EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych 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

(2010/C 190/02)

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. 8,

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

uwzględniając rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych ([2]), w szczególności jego art. 41,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ

I. **WPROWADZENIE**

1. W dniu 19 lutego 2010 r. Komisja przyjęła wniosek dotyczący 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 ([3]).

2. Nie przeprowadzono konsultacji z EIOD, czego wymaga art. 28 ust. 2 rozporządzenia (WE) nr 45/2001. Podstawą niniejszej opinii jest zatem art. 41 ust. 2 tego rozporządzenia. EIOD zaleca, aby w preambule decyzji zawrzeć odniesienie do niniejszej opinii.

3. EIOD stwierdził pewne niedociągnięcia i brak jasności w kwestii ochrony danych osobowych. Po opisie kontekstu i podstawy wniosku w rozdziale III komentarze zostaną przedstawione w rozdziale IV.

II. **KONSULTACJE Z EIOD**

4. EIOD wydał dokument strategiczny, w którym została opisana jego rola konsultacyjna: EIOD jako doradca instytucji wspólnotowych w sprawie wniosków dotyczących przepisów i powiązanych dokumentów ([4]). Podstawą roli konsultacyjnej jest art. 28 ust. 2 i art. 41 rozporządzenia (WE) nr 45/2001. Ponadto motyw 17 rozporządzenia stanowi, że „[s]kuteczność ochrony osoby fizycznej w odniesieniu do przetwarzania danych osobowych w Unii zakłada spójność odpowiednich przepisów i procedur mających zastosowanie do czynności wchodzących w zakres różnych kontekstów prawnych". Spójność należy postrzegać jako niezbędny element osiągnięcia wysokiego poziomu ochrony danych na szczeblu europejskim, co obejmuje również działanie Unii na zewnątrz.

5. Komisja uznała taki szeroki zakres odpowiedzialności EIOD, a zgodnie z obowiązującą praktyką Komisja przeprowadza konsultacje z EIOD w przypadku wszystkich odpowiednich wniosków dotyczących zarówno instrumentów legislacyjnych, jak i nielegislacyjnych. Zakres działalności doradczej EIOD dotyczy „(wszystkich kwestii) związanych z przetwarzaniem danych osobowych". Oznacza to, że wszystkie akty, które zawierają przepisy o przetwarzaniu danych osobowych lub zawierają przepisy wywołujące skutek (lub potencjalny skutek) w odniesieniu do przetwarzania danych powinny być przedmiotem konsultacji. To samo dotyczy wszystkich instrumentów podlegających zewnętrznym kompetencjom Unii.

([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) 55 wersja ostateczna.
([4]) Dokument strategiczny jest dostępny na stronie internetowej: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/05-03-18_PP_EDPSadvisor_EN.pdf

6. W dokumencie strategicznym został również określony czas na konsultacje. Konsultacje na wczesnym etapie procesu legislacyjnego umożliwiają EIOD skuteczne działanie i proponowanie zmian w tekście. Właściwe służby Komisji przesyłają EIOD projekt tekstu do nieformalnej konsultacji, w stosownym przypadku – przed przyjęciem formalnego wniosku. Po przyjęciu wniosku kolejnym etapem jest formalna konsultacja. Na tym etapie opinia EIOD jest publikowana w Dzienniku Urzędowym (seria C).

7. W przypadku niniejszego wniosku, jak wspomniano powyżej, EIOD nie otrzymał do konsultacji ani projektu wniosku, ani samego wniosku po jego przyjęciu. EIOD wyraża rozczarowanie takim biegiem wypadków, ponieważ, jak wyjaśni poniżej, jego wkład byłby doskonałą okazją do podniesienia wartości wniosku.

III. KONTEKST I PODSTAWA WNIOSKU

8. Celem wniosku jest wzajemne uznanie programów upoważnionego przedsiębiorcy w Unii i Japonii za kompatybilne i równoważne, zaś odpowiednich przyznanych statusów AEO za wzajemnie zaakceptowane.

9. Stosunki między UE a Japonią w obszarze ceł opierają się na Umowie o współpracy i wzajemnej pomocy administracyjnej w sprawach celnych (CCMAAA) ([1]), która weszła w życie w dniu 1 lutego 2008 r. Zgodnie z CCMAAA współpraca celna obejmuje wszystkie dziedziny związane ze stosowaniem przepisów celnych. CCMAAA zawiera wezwanie skierowane do Unii i Japonii o podjęcie starań w zakresie współpracy w celu wprowadzania dalszych ułatwień w handlu w dziedzinie ceł zgodnie ze standardami międzynarodowymi ([2]). Wzajemne uznawanie programów upoważnionego przedsiębiorcy i środków bezpieczeństwa przyczynia się jednocześnie do poprawy bezpieczeństwa całego łańcucha dostaw, jak i do ułatwienia wymiany handlowej.

10. Wniosek stanowi również, że oprócz innych kwestii, organy celne utrzymują zgodność między systemami, a każdy organ celny przyznaje porównywalne korzyści przedsiębiorcom korzystającym ze statusu AEO. Znajduje się w nim również zapis, że organy celne muszą usprawniać komunikację, a także wymianę informacji. Wniosek zawiera wykaz szczegółowych informacji na temat AEO, które podlegają wymianie.

IV. ANALIZA WNIOSKU

IV.1. Zastosowanie przepisów o ochronie danych osobowych

11. Artykuł IV załącznika do wniosku dotyczy wymiany informacji i komunikacji. Znajduje się w nim zapis, że informacje i związane z nimi dane, w szczególności dotyczące podmiotów objętych programem, wymieniane są w sposób systematyczny w formie elektronicznej. Określono podlegające wymianie informacje dotyczące upoważnionych przedsiębiorców objętych programami AEO, w tym imię i nazwisko/nazwę przedsiębiorcy posiadającego status AEO, adres danego przedsiębiorcy itp.

12. System AEO został określony w art. 5a rozporządzenia (WE) nr 648/2005 Parlamentu Europejskiego i Rady ([3]). Stanowi on, że „1. (…). Upoważniony podmiot gospodarczy korzysta z ułatwień odnoszących się do kontroli celnej dotyczącej bezpieczeństwa i ochrony i/lub z uproszczeń przewidzianych w ramach przepisów celnych. (…)".

13. Przedsiębiorca został określony w art. 1 pkt 12 rozporządzenia Komisji (WE) nr 1875/2006 ([4]) jako „osob[a], która w ramach prowadzonej działalności gospodarczej jest włączona w czynności określone przepisami prawa celnego". Przedsiębiorca może być zatem osobą fizyczną lub prawną. Zgodnie z ust. 9 pojęcie przedsiębiorcy obejmuje AEO. Zatem informacje o niektórych AEO mogą być uważane za „dane osobowe" zgodnie z definicją w art. 2 ust. a) rozporządzenia (WE) nr 45/2001 i dyrektywie 95/46/WE, a przynajmniej informacje dotyczące tych AEO, które są osobami fizycznymi. Nawet informacje o AEO będących osobami prawnymi mogą w niektórych przypadkach być uznawane za dane osobowe. W takich przypadkach czynnikiem determinującym jest fakt, czy informacja „odnosi się do" „identyfikowalnej" osoby fizycznej ([5]). W konsekwencji nie ma wątpliwości, czy dane osobowe mogą podlegać wymianie w kontekście przedmiotowego wniosku.

14. Dane osobowe będą przetwarzane przez organy celne. Artykuł I pkt 2 załącznika do wniosku przewiduje, że „[o]rgany celne, o których mowa w art. 1 lit. c) CCMAAA (…) są odpowiedzialne za wdrożenie niniejszej decyzji". Definicja, do której artykuł się odnosi, brzmi: „»organ celny« oznacza (…) we Wspólnocie – właściwe służby Komisji Wspólnot Europejskich odpowiedzialne za sprawy celne oraz organy celne państw członkowskich Wspólnoty". Zatem zarówno rozporządzenie (WE) nr 45/2001, jak i dyrektywa 95/46/WE, będą mieć zastosowanie w niniejszym kontekście ([6]). Rozporządzenie (WE) nr 45/2001 ma zastosowanie do przetwarzania danych przez Komisję, zaś dyrektywa 95/46/WE – do przetwarzania danych przez krajowe organy celne.

([1]) Dz.U. L 62 z 6.3.2008, s. 24.
([2]) Artykuł 4 CCMAAA.
([3]) Dz.U. L 117 z 4.5.2005, s. 13.
([4]) Dz.U. L 360 z 19.12.2006, s. 64.
([5]) Zob. opinię nr 4/2007 Grupy Roboczej ds. Ochrony Danych powołanej na mocy art. 29 w sprawie pojęcia danych osobowych, WP 136, dostępnej na stronie internetowej: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_pl.pdf, w szczególności s. 23 i 24.
([6]) Artykuł 3 ust. 1 rozporządzenia (WE) nr 45/2001 i dyrektywy 95/46/WE.

IV.2. **Międzynarodowe przekazywanie danych osobowych**

15. Zarówno dyrektywa, jak i rozporządzenie przewidują analogiczne przepisy dotyczące transgranicznego przepływu danych osobowych, odpowiednio w art. 25–26 i art. 9. Zasada tam ustanowiona zakłada, że dane osobowe nie mogą być przekazywane z państwa członkowskiego do kraju trzeciego, chyba że kraj trzeci zapewni odpowiedni poziom ochrony (lub zostaną przyjęte odpowiednie zabezpieczenia albo zastosowanie będzie miał jeden z przewidzianych wyjątków).

Oświadczenie o odpowiednim poziomie ochrony we wniosku

16. Uzupełnienie zawiera punkt dotyczący ochrony danych (pkt 11). Zgodnie z pkt 11 japoński system ochrony danych jest odpowiedni w rozumieniu art. 9 rozporządzenia (WE) nr 45/2001. Artykuł 9 dotyczy systemu, który należy stosować w przypadku przekazywania danych osobowych odbiorcom innym niż instytucje i organy wspólnotowe niepodlegające dyrektywie 95/46/WE, co odnosi się do krajów trzecich, takich jak Japonia.

17. Artykuł 9 ust. 1 stanowi, że „[d]ane osobowe są przekazywane odbiorcom innym niż instytucje i organy wspólnotowe, a które nie podlegają prawu krajowemu przyjętemu zgodnie z dyrektywą 95/46/WE, jedynie wtedy, gdy w kraju odbiorcy lub w organizacji międzynarodowej, do jakiej należy odbiorca, zapewniony jest odpowiedni poziom ochrony i dane są przekazywane jedynie w celu spełnienia zadań należących do administratora danych".

18. Zgodnie z art. 9 ust. 2 ocena poziomu ochrony zapewnianej przez kraj trzeci lub organizację międzynarodową powinna zostać przeprowadzona w świetle „wszystkich okoliczności dotyczących operacji przekazania danych lub zestawu takich operacji". Ponadto artykuł zawiera kilka przykładów aspektów, które należy uwzględnić podczas oceny: „(…) szczególną uwagę należy zwrócić na charakter danych, cel i czas trwania proponowanych operacji przetwarzania, państwo trzecie będące odbiorcą lub organizację międzynarodową będącą odbiorcą, przepisy prawa, zarówno ogólnego, jak i branżowego obowiązującego w państwie trzecim lub organizacji międzynarodowej, o których mowa, oraz zasady zawodowe i środki bezpieczeństwa stosowane w tym państwie trzecim lub organizacji międzynarodowej". Wykaz nie jest wyczerpujący, można również uwzględnić inne elementy w zależności od danej sprawy.

19. Artykuł 9 rozporządzenia należy interpretować w świetle art. 25 i 26 dyrektywy 95/46/WE. Artykuł 25 ust. 6 dyrektywy stanowi, że „Komisja może stwierdzić, zgodnie z procedurą określoną w art. 31 ust. 2, że państwo trzecie zapewnia odpowiedni stopień ochrony w znaczeniu ust. 2 niniejszego artykułu, co wynika z jego prawa krajowego lub międzynarodowych zobowiązań, jakie państwo to przyjęło (…)". Należy zatem stosować procedurę wymaganą w art. 31 ust. 2 dyrektywy, czyli procedurę komitologii, w celu stwierdzenia, że kraj trzeci zapewnia odpowiedni poziom ochrony.

20. W kontekście niniejszego wniosku procedura nie została zastosowana; w konsekwencji oświadczenie w pkt 11 co do odpowiedniego poziomu ochrony japońskiego systemu stanowi naruszenie art. 25 ust. 6 dyrektywy. EIOD zdecydowanie zaleca zatem uchylenie tego oświadczenia.

21. EIOD przyznaje, że art. IV pkt 5 załącznika do wniosku stanowi, że „[o]rgany celne zapewniają ochronę danych zgodnie z Umową o współpracy i wzajemnej pomocy administracyjnej w sprawach celnych, w szczególności jej art. 16". Artykuł 16 dotyczy „Wymiany informacji i poufności", a jego ust. 2 stanowi, że „[d]ane osobowe mogą być wymieniane tylko w przypadku, gdy Umawiająca się Strona mająca je otrzymać zobowiąże się do ochrony tych danych w co najmniej równorzędnym zakresie do ochrony zapewnianej w danym przypadku przez Umawiającą się Stronę mającą przekazać informacje. Umawiająca się Strona przekazująca informacje nie zastrzega bardziej rygorystycznych warunków niż te, które mają zastosowanie w ramach jej jurysdykcji".

22. EIOD chciałby jednak podkreślić, że zgodnie z opisem powyżej, system oceny poziomu ochrony kraju trzeciego jest systemem opartym nie na „równoważności", lecz na „odpowiednim poziomie ochrony" (obecne zobowiązania międzynarodowe Unii) ([1]). W każdym razie wydaje się, że art. 16 ma charakter deklaratywny, zatem CCMAAA nie zawiera żadnego dowodu na występowanie rzeczywistej „równoważności". Ponadto nie ma w nim odniesienia do przeprowadzonej analizy „równoważności", ani nawet do „odpowiedniego poziomu ochrony". Zatem zwykłe oświadczenie w art. 16 nie może być uznane za decydujący element w ocenie odpowiedniego poziomu ochrony i nie może być podstawą do oświadczenia zamieszczonego w pkt 5.1 uzasadnienia.

Szersza perspektywa w odniesieniu do szczególnych cech sprawy

23. Należy zauważyć, że ocena poziomu ochrony w danym kraju może być przeprowadzana na różnych poziomach z różnymi skutkami prawnymi przez Komisję Europejską, organy odpowiedzialne za ochronę danych i administratorów danych. Ustalenie odpowiedniego poziomu ochrony przez Komisję Europejską na podstawie art. 25 ust. 6 dyrektywy 95/46/WE jest wiążące dla państw członkowskich. Ma to również zastosowanie do instytucji i organów Unii Europejskiej na mocy art. 9 ust. 5 rozporządzenia. Wobec braku takiej decyzji, w wielu państwach członkowskich ocenę odpowiedniego poziomu ochrony powierza się organom odpowiedzialnym za ochronę danych, w innych – administratorom danych pod

([1]) Zob. art. XIV GATS: „Pod warunkiem że środki takie nie są stosowane w sposób, który mógłby tworzyć narzędzie arbitralnej albo nieuzasadnionej dyskryminacji między krajami, gdzie panują podobne warunki, albo ukrytego ograniczenia dla handlu usługami, nic w niniejszym Układzie nie będzie interpretowane jako przeszkoda w przyjęciu i stosowaniu przez któregokolwiek Członka środków: (…) c) niezbędnych dla zapewnienia przestrzegania ustaw i przepisów, które nie są sprzeczne z postanowieniami niniejszego Układu, łącznie z odnoszącymi się do: (…) (ii) ochrony życia prywatnego osób w zakresie przetwarzania i rozpowszechniania danych osobistych oraz ochrony poufności ich osobistych akt i rachunków; (…)".

nadzorem organów odpowiedzialnych za ochronę danych. Artykuł 9 rozporządzenia opiera się na tym ostatnim modelu.

24. Oznacza to, że nawet jeżeli nie uznano, że dany kraj w całości zapewnia „odpowiednią" ochronę zgodnie z procedurą, o której mowa w art. 25 ust. 6 dyrektywy, prawny system ochrony danych mający zastosowanie do specjalnych operacji przekazywania danych lub specjalnego zestawu takich operacji może zostać uznany za „odpowiedni" przez kontrolera (w kontekście wyjaśnionym poniżej).

25. W świetle art. 9 ust. 2 rozporządzenia (a także art. 25 ust. 2 dyrektywy) administrator danych powinien ocenić wszystkie okoliczności, w jakich odbywa się operacja przekazywania danych lub zestaw takich operacji. Analizę należy przeprowadzać *in concreto*, uwzględniając szczególne cechy (gwarancje lub ryzyko) przedmiotowych operacji przekazywania danych lub zestawu takich operacji. W wyniku oceny należy określić istniejący poziom ochrony w odniesieniu do specjalnych operacji transferu lub zestawu takich operacji. Ocena powinna ograniczać się do celów uwzględnionych przez administratora danych i odbiorców w kraju przeznaczenia. W takim przypadku administrator powinien ponosić odpowiedzialność za sprawdzenie, czy warunki „odpowiedniego poziomu ochrony" są spełnione. Po przeprowadzeniu oceny przez administratora danych wynik jest objęty nadzorem organu odpowiedzialnego za ochronę danych.

26. Punkt 11 uzasadnienia stanowi, że japoński system jest zdefiniowany w japońskim prawie celnym (art. 108–2), ustawie o międzynarodowej pomocy w prowadzeniu dochodzeń i innych powiązanych z nimi kwestiach (art. 1 i 3), ustawie o państwowej służbie publicznej (art. 100), ustawie o ochronie danych osobowych znajdujących się w posiadaniu organów administracji (art. 8) i ustawie o dostępie do informacji znajdujących się w posiadaniu organów administracji (art. 5).

27. EIOD nie posiada dowodów na to, że system został oceniony w świetle dokumentu roboczego (WP12) Grupy Roboczej ds. Ochrony Danych powołanej na mocy art. 29 zatytułowanego „Przekazywanie danych osobowych krajom trzecim: stosowanie art. 25 i 26 dyrektywy w sprawie ochrony danych w UE" (ang. *Transfer of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*) oraz w sposób zgodny z zasadami w nim ustanowionymi ([1]).

28. Należy również pamiętać, że metoda oceny „odpowiedniego poziomu ochrony" oznacza, że zarówno litera, jak i praktyka prawa powinny zostać uwzględnione (obiektywne i funkcjonalne podejście). Zatem analiza samego systemu prawnego nie jest dostatecznym dowodem stosowania jego zasad w praktyce.

29. Oznacza to, że należy sprawdzić skuteczne wdrożenie i stosowanie wspomnianych zasad w praktyce przed ustaleniem, czy operacja przekazywania danych lub zestaw takich operacji jest skutecznie objęty odpowiednim poziomem ochrony; w omawianym przypadku dotyczy to wymiany informacji w kontekście programów AEO.

30. W tym kontekście administratorzy (w omawianym przypadku właściwe służby Komisji Europejskiej odpowiedzialne za sprawy celne oraz organy celne państw członkowskich Unii) muszą przeprowadzać ocenę w celu sprawdzenia, czy kraj przeznaczenia (w tym przypadku Japonia) skutecznie zapewnia odpowiedni poziom ochrony specjalnych operacji przekazywania danych ograniczonych do specjalnych celów i odbiorców w tym kraju ([2]) (to jest wymiany danych w celu wdrożenia programów AEO). Taka ocena nie została jednak przeprowadzona.

31. We wniosku można było uwzględnić takie podejście jako alternatywę dla procedury oceny „odpowiedniego poziomu" ochrony danych w Japonii zgodnie z opisem powyżej.

Inne alternatywy

32. We wniosku można było również rozważyć, czy administratorzy mogą powoływać się na inne rodzaje „odpowiednich zabezpieczeń", zgodnie z art. 9 ust. 7 rozporządzenia i art. 26 ust. 2 dyrektywy lub, czy wszelkie inne wyjątki określone w art. 9 ust. 6 rozporządzenia lub art. 26 ust. 1 dyrektywy mają zastosowanie ([3]).

IV.3. **Dodatkowe wymogi w prawie ochrony danych**

Jakość danych

33. Zasada jakości danych jest opisana w art. 4 rozporządzenia. Zgodnie z definicją w nim zawartą, oprócz innych elementów, „[d]ane osobowe muszą być: (…) c) prawidłowe, stosowne oraz nienadmierne w stosunku do celów, dla których są gromadzone i/lub przetwarzane dalej; (…)". Kategorie danych wymienione w art. IV pkt 4 wydają się być zgodne z tą zasadą.

34. Ponadto art. 4 rozporządzenia stanowi: „[d]ane osobowe muszą być: (…) e) przetrzymywane w formie, która pozwala na zidentyfikowanie podmiotów danych przez czas nie dłuższy niż jest to konieczne do celów, dla których dane były gromadzone lub dla których są przetwarzane dalej. (…)". Zatem trzeba będzie określić okres przechowywania danych osobowych podlegających przetworzeniu.

([1]) Dokument roboczy Grupy Roboczej ds. Ochrony Danych powołanej na mocy art. 29 „Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive", dostępny na stronie internetowej: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf

([2]) EIOD zawarł podobną interpretację w kontekście konsultacji na wniosek OLAF-u w sprawie dokumentu „Transfers of personal data to third countries: »adequacy« of signatories to Council of Europe Convention 108 (case 2009–0333)", dostępną na stronie internetowej: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2009/09-07-02_OLAF_transfer_third_countries_EN.pdf

([3]) Jeżeli chodzi o art. 26 ust. 1 dyrektywy, zob. dokument roboczy Grupy Roboczej ds. Ochrony Danych powołanej na mocy art. 29 w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE, WP114, dostępny na stronie internetowej: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_pl.pdf

Prawa podmiotu danych

35. Komisja będzie musiała zapewnić mechanizmy gwarantujące prawa podmiotu danych, takie jak prawo dostępu i poprawy danych (art. 13 i 14 rozporządzenia).

Obowiązek przekazania informacji

36. Artykuły 11 i 12 rozporządzenia określają informacje, które należy przekazać zainteresowanej osobie oraz czas na ich przekazanie. Komisja będzie musiała ustanowić procedurę pozwalającą ustalić, na przykład, czy informacje będą przekazywane w momencie gromadzenia danych (przez kraj trzeci) czy przez samą Komisję.

V. **WNIOSKI I ZALECENIA**

37. EIOD jest rozczarowany, że nie przeprowadzono procedury konsultacji opisanej w rozdziale II.

38. EIOD zaleca usunięcie oświadczenia o odpowiednim poziomie ochrony japońskiego systemu, które znajduje się w pkt 11 uzasadnienia, ponieważ oświadczenie to jest niezgodne z wymogami rozporządzenia (WE) nr 45/2001 i dyrektywy 95/46/WE. Ponadto zaleca rozważenie różnych możliwości oferowanych przez rozporządzenie i dyrektywę w celu zapewnienia stosowania przepisów dotyczących międzynarodowych operacji przekazywania danych.

39. EIOD rekomenduje, aby Komisja:

— określiła okres przechowywania danych osobowych podlegających przetworzeniu,

— przewidziała mechanizmy gwarantowania praw podmiotów danych,

— ustanowiła procedurę przekazywania informacji podmiotom danych.

Sporządzono w Brukseli dnia 12 marca 2010 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych