I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego decyzji Rady w sprawie stanowiska Unii w ramach Wspólnego Komitetu UE-Stany Zjednoczone dotyczącego wzajemnego uznawania programu upoważnionego przedsiębiorcy Unii Europejskiej i Partnerstwa celno-handlowego Stanów Zjednoczonych przeciwko terroryzmowi

(2012/C 160/01)

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, w szczególności jego art. 41 ([2]),

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. WPROWADZENIE

I.1. Konsultacje z EIOD i cel niniejszej opinii

1. W dniu 5 stycznia 2011 r. Komisja przyjęła wniosek dotyczący decyzji Rady w sprawie stanowiska Unii w ramach Wspólnego Komitetu UE-Stany Zjednoczone dotyczącego wzajemnego uznawania programu upoważnionego przedsiębiorcy Unii Europejskiej i Partnerstwa celno-handlowego Stanów Zjednoczonych przeciwko terroryzmowi ([3]) (zwany dalej „wnioskiem"). Tego samego dnia wniosek przekazano do EIOD do konsultacji.

2. Wcześniej odbyły się nieformalne konsultacje z EIOD i przesłał on Komisji szereg nieformalnych uwag. Celem obecnej opinii jest uzupełnienie tych uwag w świetle obecnego wniosku oraz publiczne udostępnienie poglądów EIOD.

3. EIOD uznaje, że przetwarzanie danych osobowych nie stanowi głównego przedmiotu wniosku. Większość przetwarzanych informacji nie będzie zawierać danych osobowych zdefiniowanych w prawie o ochronie danych ([4]). W stosownych przypadkach prawo o ochronie danych należy jednak przestrzegać również w tych okolicznościach, co zostanie wyjaśnione poniżej.

([1]) Dz.U. L 281 z 23.11.1995, s. 31.
([2]) Dz.U. L 8 z 12.1.2001, s. 1.
([3]) COM(2011) 937 wersja ostateczna.
([4]) Jak określono w pkt 8–9 niniejszej opinii.

I.2. **Kontekst wniosku**

4. Celem wniosku jest ustanowienie wzajemnego uznawania programów partnerstwa handlowego UE i Stanów Zjednoczonych – a mianowicie programu upoważniony przedsiębiorca (AEO) UE i Partnerstwa celno-handlowego Stanów Zjednoczonych przeciwko terroryzmowi (C-TPAT) – aby ułatwić wymianę handlową między przedsiębiorcami, którzy zainwestowali w bezpieczeństwo łańcucha dostaw oraz są uczestnikami jednego z tych programów.

5. Stosunki między Unią Europejską a Stanami Zjednoczonymi w dziedzinie ceł reguluje Umowa o współpracy i wzajemnej pomocy w sprawach celnych ([1]). W ramach tej umowy utworzono Wspólny Komitet Współpracy Celnej, w którego skład wchodzą przedstawiciele organów celnych UE i Stanów Zjednoczonych. Wzajemne uznawanie zostanie wprowadzone decyzją tego komitetu. Treść wniosku składa się zatem z:

— uzasadnienia,

— wniosku dotyczącego decyzji Rady, w którym stwierdza się, że UE zajmie na forum Wspólnego Komitetu Współpracy Celnej stanowisko określone w projekcie decyzji w sprawie wzajemnego uznawania,

— projektu decyzji Wspólnego Komitetu Współpracy Celnej ustawiającej wzajemne uznawanie AEO EU i C-TPAT Stanów Zjednoczonych (zwanego dalej „projektem decyzji") ([2]).

6. Projekt decyzji zostanie wdrożony przez organy celne, które określiły proces wspólnego zatwierdzania (procedura ubiegania się przez przedsiębiorców o przyznanie statusu uczestnika programu, ocena wniosków, przyznawanie statusu uczestnika programu oraz monitorowanie tego statusu).

7. Dobre funkcjonowanie wzajemnego uznawania opiera się zatem na wymianie informacji między organami celnymi UE i Stanów Zjednoczonych dotyczących przedsiębiorców handlowych będących już członkami programu partnerstwa.

II. **ANALIZA PROJEKTU DECYZJI**

II.1. **Przetwarzanie danych dotyczących osób fizycznych**

8. Chociaż celem projektu decyzji nie jest przetwarzanie danych osobowych, niektóre z wymienianych informacji będą dotyczyć osób fizycznych, szczególnie jeżeli przedsiębiorca jest osobą fizyczną ([3]) lub jeżeli nazwa oficjalna osoby prawnej prowadzącej działalność jako przedsiębiorca identyfikuje osobę fizyczną ([4]).

9. Znaczenie ochrony danych w tym kontekście podkreślił Trybunał Sprawiedliwości w swoim orzeczeniu w sprawie Schecke. Zdaniem Trybunału osoby prawne mogą się powoływać na ochronę praw do prywatności i na ochronę danych, uznanych w Karcie praw podstawowych Unii Europejskie, jeżeli nazwa oficjalna osoby prawnej identyfikuje co najmniej jedną osobę fizyczną ([5]). W niniejszej opinii zostanie zatem dokonana analiza sposobu, w jaki w projekcie decyzji reguluje się wymianę danych osobowych dotyczących przedsiębiorców.

([1]) Umowa między Wspólnotą Europejską a Stanami Zjednoczonymi Ameryki o współpracy i wzajemnej pomocy w sprawach celnych (Dz.U. L 222 z 12.8.1997, s. 17), dostępna pod adresem http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=308 (streszczenie i pełny tekst).

([2]) Wniosek dotyczący decyzji w sprawie wniosku dotyczącego decyzji Rady w sprawie stanowiska Unii w ramach Wspólnego Komitetu UE-Stany Zjednoczone dotyczącego wzajemnego uznawania programu upoważnionego przedsiębiorcy Unii Europejskiej i Partnerstwa celno-handlowego Stanów Zjednoczonych przeciwko terroryzmowi.

([3]) Dane osobowe są zdefiniowane w art. 2 lit. a) dyrektywy 95/46/WE i w art. 2 lit. a) rozporządzenia (WE) nr 45/2001 jako „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej".

([4]) Zob. również Opinia EIOD w sprawie wniosku dotyczącego decyzji Rady w sprawie stanowiska Unii w ramach Wspólnego Komitetu Współpracy Celnej UE-Japonia dotyczącego wzajemnego uznawania programów upoważnionego przedsiębiorcy w Unii Europejskiej i w Japonii, dostępna pod adresem http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:190:0002:0006:PL:PDF

([5]) Trybunał Sprawiedliwości, z dnia 9 listopada 2010 r., Volker und Markus Schecke, C-92/09 i C-93/09, pkt 53 (dostępny pod adresem http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?where=&lang=en&num=79898890C19090092&doc=T&ouvert=T&seance=ARRET).

II.2. **Stosowanie ram ochrony danych UE**

10. Przetwarzania danych dokonują organy celne, o których mowa w art. 1 lit. b) Umowy o współpracy i wzajemnej pomocy w sprawach celnych ([1]). Definicja ta dotyczy, w UE, „właściwych służb" Komisji Europejskiej oraz organów celnych państw członkowskich UE. Zgodnie z przepisami UE dotyczącymi ochrony danych przetwarzanie przez państwa członkowskie UE podlega dyrektywie 95/46/WE (zwanej dalej „dyrektywą o ochronie danych") oraz przepisom krajowym dotyczącym ochrony danych wykonującym przepisy dyrektywy o ochronie danych, natomiast przetwarzanie danych osobowych przez instytucje i organy UE podlega rozporządzeniu (WE) nr 45/2001 (zwanemu dalej „rozporządzeniem"). W tym przypadku zastosowanie ma zatem zarówno dyrektywa o ochronie danych, jak i rozporządzenie.

II.3. **Stopień ochrony**

11. Informacje mają być wymieniane w formie elektronicznej i zgodnie z Umową o współpracy i wzajemnej pomocy w sprawach celnych. Artykuł 17 ust. 2 Umowy o współpracy i wzajemnej pomocy w sprawach celnych stanowi, że strony umowy mogą przekazywać między sobą dane osobowe, jeżeli strona, która otrzyma te dane, gwarantuje ochronę w stopniu co najmniej odpowiadającym stopniowi ochrony, jaki do tego szczególnego przypadku stosuje państwo, które dostarcza te dane.

12. EIOD z zadowoleniem przyjmuje to postanowienie, które należy rozumieć jako ukierunkowane na przestrzeganie prawa o ochronie danych UE. Zgodnie z art. 25 dyrektywy o ochronie danych i art. 9 rozporządzenia obowiązuje główna zasada, zgodnie z którą dane można przekazywać z UE do państwa trzeciego tylko, jeżeli państwo otrzymujące informacje zapewnia „odpowiedni" stopień ochrony ([2]). Artykuł 17 ust. 2 Umowy o współpracy i wzajemnej pomocy w sprawach celnych wydaje się zatem bardziej restrykcyjny od dyrektywy o ochronie danych.

13. Należy zatem zbadać na podstawie wszystkich istotnych okoliczności, czy otrzymujące informacje organy Stanów Zjednoczonych faktycznie gwarantują odpowiadający stopień ochrony (lub przynajmniej „odpowiedni" stopień). Analizę prawidłowości stopnia ochrony należy przeprowadzić w świetle wszystkich okoliczności towarzyszących przekazaniu lub przekazywaniu ([3]).

14. Komisja Europejska nie ustaliła, że Stany Zjednoczone jako całość zapewniają odpowiedni stopień ochrony. W świetle braku decyzji o ogólnej prawidłowości poziomu ochrony administratorzy danych ([4]), pod nadzorem organów ochrony danych ([5]), mogą uznać, że w konkretnym przypadku zapewniono odpowiedni stopień ochrony. Państwa członkowskie UE (lub EIOD, jeżeli przekazywania dokonują instytucje lub organy UE) mogą również zezwolić na konkretne przekazanie lub przekazywanie danych osobowych do państwa trzeciego, jeżeli administrator danych zaleci odpowiednie gwarancje ([6]).

15. W tym przypadku te decyzje *ad hoc* o prawidłowości poziomu ochrony można by stosować, gdyby krajowe organy celne i służby Komisji Europejskiej odpowiedzialne za sprawy celne przedstawiły wystarczające dowody potwierdzające twierdzenie o przyjęciu odpowiednich gwarancji przez organy celne Stanów Zjednoczonych w odniesieniu do przekazywanie przewidzianego w projekcie decyzji ([7]).

16. EIOD nie posiada jednak wystarczających dowodów, że organy celne Stanów Zjednoczonych zapewniają ochronę danych w stopniu „odpowiednim" lub „co najmniej odpowiadającym stopniowi ochrony, jaki do tego szczególnego przypadku stosuje państwo, które dostarcza te dane" zgodnie z wymogami art. 17 ust. 2 Umowy o współpracy i wzajemnej pomocy w sprawach celnych.

([1]) Zob. sekcja I ust. 2 projektu decyzji.
([2]) Rozporządzenie stanowi również, że przekazywanie może mieć miejsce tylko, jeżeli dane przekazuje się „jedynie w celu spełnienia zadań należących do administratora danych".
([3]) Zob. art. 9 ust. 1 i art. 9 ust. 2 rozporządzenia, art. 25 ust. 1 i art. 25 ust. 2 dyrektywy o ochronie danych i wykonujące je przepisy krajowe dotyczące ochrony danych. Zob. również wyżej wspomnianą opinię EIOD w sprawie Współpracy Celnej UE-Japonia.
([4]) W tym przypadku organy celne UE i jej państw członkowskich.
([5]) W niektórych państwach członkowskich wyłącznie organy ochrony danych mogą wydać zezwolenie na przekazanie danych.
([6]) Artykuł 26 ust. 2 dyrektywy o ochronie danych i art. 9 ust. 7 rozporządzenia.
([7]) Zob. pismo EIOD w sprawie dokumentu „Transfers of personal data to third countries: »adequacy« of signatories to Council of Europe Convention 108 (Case 2009-0333)" dostępne na stronie internetowej http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Adminmeasures/2009/09-07-02_OLAF_transfer_third_countries_EN.pdf

17. EIOD wzywa zatem do dopilnowania, aby dowody wykazujące, że organy celne Stanów Zjednoczonych zapewniają ochronę danych w stopniu „odpowiednim" lub „co najmniej odpowiadającym stopniowi ochrony, jaki do tego szczególnego przypadku stosuje państwo, które dostarcza te dane" zgodnie z wymogami art. 17 ust. 2 Umowy o współpracy i wzajemnej pomocy w sprawach celnych, były dostępne dla EIOD i dla krajowych organów ochrony danych. Powinno to stanowić wymów zawarty w przepisie projektu decyzji.

18. Ponadto można również zezwolić na przekazywanie danych osobowych z UE do państw, które nie gwarantują „odpowiedniego" stopnia ochrony, jeżeli ma zastosowanie któryś z wyjątków zawartych w art. 26 ust. 1 dyrektywy o ochronie danych lub w art. 9 ust. 6 rozporządzenia. W tym konkretnym przypadku można by argumentować, że przekazanie danych jest „konieczne lub wymagane przez prawo z ważnych względów publicznych" ([1]). Wyjątki te muszą być jednak interpretowane w sposób ścisły i nie mogą stanowić podstawy dla masowego lub systematycznego przekazywania danych osobowych ([2]). W opinii EIOD wyjątki te nie są przydatne w omawianej sprawie.

II.4. **Zasada celowości**

19. Sekcja V ust. 1 projektu decyzji stanowi, że organy celne otrzymujące dane podlegające wymianie mogą je przetwarzać do celów wykonywania projektu decyzji zgodnie z art. 17 Umowy o współpracy i wzajemnej pomocy w sprawach celnych.

20. W sekcji V ust. 3 tiret czwarte i w art. 17 ust. 3 Umowy o współpracy i wzajemnej pomocy w sprawach celnych przewidziano jednak również przetwarzanie danych do innych celów. Biorąc pod uwagę fakt, że cele projektu decyzji wykraczają poza współpracę celną i obejmują walkę z terroryzmem, EIOD zaleca określenie w tekście decyzji wszystkich ewentualnych celów przekazywania danych osobowych. Ponadto wszystkie przekazywane dane powinny być konieczne i proporcjonalne do osiągnięcia tych celów. Należy również stwierdzić, że osobom, których dane dotyczą, należy przekazywać kompleksowe informacje na temat wszystkich celów i warunków przetwarzania ich danych osobowych.

II.5. **Kategorie danych, które mają podlegać wymianie**

21. Dane, które mają podlegać wymianie między organami celnymi, dotyczące uczestników programów partnerstwa handlowego obejmują: nazwę; adres; status uczestnictwa; datę zatwierdzenia lub pozwolenia; zawieszenia i cofnięcia; niepowtarzalny numer pozwolenia lub niepowtarzalny numer identyfikacyjny; oraz „szczegóły, które mogą zostać wspólnie określone przez organy celne, objęte – w stosownych przypadkach – wszelkimi koniecznymi gwarancjami" ([3]). Ponieważ ostatnia pozycja ma zbyt otwarty charakter, EIOD zaleca określenie kategorii danych, które może ona obejmować.

22. EIOD zauważa również, że wymieniane dane mogą również obejmować dane dotyczące przestępstw lub podejrzeń o popełnienie przestępstwa, na przykład dane związane z zawieszeniem i cofnięciem uczestnictwa. EIOD podkreśla, że w prawie o ochronie danych UE ogranicza się przetwarzanie danych dotyczących przestępstw, wyroków skazujących i środków bezpieczeństwa ([4]). Przetwarzanie tych kategorii danych może podlegać kontroli wstępnej dokonywanej przez EIOD i krajowe organy ochrony danych UE ([5]).

II.6. **Dalsze przekazywanie**

23. W sekcji V ust. 3 tiret trzecie zezwala się na przekazywanie danych państwom trzecim lub organizacjom międzynarodowym, jeżeli organ dostarczający informacji wyraził wcześniejszą zgodę i na warunkach określonych przez ten organ. Dalsze przekazywanie danych nie powinno być dozwolone bez przedstawienia uzasadnienia.

([1]) Zob. art. 9 ust. 6 lit. d) rozporządzenia lub art. 26 ust. 1 lit. d) dyrektywy o ochronie danych, które zgodnie z motywem 58 dyrektywy o ochronie danych obejmują przekazywanie danych między organami podatkowymi lub celnymi.

([2]) Zob. art. 29 dokumentu grupy roboczej z dnia 25 listopada 2005 r. w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z 24 października 1995 r. (WP114), s. 7–9, dostępny na stronie internetowej http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_pl.pdf

([3]) Zob. sekcja IV ust. 3 lit. a)–g) projektu decyzji.

([4]) Zob. art. 8 ust. 5 dyrektywy 95/46/WE i art. 10 ust. 5 rozporządzenia (WE) nr 45/2001.

([5]) Zob. art. 27 lit. a) rozporządzenia (WE) nr 45/2001 i przepisy krajowe dotyczące ochrony danych UE wykonujące art. 20 dyrektywy 95/46/WE.

24. W związku z tym wydaje się, że w sekcji V ust. 3 należy zawrzeć przepis podobny to przepisu zawartego w art. 17 ust. 2 Umowy o współpracy i wzajemnej pomocy w sprawach celnych stanowiący, że dane osobowe można przekazywać państwu trzeciemu tylko, jeżeli państwo otrzymujące te dane gwarantuje ochronę w stopniu co najmniej odpowiadającym stopniowi wymaganemu w projekcie decyzji. W przeciwnym razie możliwe byłoby obejście ochrony danych osobowych przyznanej na mocy tego projektu decyzji poprzez dalsze przekazywanie danych.

25. W każdym przypadku w przepisie tym należy określić cele takiego przekazywania i konkretne sytuacje, w których jest ono dozwolone. Należy również wyraźnie stwierdzić, że należy ocenić niezbędność i proporcjonalność międzynarodowego dalszego przekazywania w poszczególnych przypadkach i że nie zezwala się na masowe lub systematyczne przekazywanie. W tekście należy również zawrzeć obowiązek informowania osób, których dane dotyczą, o możliwości międzynarodowego dalszego przekazywania.

II.7. **Zatrzymywanie danych**

26. EIOD z zadowoleniem przyjmuje sekcję V ust. 2, w której zabrania się przetwarzania lub przetrzymywania informacji dłużej niż jest to konieczne do celów, dla których są one przekazane. Należy jednak również określić maksymalny okres zatrzymywania.

II.8. **Bezpieczeństwo i odpowiedzialność**

27. Sekcja IV stanowi, że informacje będą wymieniane w formie elektronicznej. Według EIOD należy zapewnić więcej szczegółów dotyczących systemu wymiany informacji, który ma zostać utworzony. W każdym razie w ramach wybranego systemu należy zintegrować ochronę prywatności i ochronę danych już na etapie opracowywania (wbudowana ochrona prywatności).

28. W tym względzie EIOD z zadowoleniem przyjmuje gwarancje w zakresie bezpieczeństwa przewidziane w sekcji V ust. 3 tiret pierwszy i drugi, które obejmują kontrole dostępu, ochronę przed „nieautoryzowanym dostępem, rozpowszechnianiem i dokonywaniem zmian, usunięciem lub zniszczeniem" oraz kontrolowanie, aby dane wykorzystywano wyłącznie do celów projektu decyzji. Z zadowoleniem przyjmuje on również rejestry dostępu przewidziane w sekcji V ust. 3 tiret 5.

29. EIOD zaleca również zawarcie w tych przepisach obowiązku przeprowadzania oceny skutków w zakresie ochrony danych (w tym oceny ryzyka) przed rozpoczęciem wymiany danych. Ocena powinna obejmować ocenę ryzyka i środki przewidywane w celu zapobiegania ryzykom ([1]). W tekście należy również stwierdzić, że należy okresowo przeprowadzać kontrole i sporządzać sprawozdania dotyczące zgodności z tymi środkami i ich wykonania. Jest to jeszcze bardziej istotne w świetle możliwości, że zostaną przetworzone dane szczególnie chronione.

II.9. **Jakość danych i prawa osób, których dane dotyczą**

30. EIOD z zadowoleniem przyjmuje obowiązek organów celnych polegający na dopilnowaniu, aby informacje, które podlegają wymianie, były dokładne i okresowo aktualizowane (zob. sekcja V ust. 2 i 5). Z zadowoleniem przyjmuje on również sekcję V ust. 4, w którym gwarantuje się przedsiębiorcom będącym członkami programów partnerstwa prawo dostępu do ich danych osobowych i ich poprawiania.

31. EIOD zauważa jednak, że egzekwowanie tych praw podlega przepisom krajowym organu celnego. Jeżeli chodzi o dane dostarczane przez organy celne UE oraz w celu zagwarantowania „odpowiedniego" stopnia ochrony (zob. sekcja II.3 niniejszej opinii) prawa te należy ograniczyć tylko, jeżeli takie ograniczenie jest konieczne do ochrony ważnych interesów gospodarczych lub finansowych.

32. EIOD z zadowoleniem przyjmuje również fakt, że organy celne muszą usuwać uzyskane dane, jeżeli ich gromadzenie lub dalsze przetwarzanie narusza projekt decyzji lub Umowę o współpracy celnej i wzajemnej pomocy w sprawach celnych ([2]). EIOD pragnie przypomnieć, że zgodnie z art. 17 ust. 2 Umowy o współpracy celnej i wzajemnej pomocy w sprawach celnych przepis ten miałby zastosowanie do każdego przypadku przetwarzania, w ramach którego nie przestrzega się prawa o ochronie danych UE.

([1]) Przewidziane już w art. 33 nowego wniosku dotyczącego rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012) 11/4 projekt).

([2]) Zob. sekcja V ust. 5 projektu decyzji.

33. EIOD z zadowoleniem przyjmuje obowiązek organów celnych do udzielania informacji członkom programu o ich możliwościach odwołania ([1]). Należy jednak wyjaśnić, jakie możliwości odwołania przysługują w przypadku naruszenia gwarancji ochrony danych zapewnionych w projekcie decyzji. W przepisie tym należy również stwierdzić, że inne osoby, których dane dotyczą (czyli przedsiębiorcy, którzy ubiegają się o członkostwo), również należy informować o możliwościach odwołania.

II.10. **Nadzór**

34. EIOD z zadowoleniem przyjmuje sekcję V ust. 6, zgodnie z którą cała sekcja V podlega „niezależnemu nadzorowi i przeglądowi" prowadzonemu przez Głównego Urzędnika ds. Prywatności w Departamencie Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (US Department of Homeland Security's Chief Privacy Officer) i krajowe organy ochrony danych.

35. Należy również stwierdzić, że zadaniem EIOD i krajowych organów ochrony danych, powinno być dopilnowanie, aby stopień ochrony danych osobowych zapewniony przez organy celne otrzymujące te dane był „odpowiedni" (zob. sekcja III.1.). Sekcja IV również powinna podlegać nadzorowi i przeglądowi.

III. **WNIOSKI**

36. EIOD z zadowoleniem przyjmuje gwarancje przewidziane w projekcie decyzji, szczególnie w odniesieniu do bezpieczeństwa danych. EIOD i krajowe organy ochrony danych powinny mieć jednak dostęp do dowodów wykazujących, że organy celne Stanów Zjednoczonych zapewniają ochronę danych w stopniu „odpowiednim" lub „co najmniej odpowiadającym stopniowi ochrony, jaki do tego szczególnego przypadku stosuje państwo, które dostarcza te dane" zgodnie z wymogami art. 17 ust. 2 Umowy o współpracy i wzajemnej pomocy w sprawach celnych. Powinno to stanowić wymów zawarty w przepisie projektu decyzji.

37. Ponadto EIOD zaleca, aby:

— określono cele wymiany danych przewidzianej w projekcie decyzji, która powinna być niezbędna i proporcjonalna,

— określono kategorie danych objętych sekcją IV ust. 3 lit. g),

— stwierdzono, że, jeżeli konieczność dalszego międzynarodowego przekazywania danych jest uzasadniona, można zezwolić na takie przekazywanie tylko w poszczególnych przypadkach, do odpowiednich celów i jeżeli państwo otrzymujące dane gwarantuje ochronę w stopniu co najmniej odpowiadającym stopniowi zapewnionemu w projekcie decyzji,

— zawarto obowiązek poinformowania o powyższym wszystkich osób, których dane dotyczą,

— uzupełniono przepisy dotyczące bezpieczeństwa,

— określono maksymalne okresy zatrzymywania danych,

— nie ograniczano praw osób z UE, których dane dotyczą, chyba że takie ograniczenie jest niezbędne do ochrony ważnych interesów gospodarczych lub finansowych,

— zagwarantowano prawo do odniesienia,

— poddano sekcję IV nadzorowi i przeglądowi,

— określono, że zadaniem EIOD, krajowych organów ochrony danych UE i Głównego Urzędnika ds. Prywatności w Departamencie Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych powinno być dopilnowanie, aby gwarancje stosowane przez organy celne otrzymujące dane w celu zapewnienia odpowiedniego stopnia ochrony danych osobowych były skuteczne i zgodne z wymogami UE.

([1]) Zob. sekcja V ust. 4 ostatnie zdanie.

38. EIOD zauważa również, że wniosek może oznaczać przetwarzanie danych osobowych związanych z przestępstwami lub podejrzeniami o popełnienie przestępstwa. W prawie UE dane te podlegają bardziej rygorystycznym gwarancjom i mogą podlegać kontroli wstępnej dokonywanej przez EIOD i przez krajowe organy ochrony danych UE.

Sporządzono w Brukseli dnia 9 lutego 2012 r.

Giovanni BUTTARELLI

Zastępca Europejskiego Inspektora Ochrony Danych