I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych na temat wniosku dotyczącego rozporządzenia w sprawie wprowadzania do obrotu i używania prekursorów materiałów wybuchowych

(2011/C 101/01)

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 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**

1. W dniu 20 września 2010 r. Komisja Europejska przyjęła wniosek dotyczący rozporządzenia w sprawie wprowadzania do obrotu i używania prekursorów materiałów wybuchowych [3] (zwany dalej „wnioskiem"). W dniu 11 listopada 2010 r. wniosek przyjęty przez Komisję przekazano EIOD do konsultacji zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001. EIOD z zadowoleniem przyjął fakt, że Komisja się z nim skonsultowała i że odniesienie do tej konsultacji znajduje się w motywach wniosku.

2. Głównym celem zaproponowanych środków jest ograniczenie ryzyka ataków terrorystów lub innych przestępców za pomocą wytworzonych domowym sposobem urządzeń wybuchowych. W tym celu rozporządzenie ogranicza dostęp przeciętnych użytkowników do niektórych substancji chemicznych, które mogą być niewłaściwe używane jako prekursory wytwarzanych domowym sposobem materiałów wybuchowych. Ponadto wniosek obejmuje sprzedaż takich substancji chemicznych ściślejszą kontrolą poprzez zgłaszanie podejrzanych transakcji i kradzieży.

3. W niniejszej opinii EIOD zwraca uwagę prawodawców na kilka istotnych kwestii ochrony danych i przedstawia zalecenia, których celem jest zapewnienie prawa podstawowego do ochrony danych osobowych.

II. **ANALIZA WNIOSKU I ISTOTNYCH KWESTII OCHRONY DANYCH**

1. **Środki zaproponowane przez Komisję**

4. Wniosek dotyczy problemów związanych z niewłaściwymi używaniem niektórych substancji chemicznych, które są szeroko dostępne na rynku dla przeciętnych użytkowników, jako prekursory wytwarzanych domowym sposobom materiałów wybuchowych. Art. 4 i 5 wniosku odnosi się zakazu sprzedaży przeciętnym użytkownikom niektórych substancji, który powiązany jest z systemem koncesji i wymogiem odnotowania w ewidencji wszystkich koncesjonowanych transakcji. Art. 6 wymaga od podmiotów gospodarczych zgłaszania podejrzanych transakcji i kradzieży. W końcu art. 7 dotyczy konieczności ochrony danych.

Artykuły 4 i 5: Zakaz sprzedaży, koncesjonowanie i ewidencja transakcji

5. Zakazana jest powszechna sprzedaż niektórych substancji chemicznych w stężeniach przekraczających określone progi. Substancje te w wyższych stężeniach można byłoby sprzedawać wyłącznie użytkownikom, którzy mogą udokumentować, że potrzebują ich w zgodnych z prawem celach.

[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) 473.

6. Zakres wniosku ogranicza się do krótkiego wykazu substancji chemicznych i ich mieszanin (zobacz załącznik I do wniosku) oraz do ich sprzedaży przeciętnym użytkownikom. Ograniczenia te nie znajdują zastosowania wobec użytkowników specjalistycznych ani między przedsiębiorstwami. Ponadto dostępność dla przeciętnych użytkowników substancji chemicznych z krótkiego wykazu zostaje ograniczona wyłącznie wtedy, gdy substancje te przekraczają określone progi stężenia. Substancje można nadal nabyć za okazaniem koncesji wydanej przez organ publiczny (dokumentującej, że są one wykorzystywane w zgodnych z prawem celach). Wyjątek stosuje się także do rolników, którzy mogą nabyć azotan amonowy w celu wykorzystania jako nawóz bez koncesji, niezależnie od poziomu stężenia.

7. Koncesja będzie również wymagana, gdy przeciętny użytkownik zamierza sprowadzić do Unii Europejskiej substancje wyszczególnione w krótkim wykazie.

8. Podmiot gospodarczy udostępniający substancję lub mieszaninę koncesjonowanemu przeciętnemu użytkownikowi musi sprawdzić koncesję oraz odnotowuje transakcję w ewidencji.

9. Od każdego państwa członkowskiego wymaga się ustanowienia przepisów dotyczących udzielania koncesji. Właściwy organ w państwie członkowskim odmawia udzielenia wnioskodawcy koncesji, jeżeli istnieją zasadne powody, by wątpić w zgodność z prawem zamierzonego użycia. Udzielone koncesje są ważne we wszystkich państwach członkowskich. Komisja sporządza wytyczne na temat szczegółowych aspektów technicznych koncesji, by pomóc w ich wzajemnym uznawaniu.

Artykuł 6: Zgłaszanie podejrzanych transakcji i kradzieży

10. Sprzedaż odnośnych substancji chemicznych w szerszym zakresie (substancji wymienionych w załączniku II, obok wszystkich substancji wymienionych w załączniku I, które podlegają już wymogowi koncesjonowania) podlega zgłoszeniu podejrzanych transakcji i kradzieży.

11. Wniosek wymaga od każdego państwa członkowskiego ustanowienia krajowego punktu kontaktowego (wyraźnie podając jego numer telefonu i adres poczty internetowej) na potrzeby zgłaszania podejrzanych transakcji i kradzieży. Od podmiotów gospodarczych wymaga się niezwłocznego zgłoszenia podejrzanych transakcji i kradzieży, z podaniem w miarę możliwości tożsamości klienta.

12. Komisja sporządza i aktualizuje wytyczne, by wspomóc podmioty gospodarcze w rozpoznawaniu i zgłaszaniu podejrzanej transakcji. Wytyczne będą obejmować również regularnie aktualizowany wykaz dodatkowych substancji niezawartych w załączniku I ani II, w przypadku których zachęca się do dobrowolnego zgłaszania podejrzanych transakcji i kradzieży.

Artykuł 7: Ochrona danych

13. Motyw 11 i art. 7 zawierają wyraźny wymóg, by przetwarzanie danych osobowych na mocy rozporządzenia odbywało się zawsze zgodnie z unijnymi przepisami o ochronie danych, w szczególności z dyrektywą 95/46/WE [4] oraz krajowymi przepisami o ochronie danych przyjętymi w celu wdrożenia tej dyrektywy. Wniosek nie zawiera innych przepisów w zakresie ochrony danych.

2. **Bardziej szczegółowe przepisy są niezbędne dla odpowiedniej ochrony danych osobowych**

14. Zgłaszanie podejrzanych transakcji i kradzieży oraz system koncesjonowania i ewidencji przewidziane w rozporządzeniu wymagają przetwarzania danych osobowych. Oba wiążą się z – zawsze w pewnym stopniu – zakłóceniem życia prywatnego i prawem do ochrony danych osobowych, przez co wymagają odpowiednich zabezpieczeń.

15. EIOD z zadowoleniem przyjmuje fakt, że wniosek zawiera oddzielny przepis (art. 7) dotyczący ochrony danych. Ten pojedynczy – i bardzo ogólny – przepis przewidziany we wniosku jest jednak niewystarczający dla odpowiedniego potraktowania kwestii ochrony danych, z jakimi wiążą się zaproponowane środki. Ponadto właściwe artykuły wniosku (art. 4, 5 i 6) również nie opisują dostatecznie szczegółowo specyfiki przewidzianych operacji przetwarzania danych.

16. Dla przykładu, w zakresie koncesji rozporządzenie wymaga od podmiotu gospodarczego odnotowania w ewidencji koncesjonowanych transakcji, jednak bez określenia, jakie dane osobowe ewidencja ta powinna zawierać, jak długo należy ją zatrzymywać, komu i na jakich warunkach można ją ujawnić. Nie określono również, jakie dane będę gromadzone przy przetwarzaniu wniosków o koncesję.

17. Jeśli chodzi o wymóg zgłaszania podejrzanych transakcji i kradzieży, wniosek ustanawia wymóg zgłaszania, nie określając jednak, co stanowi podejrzaną transakcję, jakie dane osobowe należy zgłosić, jak długo zgłoszone informacje powinny być zatrzymywane, komu i na jakich warunkach można je ujawnić. Wniosek nie opisuje także szczegółowo „krajowych punktów kontaktowych", które należy ustanowić, ani bazy danych, jaką te punkty kontaktowe mogą ustanowić dla swoich państw członkowskich, ani ewentualnej bazy danych, jaka może powstać na poziomie UE.

18. Z punktu widzenia ochrony danych gromadzenie danych dotyczących podejrzanych transakcji to najdelikatniejsza kwestia we wniosku. Właściwe przepisy należy ująć wyraźnie w taki sposób, by zapewnić proporcjonalność przetwarzania danych i zapobiec naruszeniom. W tym celu należy wyraźnie określić warunki przetwarzania danych i zastosować odpowiednie zabezpieczenia.

[4] Przytoczone w przypisie 1.

19. Co ważniejsze, danych nie powinno się wykorzystywać do żadnego innego celu niż zwalczanie terroryzmu (i innych przestępstw związanych z niewłaściwym używaniem substancji chemicznych jako wytwarzanych domowym sposobem materiałów wybuchowych). Danych nie powinno się również zatrzymywać w dłuższych okresach, szczególnie jeśli liczba potencjalnych i faktycznych odbiorców miałaby być duża lub jeśli dane miałyby być wykorzystane do eksploracji danych. Jest to jeszcze ważniejsze w przypadkach, w których można wykazać, że początkowe podejrzenie był bezpodstawne. W takich przypadkach musi istnieć konkretne uzasadnienie dla dalszego zatrzymywania danych. Dla przykładu EIOD odwołuje się w tym kontekście do orzeczenia Europejskiego Trybunału Praw Człowieka w sprawie S i Marper przeciwko Zjednocznemu Królestwu (2008 r.) ([5]), zgodnie z którym długoterminowe zatrzymywanie DNA osób nieskazanych za przestępstwo było naruszeniem ich prawa do prywatności zgodnie z art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności.

20. Z tych względów EIOD zaleca, by art. 5, 6 i 7 wniosku zawierały więcej bardziej szczegółowych przepisów, aby odpowiednio potraktować te kwestie. Bardziej szczegółowe zalecenia przedstawiono poniżej.

21. Ponadto należy również rozważyć, czy można przygotować właściwe, bardziej szczegółowe przepisy w decyzji wykonawczej Komisji zgodnie z art. 10, 11 i 12 wniosku w celu objęcia dodatkowych kwestii ochrony danych na poziomie praktycznym.

22. EIOD zaleca również, by wytyczne Komisji na temat podejrzanych transakcji i szczegółowych aspektów technicznych koncesji zawierały więcej szczegółowych przepisów dotyczących przetwarzania danych i ochrony danych. Zarówno wytyczne, jak i ewentualna decyzja wykonawcza w dziedzinie ochrony danych, powinny zostać przyjęte po konsultacji z EIOD i – gdy w grę wchodzi wdrażanie na poziomie krajowym – z grupą roboczą art. 29 ds. ochrony danych. Należy przewidzieć to wyraźnie w samym rozporządzeniu i należy wyraźnie wymienić w nim główne kwestie, jakie należy objąć wytycznymi/decyzją wdrażającą.

3. **Zalecenia w odniesieniu do koncesjonowania i ewidencji transakcji**

3.1. ***Zalecenia do art. 5 wniosku***

Maksymalny okres zatrzymywania danych i kategorie gromadzonych danych

23. EIOD zaleca, by art. 5 rozporządzenia określał maksymalny okres zatrzymywania danych (*prima facie* nieprzekraczający dwóch lat) oraz kategorie danych osobowych, które należy odnotować w ewidencji (niewykraczające poza nazwisko, numer koncesji i zakupione artykuły). Zalecenia te wynikają z zasady konieczności i proporcjonalności: gromadzenie i zatrzymywanie danych osobowych powinno ograniczać się do tego, co ściśle niezbędne do zamierzonych celów (zobacz art. 6 lit. c) i e) dyrektywy 95/46/WE). Jeśli takie szczegóły zostawi się prawu krajowemu lub praktyce, będzie to prawdopodobnie prowadzić do niepotrzebnych wątpliwości i nierównego traktowania podobnych sytuacji w praktyce.

Zakaz gromadzenia „szczególnych kategorii danych"

24. Ponadto art. 5 rozporządzenia powinien również wyraźnie zakazać – w powiązaniu z procedurą koncesjonowania – gromadzenia i przetwarzania „szczególnych kategorii danych" (określonych w art. 8 dyrektywy 95/46/WE), takich jak m.in. danych osobowych ujawniających pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub światopoglądowe.

25. To powinno również ułatwić dopilnowanie, by wnioskodawcy nie byli traktowani w dyskryminujący sposób, na przykład ze względu na ich rasę, narodowość, przynależność polityczną lub religijną. W tym kontekście EIOD podkreśla, że zapewnienie wysokiego poziomu ochrony danych jest również środkiem przyczyniającym się do zwalczania rasizmu, ksenofobii i dyskryminacji, co z kolei może przyczynić się do zapobiegania radykalizacji postaw i werbowaniu terrorystów.

3.2. ***Zalecenie do wytycznych/decyzji wykonawczej***

Dane gromadzone w trakcie procesu koncesjonowania

26. Rozporządzenie stanowi, że wnioski o koncesję należy odrzucić, jeżeli istnieją zasadne powody, by wątpić w zgodność z prawem zamierzonego użycia. W tym względzie dobrze by było, gdyby wytyczne lub decyzja wykonawcza określały/a dane, które organy udzielające koncesji mogą gromadzić w związku z wnioskiem o koncesję.

Zasada celowości

27. Wytyczne lub decyzja wykonawcza powinny stanowić, że ewidencję należy ujawnić wyłącznie właściwym organom ścigania badającym działalność terrorystyczną lub inne podejrzane zastosowania prekursorów materiałów wybuchowych o charakterze przestępczym. Informacji nie należy wykorzystywać do dodatkowych celów (zobacz art. 6 lit. b) dyrektywy 95/46/WE).

Informacje dla osób, których dane dotyczą, na temat ewidencji transakcji (i ewidencji podejrzanych transakcji)

28. EIOD zaleca ponadto, by wytyczne lub decyzja wykonawcza precyzowały, że organ udzielający koncesji – który najlepiej nadaje się do dostarczenia takiego pisma bezpośrednio osobom, których dane dotyczą – powinien poinformować posiadaczy koncesji o tym, że ich transakcje będę przedmiotem ewidencji i mogą być przedmiotem zgłoszenia, jeśli okażą się „podejrzane" (zobacz art. 10 i 11 dyrektywy 95/46/WE).

([5]) S. i Marper przeciwko Zjednoczonemu Królestwu (4 grudzień 2008 r.) (wnioski nr 30562/04 i 30566/04).

4. Zalecenia w zakresie zgłaszania podejrzanych transakcji i kradzieży

4.1. *Zalecenia do art. 6 wniosku*

29. EIOD zaleca, by we wniosku wyraźnie określono rolę i charakter krajowych punktów kontaktowych. Ocena wpływu w pkt 6.33 odnosi się do możliwości, zgodnie z którą te punkty kontaktowe mogą być nie tylko „organami ścigania", ale również „stowarzyszeniami". Akty prawne nie zawierają żadnych innych informacji w tym względzie. Należy to w szczególności wyjaśnić w art. 6 ust. 2 wniosku. Zasadniczo dane powinny być zatrzymywane przez organy ścigania – jeśli nie, należy bardzo wyraźnie podać powody takie sytuacji.

30. Ponadto art. 6 rozporządzenia powinien określać dane osobowe podlegające ewidencji (niewykraczające poza nazwisko, numer koncesji, nabywane artykuły i powody powstania podejrzenia). Zalecenia te wynikają z zasady konieczności i proporcjonalności: gromadzenie danych osobowych powinno ograniczać się do tego, co ściśle niezbędne do zamierzonych celów (zobacz art. 6 lit. c) dyrektywy 95/46/WE). W tym kontekście zastosowanie mają analogiczne rozważania jak w pkt 23.

31. Art. 6 rozporządzenia powinien również wyraźnie zakazać – w powiązaniu z procedurą koncesjonowania – gromadzenia i przetwarzania „szczególnych kategorii danych" (określonych w art. 8 dyrektywy 95/46/WE), takich jak m.in. danych osobowych ujawniających pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub światopoglądowe (zobacz również pkt 24–25).

32. Art. 6 powinien również określać maksymalny okres zatrzymywania danych, z uwzględnieniem celów przechowywania danych. EIOD zaleca, by – chyba że dana podejrzana transakcja lub kradzież doprowadziły do konkretnego dochodzenia i dochodzenie jest nadal w toku – wszystkie zgłaszane podejrzane transakcje i przypadki kradzieży usuwać z bazy danych po upływie określonego czasu (*prima facie* najpóźniej po dwóch latach od daty zgłoszenia). To powinno ułatwić dopilnowanie, by w przypadkach braku potwierdzenia podejrzenia (lub umorzenia dochodzenia) niewinne osoby nie znajdowały się na „czarnej liście" lub nie były „podejrzane" przez nadmiernie długi okres (zobacz art. 6 lit. e) dyrektywy 95/46/WE). Należy uniknąć zbyt dużych rozbieżności w tym względzie na poziomie krajowym.

33. Ograniczenie to jest również konieczne w celu zapewnienia przestrzegania zasady jakości danych (zobacz art. 6 lit. d) dyrektywy 95/46/WE) oraz innych ważnych zasad prawa, takich jak domniemanie niewinności. Dzięki temu można uzyskać nie tylko bardziej odpowiedni poziom ochrony osób fizycznych, ale jednocześnie powinno to umożliwić organom ścigania bardziej skuteczne skoncentrowanie się na tych poważniejszych sprawach, w których podejrzenie prawdopodobnie zostanie ostatecznie potwierdzone.

4.2. *Zalecenie do wytycznych/decyzji wykonawczej*

Należy określić kryteria podejrzanych transakcji

34. We wniosku nie określono, jaką transakcję można uznać za „podejrzaną". Art. 6 ust. 6 lit. a) wniosku przewiduje jednak, że Komisja „sporządza i aktualizuje wytyczne" i dostarcza informacje, „w jaki sposób rozpoznać i zgłosić podejrzaną transakcję".

35. EIOD z zadowoleniem przyjmuje fakt, że wniosek wymaga od Komisji sporządzenia wytycznych. Powinny być one dostatecznie wyraźne i konkretne oraz zapobiegać zbyt szerokiej wykładni, by ograniczyć do minimum przekazywanie danych osobowych organom ścigania i zapobiec arbitralnym lub dyskryminacyjnym praktykom, np. ze względu na rasę, narodowość, przynależność polityczną lub religijną.

Zasada celowości, poufność, bezpieczeństwo i dostęp

36. Wytyczne lub przepisy wykonawcze powinny ponadto stanowić, że informacje należy zatrzymywać w bezpieczny i poufny sposób oraz należy je ujawnić wyłącznie właściwym organom ścigania badającym działalność terrorystyczną lub inne podejrzane zastosowania prekursorów materiałów wybuchowych o charakterze przestępczym. Informacji nie należy wykorzystywać do dodatkowych celów, np. do ścigania przez organy podatkowe lub imigracyjne niepowiązanych spraw.

37. Wytyczne/decyzja wykonawcza powinny/a dalej określać, kto ma dostęp do danych uzyskanych (i przechowywanych) przez krajowe punkty kontaktowe. Dostęp/ujawnianie powinien/powinno być ściśle zgodne z zasadą ograniczonego dostępu. Należy rozważyć publikację wykazu ewentualnych odbiorców.

Prawa dostępu dla osób, których dane dotyczą

38. Wytyczne/decyzja wykonawcza powinny/a zapewniać prawa dostępu dla osób, których dane dotyczą, w tym w stosownych przypadkach – poprawienie lub usuwanie danych (zobacz art. 12–14 dyrektywy 95/46/WE). Istnienie tego prawa – lub ewentualnych wyjątków zgodnie z art. 13 – może mieć poważne skutki. Na przykład, zgodnie z ogólnymi przepisami osoba, której dane dotyczą, ma również prawo wiedzieć, czy jej transakcja została zgłoszona jako podejrzana. (Ewentualne) wykonanie tego prawa mogłoby jednak zniechęcić sprzedawcę prekursorów materiałów wybuchowych do zgłaszania podejrzanych transakcji nabywcy. Stąd wyjątki należy wyraźnie uzasadnić i szczegółowo określić, najlepiej w rozporządzeniu, lub ewentualnie w wytycznych/decyzji wykonawczej. Należy przewidzieć również mechanizm odwoławczy, z zaangażowaniem krajowych punktów kontaktowych.

5. **Dodatkowe uwagi**

Okresowy przegląd skuteczności

39. EIDO z zadowoleniem przyjął fakt, że art. 16 wniosku ustanawia przegląd rozporządzenia [po pięciu latach od daty przyjęcia]. EIOD jest bowiem zdania, iż w odniesieniu do wszystkich nowych instrumentów powinno się wykazać w okresowych przeglądach, że nadal stanowią skuteczne środki zwalczania terroryzmu (i innej działalności przestępczej). EIOD zaleca, by rozporządzenie wyraźnie stanowiło, że w trakcie takiego przeglądu uwzględniono również skuteczność rozporządzenia, jak i jego wpływ na prawa podstawowe, w tym ochronę danych.

III. **WNIOSKI**

40. EIOD zaleca dodanie do wniosku nowych, bardziej szczegółowych informacji w celu odpowiedniego potraktowania kwestii ochrony danych. Ponadto wytyczne Komisji na temat podejrzanych transakcji i szczegółowych aspektów technicznych koncesji – i ewentualna decyzja wykonawcza w sprawie ochrony danych – powinny również zawierać więcej szczegółowych przepisów dotyczących przetwarzania danych i ochrony danych. Wytyczne (i ewentualnie decyzja wykonawcza) powinny zostać przyjęte po konsultacji z EIOD i – w stosownym przypadku – z grupą roboczą art. 29 z przedstawicielami organów ochrony danych w państwach członkowskich.

41. Art. 5 rozporządzenia powinien określać maksymalny okres zatrzymywania danych (*prima facie* nieprzekraczający dwóch lat) dla odnotowanych w ewidencji transakcji oraz kategorie danych osobowych, które należy odnotować w ewidencji (niewykraczające poza nazwisko, numer koncesji i zakupione artykuły). Należy wyraźnie zakazać przetwarzania szczególnych kategorii danych.

42. W art. 6 wniosku należy wyraźnie określić rolę i charakter krajowych punktów kontaktowych. Przepis ten powinien również określać maksymalny okres zatrzymywania danych dla danych zgłoszonych do podejrzanych transakcji (*prima facie* nieprzekraczający dwóch lat) oraz dane osobowe, które należy odnotować w ewidencji (niewykraczające poza nazwisko, numeru koncesji, nabywane artykuły i powody powstania podejrzenia). Należy wyraźnie zakazać przetwarzania szczególnych kategorii danych.

43. Ponadto wytyczne/decyzja wykonawcza powinny/a określać dane, które organy udzielające koncesji mogą gromadzić w związku z wnioskiem o koncesję. Powinny one także wyraźnie wydzielać cele, dla których dane można wykorzystać. Podobne przepisy powinny również mieć zastosowanie do ewidencji podejrzanych transakcji. Wytyczne/decyzja wykonawcza powinny/a precyzować, że organ udzielający koncesji powinien poinformować posiadaczy koncesji o tym, że ich transakcje będę przedmiotem ewidencji i mogą być przedmiotem zgłoszenia, jeśli okażą się „podejrzane". Wytyczne/decyzja wykonawcza powinny/a dalej określać, kto ma dostęp do danych uzyskanych (i przechowywanych) przez krajowe punkty kontaktowe. Dostęp/ujawnianie powinien/powinno być ściśle zgodne z zasadą ograniczonego dostępu. Wytyczne powinny również zapewniać odpowiednie prawa dostępu osobom, których dane dotyczą, i wyraźnie określać i uzasadniać wyjątki.

44. Skuteczność przewidzianych środków powinna podlegać okresowemu przeglądowi przy jednoczesnym uwzględnieniu ich wpływu na prywatność.

Sporządzono w Brukseli dnia 15 grudnia 2010 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych