I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosków Komisji dotyczących rozporządzenia Parlamentu Europejskiego i Rady w sprawie wykorzystywania informacji poufnych i manipulacji na rynku oraz dyrektywy Parlamentu Europejskiego i Rady w sprawie sankcji karnych za wykorzystywanie informacji poufnych i manipulacje na rynku

(2012/C 177/01)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

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

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

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

uwzględniając 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. 28 ust. 2,

WYDAJE NASTĘPUJĄCĄ OPINIĘ:

1. WPROWADZENIE

1.1. Konsultacja z EIOD

1. Niniejsza opinia wchodzi w skład pakietu czterech opinii EIOD dotyczących sektora finansowego, wydanych tego samego dnia ([3]).

2. W dniu 20 października 2011 r. Komisja przyjęła wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie wykorzystywania informacji poufnych i manipulacji na rynku („proponowane rozporządzenie") oraz wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie sankcji karnych za wykorzystywanie informacji poufnych i manipulacje na rynku („proponowana dyrektywa"). Proponowane rozporządzenie i proponowana dyrektywa (zwane łącznie „wnioskami") zostały przesłane przez Komisję do EIOD w celu konsultacji i odebrane w dniu 31 października 2011 r. Dnia 6 grudnia 2011 r. Rada Unii Europejskiej wystąpiła o przeprowadzenie przez EIOD konsultacji w sprawie wniosków.

([1]) Dz.U. L 281 z 23.11.1995, s. 31.
([2]) Dz.U. L 8 z 12.1.2001, s. 1.
([3]) Opinie EIOD z dnia 10 lutego 2012 r. w sprawie pakietu ustawodawczego dotyczącego przeglądu ustawodawstwa bankowego, agencji ratingowych, rynków instrumentów finansowych (MIFID/MIFIR) oraz nadużyć na rynku.

3. Przed przyjęciem proponowanego rozporządzenia przeprowadzono nieformalną konsultację z EIOD. EIOD odnotowuje fakt, iż kilka z jego uwag zostało uwzględnionych we wniosku.

4. EIOD z uznaniem przyjmuje wystąpienie Komisji i Rady o przeprowadzenie konsultacji.

1.2. **Cele i zakres wniosków**

5. Dyrektywa w sprawie nadużyć na rynku („MAD") ([1]), przyjęta na początku 2003 r., wprowadziła wspólne unijne ramy prawne dotyczące przeciwdziałania wykorzystywaniu informacji poufnych i manipulacjom na rynku, ich wykrywania oraz nakładania związanych z nimi sankcji.

6. Po kilkuletnim okresie funkcjonowania MAD Komisja dokonała oceny jej stosowania, wykrywając wiele problemów, takich jak braki uregulowań dotyczących niektórych instrumentów i rynków, niedostatecznie skuteczne wykonanie (regulatorzy nie posiadają pewnych informacji i uprawnień, a sankcje nie zostały przewidziane lub nie są wystarczająco odstraszające), brak przejrzystości niektórych kluczowych pojęć oraz obciążenia administracyjne emitentów.

7. W świetle powyższych problemów, a także istotnych zmian w otoczeniu finansowym wywołanych procesami ustawodawczymi, rynkowymi i technologicznymi, Komisja przyjęła wnioski ustawodawcze w celu zreformowania MAD, którymi są proponowane rozporządzenie oraz proponowana dyrektywa. Cele polityczne proponowanej zmiany to zwiększenie zaufania inwestorów i poprawa integralności rynku, a także nadążenie za nowościami w sektorze finansowym.

8. Proponowane rozporządzenie w szczególności rozszerza ramy prawne dotyczące nadużyć na rynku, dokonuje kwalifikacji próby manipulacji na rynku i próby wykorzystywania informacji poufnych jako odrębnych przestępstw, wzmacnia uprawnienia dochodzeniowe przyznane właściwym organom oraz wprowadza reguły minimalne dotyczące środków administracyjnych, sankcji i kar.

9. Proponowana dyrektywa zobowiązuje państwa członkowskie do wprowadzenia sankcji karnych za celowe wykorzystywanie informacji poufnych lub manipulację na rynku oraz za podżeganie do popełnienia, pomocnictwo w popełnieniu lub usiłowanie popełnienia jednego z tych przestępstw. Rozszerza ono również zakres odpowiedzialności na osoby prawne, z uwzględnieniem, o ile jest to możliwe, odpowiedzialności karnej osób prawnych.

1.3. **Cel opinii EIOD**

10. Wiele środków zaplanowanych we wnioskach w celu poprawy integralności rynku i ochrony inwestorów ma wpływ na prawa osób fizycznych w związku z przetwarzaniem ich danych osobowych.

11. Dane osobowe będą gromadzone, przetwarzane i wymieniane szczególnie w związku z prowadzeniem przez właściwe organy dochodzeń lub współpracy w celu wykrywania przypadków wykorzystywania informacji poufnych lub nadużyć na rynku, ich zgłaszania lub nakładania związanych z nimi sankcji. Ponadto mechanizm mający zachęcić do zgłaszania przypadków naruszenia będzie również obejmował przetwarzanie danych osobowych dotyczących zarówno osoby zgłaszającej przypadek naruszenia, jak i osoby „oskarżonej". W końcu, system sankcji będzie miał wpływ na prawo do ochrony danych osobowych, o ile sankcje będą upubliczniane ze wskazaniem tożsamości osoby odpowiedzialnej za naruszenie proponowanego rozporządzenia.

12. O ile proponowane rozporządzenie zawiera wiele przepisów, które mogą mieć wpływ na prawo osoby fizycznej do ochrony własnych danych osobowych, o tyle proponowana dyrektywa jako taka nie wiąże się z przetwarzaniem danych osobowych. W związku z tym niniejsza opinia będzie koncentrować się na proponowanym rozporządzeniu, a w szczególności na następujących kwestiach: 1) stosowanie ustawodawstwa dotyczącego ochrony danych; 2) listy osób mających dostęp do informacji poufnych; 3) uprawnienia właściwych organów; 4) dostępne systemy służące do wykrywania i zgłaszania podejrzanych transakcji; 5) wymiana informacji z państwami trzecimi; 6) publikacja sankcji i zgłaszanie przypadków naruszenia.

([1]) 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.

2. ANALIZA WNIOSKÓW

2.1. Stosowanie ustawodawstwa dotyczącego ochrony danych

13. W motywach ([1]) i przepisach ([2]) proponowanego rozporządzenia wymienione są następujące dokumenty: Karta praw podstawowych, dyrektywa 95/46/WE i rozporządzenie (WE) nr 45/2001. W szczególności, w art. 22 proponowanego rozporządzenia określono wyraźnie ogólną zasadę, w myśl której „w przetwarzaniu danych osobowych przez państwa członkowskie w ramach niniejszego rozporządzenia właściwe organy stosują przepisy dyrektywy 95/46/WE. W przetwarzaniu danych osobowych przez EUNGiPW w ramach niniejszego rozporządzenia EUNGiPW stosuje przepisy rozporządzenia (WE) nr 45/2001". Ponadto w przepisie tym określono, że maksymalny okres przechowywania danych osobowych wynosi 5 lat.

14. EIOD z dużym uznaniem przyjmuje tego rodzaju nadrzędny przepis oraz, w ujęciu ogólnym, docenia fakt, że w proponowanym rozporządzeniu ustawodawstwo dotyczące ochrony danych potraktowano z wyjątkową uwagą. EIOD sugeruje jednak przeformułowanie treści przepisu, aby podkreślić stosowanie istniejącego ustawodawstwa dotyczącego ochrony danych. Ponadto należałoby ujednoznacznić odniesienie do dyrektywy 95/46/WE poprzez wskazanie, iż przepisy będą stosowane zgodnie z regulacjami krajowymi wprowadzającymi w życie dyrektywę 95/46/WE. EIOD zwraca uwagę na to, że niektóre przepisy proponowanego rozporządzenia wyraźnie odnoszą się do dyrektywy 95/46/WE lub rozporządzenia (WE) nr 45/2001. W ten sposób podkreślono fakt stosowania w określonych przypadkach odnośnych zasad dotyczących ochrony danych, choć nie wynika z tego, że zasady te nie mają zastosowania, jeżeli nie zostały wyraźnie wymienione w każdym przepisie (potencjalnie) wiążącym się z przetwarzaniem danych osobowych.

15. Zgodnie z motywem 33, w pozostałych motywach należy konsekwentnie stosować sformułowanie, iż państwa członkowskie „są obowiązane", a nie jedynie „powinny" przestrzegać odnośnego ustawodawstwa dotyczącego ochrony danych, ponieważ pozostaje ono w mocy, a jego stosowanie nie jest uznaniowe.

2.2. Listy osób mających dostęp do informacji poufnych

16. Proponowane rozporządzenie zobowiązuje emitentów instrumentów finansowych lub uczestników rynku handlu uprawnieniami do emisji do sporządzania listy osób pracujących dla nich, na podstawie umowy o pracę lub na innych warunkach, i posiadających dostęp do informacji poufnych (art. 13 ust. 1). Z takiego obowiązku zwolnieni są emitenci instrumentów finansowych, których instrumenty finansowe dopuszczono do obrotu na rynku na rzecz wzrostu MŚP, o ile nie zostaną do tego wezwani przez właściwy organ (art. 13 ust. 2).

17. EIOD uznaje konieczność sporządzenia takiej listy jako istotnego narzędzia właściwych organów do badania ewentualnych przypadków wykorzystywania informacji poufnych lub nadużyć na rynku. Jeżeli jednak listy takie będą się wiązać z przetwarzaniem danych osobowych, wówczas w akcie podstawowym należy określić główne zasady i gwarancje dotyczące ochrony danych. Z tego względu EIOD zaleca uwzględnienie wyraźnego odniesienia do celu takiej listy w jednym z materialnoprawnych przepisów proponowanego rozporządzenia. Zgodnie z art. 6 dyrektywy 95/46/WE, cel jest bowiem jednym z istotnych elementów każdej operacji przetwarzania.

18. Zgodnie z art. 13 ust. 3 proponowanego rozporządzenia Komisja przyjmuje – w drodze aktów delegowanych – środki ustanawiające warunki dotyczące zawartości list (w tym informacji dotyczących tożsamości i przyczyn uwzględnienia tych osób na liście osób mających dostęp do informacji poufnych) oraz warunki sporządzania takich list (w tym warunki uaktualniania takich list, czas ich przechowywania oraz obowiązki osób na nich się znajdujących). EIOD zaleca jednak:

— wskazanie w treści samego proponowanego rozporządzenia głównych elementów listy (w każdym przypadku – uzasadnienie umieszczenia danej osoby na liście),

— uwzględnienie zapisu o konieczności przeprowadzenia konsultacji z EIOD w zakresie, w jakim dany akt delegowany dotyczy przetwarzania danych osobowych.

2.3. Uprawnienia właściwych organów

19. W art. 17 ust. 2 wymieniono minimalne uprawnienia nadzorcze i śledcze, które posiadają właściwe organy w celu wykonywania obowiązków wynikających z proponowanego rozporządzenia.

([1]) Zob. motywy 33, 35, 39 i 40 proponowanego rozporządzenia.
([2]) Zob. art. 17 ust. 4, art. 22, art. 23 i art. 29 ust. 1 lit. c) proponowanego rozporządzenia.

20. W szczególności dwa spośród powyższych uprawnień wymagają szczególnej uwagi ze względu na ingerencję w prawo do prywatności i do ochrony danych: uprawnienie do wchodzenia na teren prywatny w celu zajęcia dokumentów w każdej formie oraz uprawnienie do żądania wydania rejestrów połączeń telefonicznych i rejestrów przesyłu danych.

2.3.1. *Uprawnienie do wchodzenia na teren prywatny*

21. Uprawnienie do wchodzenia na teren prywatny w celu zajęcia dokumentów w każdej formie ma charakter daleko idącej ingerencji i wchodzi w kolizję z prawem do prywatności. Z tego względu powinno ono podlegać ściśle określonym warunkom i odpowiednim zabezpieczeniom ([1]). Zgodnie z art. 17 ust. 2 lit. e) dostęp do terenu prywatnego wymaga uprzedniego uzyskania upoważnienia od organu sądowego zgodnie z prawem krajowym oraz wystąpienia uzasadnionego podejrzenia, że dokumenty związane z przedmiotem kontroli mogą mieć znaczenie dla udowodnienia przypadku wykorzystywania informacji poufnych lub manipulacji na rynku. EIOD docenia fakt, iż w tekście dokonano kwalifikacji uprawnień właściwych organów poprzez uzależnienie dostępu do terenu prywatnego od wystąpienia uzasadnionego podejrzenia naruszenia proponowanego rozporządzenia lub dyrektywy oraz uprzedniego uzyskania upoważnienia od organu sądowego. EIOD wyraża jednak pogląd, iż ogólny wymóg uprzedniego uzyskania upoważnienia od organu sądowego niezależnie od tego, czy wymaga tego prawo krajowe, jest zarówno uzasadniony, jak i niezbędny w świetle potencjalnie ingerencyjnego charakteru przedmiotowego uprawnienia.

22. W motywie 30 proponowanego rozporządzenia wskazano przypadki, gdy dostęp do terenu prywatnego jest niezbędny, tj. gdy osoba, od której zażądano już informacji, nie wykonała tego żądania (częściowo lub w całości), lub istnieją uzasadnione podstawy, aby sądzić, że w przypadku takiego żądania nie zostałoby ono wykonane lub że dokumenty lub informacje, których żądanie to dotyczy, zostałyby usunięte, zniszczone lub wprowadzono by do nich zmiany. EIOD z uznaniem przyjmuje powyższe zapisy. Inspektor uznaje jednak, iż stanowią one dodatkowe zabezpieczenia, które są konieczne dla zapewnienia zgodności prawem do prywatności, a tym samym należy je umieścić w jednym z przepisów materialnoprawnych jako warunek dostępu do terenu prywatnego.

2.3.2. *Uprawnienie do żądania wydania rejestrów połączeń telefonicznych i rejestrów przesyłu danych*

23. Zgodnie z art. 17 ust. 2 lit. f) właściwe organy są uprawnione do „żądania wydania rejestrów połączeń telefonicznych i rejestrów przesyłu danych operatora telekomunikacyjnego lub firmy inwestycyjnej", przy czym określono, iż warunkiem takiego żądania jest wystąpienie „uzasadnionego podejrzenia", że takie rejestry „mogą mieć znaczenie dla udowodnienia przypadku wykorzystywania informacji poufnych lub manipulacji na rynku" w świetle proponowanego rozporządzenia lub proponowanej dyrektywy. Rejestry takie nie obejmują jednak „treści połączenia, do którego się odnoszą". Ponadto w art. 17 ust. 3 określono, iż uprawnienia, o których mowa w ust. 2, wykonywane są zgodnie z prawem krajowym.

24. Dane związane z wykorzystaniem środków łączności elektronicznej mogą być źródłem różnorodnych informacji osobowych, takich jak tożsamość osób wykonujących i odbierających połączenie, czas i długość połączenia, wykorzystywana sieć, lokalizacja geograficzna użytkownika w przypadku urządzeń przenośnych itp. Niektóre dane o ruchu dotyczące korzystania z Internetu i poczty elektronicznej (np. wykaz odwiedzonych stron internetowych) mogą również być źródłem szczegółowych informacji na temat treści komunikacji. Ponadto przetwarzanie danych o ruchu koliduje z tajemnicą korespondencji. W świetle tego, dyrektywą 2002/58/WE ([2]) (dyrektywa o prywatności i łączności elektronicznej) wprowadzono zasadę, że dane o ruchu muszą zostać usunięte lub uzyskać formę anonimową, gdy nie są już potrzebne do celów transmisji komunikatu ([3]). Zgodnie z art. 15 ust. 1 tej dyrektywy państwa członkowskie mogą wprowadzić w prawodawstwie krajowym odstępstwa dla szczególnych, prawnie dopuszczalnych celów, przy czym muszą one być niezbędne, właściwe i proporcjonalne do zapewnienia realizacji tych celów w ramach społeczeństwa demokratycznego ([4]).

([1]) Zob. w szczególności ETPC z dnia 23 lutego 1993 r., *Funke przeciwko Francji*, 10828/84.

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

([3]) Zob. art. 6 ust. 1 dyrektywy 2002/58/WE (Dz.U. L 201 z 31.7.2002, s. 37).

([4]) Zgodnie z art. 15 ust. 1 dyrektywy 2002/58/WE ograniczenia takie „stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (tj. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej, jak określono w art. 13 ust. 1 dyrektywy 95/46/WE. W tym celu, państwa członkowskie mogą, między innymi, uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie […]".

25. EIOD przyznaje, że cele określone przez Komisję w proponowanym rozporządzeniu są prawnie dopuszczalne. Rozumie on potrzebę inicjatyw zmierzających do wzmocnienia nadzoru rynków finansowych w celu zachowania ich solidności oraz lepszej ochrony inwestorów i gospodarki ogółem. Uprawnienia śledcze dotyczące bezpośrednio danych o ruchu, przez wzgląd na swój potencjalnie ingerencyjny charakter, muszą jednak spełniać wymogi niezbędności i proporcjonalności, tj. muszą ograniczać się do tego, co właściwe dla osiągnięcia zamierzonego celu, i nie wykraczać poza to, co niezbędne dla jego realizacji [1]. W tym kontekście jest więc istotne, by przepisy zostały przejrzyście sformułowane pod kątem zakresu podmiotowego i przedmiotowego, a także okoliczności i warunków ich stosowania. Ponadto należy zapewnić odpowiednie gwarancje pod kątem ryzyka nadużyć.

26. Rejestry rozmów telefonicznych i przepływu danych w oczywisty sposób będą wiązały się z danymi osobowymi w rozumieniu dyrektywy 95/46/WE, dyrektywy 2002/58/WE i rozporządzenia (WE) nr 45/2001. W motywie 31 proponowanego rozporządzenia wskazano, iż: „dzięki rejestrom połączeń telefonicznych i przesyłu danych można zidentyfikować osobę odpowiedzialną za rozpowszechnienie fałszywych lub wprowadzających w błąd informacji, ustalić, że dane osoby kontaktowały się w określonym czasie oraz że istnieje powiązanie między co najmniej dwiema osobami" [2]. Z tego względu należy zadbać o pełne poszanowanie warunków uczciwego i zgodnego z prawem przetwarzania danych osobowych określonych w powyższych dyrektywach i rozporządzeniu.

2.3.3. *Wymóg uzyskania upoważnienia od organu sądowego*

27. EIOD zwraca uwagę na fakt, iż w myśl art. 17 ust. 3 uprawnienie to wykonywane jest zgodnie z prawem krajowym, bez wyraźnego odniesienia do uprzedniego uzyskania upoważnienia od organu sądowego, jak ma to miejsce w przypadku uprawnienia do wchodzenia na teren prywatny. EIOD uważa, że ogólny wymóg uprzedniego uzyskania upoważnienia od organu sądowego we wszystkich przypadkach – niezależnie od tego, czy jest on określony w prawie krajowym – byłby uzasadniony ze względu na potencjalnie ingerencyjny charakter przedmiotowego uprawnienia oraz sprzyjałby zharmonizowanemu stosowaniu ustawodawstwa we wszystkich państwach członkowskich UE. Należy również uwzględnić fakt, że w różnych regulacjach prawnych państw członkowskich przewidziano szczególne gwarancje ochrony miru domowego przed przypadkami nieproporcjonalnych i niedostatecznie uregulowanych kontroli, rewizji lub konfiskat, szczególnie przeprowadzanych przez instytucje o charakterze administracyjnym.

28. Ponadto EIOD zaleca wprowadzenie wymogu, zgodnie z którym występowanie przez właściwe organy z żądaniem wydania rejestrów połączeń telefonicznych i rejestrów przesyłu danych musiałoby odbywać się w drodze formalnej decyzji, określającej podstawę prawną i cel takiego żądania, żądane informacje, termin udostępnienia informacji oraz prawo adresata decyzji do jej zaskarżenia do Trybunału Sprawiedliwości.

2.3.4. *Definicja rejestru połączeń telefonicznych i rejestru przesyłu danych*

29. W proponowanym rozporządzeniu brak jest definicji pojęć „rejestr połączeń telefonicznych i rejestr przesyłu danych". W dyrektywie 2002/58/WE (o prywatności i łączności elektronicznej) jest mowa jedynie o „danych ruchu", bez odniesienia do „rejestrów połączeń telefonicznych i rejestrów przesyłu danych". Nie ulega wątpliwości, że ścisłe znaczenie tych pojęć determinuje wpływ, jaki na prywatność i ochronę danych zainteresowanych osób mogą mieć uprawnienia śledcze. EIOD sugeruje wykorzystanie terminologii już dostępnej w definicji „danych o ruchu" w dyrektywie 2002/58/WE.

30. Artykuł 17 ust. 2 lit. f) odnosi się do „rejestrów połączeń telefonicznych i rejestrów przesyłu danych operatora telekomunikacyjnego lub firmy inwestycyjnej". W dyrektywie o prywatności i łączności elektronicznej wprowadzono zasadę, zgodnie z którą dane o ruchu należy usuwać, kiedy przestają one być potrzebne do celów handlowych, do których je gromadzono. Na mocy art. 15 ust. 1 dyrektywy o prywatności i łączności elektronicznej państwa członkowskie mogą jednak stosować odstępstwa od tego wymogu dla celów egzekwowania prawa. Uzgodnienie inicjatyw państw członkowskich wynikających z art. 15 ust. 1 dyrektywy o prywatności, w zakresie, w jakim dotyczą one zatrzymywania danych w celu dochodzenia, wykrywania i ścigania „poważnych" przestępstw, jest przedmiotem dyrektywy w sprawie zatrzymywania danych.

[1] Zob. np. wyrok z dnia 9 listopada 2010 r. w sprawach połączonych C-92/09 i C-93/09, *Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-92/09) przeciwko Land Hessen*, dotychczas nieopublikowany w Zb.Orz., pkt 74.

[2] Zob. również pkt 12 uzasadnienia proponowanego rozporządzenia.

31. Nasuwa się pytanie, czy rejestry połączeń telefonicznych i rejestry przepływu danych, o których mowa w art. 17 ust. 2 lit. f) dotyczą danych dostępnych dzięki przechowywaniu danych o ruchu i lokalizacji regulowanych przez dyrektywę o prywatności i łączności elektronicznej, czy też dodatkowych danych wymaganych przez dyrektywę w sprawie zatrzymywania danych. Wariant drugi stwarzałby poważne problemy, ponieważ stosowanie odstępstw przewidzianych w art. 15 ust. 1 dyrektywy o prywatności i łączności elektronicznej (tj. zapobieganie przestępstwom, ich wykrywanie, dochodzenie i karanie) rozszerzałoby zakres celów zatrzymywania danych na podstawie dyrektywy w sprawie zatrzymywania danych (tj. dochodzenie, wykrywanie i ściganie „poważnych" przestępstw). Innymi słowy, dane zatrzymywane na podstawie dyrektywy w sprawie zatrzymywania danych byłyby tym samym wykorzystywane do celów nieprzewidzianych w tej dyrektywie. Sugerowałoby to europejską zachętę do wykorzystywania „luki prawnej", która należy do głównych braków obecnej dyrektywy w sprawie zatrzymywania danych ([1]).

32. W związku z powyższym EIOD zdecydowanie zaleca określenie kategorii rejestrów połączeń telefonicznych i rejestrów przepływu danych, których wydania mogą żądać właściwe organy. Dane takie muszą być adekwatne, odpowiednie i nienadmierne w stosunku do celu ich oceny lub przetwarzania. Ponadto EIOD zaleca ograniczenie art. 17 ust. 2 lit. f) do danych zwykle przetwarzanych przez (będących „w posiadaniu") operatorów telekomunikacyjnych na podstawie dyrektywy 2002/58/WE o prywatności i łączności elektronicznej. Z zasady wyklucza to dostęp do danych zatrzymywanych dla celów dyrektywy w sprawie zatrzymywania danych, o ile dostęp taki nie ma na celu dochodzenia, wykrywania i ścigania „poważnych" przestępstw ([2]).

33. W art. 17 ust. 2 lit. f) przewidziano dostęp do „rejestrów połączeń telefonicznych i rejestrów przesyłu danych operatora telekomunikacyjnego lub firmy inwestycyjnej". W tekście należy określić kategorie rejestrów i wyjaśnić, jakich firm dotyczy cytowany przepis. EIOD zakłada, że rejestry takie będą pokrywać się z rejestrami, o których mowa we wniosku dotyczącym dyrektywy Parlamentu Europejskiego i Rady w sprawie rynków instrumentów finansowych („proponowana dyrektywa MIFID"). Inspektor podkreśla fakt, iż w związku z tym wnioskiem przedstawił wiele uwag, w których również zalecił wyjaśnienie tych kwestii ([3]). Ponadto, w zakresie, w jakim dane połączeń o połączeniach telefonicznych i ruchu dotyczyłyby rozmów telefonicznych i korespondencji elektronicznej, o których mowa w art. 16 ust. 7 proponowanej dyrektywy MIFID, EIOD zalecił zdefiniowanie celu ewidencjonowania takiej komunikacji, z podaniem rodzaju komunikacji oraz kategorii danych o takiej komunikacji podlegających ewidencji ([4]).

34. W końcu, EIOD z zadowoleniem odnotowuje w uwzględnienie w tekście uzależnienia dostępu do rejestrów od istnienia uzasadnionego podejrzenia naruszenia proponowanego rozporządzenia lub proponowanej dyrektywy oraz wyraźne wykluczenie w nim możliwości dostępu właściwych organów do treści połączenia.

2.4. **Dostępne systemy służące do wykrywania i zgłaszania podejrzanych transakcji**

35. W art. 11 ust. 1 proponowanego rozporządzenia określono, iż każda osoba prowadząca działalność gospodarczą w postaci systemu obrotu przyjmuje i utrzymuje skuteczne ustalenia i procedury mające na celu zapobieganie nadużyciom na rynku i wykrywanie ich. Ponadto ust. 2 stanowi, iż każda osoba zajmująca się zawodowo pośredniczeniem w zawieraniu transakcji i zawieraniem transakcji dotyczących instrumentów finansowych będzie posiadała odpowiednie systemy wykrywania i powiadamiania

([1]) W tej kwestii zob. opinia EIOD z dnia 31 maja 2011 r. na temat sprawozdania z oceny Komisji dla Rady i Parlamentu Europejskiego w sprawie dyrektywy w sprawie zatrzymywania danych (dyrektywa 2006/24/WE), np. pkt 24.

([2]) EIOD pragnie przypomnieć problemy związane z brakiem europejskiej definicji „poważnego przestępstwa". Inspektor wskazał mianowicie, że, jak pokazuje sprawozdanie Komisji z oceny dyrektywy w sprawie zatrzymywania danych, w efekcie decyzji o pozostawieniu do decyzji państw członkowskich ścisłej definicji tego, co stanowi „poważne" przestępstwo, pojawiła się duża różnorodność celów wykorzystywania danych. Komisja stwierdza, iż „większość transponujących państw członkowskich pozwala na podstawie swoich przepisów na dostęp do zatrzymanych danych i korzystanie z nich do celów wykraczających poza cele objęte dyrektywą, w tym do zapobiegania i zwalczania przestępczości, a także zapobiegania zagrożeniom dla zdrowia i życia". Zob. opinia z dnia 31 maja 2011 r. w sprawie sprawozdania z oceny Komisji dla Rady i Parlamentu Europejskiego w sprawie dyrektywy w sprawie zatrzymywania danych (dyrektywa 2006/24/WE), pkt 23, 71 i 72.

([3]) Zgodnie z art. 71 ust. 2 lit. d) właściwe organy mogą na podstawie proponowanej dyrektywy MIFID żądać wydania rejestrów połączeń telefonicznych i rejestrów przesyłu danych w posiadaniu firm inwestycyjnych, jeżeli istnieje uzasadnione podejrzenie naruszenia proponowanej dyrektywy MIFID.

([4]) Zob. opinia EIOD z dnia 10 lutego 2012 r. na temat wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie rynków instrumentów finansowych uchylającej dyrektywę 2004/39/WE Parlamentu Europejskiego i Rady (wersja przekształcona) oraz wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków instrumentów finansowych oraz zmieniającego rozporządzenie [EMIR] w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, partnerów centralnych i repozytoriów transakcji.

o zleceniach i transakcjach, które mogą stanowić wykorzystywanie informacji poufnych, manipulację na rynku lub próbę zaangażowania się w manipulację na rynku lub w wykorzystywanie informacji poufnych. W przypadku podejrzenia należy bezzwłocznie powiadomić właściwy organ. Komisja zatwierdza regulacyjne standardy techniczne wymienione w akapicie pierwszym w celu przyjęcia odpowiednich ustaleń i procedur oraz określenia systemów i wzorów formularzy powiadomienia, o których mowa w akapicie drugim (art. 11 ust. 3 ostatnie zdanie).

36. Ze względu na to, że powyższe systemy będą najprawdopodobniej obejmować dane osobowe (np. monitoring transakcji dokonywanych przez osoby wymienione na liście osób mających dostęp do informacji poufnych), EIOD pragnie podkreślić, że standardy takie należy tworzyć zgodnie z zasadą „ochrony prywatności w fazie projektowania", tj. integracji ochrony danych i prywatności od samego początku procesu powstawania nowych produktów, usług i procedur związanych z przetwarzaniem danych osobowych ([1]). Ponadto EIOD zaleca wprowadzenie zapisu o konieczności przeprowadzenia konsultacji z EIOD w zakresie, w jakim takie regulacyjne standardy dotyczą przetwarzania danych osobowych.

2.5. **Wymiana informacji z państwami trzecimi**

37. EIOD odnotowuje odniesienie do dyrektywy 95/46/WE, w szczególności do art. 25 lub 26, oraz szczególne gwarancje, o których mowa w art. 23 proponowanego rozporządzenia w związku z ujawnianiem danych osobowych państwom trzecim. Za odpowiednie gwarancje w kontekście ryzyk dotyczących takiego przekazywania danych uznaje się w szczególności indywidualną ocenę poszczególnych przypadków, zapewnienie niezbędności przekazania danych, wymóg uprzedniego uzyskania wyraźnego upoważnienia właściwego organu na przekazanie danych dalej do państwa trzeciego i przez państwo trzecie oraz istnienie odpowiedniego poziomu ochrony danych osobowych w państwie trzecim otrzymującym dane osobowe.

2.6. **Publikacja sankcji**

2.6.1. *Obowiązkowa publikacja sankcji*

38. Artykuł 26 ust. 3 proponowanego rozporządzenia zobowiązuje państwa członkowskie do zadbania o to, by właściwe organy bez zbędnej zwłoki publikowały informacje o każdym środku administracyjnym i sankcji nałożonej za naruszenie przepisów proponowanego rozporządzenia, uwzględniając przynajmniej informacje na temat rodzaju i charakteru naruszenia oraz tożsamości osób odpowiedzialnych za naruszenie, chyba że opublikowanie tych informacji stanowiłoby poważne zagrożenie dla stabilności rynków finansowych.

39. Publikacja sankcji przyczyniłaby się do wzmocnienia działania odstraszającego, ponieważ faktycznych i potencjalnych sprawców zniechęcałaby do popełniania przestępstw perspektywa poważnego uszczerbku dla reputacji. Zwiększyłaby ona również przejrzystość, ponieważ podmioty gospodarcze dowiadywałyby się o popełnieniu naruszenia przez konkretną osobę. Wymóg ten został złagodzony jedynie w sytuacji, gdy publikacja wyrządziłaby niewspółmierną szkodę zaangażowanym stronom; w takim przypadku właściwe organy publikują informacje o nałożonych sankcjach w sposób anonimowy.

40. EIOD z uznaniem przyjmuje zawarte w motywie 35 odniesienie do Karty praw podstawowych, w szczególności do prawa do ochrony danych osobowych, w związku z przyjmowaniem i publikacją sankcji. Inspektor nie jest jednak przekonany, czy obowiązkowa publikacja sankcji, zgodnie z obecnym sformułowaniem, spełnia wymogi przepisów dotyczących ochrony danych w wykładni Trybunału Sprawiedliwości przedstawionej w wyroku w sprawie *Schecke* ([2]). EIOD jest zdania, iż cel, niezbędność i proporcjonalność środka nie zostały w wystarczającym stopniu ustalone, oraz że, w każdym przypadku, należało określić odpowiednie gwarancje pod kątem ryzyk dla praw osób fizycznych.

2.6.2. *Niezbędność i proporcjonalność publikacji*

41. W wyroku w sprawie *Schecke* Trybunał Sprawiedliwości stwierdził nieważność przepisów rozporządzenia Rady i rozporządzenia Komisji, w których przewidziano obowiązkową publikację informacji dotyczących beneficjentów funduszy rolnych, w tym tożsamości beneficjentów i otrzymanych kwot. Trybunał uznał, iż rzeczona publikacja stanowi przetwarzanie danych osobowych podlegające art. 8 ust. 2 europejskiej Karty praw podstawowych („Karta"), a tym samym stanowi ingerencję w prawa uznane w art. 7 i 8 Karty.

([1]) Zob. opinia EIOD z dnia 14 stycznia 2011 r. w sprawie komunikatu Komisji do Parlamentu Europejskiego, Rady, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej" (Dz.U. C 181 z 22.6.2011, s. 1), pkt 108–115.

([2]) Wyrok w sprawach połączonych C-92/09 i C-93/09, *Schecke*, pkt 56–64.

42. Stwierdziwszy, iż „odstępstwa i ograniczenia ochrony danych powinny ograniczać się do tego, co absolutnie konieczne", Trybunał przystąpił do zbadania celu publikacji oraz jej proporcjonalności. Uznał on, iż nic nie wskazuje na to, by przyjmując przedmiotowe ustawodawstwo Rada i Komisja rozpatrzyły szczegółowe zasady publikacji informacji, które byłyby zgodne z celem takiej publikacji, a jednocześnie mniej ingerowały w prawa tych beneficjentów.

43. Wydaje się, że art. 26 ust. 3 proponowanego rozporządzenia wykazuje te same braki, które podkreślił ETS w wyroku w sprawie *Schecke*. Należy wziąć pod uwagę, że w celu dokonania oceny zgodności przepisu wymagającego publicznego ujawnienia informacji osobowych z wymogami ochrony danych kluczowe znaczenie ma istnienie jasnego i dobrze zdefiniowanego celu, któremu ma służyć zamierzona publikacja. Jedynie w oparciu o jasny i dobrze zdefiniowany cel mona ocenić, czy dana publikacja danych osobowych jest faktycznie niezbędna i proporcjonalna ([1]).

44. Po zapoznaniu się z wnioskiem i dokumentami towarzyszącymi (tj. ze sprawozdaniem z oceny skutków) EIOD ma wrażenie, iż cel taki, a w następstwie tego – konieczność przedmiotowego środka nie została jednoznacznie ustalona. O ile w motywach brak jest jakiejkolwiek wzmianki na temat tych kwestii, o tyle w ocenie skutków jest mowa tylko o ogólnych skutkach pozytywnych (tj. działaniu odstraszającym od nadużyć na rynku, przyczynianiu się do ochrony inwestorów, równym traktowaniu emitentów, poprawie egzekucji) i wspomina się jedynie, że „publikacja sankcji ma istotne znaczenie dla poprawy przejrzystości i utrzymania zaufania do rynków finansowych" oraz że „publikacja nakładanych sankcji przyczyni się do celu odstraszania oraz poprawi integralność rynku i ochronę inwestorów" ([2]). Wydaje się, że tego rodzaju ogólne stwierdzenie nie wystarcza do wykazania niezbędności zaproponowanego środka. Jeżeli celem ogólnym jest wzmocnienie działania odstraszającego, to, jak można sądzić, Komisja powinna była wyjaśnić, w szczególności, dlaczego nie wystarczyłyby tu wyższe kary finansowe (bądź inne sankcje niemające charakteru napiętnowania).

45. Ponadto wydaje się, że w sprawozdaniu z oceny skutków nie wzięto pod uwagę mniej ingerencyjnych metod, takich jak publikacja na podstawie indywidualnej decyzji dotyczącej danego przypadku. W szczególności ten ostatni wariant może wydawać się rozwiązaniem *prima facie* bardziej proporcjonalnym, zwłaszcza biorąc pod uwagę fakt, że – jak uznano w art. 26 ust. 1 lit. d) – publikacja jest sankcją, która w związku z tym powinna być oceniana indywidualnie przy uwzględnieniu istotnych okoliczności, takich jak waga naruszenia, stopień odpowiedzialności osobistej, recydywa, straty osób trzecich itp ([3]).

46. W sprawozdaniu z oceny skutków nie wyjaśniono, dlaczego publikacja indywidualna nie jest wariantem wystarczającym. Wspomina się jedynie, że publikacja nakładanych sankcji „przyczyni się do realizacji celu eliminowania tam, gdzie to możliwe, wariantów i uznaniowości, poprzez zniesienie obecnej możliwości uznaniowej rezygnacji państw członkowskich z wymogu takiej publikacji" ([4]). W opinii EIOD możliwość oceny danego przypadku w świetle szczególnych okoliczności jest bardziej proporcjonalnym, a tym samym bardziej preferowanym wariantem niż obowiązkowa publikacja we wszystkich przypadkach. Uznaniowość ta pozwoliłaby właściwemu organowi np. uniknąć publikacji w przypadku mniej poważnego naruszenia, gdy naruszenie takie nie spowodowało poważnych szkód, gdzie strona wykazała gotowość do współpracy itd. Tym samym ocena przedstawiona w ocenie skutków nie rozwiewa wątpliwości co do niezbędności i proporcjonalności przedmiotowego środka.

2.6.3. *Potrzeba odpowiednich gwarancji*

47. W proponowanym rozporządzeniu należało określić odpowiednie gwarancje w celu sprawiedliwego zrównoważenia różnych zaangażowanych interesów. Po pierwsze, konieczne są gwarancje w związku z prawem oskarżonego do zaskarżenia decyzji w sądzie oraz w związku z domniemaniem

([1]) W tej kwestii zob. również opinia EIOD z dnia 15 kwietnia 2011 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie reguł finansowych mających zastosowanie do budżetu rocznego Unii (Dz.U. C 215 z 21.7.2011, s. 13).
([2]) Zob. ocena skutków, s. 166.
([3]) To jest zgodnie z art. 27 proponowanego rozporządzenia zawierającym kryteria określania sankcji.
([4]) Zob. ocena skutków, s. 167.

niewinności. W tym kontekście należało w tekście art. 26 ust. 3 zastosować odpowiednie sformułowania, aby zobowiązać właściwe organy do podjęcia odpowiednich środków w sytuacji, gdy decyzja zostaje zaskarżona, i gdy zostaje ostatecznie uchylona przez sąd ([1]).

48. Po drugie, w proponowanym rozporządzeniu należy zagwarantować czynne poszanowanie praw osób, których dane dotyczą. EIOD docenia fakt, że w wersji ostatecznej wniosku przewidziano możliwość wykluczenia publikacji w sytuacji, gdy wyrządziłaby ona niewspółmierną szkodę. Podejście czynne powinno jednakże oznaczać, że osoby, których dane dotyczą, będą z wyprzedzeniem informowane o tym, że decyzja nakładająca na nie sankcje zostanie opublikowana, oraz że zgodnie z art. 14 dyrektywy 95/46/WE przysługuje im prawo sprzeciwu z ważnych i uzasadnionych przyczyn ([2]).

49. Po trzecie, choć proponowane rozporządzenie nie precyzuje, jakie medium powinno być wykorzystane do publikacji przedmiotowych informacji, w praktyce, jak można sobie wyobrazić, w większości państw członkowskich publikacja będzie miała miejsce w Internecie. Publikacje internetowe wiążą się ze szczególnymi problemami i ryzykami, dotyczącymi w szczególności potrzeby zadbania o to, by informacje nie były udostępnianie w trybie online dłużej, niż to niezbędne, oraz by nie mogły one zostać zmanipulowane lub zmodyfikowane. Również fakt wykorzystania zewnętrznych wyszukiwarek niesie ze sobą ryzyko wyrwania informacji z kontekstu oraz przekazywania ich w sieci i poza nią w sposób trudny do kontrolowania ([3]).

50. W związku z powyższym należy zobowiązać państwa członkowskie do zadbania o to, by dane osobowe zainteresowanych osób były udostępnianie w trybie online wyłącznie przez uzasadniony okres, po którym będą systematycznie usuwane ([4]). Ponadto należy zobowiązać państwa członkowskie do zapewnienia odpowiednich środków bezpieczeństwa i gwarancji, szczególnie mających chronić przed ryzykiem związanym z wykorzystaniem zewnętrznych wyszukiwarek ([5]).

2.6.4. *Wnioski*

51. EIOD wyraża przekonanie, że przepis dotyczący obowiązkowej publikacji sankcji – w obecnym brzmieniu – jest niezgodny z podstawowym prawem do prywatności i prawem do ochrony danych. Ustawodawca powinien dokonać starannej oceny niezbędności proponowanego systemu i zbadać, czy obowiązek publikacji nie wykracza poza to, co konieczne dla realizacji przyjętego celu leżącego w interesie ogółu, oraz czy nie są dostępne mniej restrykcyjne środki dla realizacji tego samego celu. Niezależnie od wyniku takiego testu proporcjonalności, obowiązkowi publikacji w każdym przypadku powinny towarzyszyć odpowiednie gwarancje w celu zapewnienia poszanowania zasady domniemania niewinności, prawa zainteresowanej osoby do sprzeciwu, bezpieczeństwa/poprawności danych oraz ich usuwania po upływie odpowiedniego okresu.

2.7. **Zgłaszanie przypadków naruszenia**

52. Artykuł 29 proponowanego rozporządzenia zobowiązuje państwa członkowskie do ustanowienia skutecznych mechanizmów zgłaszania przypadków naruszenia, zwanych również systemami informowania o nieprawidłowościach (ang. *whistle-blowing schemes*). Choć mogą one być skutecznym narzędziem do zapewniania zgodności, to z punktu widzenia ochrony danych systemy takie wiążą się z istotnymi problemami ([6]).

([1]) Organy krajowe mogłyby rozważyć wprowadzenie np. następujących środków: opóźnienie publikacji do czasu oddalenia odwołania lub, jak zaproponowano w sprawozdaniu z oceny skutków, wyraźne wskazanie, iż od danej decyzji złożono odwołanie i zainteresowana osoba fizyczna winna być uznawana za niewinną do czasu uprawomocnienia się decyzji, publikacja sprostowania w przypadku uchylenia decyzji przez sąd.

([2]) Zob. opinia EIOD z dnia 10 kwietnia 2007 r. w sprawie finansowania wspólnej polityki rolnej (Dz.U. C 134 z 16.6.2007, s. 1).

([3]) W tej kwestii zob. również dokument opublikowany przez włoski organ ds. ochrony danych „Dane osobowe zawarte m.in. w rejestrach i dokumentach organów administracji publicznej: wytyczne dotyczące ich przetwarzania przez organy publiczne w ramach łączności i dystrybucji internetowej" dostępny na stronie internetowej włoskiego organu ds. ochrony danych: http://www.garanteprivacy.it/garante/doc.jsp?ID=1803707

([4]) Omawiane problemy wiążą się również z bardziej ogólnym prawem do bycia zapomnianym, którego włączenie do nowych ram ustawodawczych dotyczących ochrony danych osobowych jest obecnie przedmiotem dyskusji.

([5]) Tego rodzaju środki i gwarancje mogą polegać np. na wykluczeniu indeksacji danych przy pomocy zewnętrznych wyszukiwarek.

([6]) Grupa Robocza Art. 29 opublikowała w 2006 opinię w sprawie takich systemów, koncentrując się na aspektach tego zjawiska związanych z ochroną danych: opinia 1/2006 w sprawie zastosowania unijnych zasad ochrony danych do wewnętrznych systemów informowania o nieprawidłowościach w dziedzinie księgowości, wewnętrznych kontroli księgowych, spraw związanych z audytem, zwalczania przekupstwa oraz przestępstw bankowych i finansowych (opinia Grupy w sprawie systemów informowania o nieprawidłowościach). Opinia dostępna jest na stronie internetowej Grupy Roboczej Art. 29: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm)

53. EIOD z uznaniem odnotowuje fakt, że w treści proponowanego rozporządzenia uwzględniono szczególne gwarancje – które mają być dalej rozwijane na poziomie krajowym – w związku z ochroną osób zgłaszających domniemane przypadki naruszenia, a w bardziej ogólnym ujęciu, z ochroną danych. EIOD jest świadomy faktu, że proponowane rozporządzenie określa jedynie główne elementy systemu, który ma być wdrażany przez państwa członkowskie. Inspektor pragnie jednak zwrócić uwagę na opisane poniżej kwestie dodatkowe.

54. Podobnie jak w przypadku innych opinii ([1]), EIOD podkreśla potrzebę wprowadzenia szczególnego zapisu o konieczności zachowania poufności tożsamości osób zgłaszających przypadki naruszenia (ang. *whistleblowers*) i informatorów. EIOD podkreśla, iż położenie osób zgłaszających przypadki naruszenia jest położeniem ryzykownym. Osobom, które udzielają takich informacji, należy zagwarantować poufność tożsamości, szczególnie wobec osób, których dotyczy zgłoszenie domniemanego przypadku naruszenia ([2]). Poufność tożsamości osób zgłaszających przypadki naruszenia należy zagwarantować na wszystkich etapach postępowania, o ile nie koliduje to z krajowymi przepisami dotyczącymi postępowania sądowego. Konieczność ujawnienia tożsamości może występować szczególnie w kontekście dalszego śledztwa lub postępowania sądowego wszczętego w dalszym trybie w związku z dochodzeniem (w tym także w przypadku ustalenia, iż umyślnie złożono fałszywe zeznanie na temat danej osoby) ([3]). W związku z powyższym EIOD zaleca dodanie w art. 29 ust. 1 lit. b) następującego zapisu: „na wszystkich etapach postępowania należy zapewnić ochronę tożsamości takich osób, o ile jej ujawnienie nie jest wymagane przez przepisy krajowe w kontekście dalszego śledztwa lub wszczętego w dalszym trybie postępowania sądowego".

55. EIOD z zadowoleniem odnotowuje fakt, iż art. 29 ust. 1 lit. c) zobowiązuje państwa członkowskie do ochrony danych osobowych zarówno osoby oskarżonej, jak i osoby oskarżającej, zgodnie z zasadami określonymi w dyrektywie 95/46/WE. Inspektor proponuje jednak wykreślenie słów „zasadami określonymi w", aby odniesienie do dyrektywy było bardziej wszechstronne i wiążące. W kwestii konieczności przestrzegania ustawodawstwa dotyczącego ochrony danych w ramach praktycznego wdrożenia systemów EIOD pragnie w szczególności podkreślić zalecenia przedstawione przez Grupę Roboczą Art. 29 w opinii w sprawie informowania o nieprawidłowościach z 2006 r. W trakcie wdrażania systemów krajowych zaangażowane podmioty powinny m.in. uwzględnić potrzebę zachowania proporcjonalności poprzez ograniczenie, w miarę możliwości, kategorii osób uprawnionych do zgłaszania, kategorii osób, które mogą zostać oskarżone oraz przypadków naruszenia, o które mogą one zostać oskarżone, potrzebę propagowania zidentyfikowanych i poufnych zgłoszeń w stosunku do zgłoszeń anonimowych, potrzebę dopuszczenia ujawnienia tożsamości osób zgłaszających przypadki naruszenia w przypadku, gdy osoba zgłaszająca przypadki naruszenia umyślnie złożyła fałszywe oświadczenie, oraz potrzebę zachowania ścisłych okresów zatrzymywania danych.

3. **WNIOSKI**

56. EIOD z uznaniem odnotowuje szczególną uwagę, jaką w treści proponowanego rozporządzenia poświęcono kwestii ochronie danych.

57. EIOD zaleca, co następuje:

— określenie w art. 13 celu sporządzenia listy osób mających dostęp do informacji poufnych,

— dodanie w przepisie art. 17 ust. 2 lit. e) dotyczącym uprawnienia do wchodzenia na teren prywatny ogólnego wymogu uprzedniego uzyskania upoważnienia sądowego,

— dodanie w przepisie art. 17 ust. 2 lit. f) dotyczącym uprawnienia do żądania wydania danych o połączeniach telefonicznych i ruchu ogólnego wymogu uprzedniego uzyskania upoważnienia sądowego oraz wymogu formalnej decyzji określającej: (i) podstawę prawną; (ii) cel żądania; (iii) żądane informacje; (iv) termin udostępnienia informacji oraz (v) prawo adresata do zaskarżenia decyzji do Trybunału Sprawiedliwości,

([1]) Zob. np. opinia w sprawie reguł finansowych mających zastosowanie do budżetu rocznego Unii z dnia 15 kwietnia 2011 r. oraz opinia w sprawie dochodzeń prowadzonych przez OLAF z dnia 1 czerwca 2011 r., obie dostępne na stronie: http://www.edps.europa.eu

([2]) Istotność ochrony poufności tożsamości osoby zgłaszającej przypadki naruszenia EIOD podkreślił już w piśmie do Europejskiego Rzecznika Praw Obywatelskich z dnia 30 lipca 2010 r. w sprawie 2010-0458, które jest dostępne na stronie EIOD (http://www.edps.europa.eu). Zob. również opinie EIOD w sprawie kontroli wstępnej z dnia 3 lutego 2012 r., z dnia 23 czerwca 2006 r., w sprawie dochodzeń wewnętrznych OLAF (sprawa 2005-0418), oraz z dnia 4 października 2007 r. w sprawie dochodzeń zewnętrznych OLAF (sprawy 2007-47, 2007-48, 2007-49, 2007-50, 2007-72).

([3]) 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

— określenie kategorii rejestrów połączeń telefonicznych i rejestrów przesyłu danych w posiadaniu operatora telekomunikacyjnego i firm inwestycyjnych, których wydania mogą żądać właściwe organy, oraz ograniczenie art. 17 ust. 2 lit. f) do danych zazwyczaj przetwarzanych przez (będących „w posiadaniu") operatorów telekomunikacyjnych na podstawie dyrektywy 2002/58/WE,

— dodanie w art. 29 ust. 1 lit. b) zapisu, iż „na wszystkich etapach postępowania należy zapewnić ochronę tożsamości takich osób, o ile jej ujawnienie nie jest wymagane przez przepisy krajowe w kontekście dalszego śledztwa lub wszczętego w dalszym trybie postępowania sądowego",

— w świetle wątpliwości wyrażonych w niniejszej opinii – dokonanie oceny niezbędności i proporcjonalności proponowanego systemu obowiązkowej publikacji sankcji. Niezależnie od wyniku takiego testu proporcjonalności, obowiązkowi publikacji w każdym przypadku powinny towarzyszyć odpowiednie gwarancje w celu zapewnienia poszanowania zasady domniemania niewinności, prawa zainteresowanej osoby do sprzeciwu, bezpieczeństwa/poprawności danych oraz ich usuwania po upływie odpowiedniego okresu.

Sporządzono w Brukseli dnia 10 lutego 2012 r.

Giovanni BUTTARELLI

Zastępca Europejskiego Inspektora Ochrony Danych