodzeń zgodnie z przepisami art. 20 rozporządzenia (WE) nr 45/2001, EIOD sugeruje, aby tekst jednoznacznie wskazywał:

— informacje, które należy dostarczyć osobie, której dotyczą dane, w celu zapewnienia zgodności z przepisami w zakresie ochrony danych (art. 11 i 12 rozporządzenia (WE) nr 45/2001) w kontekście różnych etapów prowadzonych przez OLAF dochodzeń ([30]): (i) przesłuchań (art. 7a ust. 2); (ii) dostarczania informacji w przypadku, gdy osoba może być objęta dochodzeniem (art. 7a ust. 3) oraz (iii) po zakończeniu dochodzenia (art. 7a ust. 4),

— rodzaj informacji, których przekazanie może zostać odroczone przez OLAF z uwagi na konieczność zapewnienia poufności dochodzenia, z wyraźnie określonymi warunkami takiego odroczenia i kategorii osób, których dotyczą dane, wobec których można je zastosować,

— informacje, które powinny zostać dostarczone osobie, której dotyczą dane, w celu zapewnienia zgodności z przepisami w zakresie ochrony danych w przypadku zastosowania odroczenia przekazania informacji zgodnie z przepisami art. 11 lub 12 lub w przypadku, gdy prawo do dostępu lub sprostowania podlega ograniczeniu (tj. informacji, o których mowa w art. 20 ust. 3 rozporządzenia (WE) nr 45/2001), z uwzględnieniem wyjątku związanego z możliwością zastosowania dodatkowego odroczenia przekazania informacji zgodnie z przepisami art. 20 ust. 5 rozporządzenia (WE) nr 45/2001.

([29]) Artykuł 4 ust. 6 – „Dochodzenia wewnętrzne" – brzmi następująco: „Jeżeli w wyniku dochodzeń okaże się, że członek lub członek personelu może być objęty dochodzeniem wewnętrznym, o fakcie tym informowana jest jego instytucja, organ, urząd lub agencja. W wyjątkowych przypadkach, gdy nie można zapewnić poufności dochodzenia, Urząd korzysta z odpowiednich alternatywnych kanałów przekazywania informacji". Artykuł 6 ust. 5 – „Procedura dochodzeń" – brzmi następująco: „Jeżeli z dochodzenia wynika, że wskazane może być podjęcie zapobiegawczych środków administracyjnych w celu ochrony interesów finansowych Unii, Urząd bez zbędnej zwłoki informuje zainteresowaną instytucję, zainteresowany organ lub urząd lub zainteresowaną agencję o toczącym się dochodzeniu. Przekazywane informacje obejmują następujące elementy: a) tożsamość członka lub członka personelu objętego dochodzeniem oraz streszczenie odnośnego stanu faktycznego; b) wszelkie informacje, które mogą pomóc instytucji, organowi, urzędowi lub agencji w podjęciu decyzji o ewentualnym zastosowaniu zapobiegawczych środków administracyjnych w celu ochrony interesów finansowych Unii; c) informacje o wszelkich zalecanych specjalnych środkach służących zachowaniu poufności, szczególnie w sprawach wiążących się z zastosowaniem środków dochodzeniowych należących do zakresu kompetencji krajowych organów sądowych lub, w przypadku dochodzeń zewnętrznych, do zakresu kompetencji organów krajowych, zgodnie z prawem krajowym mającym zastosowanie do dochodzeń. […]", podkreślenie dodane.

([30]) Jak wspomniano powyżej, po przekazaniu informacji osobie, której dotyczą dane, ponowne przekazanie tych samych informacji na późniejszych etapach nie jest konieczne.

3.2. **Polityka informacyjna**

43. EIOD zwraca uwagę na fakt, że jakiekolwiek informacje dotyczące dochodzeń, które mogą zostać upublicznione przez OLAF, mogą zawierać wrażliwe dane osobowe, a konieczność ich opublikowania musi zostać każdorazowo poddana dokładnej ocenie. W swoim wyroku w sprawie *Nikolaou* z 2007 r. ([31]) Sąd Pierwszej Instancji (obecnie Sąd) orzekł, że OLAF naruszył przepisy art. 8 ust. 3 rozporządzenia (WE) nr 1073/1999 ([32]) oraz rozporządzenia (WE) nr 45/2001, nie wykonując należycie spoczywającego na nim obowiązku zapewnienia ochrony danych osobowych w kontekście „przecieku" ([33]) oraz opublikowania komunikatu prasowego ([34]).

44. W związku z tym EIOD z zadowoleniem przyjmuje fakt dodania art. 8 ust. 5, który wprost stanowi, że dyrektor generalny dba o to, by informacje przeznaczone do wiadomości publicznej były podawane „w sposób neutralny, bezstronny" i w poszanowaniu zasad ustanowionych w art. 8 oraz art. 7a. W świetle poczynionych powyżej uwag dotyczących restrykcyjnego podejścia art. 7a do przepisów rozporządzenia (WE) nr 45/2001, EIOD ze szczególnym zadowoleniem przyjmuje szczególnie zawarte w art. 8 ust. 5 odniesienie do bardziej ogólnego przepisu art. 8, który stanowi, że jakiekolwiek przetwarzanie danych w kontekście informacji udostępnianych publicznie przeprowadza się zgodnie ze wszystkimi przepisami rozporządzenia (WE) nr 45/2001.

3.3. **Poufność informacji dotyczących tożsamości osób zgłaszających przypadki naruszenia (ang. „whistleblowers") oraz informatorów**

45. W kontekście przedmiotowego przeglądu EIOD pragnie zwrócić szczególną uwagę na konieczność wprowadzenia szczególnego przepisu gwarantującego poufność informacji dotyczących tożsamości osób zgłaszających przypadki naruszenia oraz informatorów. EIOD podkreśla fakt, że sytuacja osób zgłaszających przypadki naruszenia jest delikatna. Należy zagwarantować poufność informacji dotyczących tożsamości osób dostarczających tego rodzaju informacji, w szczególności wobec osoby, której dotyczą informacje o domniemanych nadużyciach ([35]). Obecne gwarancje (komunikat Komisji SEC/2004/151/2) wydają się być niewystarczające z prawnego punktu widzenia. EIOD zauważa, że tego rodzaju przepis byłby zgodny z opinią grupy roboczej art. 29 ds. ochrony danych w sprawie wewnętrznych systemów zgłaszania przypadków naruszeń ([36]).

46. EIOD zaleca zmianę aktualnego tekstu wniosku oraz zapewnienie poufnego traktowania tożsamości osób zgłaszających przypadki naruszenia i informatorów w trakcie dochodzeń w zakresie, w jakim nie narusza to przepisów krajowych regulujących procedury sądowe. W szczególności osoba, której dotyczą zarzuty, może mieć prawo do uzyskania informacji dotyczących tożsamości osoby zgłaszającej przypadki naruszenia lub tożsamości informatora w celu wszczęcia postępowań sądowych przeciwko takim osobom, jeżeli zostanie ustalone, że umyślnie złożyły one fałszywe zeznania na temat zainteresowanej osoby ([37]).

3.4. **Przekazywanie danych osobowych z OLAF**

Współpraca z Eurojustem i Europolem

47. EIOD z zadowoleniem przyjmuje specyfikacje zawarte w motywie 6 i art. 10a, a w szczególności wprowadzenie wymogu jasnych podstaw prawnych współpracy z Eurojustem i Europolem, co jest całkowicie zgodne z rozporządzeniem (WE) nr 45/2001. Wniosek powinien mieć jednak bardziej szczegółowy charakter, tak aby odzwierciedlał różne systemy ochrony danych dla Eurojustu i Europolu.

48. Do tej pory OLAF wprowadził w życie praktyczne porozumienie z Eurojustem, w którym określono ([38]) warunki, na jakich można realizować przekazywanie danych osobowych. Współpraca pomiędzy OLAF a Eurojustem obejmuje w szczególności wymianę streszczeń spraw oraz związanych ze sprawami informacji strategicznych i operacyjnych, udział w spotkaniach oraz pomoc wzajemną, która może być przydatna w skutecznym i wydajnym realizowaniu właściwych zadań. W praktycznym porozumieniu ([39]) przede wszystkim zdefiniowano sposób działania w odniesieniu do wymiany informacji, w tym danych osobowych, zaś w niektórych przypadkach podkreślono również lub wskazano konkretne elementy istniejących ram prawnych.

([31]) Sprawa T-259/03, *Nikolaou przeciwko Komisji*, dnia 12 lipca 2007 r., Dz.U. C 247 z 20.10.2007, s. 23.

([32]) Artykuł w szczególności odnosi się do przepisów w dziedzinie ochrony danych.

([33]) *Nikolaou*, pkt 213.

([34]) *Nikolaou*, pkt 232.

([35]) EIOD podkreślił już znaczenie poufnego traktowania tożsamości osoby zgłaszającej przypadki naruszenia w piśmie do Europejskiego Rzecznika Praw Obywatelskich z dnia 30 lipca 2010 r. w sprawie 2010-0458, które można znaleźć na stronie EIOD (http://www.edps.europa.eu). Zob. również opinia EIOD w sprawie kontroli wstępnej z dnia 23 czerwca 2006 r. dotycząca dochodzeń wewnętrznych OLAF (sprawa 2005-0418) oraz opinia z dnia 4 października 2007 r. dotycząca dochodzeń zewnętrznych OLAF (sprawy 2007-47, 2007-48, 2007-49, 2007-50, 2007-72).

([36]) Zob. opinia nr 1/2006 grupy roboczej art. 29 z dnia 1 lutego 2006 r. w sprawie zastosowania unijnych zasad ochrony danych do wewnętrznych systemów zgłaszania przypadków naruszenia w dziedzinie księgowości, wewnętrznych kontroli księgowych, spraw związanych z audytem, zwalczania przekupstwa oraz przestępstw bankowych i finansowych, która znajduje się na stronie: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

([37]) Zob. opinia w sprawie reguł finansowych mających zastosowanie do budżetu rocznego Unii z dnia 15 kwietnia 2011 r., dostępna na stronie http://www.edps.europa.eu

([38]) Praktyczne porozumienie w sprawie zasad współpracy między Eurojustem a OLAF z dnia 24 września 2008 r.: zob. przypis 12 powyżej.

([39]) Praktyczne porozumienie między Eurojustem a OLAF, pkt 4.1.

49. Jeśli chodzi o Europol, nie istnieje podobne porozumienie z OLAF ([40]), jednakże decyzja ustanawiająca Europol dopuszcza bezpośrednie otrzymywanie, wykorzystywanie i przekazywanie przez Europol informacji, w tym danych osobowych, między innymi od OLAF, również przed zawarciem formalnego porozumienia o wymianie danych, jeśli jest to konieczne do uzasadnionego wykonywania zadań własnych przez Europol i OLAF ([41]). Wymiana podlega również wymogom porozumienia o poufności pomiędzy tymi dwoma podmiotami. W art. 24 decyzji ustanawiającej Europol określono warunki, których Europol powinien przestrzegać w odniesieniu do wszelkich przypadków przekazywania danych mających miejsce przed zawarciem formalnego porozumienia o wymianie: „Europol jest odpowiedzialny za to, by przekazywanie danych odbywało się w sposób zgodny z prawem. Europol prowadzi ewidencję danych przekazywanych na mocy niniejszego artykułu oraz podstaw ich przekazania. Przekazywanie danych jest dopuszczalne tylko w przypadku, gdy odbiorca zobowiąże się do wykorzystania danych jedynie do celów, do jakich zostały przekazane.". W art. 29 tej samej decyzji określono, kiedy odpowiedzialność za dane przekazywane przez strony trzecie spada na Europol.

50. EIOD stanowczo popiera zawarcie specjalnego porozumienia z Europolem na temat przekazywania danych, a fakt, że nie zostało ono do tej pory podpisane, dodatkowo podkreśla potrzebę szczególnych gwarancji zawartych w treści wniosku. W świetle różnych systemów ochrony danych dotyczących przekazywania danych osobowych z OLAF do Eurojustu i Europolu oraz w drugą stronę EIOD jest zdania, że we wniosku należy w bardziej przejrzysty sposób zawrzeć gwarancje i standardy, które powinny rządzić współpracą pomiędzy OLAF a tymi organami i być uwzględniane w bieżących i przyszłych porozumieniach roboczych między nimi.

51. Celem podkreślenia potrzeby zawarcia porozumień administracyjnych przepisowi art. 10a ust. 2 należy nadać brzmienie „Urząd zawiera porozumienia administracyjne […]". Takie sformułowanie byłoby odzwierciedleniem podobnego przepisu w decyzji ustanawiającej Europol ([42]), który przewiduje, że Europol może zawierać porozumienia lub dokonywać uzgodnień roboczych z innymi instytucjami, organami, biurami i agencjami Unii. Ponadto we wniosku można byłoby zawrzeć w art. 10a wyjaśnienie, że wymiana danych osobowych z Eurojustem i Europolem powinna zasadniczo ograniczać się do zakresu, w jakim jest to *niezbędne* do właściwego wykonywania obowiązków powierzonych OLAF, Europolowi i Eurojustowi. We wniosku powinno się również wprowadzić obowiązek przechowywania przez OLAF rejestru wszystkich przypadków przekazywania danych oraz przyczyn takiego przekazywania, celem wzmocnienia odpowiedzialności OLAF za wdrożenie obowiązków nałożonych rozporządzeniem (WE) nr 45/2001 w odniesieniu do przekazywania danych osobowych.

Współpraca z państwami trzecimi i organizacjami międzynarodowymi

52. W art. 10a ust. 3 wspomina się, że „Urząd może także w razie potrzeby zawrzeć podobne porozumienia administracyjne z właściwymi służbami w państwach trzecich i organizacjami międzynarodowymi. Urząd koordynuje działania z działaniami zainteresowanych służb Komisji oraz Europejskiej Służby Działań Zewnętrznych.".

53. EIOD przyjmuje z zadowoleniem fakt, że współpraca OLAF z państwami trzecimi i organizacjami międzynarodowymi jest powiązana z zawieraniem porozumień administracyjnych. Jednakże związane z ochroną danych osobowych konsekwencje wynikające z możliwej wymiany danych z państwami trzecimi i organizacjami międzynarodowymi powinny zostać bardziej szczegółowo ujęte we wniosku.

54. Wniosek powinien być bardziej szczegółowy w odniesieniu do konkretnych wymagań i warunków możliwych przypadków przekazywania danych od i do państw trzecich i organizacji. EIOD sugeruje, by art. 10a ust. 3 zawierał również następującą treść: „W zakresie, w jakim współpraca z międzynarodowymi organizacjami i państwami trzecimi zakłada przekazywanie danych osobowych z OLAF do innych jednostek, przekazywanie takie powinno być zgodne z kryteriami zawartymi w art. 9 rozporządzenia (WE) nr 45/2001.".

Dostęp Komitetu Nadzoru do danych osobowych

55. EIOD z zadowoleniem przyjmuje sformułowanie art. 11 wniosku, zgodnie z którym „Komitet Nadzoru może zwrócić się do Urzędu o dodatkowe informacje na temat dochodzeń w należycie uzasadnionych sytuacjach, nie ingerując przy tym jednak w przebieg prowadzonych dochodzeń", ponieważ takie sformułowanie ucieleśnia zasadę niezbędności wszelkich możliwych przypadków przekazywania danych z OLAF do Komitetu Nadzoru.

56. Zagadnienie dostępu Komitetu Nadzoru do danych osobowych osób objętych lub potencjalnie objętych dochodzeniami powinno zostać również wyjaśnione w kontekście regulaminu, który ma zostać przyjęty przez Komitet zgodnie z nowym art. 11 ust. 6. EIOD byłby zadowolony, gdyby zaangażowano go w proces przyjmowania regulaminu Komitetu Nadzoru. Zapis o konsultacji z EIOD mógłby zostać również zamieszczony w tekście wniosku jako wymóg przyjęcia regulaminu.

([40]) Porozumienie administracyjne z dnia 8 kwietnia 2004 r. ograniczone jest do wymiany informacji strategicznych i wyraźnie wyklucza wymianę danych osobowych, która to kwestia miałaby być przedmiotem kolejnego porozumienia pomiędzy Europolem a OLAF.

([41]) Decyzja ustanawiająca Europol, art. 22 ust. 3, przypis 14 powyżej.

([42]) Decyzja ustanawiająca Europol, art. 22 ust. 3, zob. przypis 14 powyżej. „Europol może zawierać porozumienia lub dokonywać uzgodnień roboczych z podmiotami, o których mowa w ust. 1" (Eurojust, OLAF, Frontex, CEPOL, EBC i EMCDDA).

4. PLANOWANIE STRATEGICZNE

57. W uzupełnieniu wszystkich konkretnych punktów wspomnianych powyżej EIOD chciałby zachęcić Komisję, by zaproponowała OLAF bardziej otwarte podejście do stosowanego systemu ochrony unijnych danych. Byłby to właściwy moment do opracowania przez OLAF planowania strategicznego zgodności ochrony danych osobowych w drodze dobrowolnego wyjaśnienia praktycznego podejścia do posiadanych przez siebie licznych plików zawierających dane osobowe. OLAF mógłby aktywnie i publicznie wyjaśnić, w jaki sposób podchodzi do danych osobowych w swoich różnorakich działaniach. EIOD jest zdania, że takie szerokie i wyraźne podejście pozwoliłoby zwiększyć przejrzystość traktowania przez OLAF danych osobowych oraz podnieść przyjazność procedur dochodzeniowych.

58. Dlatego też EIOD sugeruje, by w przepisach wniosku zawarto obowiązek zapewnienia przez dyrektora generalnego dokonania szczegółowego przeglądu i aktualizacji wszystkich prowadzonych przez OLAF operacji przetwarzania, lub by zapis taki znalazł się przynajmniej w motywie wniosku. Taki przegląd – którego wyniki powinny być dostępne na przykład w sprawozdaniu rocznym lub w ramach innych rozwiązań – nie tylko wzmocniłby skuteczność różnych działań OLAF i ich współzależność, ale również zachęciłby OLAF do przyjęcia bardziej szerokiego podejścia do kwestii niezbędności i proporcjonalności operacji przetwarzania danych. Ułatwiłby on również wykazanie przez OLAF, że w prawidłowy sposób wdraża zasadę ochrony prywatności w fazie projektowania oraz zasadę odpowiedzialności.

5. WNIOSKI

59. Podsumowując, EIOD z zadowoleniem przyjmuje zmiany wprowadzone do treści wniosku, które zwiększą jego zgodność z systemem ochrony danych osobowych UE.

60. EIOD pragnie jednakże zwrócić dodatkowo uwagę na kilka braków, którymi należy zająć się w drodze modyfikacji tekstu, a w szczególności:

— we wniosku należy jasno wskazać prawo do informacji w odniesieniu do różnych kategorii podmiotów danych, jak również prawo do dostępu do danych i poprawienia ich w odniesieniu do wszystkich etapów dochodzeń prowadzonych przez OLAF,

— we wniosku należy wyjaśnić relację pomiędzy koniecznością zachowania poufności dochodzeń a systemem ochrony danych osobowych mającym zastosowanie w trakcie dochodzeń: EIOD sugeruje, że prawa osób, których dane dotyczą powinny być jasno zdefiniowane i oddzielone, tak samo jak możliwe wyjątki wynikające z wymogów dotyczących poufności i że należy w wyraźny sposób wprowadzić zabezpieczenia przewidziane w art. 20 rozporządzenia (WE) nr 45/2001,

— we wniosku należy jasno przedstawić opinii publicznej politykę informacyjną OLAF w odniesieniu do ochrony danych,

— we wniosku należy wprowadzić konkretne przepisy dotyczące poufności w odniesieniu do osób zgłaszających przypadki naruszenia oraz informatorów,

— we wniosku należy przedstawić ogólne zasady ochrony danych, w oparciu o które OLAF może wymieniać informacje, w tym dane osobowe, z innymi organami UE, państwami trzecimi i organizacjami międzynarodowymi,

— przepisy wniosku powinny zawierać obowiązek zapewnienia przez dyrektora generalnego dokonania strategicznego szczegółowego przeglądu i aktualizacji wszystkich prowadzonych przez OLAF operacji przetwarzania oraz ich przejrzystości, lub też zapis taki powinien znaleźć się przynajmniej w motywie wniosku.

Sporządzono w Brukseli dnia 1 czerwca 2011 r.

Giovanni BUTTARELLI

Zastępca Europejskiego Inspektora Ochrony Danych

Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie integralności i przejrzystości rynku energii

(2011/C 279/03)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

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

uwzględniając Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 7 i 8,

uwzględniając dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych ([1]),

uwzględniając 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 ([2]), w szczególności jego art. 41,

WYDAJE NASTĘPUJĄCĄ OPINIĘ:

I. WPROWADZENIE

1. Dnia 8 grudnia 2010 r. Komisja Europejska przyjęła wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie integralności i przejrzystości rynku energii ([3]) („wniosek").

2. Komisja nie przeprowadziła konsultacji z EIOD, choć wymaga tego art. 28 ust. 2 rozporządzenia (WE) nr 45/2001. Działając z własnej inicjatywy, EIOD wydaje niniejszą opinię w oparciu o art. 41 ust. 2 tego rozporządzenia. EIOD zdaje sobie sprawę z faktu, że niniejsza porada udzielona zostaje na późnym etapie procesu legislacyjnego. Uznaje jednak wydanie niniejszej opinii za zasadne i przydatne ze względu na istotny potencjalny wpływ wniosku na prawo do prywatności i ochronę danych osobowych. Na niniejszą opinię należy również powołać się w preambule wniosku.

3. Zasadniczym celem wniosku jest przeciwdziałanie manipulacjom na rynku i wykorzystaniu informacji wewnętrznych na hurtowych rynkach energii (gazu i energii elektrycznej). Integralność i przejrzystość rynków hurtowych, na których odbywa się obrót gazu i energii elektrycznej pomiędzy przedsiębiorstwami produkującymi energię a przedsiębiorstwami handlowymi, mają kluczowe znaczenie dla cen, jakie ostatecznie płacą konsumenci.

4. W tym celu wniosek dąży do ustanowienia kompleksowych zasad na poziomie unijnym w celu uniemożliwienia przedsiębiorstwom handlowym wykorzystywania informacji wewnętrznych dla własnych korzyści oraz manipulowania rynkiem poprzez sztuczne kształtowanie cen powyżej poziomu uzasadnionego dostępnością, kosztem produkcji oraz pojemnością magazynową lub zdolnością przesyłu energii. Proponowane zasady zakazują w szczególności:

   — wykorzystania informacji wewnętrznych w ramach sprzedaży lub zakupu energii na poziomie rynku hurtowego; informacje posiadane na wyłączność i mające wpływ na cenę należy ujawnić przed zawarciem transakcji,

   — transakcji będących źródłem nieprawdziwych lub wprowadzających w błąd sygnałów na temat podaży, popytu lub cen produktów energetycznych sprzedawanych w obrocie hurtowym, oraz

   — rozpowszechniania nieprawdziwych informacji lub plotek na temat takich produktów.

5. Za monitorowanie rynku na poziomie europejskim w celu wykrywania ewentualnych przypadków naruszenia powyższych zakazów odpowiadać będzie Agencja ds. Współpracy Organów Regulacji Energetyki („ACER") ([4]).

6. Zgodnie z wnioskiem, ACER uzyska szybki dostęp do danych na temat transakcji zawieranych na hurtowych rynkach energii. Dotyczy to informacji na temat ceny, wielkości sprzedaży oraz zaangażowanych stron. Taki zasób danych będzie również udostępniany krajowym organom regulacyjnym, które w dalszej kolejności będą zobowiązane do badania podejrzeń o nadużycie. W przypadkach powodujących skutki transgraniczne ACER będzie uprawniona do koordynowania dochodzeń. Krajowe organy regulacyjne w państwach członkowskich będą nakładały kary finansowe.

7. Wniosek jest kolejnym z wielu innych niedawnych wniosków legislacyjnych mających wzmocnić istniejące uzgodnienia w zakresie nadzoru finansowego oraz poprawę koordynacji i współpracy na poziomie unijnym, do których należy dyrektywa w sprawie wykorzystywania poufnych informacji i manipulacji na rynku („MAD") ([5]) i dyrektywa

([1]) Dz.U. L 281 z 23.11.1995, s. 31 (zwana dalej: „dyrektywa 95/46/WE").
([2]) Dz.U. L 8 z 12.1.2001, s. 1 (zwana dalej: „rozporządzenie (WE) nr 45/2001").
([3]) COM(2010) 726 wersja ostateczna.
([4]) ACER jest organem Unii Europejskiej utworzonym w 2010 r. Do jej obowiązków należy pomoc krajowym organom regulacji energii w wykonywaniu na poziomie unijnym zadań regulacyjnych realizowanych w państwach członkowskich oraz, w zależności od potrzeby, koordynacja ich działań.
([5]) Dyrektywa 2003/6/WE Parlamentu Europejskiego i Rady z dnia 28 stycznia 2003 r. w sprawie wykorzystywania poufnych informacji i manipulacji na rynku (nadużyć na rynku), Dz.U. L 96 z 12.4.2003, s. 16.

w sprawie rynków instrumentów finansowych („MiFID") ([1]). EIOD przedstawił ostatnio uwagi na temat innego ze wspomnianych niedawnych wniosków ([2]).

II. UWAGI I ZALECENIA EIOD

8. Wniosek zawiera wiele przepisów istotnych z punktu widzenia ochrony danych osobowych:

— art. 6–8 dotyczące monitorowania rynku i przekazywania danych,

— art. 9 dotyczący „ochrony danych i niezawodności operacyjnej",

— art. 10 i 11 dotyczące prowadzenia dochodzeń i egzekwowania przestrzegania przepisów, oraz

— art. 14 dotyczący „stosunków z państwami trzecimi".

II.1. **Monitorowanie rynku i przekazywanie danych (art. 6–8)**

Odnośne przepisy

9. Podstawę wniosku stanowi założenie, że w celu wykrywania nadużyć na rynku (i) konieczny jest skutecznie działający system monitorowania rynku z szybkim dostępem do kompletnych danych na temat transakcji, oraz że (ii) powinien on obejmować monitorowanie na poziomie unijnym. W związku z tym, w proponowanym rozporządzeniu przydzielono ACER zadanie gromadzenia, weryfikacji oraz udostępniania (właściwym organom krajowymi i unijnym) znacznej ilości danych ogólnych pochodzących z hurtowych rynków energii.

10. W szczególności, proponowane rozporządzenie zobowiązuje uczestników rynku do przekazywania ACER „danych na temat zawieranych transakcji", których przedmiotem są produkty energetyczne sprzedawane w obrocie hurtowym. Oprócz danych na temat transakcji uczestnicy rynku zobowiązani są również do przekazywania ACER informacji dotyczących „zdolności produkcyjnej instalacji, ich pojemności magazynowej, wielkości zużycia energii lub zdolności przesyłu energii elektrycznej lub gazu ziemnego".

11. Forma i treść przewidzianych informacji oraz termin ich przekazywania określone zostaną w aktach delegowanych Komisji.

Uwagi i zalecenia EIOD

12. Biorąc pod uwagę fakt, że kwestię określenia treści informacji, które mają być gromadzone w ramach realizacji powyższych zadań monitorowania rynku oraz przekazywania danych, rozporządzenie pozostawia w całości aktom delegowanym, nie można wykluczyć, że będą to również dane osobowe – tj. wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej ([3]). Zgodnie z obowiązującym prawem unijnym, jest to dozwolone wyłącznie w sytuacji, gdy jest to konieczne i proporcjonalne do danego celu ([4]). Proponowane rozporządzenie powinno zatem jasno określać, czy i w jakim stopniu dane na temat transakcji i zdolności, które mają być gromadzone dla celów monitorowania, mogą zawierać dane osobowe ([5]).

13. Jeżeli przewidziane jest przetwarzanie danych osobowych, mogą być również wymagane szczególne zabezpieczenia – np. dotyczące celowości, okresu zatrzymania i potencjalnych odbiorców informacji. Ze względu na ich istotny charakter, zabezpieczenia z zakresu ochrony danych należy określić bezpośrednio w tekście proponowanego rozporządzenia, nie zaś w aktach delegowanych.

14. Jeżeli natomiast nie planuje się przetwarzania danych osobowych (bądź takie przetwarzanie miałoby wyłącznie charakter wyjątku i ograniczałoby się do rzadkich przypadków, gdy przedsiębiorca zajmujący się hurtową sprzedażą energii nie jest osobą prawną, lecz fizyczną), powinno zostać to jednoznacznie określone we wniosku – przynajmniej w jednym z motywów.

II.2. **Ochrona danych i niezawodność operacyjna (art. 9)**

Odnośne przepisy

15. Zgodnie z art. 9 ust. 1 ACER „zapewnia poufność, integralność i ochronę" informacji otrzymanych na podstawie art. 7 (tj. danych na temat transakcji i zdolności gromadzonych w ramach realizacji zadania monitorowania rynku). Artykuł 9 przewiduje również, iż „w stosownych przypadkach" podczas przetwarzania danych na podstawie art. 7 ACER „stosuje się" do przepisów rozporządzenia (WE) nr 45/2001.

16. Ponadto ACER, także na podstawie art. 9 ust. 1, „określa źródła ryzyka operacyjnego i ogranicza je poprzez opracowanie odpowiednich systemów, mechanizmów kontroli i procedur".

17. Wreszcie, art. 9 ust. 2 zezwala ACER na podawanie do wiadomości publicznej części informacji będących w jej posiadaniu, „pod warunkiem że nie zostaną ujawnione wrażliwe informacje handlowe dotyczące poszczególnych uczestników rynku lub poszczególnych transakcji".

([1]) Dyrektywa 2004/39/WE Parlamentu Europejskiego i Rady z dnia 21 kwietnia 2004 r. w sprawie rynków instrumentów finansowych zmieniająca dyrektywę Rady 85/611/EWG i 93/6/EWG i dyrektywę 2000/12/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 93/22/EWG, Dz.U. L 145 z 30.4.2004, s. 1.

([2]) W kwestii szerszego kontekstu powiązanych wniosków legislacyjnych zob. opinia EIOD w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, partnerów centralnych i repozytoriów transakcji, wydana dnia 19 kwietnia 2011 r.; w szczególności jej pkt 4, 5 i 17–20.

([3]) Zob. art. 2 lit. a) dyrektywy 95/46/WE i art. 2 lit. a) rozporządzenia (WE) nr 45/2001.

([4]) Zob. art. 6 ust. 1 lit. c) i art. 7 lit. c) dyrektywy 95/46/WE i art. 4 ust. 1 lit. c) oraz art. 5 lit. b) rozporządzenia (WE) nr 45/2001.

([5]) Artykuł 9 ustęp 1 wniosku – odwołujący się do rozporządzenia (WE) nr 45/2001 – sugeruje, że tak może być w istocie, choć przepis nie zawiera żadnych dalszych szczegółów. W tej kwestii zob. również dział II.2 niniejszej opinii.

Uwagi i zalecenia EIOD

18. EIOD z uznaniem przyjmuje fakt, że art. 9 częściowo poświęcony jest ochronie danych, oraz że proponowane rozporządzenie zawiera szczególny wymóg przestrzegania przez ACER przepisów rozporządzenia (WE) nr 45/2001.

a) Zastosowanie rozporządzenia (WE) nr 45/2001 i dyrektywy 95/46/WE

19. W nawiązaniu do powyższego stwierdzenia EIOD podkreśla, że rozporządzenie (WE) nr 45/2001 ma zastosowanie do ACER w całości, na mocy tegoż rozporządzenia, w każdym przypadku przetwarzania przez nią danych osobowych. Z tego względu we wniosku należy przypomnieć, że rozporządzenie (WE) nr 45/2001 powinno mieć zastosowanie do ACER nie tylko w przypadku przetwarzania przez nią danych na podstawie art. 7, ale również we wszelkich innych sytuacjach – co istotne, również w przypadku przetwarzania przez ACER danych osobowych w związku z podejrzeniem nadużycia na rynku/naruszenia przepisów prawa na podstawie art. 11. Ponadto, dla uściślenia, EIOD zaleca zastąpienie terminu „w stosownych przypadkach" na określenie sytuacji, gdy ACER obowiązana jest stosować się do przepisów rozporządzenia (WE) nr 45/2001, frazą „w każdym przypadku, gdy przetwarzane są dane osobowe".

20. Należy również odnieść się do dyrektywy 95/46/WE, z uwagi na fakt, że dotyczy ona przetwarzania danych osobowych przez zainteresowane krajowe organy regulacyjne. Mianowicie, dla zachowania jasności, EIOD zaleca wskazanie w treści proponowanego rozporządzenia, w sposób ogólny (przynajmniej w jednym z motywów), na fakt, że o ile ACER podlega rozporządzeniu (WE) nr 45/2001, o tyle w przypadku zainteresowanych krajowych organów regulacyjnych zastosowanie ma dyrektywa 95/46/WE.

b) Rozliczalność

21. EIOD z uznaniem przyjmuje wymóg, zgodnie z którym ACER ma określać źródła ryzyka operacyjnego i ograniczać je poprzez opracowanie odpowiednich systemów, mechanizmów kontroli i procedur. Aby dodatkowo wzmocnić zasadę rozliczalności [1], w przypadku, gdyby przetwarzanie danych osobowych miało odgrywać rolę strukturalną, proponowane rozporządzenie powinno zawierać szczególny wymóg stworzenia przez ACER jasnych ram rozliczalności zapewniających zgodność z zasadami ochrony danych i dowody takiej zgodności. Tego rodzaju jasne ramy stworzone przez ACER powinny obejmować wiele elementów, takich jak:

— przyjęcie i aktualizowanie w miarę potrzeby polityki ochrony danych na podstawie oceny skutków (w tym również oceny ryzyka bezpieczeństwa). Taka polityka ochrony danych powinna również zawierać plan bezpieczeństwa,

— przeprowadzanie okresowych kontroli pod kątem stałej adekwatności i zgodności z polityką ochrony danych (w tym kontrole planu bezpieczeństwa),

— podawanie do wiadomości publicznej (przynajmniej częściowo) wyników takich kontroli w celu zapewnienia zainteresowanych stron o zgodności z zasadami ochrony danych, oraz

— informowanie inspektora ochrony danych Komisji, zainteresowanych osób, których dotyczą dane, a w razie konieczności innych zainteresowanych stron i organów, o przypadkach naruszenia zasad ochrony danych i innych incydentach związanych z bezpieczeństwem [2].

22. Analogiczne wymogi powinny mieć zastosowanie w przypadku krajowych organów regulacyjnych i innych zainteresowanych organów unijnych.

c) Upublicznianie informacji przez ACER

23. W związku z wymogiem określonym w art. 9 ust. 2, zgodnie z którym ACER powinna podawać do wiadomości publicznej części informacji będących w jej posiadaniu, EIOD przyjmuje, że celem tego przepisu nie jest zezwolenie ACER na upublicznianie danych w celu „napiętnowania" sprawcy, ani na publiczne ujawnianie bezprawnych działań przedsiębiorstw lub osób fizycznych.

24. Co więcej, we wniosku nie poruszono kwestii ewentualnego zamiaru publicznego ujawniania danych osobowych. Z tego względu, dla uniknięcia wszelkich wątpliwości, proponowane rozporządzenie powinno wyraźnie określać, że upublicznianie informacje nie powinny zawierać danych osobowych, albo precyzować, jakie dane mogą być ewentualnie ujawnianie.

25. W przypadku, gdy mają być upubliczniane dane osobowe, potrzebę ich ujawnienia (np. ze względów przejrzystości) należy dokładnie rozważyć i zestawić z innymi konkurencyjnymi względami, jak potrzeba ochrony przysługującego zainteresowanym osobom prawa do prywatności i ochrony danych osobowych.

26. Stosownie do powyższego, przed każdym przypadkiem ujawnienia danych należy dokonać oceny proporcjonalności, przy uwzględnieniu kryteriów określonych przez Europejski Trybunał Sprawiedliwości w sprawie *Schecke* [3]. W tym przypadku ETS podkreślił, iż odstępstwa i ograniczenia ochrony danych osobowych muszą ograniczać się do tego, co absolutnie konieczne. Ponadto ETS uznał, że instytucje europejskie powinny zbadać inne metody upubliczniania w celu znalezienia takiej, która

[1] Zob. pkt 7 opinii EIOD w sprawie komunikatu Komisji do Parlamentu Europejskiego, Rady, Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów – „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej", wydanej dnia 14 stycznia 2011 r. (tekst w języku angielskim: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf).

[2] Zob. pkt 6.3 powyższej opinii EIOD z dnia 14 stycznia 2011 r.

[3] Wyrok ETS z dnia 9 listopada 2010 r., sprawy połączone C-92/09 i C-93/09 (*Schecke i Eifert*); zob. zwłaszcza pkt 81, 65 i 86.

będzie zgodna z celem upublicznienia, przy jak najmniejszej ingerencji w prawa osoby, której dotyczą dane, do życia prywatnego i ochrony danych osobowych.

II.3. **Uprawnienia dochodzeniowe (art. 10)**

Odnośne przepisy

27. Wniosek przewiduje, iż monitorowanie rynku będzie połączone z dochodzeniem w przypadku, gdy występuje podejrzenie nadużycia na rynku, oraz że może to prowadzić do zastosowania odpowiednich sankcji. Artykuł 10 ustęp 1 wymaga w szczególności przyznania przez państwa członkowskie koniecznych uprawnień dochodzeniowych krajowym organom regulacyjnym w celu zapewnienia stosowania przepisów rozporządzenia dotyczących wykorzystywania informacji wewnętrznych i manipulacji na rynku ([1]).

Uwagi i zalecenia EIOD

28. EIOD z uznaniem przyjmuje zapis w art. 10 ust. 1, zgodnie z którym (i) uprawnienia dochodzeniowe wykonuje się (wyłącznie) w celu zapewnienia stosowania przepisów rozporządzenia dotyczących wykorzystania informacji poufnych i manipulacji na rynku (art. 3 i 4) oraz (ii) uprawnienia te wykonuje się w proporcjonalny sposób.

29. Co więcej, autorzy wniosku powinni pójść o krok dalej w celu zagwarantowania pewności prawa i stosownego poziomu ochrony danych osobowych. Jak zostanie wykazane poniżej, z proponowanego brzmienia art. 10 wynikają dwa poważne problemy. Po pierwsze, art. 10 nie określa wystarczająco jasno zakresu uprawnień dochodzeniowych; nie jest np. wystarczająco jasne, czy można żądać udostępnienia rejestrów prywatnych rozmów telefonicznych lub czy można przeprowadzać kontrole na miejscu w prywatnym mieszkaniu. Po drugie, art. 10 nie zapewnia koniecznych zabezpieczeń proceduralnych przed ryzykiem nieuzasadnionego naruszenia prywatności lub niewłaściwego wykorzystania danych osobowych; nie przewidziano np. wymogu uzyskania nakazu od organu sądowego.

30. Określenie zakresu uprawnień dochodzeniowych, jak i koniecznych zabezpieczeń, pozostawiono przypuszczalnie w gestii prawa krajowego. Artykuł 10 ustęp 1 *de facto* pozostawia państwom członkowskim wiele opcji otwartych, określając, iż uprawnienia dochodzeniowe „mogą być wykonywane: a) bezpośrednio, b) we współpracy z innymi organami lub przedsiębiorstwami rynkowymi lub c) poprzez składanie wniosków do właściwych organów sądowych". Wydaje się, że pozwala to na rozbieżności w praktykach krajowych, np. w kwestii tego, czy i w jakich okolicznościach wymagany jest nakaz organu sądowego.

31. Choć niektóre systemy prawa krajowego mogą już zawierać odpowiednie zabezpieczenia proceduralne i zabezpieczenia z zakresu ochrony danych, jednak w celu zagwarantowania pewności prawa osobom, których dane dotyczą, należy wprowadzić pewne objaśnienia i określić pewne wymogi minimalne dotyczące zabezpieczeń proceduralnych i zabezpieczeń z zakresu ochrony danych na poziomie unijnym, w ramach proponowanego rozporządzenia, jak zostanie to omówione poniżej.

32. EIOD podkreśla iż, co do zasady, w sytuacji, gdy prawodawstwo unijne zobowiązuje państwa członkowskie do zastosowania na poziomie krajowym środków, które mają wpływ na prawa podstawowe (takie jak prawo do prywatności i prawo do ochrony danych osobowych), prawodawstwo takie powinno również wymagać, aby jednocześnie ze środkami ograniczającymi stosowane były również skuteczne środki ochrony właściwych praw podstawowych. Innymi słowy, harmonizacji środków potencjalnie naruszających prywatność powinna towarzyszyć harmonizacja odpowiednich zabezpieczeń proceduralnych i zabezpieczeń z zakresu ochrony danych, opartych na najlepszych praktykach.

33. Tego rodzaju podejście mogłoby ułatwić przeciwdziałanie zbyt daleko idącym rozbieżnościom na poziomie krajowym oraz zapewnienie wyższego i bardziej ujednoliconego poziomu ochrony danych osobowych w całej Unii Europejskiej.

34. Jeżeli harmonizacja minimalnych zabezpieczeń na obecnym etapie nie jest możliwa, EIOD zaleca, jako minimum, wprowadzenie do rozporządzenia szczególnego wymogu przyjęcia przez państwa członkowskie krajowych środków wykonawczych w celu zapewnienia koniecznych zabezpieczeń proceduralnych i zabezpieczeń z zakresu ochrony danych. Jest to tym bardziej istotne, iż wybraną formą instrumentu prawnego jest rozporządzenie, które stosowane jest bezpośrednio, zatem zasadniczo nie musi oznaczać konieczności przyjęcia dalszych środków wykonawczych przez państwa członkowskie.

II.4. **Kontrole na miejscu (art. 10 ust. 2 lit. c))**

Odnośne przepisy

35. Wniosek wymaga, by przyznawane krajowym organom regulacyjnym uprawnienia dochodzeniowe obejmowały szczególne prawo do przeprowadzania kontroli na miejscu (art. 10 ust. 2 lit. c)).

Uwagi i zalecenia EIOD

36. Nie jest jasne, czy takie kontrole ograniczałyby się do majątku przedsiębiorstwa (lokali, gruntów i pojazdów) danego uczestnika rynku, czy mogłyby obejmować również majątek prywatny (lokale, grunty lub pojazdy) osób fizycznych. Równie niejasne jest, czy kontrole można przeprowadzać także bez uprzedzenia („naloty o świcie").

37. Jeżeli zamiarem Komisji jest zobowiązanie państw członkowskich do upoważnienia organu regulacyjnego do przeprowadzania kontroli na miejscu obejmujących majątek prywatny osób fizycznych lub na przeprowadzanie kontroli niezapowiedzianych, to, po pierwsze, należy wyraźnie to określić.

([1]) Należy zauważyć, że proponowane rozporządzenie nie przyznaje podobnych uprawnień dochodzeniowych ACER. Uprawnień takich nie przewidziano dla ACER również w rozporządzeniu (WE) nr 713/2009 Parlamentu Europejskiego i Rady z dnia 13 lipca 2009 r. ustanawiającym Agencję ds. Współpracy Organów Regulacji Energetyki, Dz.U. L 211 z 14.8.2009, s. 1.

38. Po drugie, EIOD podkreśla również, iż proporcjonalność kontroli na miejscu obejmujących majątek prywatny (np. prywatne mieszkania osób fizycznych) nie jest wcale kwestią oczywistą, zatem – jeśli jest przewidziana – wymaga szczególnego uzasadnienia.

39. Po trzecie, również w tym przypadku konieczne byłyby dodatkowe zabezpieczenia, w szczególności dotyczące warunków przeprowadzania takich kontroli. Na przykład, wniosek powinien między innymi określać, że kontrolę na miejscu można przeprowadzać w mieszkaniu osoby fizycznej wyłącznie w przypadku, gdy istnieje uzasadnione i konkretne podejrzenie, że w danym mieszkaniu są przechowywane dowody konieczne do wykazania poważnego naruszenia art. 3 i 4 rozporządzenia (tj. przepisów dotyczących zakazu wykorzystywania informacji wewnętrznych i manipulacji na rynku). Co istotne, wniosek powinien również wymagać nakazu sądowego we wszystkich państwach członkowskich ([1]).

40. Po czwarte, w celu zapewnienia proporcjonalności i zapobiegania nadmiernej ingerencji w życie prywatne, niezapowiedziane kontrole w mieszkaniach prywatnych powinny być objęte dodatkowym warunkiem, że w przypadku wizyty zapowiedzianej dowody mogłyby zostać zniszczone lub zmanipulowane. Warunek taki powinien zostać jednoznacznie określony w treści proponowanego rozporządzenia.

II.5. **Uprawnienia do żądania udostępnienia „istniejących rejestrów połączeń telefonicznych i przesyłu danych" (art. 10 ust. 2 lit. d))**

Odnośne przepisy

41. Artykuł 10 ustęp 2 litera d) wymaga, by uprawnienia krajowych organów regulacyjnych obejmowały również szczególne prawo do „żądania udostępnienia istniejących rejestrów połączeń telefonicznych i przesyłu danych".

Uwagi i zalecenia EIOD

42. EIOD docenia znaczenie rejestrów połączeń telefonicznych w przypadkach dotyczących wykorzystania informacji wewnętrznych, szczególnie dla ustalenia powiązań pomiędzy osobami posiadającymi informacje wewnętrzne a przedsiębiorstwami handlowymi. Zakres uprawnień, o których mowa, nie jest jednak wystarczająco jasno określony, a ponadto nie przewidziano również odpowiednich zabezpieczeń proceduralnych i zabezpieczeń z zakresu ochrony danych. W związku z tym EIOD zaleca doprecyzowanie rozporządzenia w sposób opisany poniżej. W szczególności uwzględnić należy następujące kwestie:

a) Jakiego rodzaju rejestry połączeń telefonicznych i przesyłu danych mogą być udostępniane na żądanie?

43. W celu zapewnienia pewności prawa wniosek powinien przede wszystkim wyjaśnić, jakiego rodzaju rejestry mogą być udostępniane w razie potrzeby na żądanie władz.

44. Wniosek powinien w szczególności ograniczać zakres uprawnień dochodzeniowych do (i) treści rejestrów połączeń telefonicznych, poczty elektronicznej i innych przesyłanych danych, które są już gromadzone – w sposób rutynowy i zgodny z prawem – przez przedsiębiorstwa dla potrzeb prowadzonej działalności gospodarczej w celu udokumentowania transakcji, oraz do (b) danych o ruchu (np. kto wykonał połączenie lub przesłał informację, do kogo i kiedy), które są już dostępne bezpośrednio u zainteresowanych uczestników rynku (przedsiębiorstw handlowych).

45. Ponadto rozporządzenie powinno określać, że rejestry muszą być gromadzone w celach legalnych i w zgodzie z obowiązującymi przepisami z zakresu ochrony danych, w tym zgodnie z wymogiem udzielania odpowiednich informacji osobom, których dane dotyczą, na mocy art. 10 i 11 dyrektywy 95/46/WE.

b) Co oznacza określenie „istniejące"?

46. EIOD z uznaniem przyjmuje fakt, że wniosek ogranicza omawiane prawo do „istniejących" rejestrów, a tym samym nie wymaga, by uprawnienia organów regulacyjnych obligowały przedsiębiorstwo handlowe lub osobę trzecią do celowego przechwytywania, monitorowania i rejestrowania połączeń telefonicznych lub przesyłu danych dla potrzeb dochodzenia.

47. W celu uniknięcia wszelkich wątpliwości zamierzenie to należy jednak doprecyzować – przynajmniej w jednym z motywów. Należy uniknąć sytuacji, w której pozostawia się pole do interpretacji proponowanego rozporządzenia jako podstawy prawnej, która sprawi, że krajowe organy regulacyjne będą mogły przechwytywać, monitorować lub rejestrować połączenia bądź transmisję danych, w sposób niejawny lub jawny, z nakazem lub bez niego.

c) Czy można żądać udostępnienia treści rozmów telefonicznych i przesyłu danych, czy jedynie danych o ruchu?

48. W tekście wniosku jest mowa o „istniejących rejestrach połączeń telefonicznych i przesyłu danych". Nie jest wystarczająco jasne, czy można żądać udostępnienia zarówno treści istniejących danych i łączności telefonicznej, jak i danych o ruchu (tj. kto wykonał połączenie lub przesłał informację, do kogo i kiedy).

49. Powyższą kwestię należy doprecyzować w przepisach proponowanego rozporządzenia. Jak wspomniano w pkt 43–45, należy jasno określić, jakiego rodzaju rejestry mogą być udostępniane na żądanie, a przede wszystkim należy zadbać o to, by rejestry takie były gromadzone zgodnie z obowiązującymi przepisami z zakresu ochrony danych.

d) Czy można żądać udostępnienia rejestrów przez dostawców usług internetowych i firmy telekomunikacyjne?

50. Wniosek powinien określać w sposób jednoznaczny, od kogo krajowe organy regulacyjne mogą żądać udostępnienia rejestrów. W tej kwestii EIOD zakłada, że art. 10

([1]) Zob. np. wyrok Europejskiego Trybunału Praw Człowieka w sprawie *Funke* przeciwko *Francji* (sprawa nr 82/1991/334/407) z dnia 25 lutego 1993 r., pkt 55–57.

ust. 2 lit. d) w zamierzeniu nie powinien zezwalać organom krajowym na żądanie udostępnienia danych o ruchu przez dostawców „publicznie dostępnych usług łączności elektronicznej" [1] (takich jak operatorzy telefoniczni lub dostawcy usług internetowych).

51. Wniosek *de facto* nie dotyczy wszystkich takich dostawców, a ponadto nie posługuje się określeniem „dane o ruchu". Co istotne, nie odnosi się on, ani w sposób domyślny, ani wyraźny, do postanowienia mówiącego o tym, że należałoby zastosować odstępstwo od wymogów dyrektywy o prywatności i łączności elektronicznej [2], która określa ogólną zasadę, iż dane o ruchu mogą być poddawane dalszemu przetwarzaniu wyłącznie do celów naliczania opłat abonenta i opłat rozliczeń międzyoperatorskich.

52. W celu uniknięcia wszelkich wątpliwości EIOD zaleca, by fakt, iż wniosek nie stanowi podstawy prawnej, na podstawie której można żądać udostępnienia danych przez dostawców publicznie dostępnych usług łączności elektronicznej, został wyraźnie uwzględniony w tekście proponowanego rozporządzenia – przynajmniej w jednym z motywów.

e) Czy można żądać udostępnienia rejestrów przez inne osoby trzecie?

53. Ponadto, wniosek powinien wyjaśniać, czy krajowe organy regulacyjne mogą żądać udostępnienia rejestrów wyłącznie przez uczestników rynku objętych dochodzeniem, czy są również uprawnione do tego, by żądać od osób trzecich udostępnienia ich rejestrów (np. od strony w transakcji z uczestnikiem rynku objętym dochodzeniem lub od hotelu, w którym przebywała osoba podejrzana o wykorzystanie informacji wewnętrznych).

f) Czy można żądać udostępnienia rejestrów prywatnych?

54. Wreszcie, wniosek powinien także wyjaśniać, czy organy mogą również żądać udostępnienia rejestrów prywatnych osób fizycznych, takich jak pracownicy lub członkowie kadry zarządzającej uczestnika rynku objętego dochodzeniem (np. wiadomości SMS przesyłanych z osobistych urządzeń przenośnych lub historii wyszukiwania domowego łącza internetowego przechowywanej na domowym komputerze).

55. Proporcjonalność żądania udostępnienia rejestrów prywatnych jest dyskusyjna, i – jeśli jest przewidziana – powinna być szczególnie uzasadniona.

56. Podobnie jak w przypadku kontroli na miejscu (zob. pkt 35–40 powyżej), wniosek powinien wymagać nakazu wystawionego przez organ sądowy, a także dalszych szczególnych zabezpieczeń w przypadku, gdy organy żądają udostępnienia jakichkolwiek rejestrów prywatnych.

II.6. **Zgłaszanie podejrzenia nadużycia na rynku (art. 11): celowość i zatrzymywanie danych**

Odnośne przepisy

57. W związku ze współpracą transgraniczną ACER przypada istotna rola ostrzegania krajowych organów regulacyjnych o potencjalnych nadużyciach na rynku i ułatwiania wymiany informacji. W celu ułatwienia współpracy art. 11 ust. 2 zawiera również szczególny wymóg, aby krajowe organy regulacyjne informowały ACER „w możliwie szczegółowy sposób" w przypadku, gdy mają uzasadnione podstawy, aby podejrzewać naruszenie proponowanego rozporządzenia. W celu zapewnienia skoordynowanego podejścia art. 11 ust. 3 wymaga również wymiany informacji pomiędzy krajowymi organami regulacyjnymi, właściwymi organami finansowymi, ACER oraz Europejskim Urzędem Nadzoru Giełd i Papierów Wartościowych („ESMA") [3].

Uwagi i zalecenia EIOD

58. Zgodnie z zasadą celowości [4], wniosek powinien określać wyraźnie, iż wszelkie dane osobowe przekazywane na podstawie art. 11 proponowanego rozporządzenia (zgłoszenia dotyczące podejrzenia nadużycia na rynku) powinny być wykorzystywane wyłącznie w celu zbadania danego zgłoszonego podejrzenia nadużycia na rynku. Informacje takie w żadnym wypadku nie powinny być wykorzystywane dla potrzeb niezgodnych z takim celem.

59. Dane nie powinny być również zatrzymywane przez długi czas. Jest to jeszcze bardziej istotne w przypadkach, gdzie można wykazać, iż pierwotne podejrzenie było nieuzasadnione. W takich przypadkach dalsze zatrzymywanie danych wymaga szczególnego uzasadnienia [5].

60. W tej kwestii wniosek powinien w pierwszej kolejności określić maksymalną długość okresu zatrzymania, przez który ACER i inni odbiorcy informacji mogą przechowywać dane, przy uwzględnieniu celu takiego przechowywania danych. O ile w efekcie podejrzenia nadużycia na rynku nie wszczęto szczegółowego dochodzenia, które nadal znajduje się w toku, po upływie takiego okresu wszelkie dane osobowe związane ze zgłoszonym podejrzeniem nadużycia na rynku powinny zostać usunięte

[1] Zob. art. 2 lit. c) dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywy ramowej), Dz.U. L 108 z 24.4.2002, s. 33.

[2] Zob. art. 6 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz.U. L 201 z 31.7.2002, s. 37.

[3] ESMA jest niezależnym organem unijnym, który przyczynia się do zabezpieczenia stabilności systemu finansowego Unii Europejskiej poprzez zapewnianie integralności, przejrzystości, efektywności i prawidłowego funkcjonowania rynków papierów wartościowych oraz lepszej ochrony inwestorów.

[4] Zob. art. 6 ust. 1 lit. b) dyrektywy 95/46/WE i art. 4 ust. 1 lit. b) rozporządzenia (WE) nr 45/2001.

[5] Dla przykładu, EIOD odwołuje się w tym kontekście do orzeczenia Europejskiego Trybunału Praw Człowieka w sprawie *S i Marper* przeciwko *Zjednoczonemu Królestwu (2008)* (4 grudnia 2008 r.) (skargi nr 30562/04 i 30566/04), zgodnie z którym długoterminowe zatrzymywanie danych osób nieskazanych za przestępstwo było naruszeniem ich prawa do prywatności wynikającego z art. 8 Konwencji o ochronie praw człowieka.

z rejestrów wszystkich odbiorców. O ile z oczywistych względów nie jest wskazany dłuższy okres zatrzymania, w opinii EIOD usunięcie danych powinno nastąpić nie później niż dwa lata po dacie zgłoszenia danego podejrzenia ([1]).

61. W przypadku, gdy podejrzenie okazuje się nieuzasadnione lub dochodzenie zostaje zamknięte bez podjęcia dalszych działań, wniosek powinien zobowiązywać zgłaszający je organ regulacyjny, ACER oraz każdą osobę trzecią posiadającą dostęp do informacji dotyczących danego podejrzenia nadużycia na rynku do niezwłocznego poinformowania tych podmiotów, tak, by były one w stanie odpowiednio zaktualizować własne rejestry (lub usunąć ze swoich rejestrów informacje dotyczące zgłoszonego podejrzenia, odpowiednio, ze skutkiem natychmiastowym bądź po upływie proporcjonalnego okresu zatrzymania) ([2]).

62. Powyższe przepisy powinny pomóc w doprowadzeniu do sytuacji, w której – w przypadku, gdy dane podejrzenie nie znajduje potwierdzenia (lub wręcz nie podjęto w jego sprawie dochodzenia) lub gdy z ustaleń wynika, że podejrzenie jest nieuzasadnione – niewinne osoby nie będą pozostawały na „czarnej liście" i „w kręgu podejrzeń" przez nadmiernie długi okres (zob. art. 6 lit. e) dyrektywy 95/46/WE i odpowiadający mu art. 4 lit. e) rozporządzenia (WE) nr 45/2001).

II.7. **Przekazywanie danych do państw trzecich (art. 14)**

Odnośne przepisy

63. Artykuły 7, 8 i 11 proponowanego rozporządzenia przewidują wymianę danych i informacji pomiędzy ACER, ESMA i organami państw członkowskich. Artykuł 14 („Stosunki z państwami trzecimi") przewiduje, że ACER „może zawierać porozumienia administracyjne z organizacjami międzynarodowymi oraz z administracjami państw trzecich." Może to prowadzić do przekazywania danych osobowych przez ACER – i ewentualnie przez ESMA lub organy państw członkowskich – organizacjom międzynarodowym i organom państw trzecich.

Uwagi i zalecenia EIOD

64. EIOD zaleca, by w art. 14 wniosku doprecyzowano, iż przekazywanie danych osobowych może odbywać się wyłącznie w zgodzie z art. 9 rozporządzenia (WE) nr 45/2001 oraz art. 25 i 26 dyrektywy 95/46/WE. W szczególności, przekazywanie danych w relacji międzynarodowej powinno odbywać się tylko wówczas, gdy dane państwo trzecie zapewnia odpowiedni poziom ochrony danych lub, w przypadku osób prawnych lub fizycznych niezapewniających odpowiedniej ochrony, gdy administrator danych powołuje się na stosowne zabezpieczenia dotyczące ochrony prywatności, praw podstawowych oraz wolności osób fizycznych i związane z wykonaniem odpowiednich praw.

65. EIOD podkreśla, że stosowanie odstępstw (takich jak wymienione w art. 9 ust. 6 rozporządzenia (WE) nr 45/2001 i w art. 26 ust. 1 dyrektywy) zasadniczo nie powinno służyć uzasadnieniu masowego, systematycznego lub strukturalnego przekazywania danych do państw trzecich.

II.8. **Uprzednie sprawdzanie działań koordynacyjnych ACER w związku z dochodzeniami**

66. Niektóre dane wymieniane pomiędzy ACER, ESMA i różnymi organami państw członkowskich w związku z podejrzeniami naruszenia przepisów mogą zawierać dane osobowe, takie jak tożsamość domniemanych sprawców i innych zaangażowanych osób (np. świadków, osób zgłaszających przypadki naruszenia, pracowników lub innych osób występujących w imieniu przedsiębiorstw uczestniczących w transakcji).

67. Artykuł 27 ustęp 1 rozporządzenia (WE) nr 45/2001 stanowi, iż „operacje przetwarzania mogące ze swej natury, przez swój zakres lub swoje cele stworzyć konkretne zagrożenia dla praw i wolności podmiotów danych, podlegają uprzedniemu sprawdzeniu przez europejskiego inspektora ochrony danych". Artykuł 27 ustęp 2 precyzuje, że „przetwarzanie danych" dotyczących „podejrzeń o popełnienie przestępstwa" i „przestępstw" tworzy takie zagrożenia, i wymaga uprzedniego sprawdzenia. Ze względu na rolę przewidzianą dla ACER w ramach koordynowania dochodzeń wydaje się prawdopodobne, że będzie ona przetwarzać dane dotyczące „podejrzeń o popełnienie przestępstwa", a tym samym jej działania będą podlegać uprzedniemu sprawdzeniu ([3]).

68. W ramach procedury uprzedniego sprawdzania EIOD może udzielać ACER dalszych wskazówek i szczegółowych zaleceń dotyczących zgodności z przepisami dotyczącymi ochrony danych. Uprzednie sprawdzanie działań ACER może być również źródłem wartości dodanej, ze względu na fakt, że rozporządzenie (WE) nr 713/2009 ustanawiające ACER nie zawiera żadnego odniesienia do kwestii ochrony danych osobowych, i nie było przedmiotem opinii legislacyjnej EIOD.

III. **WNIOSKI**

69. Wniosek powinien doprecyzować, czy w kontekście monitorowania rynku i przekazywania danych mogą być przetwarzane dane osobowe, a także jakie zabezpieczenia mają zastosowanie. Jeżeli natomiast nie przewiduje się przetwarzania danych osobowych (lub takie przetwarzanie miałoby wyłącznie charakter wyjątkowy i ograniczałoby się do rzadkich przypadków, gdy przedsiębiorca zajmujący się hurtową sprzedażą energii nie jest osobą prawną, lecz osobą fizyczną), należy to jednoznacznie określić w rozporządzeniu – przynajmniej w jednym z motywów.

([1]) W przypadkach, gdy podejrzenie okazuje się uzasadnione i powoduje przeprowadzenie dochodzenia, wniosek powinien określać konkretny – nienadmierny – okres zatrzymania danych po zakończeniu dochodzenia.

([2]) Informacje takie należy również udostępnić osobie, której dane dotyczą.

([3]) Należy podkreślić, że przetwarzanie danych przez organy krajowe może również podlegać uprzedniemu sprawdzeniu przez krajowe lub regionalne organy ds. ochrony danych na podstawie krajowych przepisów z zakresu ochrony danych przyjętych na mocy art. 20 dyrektywy 95/46/WE.

70. Należy doprecyzować i wzmocnić przepisy dotyczące ochrony danych, bezpieczeństwa danych i rozliczalności, zwłaszcza jeśli przetwarzanie danych osobowych miałoby odgrywać bardziej zasadniczą rolę. Komisja powinna zadbać o stosowne mechanizmy kontroli w celu zapewnienia zgodności z zasadami ochrony danych i dowodów takiej zgodności („rozliczalność").

71. Wniosek powinien doprecyzować, czy kontrole na miejscu byłyby ograniczone do majątku przedsiębiorstwa (lokale i pojazdy) danego uczestnika rynku, czy obejmowałyby również majątek prywatny (lokale lub pojazdy) osób fizycznych. W tym ostatnim przypadku należałoby jednoznacznie uzasadnić konieczność i proporcjonalność takiego prawa oraz wprowadzić wymóg nakazu sądowego i dodatkowych zabezpieczeń. Kwestie te powinny być określone w proponowanym rozporządzeniu w sposób jednoznaczny.

72. Należy doprecyzować zakres uprawnień do żądania udostępnienia „istniejących rejestrów połączeń telefonicznych i przesyłu danych". Wniosek powinien określać w sposób jednoznaczny, jakie rejestry mogą być udostępniane na żądanie, i przez kogo. Fakt, że nie można żądać udostępnienia danych przez dostawców publicznie dostępnych usług łączności elektronicznej, powinien być wyraźnie wzmiankowany w tekście proponowanego rozporządzenia – przynajmniej w jednym z motywów. Wniosek powinien również doprecyzować, czy organy mogą żądać udostępnienia również prywatnych rejestrów osób fizycznych, np. pracowników lub członków kadry zarządzającej uczestnika rynku objętego dochodzeniem (np. wiadomości SMS wysyłanych z osobistych urządzeń przenośnych lub historii wyszukiwania domowego łącza internetowego). W takim przypadku należałoby jednoznacznie uzasadnić konieczność i proporcjonalność takiego prawa, a wniosek powinien również określać wymóg nakazu wystawionego przez organ sądowy.

73. W kwestii zgłaszania podejrzeń nadużycia na rynku wniosek powinien wyraźnie określać, że wszelkie dane osobowe zawarte w takich zgłoszeniach powinny być wykorzystywane wyłącznie do celów dochodzenia w sprawie danego zgłoszonego podejrzenia nadużycia na rynku. O ile w efekcie podejrzenia nadużycia na rynku nie wszczęto szczegółowego dochodzenia, które nadal znajduje się w toku (lub o ile podejrzenie nie okazało się uzasadnione, w efekcie czego przeprowadzono dochodzenie), po upływie wyznaczonego okresu wszelkie dane osobowe związane ze zgłoszonym podejrzeniem nadużycia na rynku powinny zostać usunięte z rejestrów wszystkich odbiorców (o ile nie występują inne przesłanki, nie później niż dwa lata od daty zgłoszenia). Ponadto w przypadku, gdy dane podejrzenie okazuje się nieuzasadnione lub dochodzenie zostaje zamknięte bez podjęcia dalszych działań, strony uczestniczące w wymianie informacji powinny również przesyłać sobie wzajemnie aktualne informacje.

74. W kwestii przekazywania danych osobowych do państw trzecich wniosek powinien doprecyzować, że przekazywanie danych osobom prywatnym lub fizycznym w kraju trzecim, który nie zapewnia odpowiedniej ochrony, możliwe jest zasadniczo wyłącznie w przypadku, gdy administrator danych powołuje się na stosowne zabezpieczenia dotyczące ochrony prywatności, praw podstawowych oraz wolności osób fizycznych i związane z wykonaniem odpowiednich praw.

75. ACER powinna wystąpić do EIOD o uprzednie sprawdzenie jej działań z zakresu przetwarzania danych osobowych w związku z koordynacją dochodzeń na podstawie art. 11 proponowanego rozporządzenia.

Sporządzono w Brukseli dnia 21 czerwca 2011 r.

Giovanni BUTTARELLI

Zastępca Europejskiego Inspektora Ochrony Danych

II

(Komunikaty)

KOMUNIKATY INSTYTUCJI, ORGANÓW I JEDNOSTEK ORGANIZACYJNYCH UNII EUROPEJSKIEJ

KOMISJA EUROPEJSKA

Brak sprzeciwu wobec zgłoszonej koncentracji

(Sprawa COMP/M.6349 – Motherson/Cross Industries/Peguform/Wethje)

(Tekst mający znaczenie dla EOG)

(2011/C 279/04)

W dniu 16 września 2011 r. Komisja podjęła decyzję o niewyrażaniu sprzeciwu wobec powyższej zgłoszonej koncentracji i uznaniu jej za zgodną ze wspólnym rynkiem. Decyzja ta została oparta na art. 6 ust. 1 lit. b) rozporządzenia Rady (WE) nr 139/2004. Pełny tekst decyzji dostępny jest wyłącznie w języku angielskim i zostanie podany do wiadomości publicznej po uprzednim usunięciu ewentualnych informacji stanowiących tajemnicę handlową. Tekst zostanie udostępniony:

— w dziale dotyczącym połączeń przedsiębiorstw na stronie internetowej Komisji poświęconej konkurencji: (http://ec.europa.eu/competition/mergers/cases/). Powyższa strona została wyposażona w różne funkcje pomagające odnaleźć konkretną decyzję w sprawie połączenia, w tym indeksy wyszukiwania według nazwy przedsiębiorstwa, numeru sprawy, daty i sektora,

— w formie elektronicznej na stronie internetowej EUR-Lex jako numerem dokumentu 32011M6349 Strona EUR-Lex zapewnia internetowy dostęp do europejskiego prawa. (http://eur-lex.europa.eu/en/index.htm).

Brak sprzeciwu wobec zgłoszonej koncentracji

(Sprawa COMP/M.6218 – Ineos/Tessenderlo Group S-PVC Assets)

(Tekst mający znaczenie dla EOG)

(2011/C 279/05)

W dniu 26 lipca 2011 r. Komisja podjęła decyzję o niewyrażaniu sprzeciwu wobec powyższej zgłoszonej koncentracji i uznaniu jej za zgodną ze wspólnym rynkiem. Decyzja ta została oparta na art. 6 ust. 1 lit. b) rozporządzenia Rady (WE) nr 139/2004. Pełny tekst decyzji dostępny jest wyłącznie w języku angielskim i zostanie podany do wiadomości publicznej po uprzednim usunięciu ewentualnych informacji stanowiących tajemnicę handlową. Tekst zostanie udostępniony:

— w dziale dotyczącym połączeń przedsiębiorstw na stronie internetowej Komisji poświęconej konkurencji: (http://ec.europa.eu/competition/mergers/cases/). Powyższa strona została wyposażona w różne funkcje pomagające odnaleźć konkretną decyzję w sprawie połączenia, w tym indeksy wyszukiwania według nazwy przedsiębiorstwa, numeru sprawy, daty i sektora,

— w formie elektronicznej na stronie internetowej EUR-Lex jako numerem dokumentu 32011M6218 Strona EUR-Lex zapewnia internetowy dostęp do europejskiego prawa. (http://eur-lex.europa.eu/en/index.htm).

IV

(Informacje)

INFORMACJE INSTYTUCJI, ORGANÓW I JEDNOSTEK ORGANIZACYJNYCH UNII EUROPEJSKIEJ

KOMISJA EUROPEJSKA

Kursy walutowe euro [1]

22 września 2011 r.

(2011/C 279/06)

1 euro =

	Waluta	Kurs wymiany		Waluta	Kurs wymiany
USD	Dolar amerykański	1,3448	AUD	Dolar australijski	1,3691
JPY	Jen	102,59	CAD	Dolar kanadyjski	1,3894
DKK	Korona duńska	7,4458	HKD	Dolar Hongkongu	10,4904
GBP	Funt szterling	0,87325	NZD	Dolar nowozelandzki	1,7185
SEK	Korona szwedzka	9,2762	SGD	Dolar singapurski	1,7547
CHF	Frank szwajcarski	1,2275	KRW	Won	1 605,66
ISK	Korona islandzka		ZAR	Rand	11,0754
NOK	Korona norweska	7,8270	CNY	Yuan renminbi	8,6040
BGN	Lew	1,9558	HRK	Kuna chorwacka	7,4845
CZK	Korona czeska	24,878	IDR	Rupia indonezyjska	12 246,50
HUF	Forint węgierski	293,06	MYR	Ringgit malezyjski	4,2744
LTL	Lit litewski	3,4528	PHP	Peso filipińskie	58,919
LVL	Łat łotewski	0,7093	RUB	Rubel rosyjski	43,2059
PLN	Złoty polski	4,4863	THB	Bat tajlandzki	41,379
RON	Lej rumuński	4,3055	BRL	Real	2,4887
TRY	Lir turecki	2,4636	MXN	Peso meksykańskie	18,6738
			INR	Rupia indyjska	66,6720

[1] *Źródło*: referencyjny kurs wymiany walut opublikowany przez ECB.

V

(Ogłoszenia)

POSTĘPOWANIA ADMINISTRACYJNE

KOMISJA EUROPEJSKA

MEDIA 2007 – ROZWÓJ, DYSTRYBUCJA, PROMOCJA I SZKOLENIA

Zaproszenie do składania wniosków – EACEA/21/11

Wspieranie rozwoju projektów produkcji filmów fabularnych, filmow dokumentalnych i filmów animowanych w ramach schematu „Projekty pojedyncze" oraz „Pakiety projektów" I i II etap

(2011/C 279/07)

1. **Cele i opis**

Niniejsze zawiadomienie o zaproszeniu do składania wniosków zostało wydane na podstawie decyzji nr 1718/2006/WE Parlamentu Europejskiego i Rady z dnia 15 listopada 2006 r. w sprawie wprowadzenia w życie programu wspierającego europejski sektor audiowizualny (MEDIA 2007).

Jednym z celów programu jest promowanie, poprzez zapewnienie wsparcia finansowego, rozwoju projektów produkcji przeznaczonych na rynek europejski i międzynarodowy, pochodzących z niezależnych wytwórni, w następujących kategoriach: film fabularny, film dokumentalny i film animowany.

2. **Kwalifikujący się wnioskodawcy**

Niniejsze zawiadomienie jest skierowane do firm europejskich, których działalność przyczynia się do osiągania wyżej wymienionych celów, a w szczególności do niezależnych wytwórni.

Wnioskodawcy muszą mieć siedzibę w jednym z następujących krajów:

— 27 krajów Unii Europejskiej,

— kraje EOG, Szwajcaria i Chorwacja.

3. **Kwalifikujące się działania**

Do dofinansowania kwalifikują się działania w zakresie przygotowywania następujących utworów audiowizualnych (pojedynczych lub seryjnych):

— projekty dotyczące produkcji filmów fabularnych przeznaczonych do komercyjnej eksploatacji o czasie trwania nie krótszym niż 50 minut,

— filmy dokumentalne przeznaczone do komercyjnej eksploatacji, o czasie trwania nie krótszym niż 25 minut (w przypadku seriali – o czasie trwania odcinka),

— projekty dotyczące produkcji filmów animowanych przeznaczonych do komercyjnej eksploatacji, o czasie trwania nie krótszym niż 24 minuty.

Do dofinansowania nie kwalifikują się działania w zakresie przygotowywania i produkcji utworów z następujących kategorii:

— nagrania na żywo, gry telewizyjne, widowiska talk show i reality show lub programy edukacyjne, szkoleniowe i instruktażowe,

— filmy dokumentalne promujące turystykę, relacje z powstania utworu, reportaże o zwierzętach, programy informacyjne i telenowele dokumentalne,

— projekty promujące, bezpośrednio lub pośrednio, przekaz sprzeczny z polityką Unii Europejskiej. Na przykład, projekty, które mogą być niezgodne z interesem zdrowia publicznego (o tematyce związanej z alkoholem, paleniem papierosów, narkotykami) i przestrzeganiem praw człowieka lub zagrażają bezpieczeństwu ludzi, wolności słowa, itd.,

— projekty promujące przemoc i/lub rasizm i/lub zawierające treści pornograficzne,

— utwory o charakterze promocyjnym,

— produkcje realizowane przez instytucje, promujące określoną organizację lub jej działalność.

Zaproszenie 21/11 przewiduje dwa terminy składania wniosków. Aby wniosek o wsparcie został uwzględniony w pierwszym terminie, należy przesłać go do Agencji między datą publikacji zaproszenia a dniem 25 listopada 2011 r. Aby został uwzględniony w drugim terminie, należy przesłać go do Agencji między dniem 26 listopada 2011 r. a dniem 13 kwietnia 2012 r., czyli datą zamknięcia zaproszenia do składania wniosków.

Ostateczna data zakończenia projektu to dzień 30 czerwca 2014 r. – w przypadku wniosków o wsparcie przedłożonych w pierwszym terminie – i dzień 30 listopada 2014 r. dla wniosków przesłanych w drugim terminie, lub data rozpoczęcia etapu produkcyjnego projektu, w zależności od tego, która z tych dat będzie wcześniejsza.

4. **Kryteria przyznania dotacji**

Łączna liczba punktów wynosi 100 i są one przydzielane według następujących wag:

Projekt pojedynczy

— Kryteria dotyczące kandydującego przedsiębiorstwa (40 punktów):

  — jakość strategii rozwoju (10),

  — spójność budżetu przeznaczonego na rozwój (10),

  — jakość strategii finansowania (10),

  — jakość strategii dystrybucji (10).

— Kryteria dotyczące przedłożonego projektu (60 punktów):

  — jakość projektu (40),

  — potencjał produkcyjny i możliwość realizacji projektu (10),

  — potencjał dystrybucyjny w skali europejskiej i międzynarodowej (10).

Pakiety projektów I i II etap

— Kryteria dotyczące kandydującego przedsiębiorstwa (60 punktów):

  — możliwości firmy w zakresie rozwoju i produkcji na poziomie europejskim (15 punktów dla pakietu projektów I etapu – 30 punktów dla pakietu projektów II etapu),

  — jakość strategii rozwoju i spójność budżetu przeznaczonego na rozwój (15 punktów dla pakietu projektów I etapu – 10 punktów dla pakietu projektów II etapu),

— jakość strategii finansowania (15 punktów dla pakietu projektów I etapu – 10 punktów dla pakietu projektów II etapu),

— jakość strategii dystrybucji (15 punktów dla pakietu projektów I etapu – 10 punktów dla pakietu projektów II etapu).

— Kryteria dotyczące przedłożonego projektu (40 punktów):

— jakość projektów (10),

— możliwości zespołu twórców (10),

— potencjał produkcyjny i możliwość realizacji projektu (10),

— potencjał dystrybucyjny w skali europejskiej i międzynarodowej (10).

5. **Budżet**

Dostępny budżet wynosi ogółem 17 mln EUR. Dofinansowanie przyznawane jest w formie dotacji.

Dla projektu pojedynczego może być przyznane maksymalne dofinansowanie w wysokości od 10 000 do 60 000 EUR. Wyjątek stanowią długometrażowe filmy animowane, przeznaczone do wyświetlania w kinach – w tym wypadku kwota maksymalnego dofinansowania może wynieść 80 000 EUR. Przyznane dofinansowanie nie może w żadnym razie przekroczyć 50 % uznanych kosztów, określonych przez producenta we wniosku (60 % w przypadku projektów szczególnie promujących europejską różnorodność kulturową).

Dla pakietu projektów I i II etapu może być przyznane maksymalne dofinansowanie w wysokości od 70 000 do 190 000 EUR. Dofinansowanie nie może w żadnym razie przekroczyć 50 % kwalifikujących się kosztów, określonych przez producenta we wniosku.

Agencja zastrzega sobie prawo do nieprzyznania wszystkich dostępnych środków.

6. **Termin składania wniosków**

Wnioski należy złożyć używając formularza zgłoszeniowego on-line Agencji Wykonawczej (EACEA) oraz wysłać w wersji papierowej pocztą poleconą lub kurierską, nie później niż do dnia zamknięcia tj. **25 listopada 2011 r. i 13 kwietnia 2012 r.** (patrz pkt 3) na poniższy adres:

Education, Audiovisual and Culture Executive Agency (EACEA) — MEDIA
Constantin DASKALAKIS
BOUR 3/30
Avenue du Bourget/Bourgetlaan 1
1140 Bruxelles/Brussel
BELGIQUE/BELGIË

Rozpatrywane będą wyłącznie wnioski złożone na oficjalnym formularzu zgłoszeniowym, podpisane przez osobę uprawnioną do zaciągania prawnie wiążących zobowiązań w imieniu organizacji składającej wniosek.

Wnioski nadesłane faksem lub pocztą elektroniczną zostaną odrzucone.

7. **Szczegółowe informacje**

Pełny tekst przewodnika wraz z formularzem zgłoszeniowym znajduje się na stronie internetowej pod następującym adresem: http://www.ec.europa.eu/media

Wnioski muszą spełniać wszelkie warunki przedstawione w przewodniku i należy je składać na odpowiednich formularzach.

MEDIA 2007 – ROZWÓJ, DYSTRYBUCJA, PROMOCJA I SZKOLENIA

Zaproszenie do składania wniosków – EACEA/22/11

Wspieranie rozwoju projektów interaktywnych online i offline

(2011/C 279/08)

1. **Cele i opis**

Niniejsze zawiadomienie o zaproszeniu do składania wniosków zostało wydane na podstawie decyzji nr 1718/2006/WE Parlamentu Europejskiego i Rady z dnia 15 listopada 2006 r. w sprawie wprowadzenia w życie programu wspierającego europejski sektor audiowizualny (MEDIA 2007).

Jednym z celów programu jest promowanie, poprzez zapewnienie wsparcia finansowego, rozwoju projektów produkcji przeznaczonych na rynek europejski i międzynarodowy, pochodzących z niezależnych europejskich wytwórni.

2. **Kwalifikujący się wnioskodawcy**

Niniejsze zawiadomienie jest skierowane do firm europejskich, których działalność przyczynia się do osiągania wyżej wymienionych celów, a w szczególności do niezależnych wytwórni.

Wnioskodawcy muszą mieć siedzibę w jednym z następujących krajów:

— 27 krajów Unii Europejskiej,

— kraje EOG, Szwajcaria i Chorwacja.

3. **Kwalifikujące się działania**

Do dofinansowania kwalifikują się następujące projekty interaktywne:

Opracowanie koncepcyjne (do pierwszej aplikacji wykorzystywanej jako gra) cyfrowych interaktywnych treści uzupełniających projekt audiowizualny (film fabularny, dokument kreatywny lub film animowany) opracowany specjalnie na jedną z poniższych platform:

— Internet,

— Komputer,

— Konsola,

— Urzadzenia przenosne,

— Telewizja interaktywna.

Te cyfrowe treści muszą posiadać następujące cechy:

— znaczny stopień interaktywności wraz z elementem narracyjnym,

— oryginalność, twórczy i innowacyjny charakter względem istniejących już dzieł,

— potencjał handlowy w Europie.

Zgłaszany utwór interaktywny może uzupełniać jedynie następujące rodzaje projektów audiowizualnych przeznaczonych do wykorzystania w celach handlowych:

— film fabularny o długości co najmniej 50 minut (całkowita długość serialu w przypadku serialu),

— dokument kreatywny o długości co najmniej 25 minut (długość odcinka w przypadku serialu),

— film animowany o długości co najmniej 24 minut (całkowita długość serialu w przypadku serialu).

Nie kwalikują się następujące projekty:

nie kwalifikują się działania w zakresie rozwoju i produkcji należące do następujących kategorii:

— źródła referencyjne (encyklopedie, atlasy, katalogi, bazy danych …),

— pomoce naukowe (programy edukacyjne, podręczniki …),

— narzędzia oraz oprogramowanie,

— usługi o charakterze informacyjnym lub czysto transakcyjnym,

— programy informacyjne i magazyny,

— projekty promujące turystykę,

— multimedialne projekty sztuki,

— strony internetowe istniejące lub przeznaczone specjalnie do platform społecznościowych, serwisów społecznościowych, for internetowych, blogów oraz innych podobnych aktywności,

— projekty promujące, bezpośrednio lub pośrednio, przekaz sprzeczny z polityką Unii Europejskiej. Na przykład, projekty, które mogą być niezgodne z interesem zdrowia publicznego (o tematyce związanej z alkoholem, paleniem papierosów, narkotykami) i przestrzeganiem praw człowieka lub zagrażają bezpieczeństwu ludzi, wolności słowa, itd.,

— projekty promujące przemoc i/lub rasizm i/lub zawierające treści pornograficzne,

— utwory o charakterze promocyjnym (zwłaszcza o zawartości reklamowej),

— produkcje realizowane przez instytucje, promujące określoną organizację lub jej działalność.

Zaproszenie 22/11 przewiduje dwa terminy składania wniosków. Aby wniosek o wsparcie został uwzględniony w pierwszym terminie, należy przesłać go do Agencji między datą publikacji zaproszenia a dniem 25 listopada 2011 r. Aby został uwzględniony w drugim terminie, należy przesłać go do Agencji między dniem 26 listopada 2011 r. a dniem 13 kwietnia 2012 r., czyli datą zamknięcia zaproszenia do składania wniosków.

Ostateczna data zakończenia projektu to dzień 30 czerwca 2014 r. – w przypadku wniosków o wsparcie przedłożonych w pierwszym terminie – i dzień 30 listopada 2014 r. dla wniosków przesłanych w drugim terminie, lub data rozpoczęcia etapu produkcyjnego projektu, w zależności od tego, która z tych dat będzie wcześniejsza.

4. **Kryteria przyznania dotacji**

Łączna liczba punktów wynosi 100 i są one przydzielane według następujących wag:

— Kryteria dotyczące kandydującego przedsiębiorstwa (40 punktów):

  — jakość strategii rozwoju (10),

— spójność budżetu przeznaczonego na rozwój (10),

— potencjał firmy do realizacji projektu (10),

— jakość strategii finansowania (10).

— Kryteria dotyczące przedłożonego projektu (60 punktów):

— jakość projektu i oryginalność pomysłu w porównaniu do istniejących utworów (20),

— innowacja, trafność zastosowanych w pracy technik oraz jakość interaktywności (20),

— potencjał eksploatacyjny w Europie i przydatność dla grupy docelowej (20).

5. **Budżet**

Dostępny budżet wynosi ogółem 2,5 mln EUR. Dofinansowanie przyznawane jest w formie dotacji.

Maksymalne przyznane dofinansowanie może wynieść od 10 000 do 150 000 EUR.

Przyznane dofinansowanie nie może w żadnym razie przekroczyć 50 % uznanych kosztów, określonych przez producenta we wniosku (60 % w przypadku projektów szczególnie promujących europejską różnorodność kulturową).

Agencja zastrzega sobie prawo do nieprzyznania wszystkich dostępnych środków.

6. **Termin składania wniosków**

Wnioski należy złożyć używając formularza zgłoszeniowego on-line Agencji Wykonawczej (EACEA) oraz wysłać w wersji papierowej pocztą poleconą lub kurierską, nie później niż do dnia zamknięcia tj. **25 listopada 2011 r. i 13 kwietnia 2012 r.** (patrz pkt 3) na poniższy adres:

Agencja Wykonawcza ds. Edukacji, Kultury i Sektora Audiowizualnego (EACEA) – MEDIA
Constantin DASKALAKIS
BOUR 3/30
Avenue du Bourget/Bourgetlaan 1
1140 Bruxelles/Brussel
BELGIQUE/BELGIË

Rozpatrywane będą wyłącznie wnioski złożone na oficjalnym formularzu zgłoszeniowym, podpisane przez osobę uprawnioną do zaciągania prawnie wiążących zobowiązań w imieniu organizacji składającej wniosek.

Wnioski nadesłane faksem lub pocztą elektroniczną zostaną odrzucone.

7. **Szczegółowe informacje**

Pełny tekst przewodnika wraz z formularzem zgłoszeniowym znajduje się na stronie internetowej pod następującym adresem:

http://ec.europa.eu/media

Wnioski muszą spełniać wszelkie warunki przedstawione w przewodniku i należy je składać na odpowiednich formularzach.

POSTĘPOWANIA ZWIĄZANE Z REALIZACJĄ POLITYKI KONKURENCJI

KOMISJA EUROPEJSKA

Zgłoszenie zamiaru koncentracji

(Sprawa COMP/M.6348 – Arla Foods/Allgäuland)

(Tekst mający znaczenie dla EOG)

(2011/C 279/09)

1. W dniu 15 września 2011 r., zgodnie z art. 4 rozporządzenia Rady (WE) nr 139/2004 ([1]), Komisja otrzymała zgłoszenie planowanej koncentracji, w wyniku której przedsiębiorstwo Hansa-Milch AG („Hansa", Niemcy) należące do Arla Foods Amba („Arla", Dania) przejmuje, w rozumieniu art. 3 ust. 1 lit. b) rozporządzenia w sprawie kontroli łączenia przedsiębiorstw, kontrolę nad całością przedsiębiorstw Allgäuland-Käsereien GmbH i AL Dienstleistungs-GmbH (zwanych dalej wspólnie „Allgäuland", Niemcy) w drodze zakupu udziałów.

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

— Arla jest spółdzielnią mleczarską należącą do producentów mleka. Jej działalność obejmuje produkcję i sprzedaż różnych produktów mlecznych. W Niemczech Arla działa głównie za pośrednictwem swojej spółki zależnej Hansa,

— Allgäuland jest spółdzielnią mleczarską i produkuje całą gamę serów wysokiej jakości oraz inne produkty mleczne, głównie w Niemczech.

3. Po wstępnej analizie Komisja uznała, że zgłoszona koncentracja może wchodzić w zakres rozporządzenia WE w sprawie kontroli łączenia przedsiębiorstw. Jednocześnie Komisja zastrzega sobie prawo do podjęcia ostatecznej decyzji w tej kwestii.

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

Komisja musi otrzymać takie uwagi w nieprzekraczalnym terminie dziesięciu dni od daty niniejszej publikacji. Można je przesyłać do Komisji faksem (+32 22964301), pocztą elektroniczną na adres: COMP-MERGER-REGISTRY@ec.europa.eu lub listownie, podając numer referencyjny: COMP/M.6348 – Arla Foods/Allgäuland, na poniższy adres Dyrekcji Generalnej ds. Konkurencji Komisji Europejskiej:

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

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

Zgłoszenie zamiaru koncentracji

(Sprawa COMP/M.6392 – Gores/Mexx)

Sprawa, która może kwalifikować się do rozpatrzenia w ramach procedury uproszczonej

(Tekst mający znaczenie dla EOG)

(2011/C 279/10)

1. W dniu 15 września 2011 r., zgodnie z art. 4 rozporządzenia Rady (WE) nr 139/2004 ([1]), Komisja otrzymała zgłoszenie planowanej koncentracji, w wyniku której przedsiębiorstwo Gores Group LLC („Gores", Stany Zjednoczone) przejmuje, w rozumieniu art. 3 ust. 1 lit. b) rozporządzenia w sprawie kontroli łączenia przedsiębiorstw, wyłączną kontrolę nad przedsiębiorstwem Mexx European Holding BV („Mexx", Niderlandy) w drodze zakupu udziałów.

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

— w przypadku przedsiębiorstwa Gores: działalność inwestycyjna na niepublicznym rynku kapitałowym w zakresie technologii, telekomunikacji, usług dla przedsiębiorstw oraz w branży przemysłowej i odzieżowej, głównie w Stanach Zjednoczonych i Europie Zachodniej,

— w przypadku przedsiębiorstwa Mexx: sprzedaż detaliczna odzieży, sprzedaż detaliczna obuwia i akcesoriów oraz sprzedaż hurtowa odzieży i obuwia w Europie i Ameryce Północnej.

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

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

Komisja musi otrzymać takie uwagi w nieprzekraczalnym terminie dziesięciu dni od daty niniejszej publikacji. Można je przesyłać do Komisji faksem (+32 22964301), pocztą elektroniczną na adres: COMP-MERGER-REGISTRY@ec.europa.eu lub listownie, podając numer referencyjny: COMP/M.6392 – Gores/Mexx, na poniższy adres Dyrekcji Generalnej ds. Konkurencji Komisji Europejskiej:

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

([1]) Dz.U. L 24 z 29.1.2004, s. 1 („rozporządzenie WE w sprawie kontroli łączenia przedsiębiorstw").
([2]) Dz.U. C 56 z 5.3.2005, s. 32 („obwieszczenie Komisji w sprawie uproszczonej procedury").

CENY PRENUMERATY w 2011 r. (bez VAT, włącznie z normalną opłatą za dostawę przesyłki)

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

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

Dla każdej wersji językowej jest otwierana osobna prenumerata.

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

Prenumerata Suplementu do Dziennika Urzędowego (seria S – Ogłoszenia o przetargach) obejmuje wszystkie 23 wersje językowe na pojedynczej płycie DVD.

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

Sprzedaż i prenumerata

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

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

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

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

Urząd Publikacji Unii Europejskiej
2985 Luksemburg
LUKSEMBURG

PL