Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA)

(2011/C 101/04)

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 wniosek o opinię zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych ([2]),

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. **WPROWADZENIE**

Opis wniosku

1. W dniu 30 września 2010 r. Komisja przyjęła wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) ([3]).

2. ENISA powołano do życia w marcu 2004 r. na wstępny okres pięciu lat na mocy rozporządzenia (WE) nr 460/2004 ([4]). W 2008 r. rozporządzenie (WE) nr 1107/2008 ([5]) przedłużyło mandat do marca 2012 r.

3. Jak wynika z art. 1 ust. 1 rozporządzenia (WE) nr 460/2004, Agencję ustanowiono w celu zapewnienia wysokiego i skutecznego poziomu bezpieczeństwa sieci i informacji w Unii oraz zapewnienia płynnego funkcjonowania rynku wewnętrznego.

4. Wniosek Komisji ma na celu modernizację Agencji, zwiększenie jej uprawnień oraz ustanowienie nowego mandatu na okres pięciu lat, który pozwoli zachować ciągłość Agencji po marcu 2012 r. ([6]).

5. Podstawą prawną zaproponowanego rozporządzenia jest art. 114 TFUE ([7]), który nadaje Unii kompetencje w zakresie przyjmowania środków, które mają na celu ustanowienie lub zapewnienie funkcjonowania rynku wewnętrznego. Artykuł 114 TFUE zastąpił dawny 95 art. wcześniejszego Traktatu WE, na którym były oparte poprzednie przepisy dotyczące ENISA ([8]).

6. Uzasadnienie dołączone do wniosku odnosi się do faktu, że po wejściu w życie traktatu lizbońskiego zapobieganie przestępczości i zwalczanie jej stało się kompetencją dzieloną. Jest to szansa dla ENISA, żeby odegrać rolę platformy dla kwestii bezpieczeństwa sieci i informacji pojawiających się przy zwalczaniu cyberprzestępczości, a także platformy do wymiany opinii i najlepszych praktyk z organami obrony przed atakami cybernetycznymi, organami ścigania i organami ochrony danych.

7. Z kilku opcji Komisja postanowiła zaproponować rozszerzenie zadań ENISA oraz dodać organy ścigania i ochrony danych jako pełnoprawnych członków do stałej grupy stron zainteresowanych. Nowa lista zadań nie obejmuje zadań operacyjnych, jedynie aktualizuje i przeformułowuje obecne zadania.

Konsultacja z EIOD

8. W dniu 1 października 2010 r. wniosek został przesłany do EIOD do konsultacji zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001. EIOD z zadowoleniem przyjął fakt, że się z nim skonsultowano w tej kwestii i polecił zamieścić odniesienie do tej konsultacji w motywach wniosku, zgodnie z przyjętą praktyką wobec aktów ustawodawczych, w sprawie których skonsultowano się z EIOD zgodnie z rozporządzeniem (WE) nr 45/2001.

9. Przed przyjęciem wniosku skonsultowano się nieoficjalnie z EIOD, który poczynił kilka nieoficjalnych uwag. Żadna z tych uwag nie została jednak uwzględniona w ostatecznej wersji wniosku.

Ocena ogólna

10. EIOD podkreśla, że bezpieczeństwo przetwarzania danych to kluczowy element ochrony danych ([9]). W tym względzie z zadowoleniem przyjmuje cel wniosku, jakim jest wzmocnienie kompetencji Agencji, by mogła ona skuteczniej

([1]) Dz.U. L 281 z 23.11.1995, s. 31.
([2]) Dz.U. L 8 z 12.1.2001, s. 1.
([3]) COM(2010) 521 wersja ostateczna.
([4]) Dz.U. L 77 z 13.3.2004, s. 1.
([5]) Dz.U. L 293 z 31.10.2008, s. 1.
([6]) W celu uniknięcia luki w prawie, gdyby procedura ustawodawcza w Parlamencie Europejskim i Radzie nie zakończyła się do daty wygaśnięcia obecnego mandatu, Komisja, w dniu 30 września 2010 r., przyjęła drugi wniosek o zmianę rozporządzenia (WE) nr 460/2004, którego wyłącznym celem jest przedłużenie terminu obecnego mandatu o 18 miesięcy. Zob. COM(2010) 520 wersja ostateczna.
([7]) Por. wyżej.
([8]) W dniu 2 maja 2006 r. Trybunał Sprawiedliwości oddalił skargę o unieważnienie wcześniejszego rozporządzenia (WE) nr 460/2004, która kwestionowała jego podstawę prawną (sprawa C-217/04).
([9]) Wymogi w zakresie bezpieczeństwa zawarto w art. 22 i 35 rozporządzenia (WE) nr 45/2001, art. 16 i 17 dyrektywy 95/46/WE i art. 4 i 5 dyrektywy 2002/58/WE.

wykonywać swoje obecne zadania i obowiązki, jednocześnie rozszerzając zakres swojej działalności. Ponadto EIOD wyraża zadowolenie z powodu dołączenia organów ochrony danych i organów ścigania jako pełnoprawnych stron zainteresowanych. Przedłużenie mandatu ENISA uznaje za sposób na promowanie na poziomie europejskim profesjonalnego i usprawnionego zarządzania środkami bezpieczeństwa w systemach informacyjnych.

11. Ogólna ocena wniosku jest pozytywna. W kilku kwestiach jednak zaproponowane rozporządzenie jest niejasne i niepełne, co budzi obawy z punktu widzenia ochrony danych. Kwestie te zostaną wyjaśnione i omówione w kolejnym rozdziale niniejszej opinii.

II. **UWAGI I ZALECENIA**

Rozszerzone zadania, które będzie wykonywać ENISA, nie są dostatecznie jasno określone

12. Rozszerzone zadania Agencji, które odnoszą się do zaangażowania organów ścigania i organów ochrony danych, zostały sformułowane w art. 3 wniosku w bardzo ogólny sposób. Uzasadnienie jest bardziej bezpośrednie w tym względzie. Odnosi się do ENISA jako Agencji współpracującej z organami ścigania cyberprzestępczości i wykonującej pozaoperacyjne zadania w walce z cyberprzestępczością. Zadania te nie zostały jednak zawarte, jeśli nawet, to ujęto je w bardzo ogólny sposób w art. 3.

13. W celu uniknięcia niepewności prawa zaproponowane rozporządzenie powinno jasno i jednoznacznie określać zadania ENISA. Jak stwierdzono, bezpieczeństwo przetwarzania danych to kluczowy element ochrony danych. ENISA będzie odgrywać coraz ważniejszą rolę w tym obszarze. Dla obywateli i organów powinno być jasne, w jakiego rodzaju działalność ENISA może się zaangażować. Wymiar ten byłby jeszcze ważniejszy, gdyby rozszerzone zadania ENISA obejmowały przetwarzanie danych osobowych (zobacz pkt 17–20 poniżej).

14. Artykuł 3 ust. 1 lit. k) wniosku stanowi, że Agencja wykonuje wszelkie inne zadania powierzone jej na mocy innego aktu ustawodawczego Unii. EIOD ma obawy co do tej otwartej klauzuli, biorąc pod uwagę, że stanowi ona potencjalną lukę, która może zaburzyć spójność instrumentu prawnego i prowadzić do „rozpłynięcia funkcji" Agencji.

15. Jedno z zadań, o których mowa w art. 3 ust. 1 lit. k) wniosku, jest zawarte w dyrektywie 2002/58/WE ([1]). Przepis stanowi, że Komisja musi skonsultować się z Agencją w zakresie technicznych środków wykonawczych mających zastosowanie do powiadomień w kontekście naruszeń danych. EIOD zaleca, by ta działalność Agencji została opisana bardziej szczegółowo przy jednoczesnym ograniczeniu jej do obszaru bezpieczeństwa. Biorąc pod uwagę potencjalny wpływ, jaki ENISA może mieć na rozwój polityki w tym obszarze, działalność ta powinna zajmować bardziej wyraźną i znaczącą pozycję w obrębie zaproponowanego rozporządzenia.

16. Ponadto EIOD zaleca włączenie odniesienia do dyrektywy 1999/5/WE do motywu 21 ([2]), biorąc pod uwagę specjalne zadanie ENISA, o którym mowa w art. 3 ust. 1 lit. c) obecnego wniosku, polegające na wspieraniu państw członkowskich oraz instytucji i organów europejskich w gromadzeniu, analizie i rozpowszechnianiu danych na temat bezpieczeństwa sieci i informacji. To powinno napędzić działania ENISA promujące najlepsze praktyki i techniki w zakresie bezpieczeństwa sieci i informacji, będzie to bowiem lepiej odzwierciedlało możliwe konstruktywne interakcje pomiędzy Agencją a organami normalizacyjnymi.

Należy wyjaśnić, czy Agencja będzie przetwarzać dane osobowe

17. Wniosek nie określa, czy zadania przypisane Agencji mogą obejmować przetwarzanie danych osobowych. Wniosek nie zawiera więc odrębnej podstawy prawnej dla przetwarzania danych osobowych, w rozumieniu art. 5 rozporządzenia (WE) nr 45/2001.

18. Niektóre z zadań powierzonych Agencji mogą jednak obejmować (przynajmniej w pewnym zakresie) przetwarzanie danych osobowych. Nie sposób, na przykład, wykluczyć, czy analiza przypadków naruszenia bezpieczeństwa i naruszenia danych lub pełnienie nieoperacyjnych funkcji w walce z cyberprzestępczością nie będą wiązały się z gromadzeniem i analizą danych osobowych.

19. Motyw 9 wniosku odnosi się do przepisów zawartych w dyrektywie 2002/21/WE ([3]), która stanowi, że w stosownych przypadkach krajowe organy regulacyjne powiadamiają Agencję o przypadkach naruszenia bezpieczeństwa. EIDO zaleca, by wniosek bardziej szczegółowo określał, jakie powiadomienia mają być wysyłane do ENISA i jak ENISA ma na nie odpowiadać. Podobnie wniosek powinien obejmować skutki przetwarzania danych osobowych, jakie może mieć (ewentualna) analiza tych powiadomień.

([1]) 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 (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

([2]) Dyrektywa Parlamentu Europejskiego i Rady 1999/5/WE z dnia 9 marca 1999 r. w sprawie urządzeń radiowych i końcowych urządzeń telekomunikacyjnych oraz wzajemnego uznawania ich zgodności, (Dz.U. L 91 z 7.4.1999, s. 10), a w szczególności jej art. 3 ust. 3 lit. c).

([3]) Dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa, Dz.U. L 108 z 24.4.2002, s. 33).

20. EIOD zachęca ustawodawcę do wyjaśnienia, czy działania wymienione w art. 3 będą obejmować przetwarzanie danych osobowych, a jeśli tak – których z nich to dotyczy.

Należy określić wewnętrzne zasady bezpieczeństwa dla ENISA

21. Choć ENISA odgrywa ważną rolę w dyskusji na temat bezpieczeństwa sieci i informacji w Europie, wniosek właściwie milczy na temat ustanowienia środków bezpieczeństwa dla samej Agencji (zarówno związanych, jak i niezwiązanych z przetwarzaniem danych osobowych).

22. EIOD jest zdania, że Agencja będzie w stanie w jeszcze większym stopniu promować dobre praktyki w zakresie bezpieczeństwa przetwarzania danych, jeśli takie środki bezpieczeństwa będą w sposób zdecydowany stosowane wewnętrznie przez samą Agencję. To umożliwi nie tylko uznanie Agencji za centrum wiedzy specjalistycznej, ale również za punkt odniesienia przy praktycznym wdrażaniu najlepszych dostępnych technik (BAT) w dziedzinie bezpieczeństwa. Dążenie do perfekcji we wdrażaniu praktyk z zakresu bezpieczeństwa powinno więc zostać wpisane do rozporządzenia regulującego procedury pracy Agencji. EIOD zaleca więc dodanie przepisu w tym duchu do wniosku, na przykład poprzez wprowadzenie wymogu stosowania przez Agencję najlepszych dostępnych technik, co oznacza najbardziej skuteczne i zaawansowane procedury bezpieczeństwa oraz metody ich funkcjonowania.

23. Podejście to umożliwi Agencji oferowanie doradztwa w zakresie praktycznej przydatności poszczególnych technik zapewniania wymaganych gwarancji bezpieczeństwa. Ponadto wdrożenie tych BAT powinno traktować priorytetowo te techniki, które umożliwiają zapewnienie bezpieczeństwa przy jednoczesnym możliwie najmocniejszym minimalizowaniu wpływu na prywatność. Należy postawić na techniki, które bardziej odpowiadają podejściu „uwzględnienia ochrony prywatności w fazie projektowania".

24. Nawet przy bardziej niejednoznacznym podejściu EIOD zaleca jako minimum, by rozporządzenie zawierało następujące wymogi: (i) stworzenie wewnętrznej polityki bezpieczeństwa po ogólnej ocenie ryzyka i uwzględnieniu międzynarodowych norm i najlepszych praktyk w państwach członkowskich; (ii) wyznaczenie urzędnika ds. bezpieczeństwa odpowiedzialnego za wdrożenie polityki, o odpowiednich zasobach i uprawnieniach; (iii) zatwierdzenie tej polityki po dokładnej ocenie pozostałego ryzyka i kontrole zaproponowane przez zarząd; oraz (iv) okresowy przegląd polityki z wyraźnym określeniem wybranych odstępów czasowych i celów przeglądu.

Należy dokładnie określić kanały współpracy z organami ochrony danych (w tym z EIOD) i grupą roboczą art. 29

25. Jak już stwierdzono, EIOD z zadowoleniem przyjął przedłużenie mandatu Agencji i wierzy, że organy ochrony danych mogą czerpać znaczne korzyści z istnienia Agencji (a Agencja ze specjalistycznej wiedzy tych organów). Ze względu na naturalną i logiczną zbieżność między bezpieczeństwem a ochroną danych wzywa się Agencję i organy ochrony danych do ścisłej współpracy.

26. Motywy 24 i 25 zawierają odniesienie do zaproponowanej dyrektywy UE w sprawie cyberprzestępczości i stwierdzają, że Agencja powinna współpracować z organami ścigania i organami ochrony danych w zakresie kwestii bezpieczeństwa danych w walce z cyberprzestępczością ([1]).

27. Wniosek powinien również zapewniać konkretne kanały i mechanizmy współpracy, które (i) zapewnią *spójność* działalności Agencji z działalnością organów ochrony danych i (ii) umożliwią *ścisłą współpracę* pomiędzy Agencją a organami ochrony danych.

28. W odniesieniu do *spójności* motyw 27 wyraźnie odnosi się do faktu, że zadania Agencji nie powinny kolidować z zadaniami organów ochrony danych państw członkowskich. EIOD z zadowoleniem przyjmuje to odniesienie, ale zauważa, że brak jest odniesienia do EIOD i grupy roboczej art. 29. EIOD zaleca ustawodawcy, by włączył również podobne przepisy o niedublowaniu prac do wniosku w odniesieniu do tych dwóch instytucji. Stworzy to wyraźniejsze warunki pracy dla wszystkich stron i opracuje mechanizmy współpracy, które umożliwią Agencji wspieranie poszczególnych organów ochrony danych i grupy roboczej art. 29.

29. Podobnie, w odniesieniu do *ścisłej współpracy*, EIOD z zadowoleniem przyjmuje włączenie przedstawicielstwa organów ochrony danych do stałej grupy stron zainteresowanych, która będzie służyć poradą Agencji w jej działalności. Zaleca, by wyraźnie określić, że takie przedstawicielstwo krajowych organów ochrony danych powinno być wyznaczane przez Agencję w oparciu o wniosek od grupy roboczej art. 29. Również dobrze byłoby, żeby włączyć odniesienie do obecności EIOD na tych spotkaniach, na których mają być omawiane kwestie istotne z punktu widzenia współpracy z EIOD. Ponadto EIOD zaleca, by Agencja (po konsultacji ze stałą grupą stron zainteresowanych i po zatwierdzeniu przez zarząd) ustanowiła grupy robocze *ad hoc* do różnych zagadnień, w których ochrona i bezpieczeństwo danych pokrywają się, w celu stworzenia ram dla tej ścisłej współpracy.

([1]) Wniosek – dyrektywa Parlamentu Europejskiego i Rady dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW, COM(2010) 517 wersja ostateczna.

30. W końcu, w celu uniknięcia możliwych nieporozumień EIDO zaleca stosowanie wyrażenia „organy ochrony danych" zamiast „organy ochrony prywatności" oraz wyjaśnienie, co to za organy poprzez włączenie odniesienia do art. 28 dyrektywy 95/46/WE i EIOD, zgodnie z rozdziałem V rozporządzenia (WE) nr 45/2001.

Nie wiadomo, którzy beneficjenci mogą zwrócić się o pomoc do ENISA

31. EIOD zauważa niespójność w zaproponowanym rozporządzeniu w odniesieniu do tych osób, które mogą zwrócić się o pomoc do ENISA. Z motywów 7, 15, 16, 18 i 36 wniosku wynika, że ENISA ma możliwość wspierania organów państw członkowskich i Unii jako całości. Artykuł 2 ust. 1 odnosi się jednak wyłącznie do Komisji i państw członkowskich, podczas gdy art. 14 ogranicza możliwość składania wniosków o pomoc do: (i) Parlamentu Europejskiego; (ii) Rady; (iii) Komisji i (iv) właściwego organu wyznaczonego przez państwo członkowskie, wykluczając pewne instytucje, organy, agencje i urzędy Unii.

32. Artykuł 3 wniosku jest bardziej dokładny i uwzględnia poszczególne rodzaje pomocy w zależności od typu beneficjentów: (i) gromadzenie i analiza danych bezpieczeństwa informacji (w przypadku państw członkowskich oraz europejskich instytucji i organów); (ii) analiza stanu bezpieczeństwa sieci i informacji w Europie (w przypadku państw członkowskich i instytucji europejskich); (iii) promowanie korzystania z dobrych praktyk z zakresu bezpieczeństwa i zarządzania ryzykiem (w całej Unii i państwach członkowskich); (iv) utworzenie środków wykrywania bezpieczeństwa sieci i informacji (w europejskich instytucjach i organach) i (v) współpraca w dialogu i współpraca z państwami trzecimi (w przypadku Unii).

33. EIOD zachęca ustawodawcę do usunięcia tej niespójności i do dostosowania wspomnianych powyżej przepisów. W tym względzie EIOD zaleca, by art. 14 zmienić tak, by faktycznie zawierał wszystkie instytucje, organy, urzędy i agencje Unii i by było jasne, jakiego rodzaju pomocy mogą wymagać poszczególne podmioty w obrębie Unii (w przypadku uwzględnienia takiego rozróżnienia przez ustawodawcę). W tym samym kierunku zaleca się, by określone podmioty prywatne i publiczne mogły zwrócić się do Agencji o pomoc, jeśli wsparcie, o które się ubiegają, stanowi wyraźny potencjał z perspektywy europejskiej i jest zgodne z celami Agencji.

Funkcje zarządu

34. Uzasadnienie określa większe kompetencje zarządu w zakresie jego nadzorczej roli. EIOD z zadowoleniem przyjmuje tę zwiększoną rolę i zaleca, by kilka aspektów odnoszących się do ochrony danych włączono do funkcji zarządu. Ponadto EIOD zaleca, by rozporządzenie określało jednoznacznie, kto jest uprawniony do: (i) ustanawiania środków w celu wykonania rozporządzenia (WE) nr 45/2001 przez Agencję, w tym środków dotyczących wyznaczenia inspektora ochrony danych; (ii) zatwierdzenia polityki bezpieczeństwa i późniejszych okresowych przeglądów oraz; (iii) opracowania protokołu w sprawie współpracy z organami ochrony danych i organami ścigania.

Stosowanie rozporządzenia (WE) nr 45/2001

35. Choć wymaga tego już rozporządzenie (WE) nr 45/2001, EIOD zaleca włączenie do art. 27 wyznaczania inspektora danych osobowych, ponieważ ma to ogromne znaczenie i powinno wiązać się z natychmiastowym ustanowieniem przepisów wykonawczych dotyczących zakresu uprawnień i zadań powierzonych inspektorowi ochrony danych zgodnie z art. 24 ust. 8 rozporządzenia (WE) nr 45/2001. W szczególności art. 27 mógłby mieć następujące brzmienie:

1) Informacje przetwarzane przez Agencję zgodnie z niniejszym rozporządzeniem podlegają rozporządzeniu (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) Zarząd ustanawia środki w celu wykonania rozporządzenia (WE) nr 45/2001 przez Agencję, w tym środki dotyczące inspektora ochrony danych Agencji.

36. W przypadku konieczności specjalnej podstawy prawnej dla przetwarzania danych osobowych, jak omówiono w pkt 17–20 powyżej, powinien on również określać niezbędne i właściwe zabezpieczenia, ograniczenia i warunki, w ramach których takie przetwarzanie miałoby miejsce.

III. **WNIOSKI**

37. Ogólna ocena wniosku jest pozytywna i EIOD z zadowoleniem przyjmuje przedłużenie mandatu Agencji oraz rozszerzenie jej zadań poprzez dołączenie organów ochrony danych i organów ścigania jako pełnoprawnych stron zainteresowanych. EIOD uważa, że ciągłość Agencji będzie promować na poziomie europejskim profesjonalne i usprawnione zarządzanie środkami bezpieczeństwa w systemach informacyjnych.

38. EIOD zaleca, by w celu uniknięcia niepewności prawa wniosek został wyraźniej sformułowany w kwestii rozszerzenia zadań Agencji, a w szczególności zadań dotyczących zaangażowania organów ścigania i organów ochrony danych. EIOD zwraca również uwagę na potencjalną lukę, jaką tworzy włączenie przepisu do wniosku, który umożliwia dodawanie nowych zadań Agencji na mocy innych aktów ustawodawczych Unii bez dodatkowych ograniczeń.

39. EIOD zachęca ustawodawcę do wyjaśnienia, czy działania ENISA będą obejmować przetwarzanie danych osobowych, a jeśli tak – których z nich to dotyczy.

40. EIOD zaleca włączenie przepisów dotyczących utworzenia polityki bezpieczeństwa dla samej Agencji w celu wzmocnienia roli Agencji jako instytucji wspierającej doskonalenie praktyk z zakresu bezpieczeństwa i jako promotora podejścia uwzględniania ochrony prywatności w fazie projektowania poprzez włączenie stosowania najlepszych dostępnych technik w bezpieczeństwie w odniesieniu do praw ochrony danych osobowych.

41. Należy dokładnie określić kanały współpracy z organami ochrony danych (w tym z EIOD) i grupą roboczą art. 29, w celu zapewnienia spójności i ścisłej współpracy.

42. EIOD zachęca ustawodawcę do pozbycia się niespójności w zakresie ograniczeń wyrażonych w art. 14 dotyczących możliwości ubiegania się o pomoc od Agencji. W szczególności EIOD zaleca, by znieść te ograniczenia i umożliwić wszystkim instytucjom, organom, agencjom i urzędom Unii ubieganie się o pomoc od Agencji.

43. W końcu EIOD zaleca, by rozszerzone kompetencje zarządu obejmowały kilka konkretnych aspektów, które mogłyby zwiększyć pewność, że w obrębie Agencji stosuje się dobre praktyki w odniesieniu do bezpieczeństwa i ochrony danych. Między innymi proponuje włączyć wyznaczanie inspektora ochrony danych i zatwierdzanie środków mających na celu prawidłowe stosowanie rozporządzenia (WE) nr 45/2001.

Sporządzono w Brukseli dnia 20 grudnia 2010 r.

Giovanni BUTTARELLI

Zastępca Europejskiego Inspektora Ochrony Danych