Opinia Europejskiego Inspektora Ochrony Danych na temat wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie norm jakości i bezpieczeństwa narządów ludzkich do przeszczepów

(2009/C 192/02)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

uwzględniając Traktat ustanawiający Wspólnotę Europejską, w szczególności jego art. 286,

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,

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,

uwzględniając wniosek o wydanie opinii zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 wysłany do Europejskiego Inspektora Ochrony Danych w dniu 8 grudnia 2008 r.,

PRZYJMUJE NINIEJSZĄ OPINIĘ:

I. WPROWADZENIE

Wniosek dotyczący dyrektywy w sprawie norm jakości i bezpieczeństwa narządów ludzkich do przeszczepów

1. W dniu 8 grudnia 2008 r. Komisja przyjęła wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie norm jakości i bezpieczeństwa narządów ludzkich do przeszczepów (zwany dalej „wnioskiem") [1]. Wniosek został przesłany przez Komisję Europejskiemu Inspektorowi Ochrony Danych z prośbą o konsultację, zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001.

2. Wniosek ma na celu zapewnienie wysokich norm jakości i bezpieczeństwa narządów ludzkich do przeszczepów, tak by zagwarantować wysoki poziom ochrony zdrowia ludzkiego. W szczególności wniosek:

   — określa podstawowe wymogi dotyczące jakości i bezpieczeństwa potrzebne w systemach działań związanych z transplantacją funkcjonujących w państwach członkowskich i przewiduje stworzenie lub wyznaczenie właściwego organu krajowego, który będzie odpowiedzialny za zapewnienie przestrzegania tych wymogów. W tym celu we wszystkich krajach ustanowione zostaną krajowe programy jakości w zakresie pobierania i przeszczepiania narządów ludzkich, obejmujące m.in. system *zgłaszania istotnych zdarzeń i reakcji niepożądanych*, a także *mechanizm śledzenia*, dzięki czemu możliwe będzie prześledzenie drogi narządu od dawcy do biorcy i w kierunku przeciwnym;

   — przewiduje ochronę dawców i biorców. Zwłaszcza co się tyczy żywych dawców, wniosek zawiera środki umożliwiające ocenę zdrowia dawcy i zapewnienie wyczerpujących informacji o ryzyku związanym z dawstwem, przewiduje wprowadzenie *rejestru żywych dawców*, a także zawiera środki, które mają zapewnić bezinteresowne i dobrowolne przekazywanie narządów przez żywych dawców;

   — ułatwia współpracę między państwami członkowskimi oraz *transgraniczną wymianę narządów* (także między państwami członkowskimi a państwami trzecimi) dzięki wprowadzeniu norm zbierania odpowiednich informacji dotyczących cech narządu i ustanowieniu mechanizmu przekazywania informacji.

3. Wprowadzenie w życie proponowanego mechanizmu dawstwa i przeszczepów narządów wymaga przetwarzania przez uprawnione do tego organizacje i osoby zawodowo związane ze służbą zdrowia w różnych państwach członkowskich danych osobowych odnoszących się do stanu zdrowia dawców i biorców narządów (danych zdrowotnych). Dane te uznawane są za dane sensytywne i podlegają bardziej rygorystycznym przepisom ochrony danych, określonym w art. 8 dyrektywy 95/46/WE dotyczącym szczególnych kategorii danych.

4. Mówiąc ściślej, dane dawcy są przetwarzane przez instytucje pobierające narządy, które dokonują charakterystyki dawcy i narządu, a tym samym stwierdzają, czy dany narząd nadaje się do przeszczepu (wykaz tych danych zawarty jest w załączniku do wniosku). Dane biorców (pacjentów) są przetwarzane przez ośrodki transplantacyjne, gdzie odbywa się sama operacja. Choć biorcy nie są przekazywane dane dawcy (nie ma też miejsca sytuacja odwrotna), istnieje wymóg utrzymania pełnej identyfikowalności danego narządu na drodze od dawcy do biorcy (i na odwrót), co powinno być możliwe również w przypadku transgranicznej wymiany narządów.

Konsultacja z EIOD

5. EIOD z zadowoleniem odnosi się do faktu, że zasięga się jego opinii i że wzmianka o tym znajduje się w preambule wniosku, zgodnie z art. 28 rozporządzenia (WE) nr 45/2001.

[1] COM(2008) 818 wersja ostateczna.

6. Wniosek przyspieszy procedury związane z dawstwem i przeszczepianiem narządów, a w ostatecznym rozrachunku powinien doprowadzić do większej dostępności narządów i zmniejszenia śmiertelności wśród osób znajdujących się na listach oczekujących na narządy. Stanowi on uzupełnienie obowiązujących ram prawnych odnoszących się do wykorzystywania materiałów ludzkiego pochodzenia ([1]). Można go również postrzegać jako część ogólnego podejścia przyjętego przez WE wobec ustanawiania różnego rodzaju wspólnych norm świadczenia usług zdrowotnych w państwach członkowskich; podstawowym celem takiego podejścia jest promowanie transgranicznej dostępności takich usług w całej Europie ([2]). Jak już stwierdził w swojej opinii w sprawie praw pacjenta w transgranicznej opiece zdrowotnej, EIOD popiera takie podejście. Podkreśla jednak ponownie, że istnieje potrzeba dobrze skoordynowanej i jednolitej wizji ochrony danych w ramach różnorakich inicjatyw związanych z opieką zdrowotną ([3]).

7. Wniosek porusza już kwestię potrzeby ochrony danych zarówno dawców, jak i biorców narządów. Najważniejszym elementem jest wymóg zachowania poufności w odniesieniu do tożsamości dawców i biorców (motyw 11 i 16, art. 10 i 17). W innych częściach wniosku można ponadto znaleźć szereg ogólnych odniesień do ochrony danych (motyw 17, art. 16, art. 4 ust. 3 lit. a), art. 15 ust. 3 i art. 19 ust. 1 lit. a), załącznik), a także bardziej konkretne odniesienia do potrzeby współpracy z krajowymi organami ochrony danych (art. 18 lit. f) i art. 20 ust. 2).

8. EIOD z zadowoleniem przyjmuje wspomniane odniesienia. Chciałby jednak wyrazić swoje zaniepokojenie związane z niektórymi przepisami, które nie są jasno sformułowane lub rozwinięte, a przez to dwuznaczne, co potencjalnie mogłoby zagrozić jednolitemu wdrożeniu wniosku przez państwa członkowskie.

9. Mówiąc ściślej, dalszego wyjaśnienia i doprecyzowania wymaga niekiedy wykluczające się stosowanie pojęć identyfikowalności narządów i anonimowości dawców i biorców. W związku z powyższym należy ponadto podkreślić potrzebę przyjęcia na poziomie państw członkowskich wzmożonych środków bezpieczeństwa służących ochronie danych dawców i biorców, tak by zagwarantować podwyższony poziom ochrony danych w różnych państwach europejskich, a także zapewnić ochronę danych przy transgranicznej wymianie narządów (w obrębie Europy lub poza nią).

10. W niniejszej opinii bardziej szczegółowo zajęto się wyżej wspomnianymi kwestiami, tak by doprowadzić do poprawienia obecnie zawartych we wniosku treści odnoszących się do ochrony danych, zarówno pod względem ich jasności, jak i spójności.

II. WYJAŚNIENIE POJĘĆ IDENTYFIKOWALNOŚCI I ANONIMOWOŚCI

Możliwość zastosowania dyrektywy 95/46/WE

11. Zgodnie z art. 2 lit. a) dyrektywy 95/46/WE w sprawie ochrony danych osobowych „dane osobowe" oznaczają „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość".

12. Materiały biologiczne ludzkiego pochodzenia, takie jak narządy, tkanki, komórki lub krew, można określić jako materiał, który może zostać pozyskany z ciała ludzkiego. Wątpliwe, czy te materiały same w sobie można uznać za dane osobowe. Nie ulega natomiast wątpliwości, że takie materiały mogą zostać wykorzystane jako *źródła* informacji osobowych na temat osoby, od której zostały pozyskane. Uzyskanie takich informacji jest często celem obróbki materiałów biologicznych. Nawet jednak, gdy nie dąży się do realizacji takiego celu, materiałom biologicznym często towarzyszą takie uzyskane informacje. W takich sytuacjach zastosowanie mają przepisy dyrektywy 95/46/WE ([4]). Dzieje się tak, o ile osoba, od której pozyskano materiał biologiczny, jest osobą (fizyczną), *zidentyfikowaną* lub *możliwą do zidentyfikowania*.

13. W motywie 26 dyrektywy 95/46/WE wyjaśniono, w jaki sposób ustalić, czy dana osoba jest możliwa do zidentyfikowania: „należy wziąć pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owej osoby". W tym samym motywie wyjaśniono ponadto, że przepisy dyrektywy 95/46/WE nie mają zastosowania, jeśli informacje odnoszą się do osoby, której nie można lub już nie można zidentyfikować: dane takie są uważane za *anonimowe*.

14. W swoim zaleceniu (2006) 4 Rada Europy zajęła się konkretną kwestią identyfikowalnych materiałów biologicznych, wprowadzając rozróżnienie między identyfikowalnymi i nieidentyfikowalnymi materiałami biologicznymi ([5]).

15. W myśl wspomnianego zalecenia *identyfikowalne materiały biologiczne* to „te materiały biologiczne, które samodzielnie lub w połączeniu z towarzyszącymi im danymi umożliwiają identyfikację danych osób bezpośrednie lub poprzez użycie kodu" ([6]). W tym ostatnim przypadku użytkownik

([1]) Ramy te obejmują dyrektywy 2002/98/WE, 2004/33/WE, 2005/61/WE i 2005/62/WE dotyczące krwi i produktów krwiopochodnych oraz dyrektywy 2004/23/WE, 2006/17/WE i 2006/86/WE dotyczące tkanek i komórek ludzkich.

([2]) Zob. również wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie stosowania praw pacjenta w transgranicznej opiece zdrowotnej, COM(2008) 414 wersja ostateczna.

([3]) Opinia EIOD z dnia 2 grudnia 2008 r. na temat wniosku dotyczącego dyrektywy w sprawie stosowania praw pacjenta w transgranicznej opiece zdrowotnej.

([4]) Grupa Robocza ds. Ochrony Danych powołana na mocy art. 29, opinia 4/2007 w sprawie pojęcia danych osobowych, s. 9.

([5]) Zalecenie Rec(2006) 4 Komitetu Ministrów dla państw członkowskich w sprawie badań materiałów biologicznych ludzkiego pochodzenia.

([6]) Art. 3 ppkt (i) zalecenia Rec(2006) 4.

materiałów biologicznych może mieć dostęp do kodu (*materiały kodowane*) lub nie mieć dostępu do kodu, nad którym kontrolę sprawuje strona trzecia (*powiązane materiały anonimowe*). W swojej opinii 4/2007 w sprawie pojęcia danych osobowych Grupa Robocza Art. 29 (zwana dalej „GR29") użyła pojęcia *dane opatrzone pseudonimem, które można odtworzyć* dla określenia informacji o osobach pośrednio możliwych do zidentyfikowania; przy użyciu tych informacji możliwe jest, pod pewnymi z góry określonymi warunkami, odtworzenie ścieżki wiodącej do osoby, od której pozyskano narząd, i ustalenie tożsamości tej osoby ([1]). Jako przykład podano *dane zakodowane za pomocą klucza*, w przypadku których dane osobowe są oznaczone kodem, podczas gdy klucz łączący kod ze wspólnymi elementami identyfikującymi osoby jest przechowywany osobno. Jeśli zastosowane kody są niepowtarzalne dla każdej osoby, możliwe jest jej zidentyfikowanie za pomocą klucza zastosowanego przy kodowaniu.

16. W zaleceniu wspomina się również o *nieidentyfikowalnych materiałach biologicznych* (zwanych też *niepowiązanymi materiałami anonimowymi*) jako „tych materiałach biologicznych, które samodzielnie lub w połączeniu z towarzyszącymi im danymi nie umożliwiają, przy rozsądnym nakładzie pracy, identyfikacji danych osób" ([2]). Takie materiały uznawane byłyby faktycznie za dane anonimowe w myśl definicji w dyrektywie 95/46/WE.

17. Jak wynika z powyższego, dyrektywa 95/46/WE ma zastosowanie do zbierania, przechowywania i obróbki możliwych do zidentyfikowania narządów oraz do informacji uzyskanych następnie z takich narządów, o ile możliwe jest – przy należytym uwzględnieniu środków, które według wszelkiego prawdopodobieństwa mogą zostać użyte – zidentyfikowanie danej osoby. Jak zostanie wykazane, stała identyfikowalność narządów przewidziana w proponowanej dyrektywie sprawia, że osoby będzie można zidentyfikować na każdym etapie procesu.

Identyfikowalność a anonimowość narządów ludzkich

18. Identyfikowalność materiału biologicznego to możliwość odtworzenia ścieżki prowadzącej wstecz do osoby, od której pozyskano dany materiał, a przez to ustalenia tożsamości tej osoby. Innymi słowy, jeśli istnieje możliwość identyfikacji osób, od których pozyskano materiały biologiczne, bezpośrednio lub pośrednio, materiały te można uznać za identyfikowalne – i na odwrót. Pojęcia możliwości śledzenia (*traceability*) i możliwości identyfikacji (*identifiability*) są zatem z zasady ściśle ze sobą powiązane. Z drugiej strony, możliwość śledzenia i anonimowość danych nie mogą występować równocześnie. To pojęcia sprzeczne. Jeśli dana informacja jest rzeczywiście anonimowa, to nie ma możliwości ustalenia i wyśledzenia tożsamości osób.

19. W kontekście omawianego wniosku możliwość śledzenia jest obowiązkowym wymogiem, który należy wprowadzić w ramach krajowych programów jakości państw członkowskich i który powinien obowiązywać w obu kierunkach, tj. odnosić się zarówno do dawców, jak i biorców. Oznacza to, że choć informacje o dawcach i biorcach są poufne, identyfikowalne są informacje dotyczące narządów. Informację na ten temat zawiera podana we wniosku, w art. 3, definicja identyfikowalności (*traceability*): „zdolność właściwych organów do umiejscowienia i zidentyfikowania narządu na każdym etapie procesu, od aktu dawstwa do przeszczepienia lub utylizacji narządu; organy te w okolicznościach określonych niniejszą dyrektywą mają prawo do identyfikacji dawcy i instytucji pobierającej narządy, identyfikacji biorcy (biorców) w ośrodku transplantacyjnym (ośrodkach transplantacyjnych), umiejscowienia i identyfikacji wszystkich istotnych informacji, innych niż dane osobowe, odnoszących się do produktów i materiałów mających kontakt z narządem".

20. Ponadto art. 10 wniosku, dotyczący identyfikowalności, stanowi w ust. 1, że „państwa członkowskie zapewniają identyfikowalność wszystkich narządów pobranych i przydzielonych na ich terytorium od dawcy do biorcy i odwrotnie w celu ochrony zdrowia dawców i biorców". W ust. 3 tego samego artykułu stwierdza się, że „państwa członkowskie zapewniają: a) przechowywanie przez właściwy organ lub inne organy uczestniczące w procesie od aktu dawstwa do przeszczepienia lub utylizacji narządu wszelkich danych koniecznych do zapewnienia identyfikowalności na wszystkich etapach tego procesu, zgodnie z krajowymi programami jakości; b) przechowywanie danych koniecznych do pełnej identyfikowalności przez co najmniej 30 lat od aktu dawstwa. Dane takie można przechowywać w formie elektronicznej".

21. Choć procedury dotyczące identyfikowalności muszą jeszcze zostać określone w środkach wykonawczych (zob. art. 25 wniosku), najbardziej prawdopodobnym rozwiązaniem wydaje się wprowadzenie systemu pośredniej identyfikacji dawców i biorców, który będzie wzorowany na dyrektywie 2004/23/WE ([3]) w sprawie tkanek i komórek i na ustanowionym w niej europejskim kodzie identyfikacyjnym lub przynajmniej będzie mógł być stosowany w zgodzie z nimi ([4]). W takim przypadku przetwarzanie

([1]) Grupa Robocza Art. 29 (ds. ochrony danych), opinia 4/2007, s. 18.
([2]) Art. 3 ppkt (ii) zalecenia Rec(2006) 4.

([3]) Jako że dawcy narządów są bardzo często dawcami tkanek, istnieje potrzeba śledzenia i zgłaszania wszelkich nieoczekiwanych niepożądanych reakcji również w ramach systemu nadzoru tkanek, i stąd wymagana jest interoperacyjność z metodą pośredniej identyfikacji stosowaną w tym systemie. Zob.: dyrektywę 2004/23/WE Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie ustalenia norm jakości i bezpiecznego oddawania, pobierania, testowania, przetwarzania, konserwowania, przechowywania i dystrybucji tkanek i komórek ludzkich, Dz.U. L 102/48 z 7.4.2004, oraz dyrektywę Komisji 2006/86/WE z dnia 24 października 2006 r. wykonującą dyrektywę 2004/23/WE Parlamentu Europejskiego i Rady w zakresie wymagań dotyczących możliwości śledzenia, powiadamiania o poważnych i niepożądanych reakcjach i zdarzeniach oraz niektórych wymagań technicznych dotyczących kodowania, przetwarzania, konserwowania, przechowywania i dystrybucji tkanek i komórek ludzkich, Dz.U. L 294/32 z 25.10.2006.

([4]) Kod ten zawiera niepowtarzalny numer identyfikacyjny każdego przypadku dawstwa, umożliwiający, wraz danymi identyfikacyjnymi banku tkanek i danymi identyfikacyjnymi produktu, odtworzenie tożsamości dawców i biorców. Mówiąc ściślej, zgodnie z art. 10 dyrektywy 2006/86/WE, „aby zapewnić właściwą identyfikację dawcy i możliwość śledzenia wszystkich pobranych materiałów oraz przekazywanie informacji dotyczących podstawowych cech i właściwości tkanek i komórek, każdemu materiałowi pobranemu w banku tkanek jest przydzielany jednolity europejski kod identyfikacyjny". Zgodnie z opisem w załączniku VII do tej dyrektywy, kod ten składa się z dwóch części: a) danych identyfikacyjnych dotyczących oddania, w tym niepowtarzalnego numeru identyfikacyjnego oddania i danych identyfikacyjnych banku tkanek oraz b) danych identyfikacyjnych produktu, w tym kodu produktu, numer podgrupy i daty ważności.

dotyczące dawców i biorców prowadzone w kontekście wniosku dotyczy powiązanych anonimowych materiałów biologicznych, czy też, jeśli użyć terminologii dotyczącej ochrony danych – danych opatrzonych pseudonimem, które można odtworzyć (zob. pkt 15 powyżej); do tych materiałów/danych mają zastosowanie przepisy dyrektywy 95/46/WE.

22. Należy jednak zauważyć, że mimo wyraźnie określonych wymogów możliwości śledzenia i możliwości identyfikacji, w pewnych częściach wniosku używany jest termin „anonimowość" i „dane anonimowe", gdy mowa jest o danych dawców i biorców. Jak wynika z poprzednich punktów, łączenie tych wymogów i terminów pociąga za sobą sprzeczność i wprowadza w błąd ([1]).

23. Mówiąc ściślej, art. 10 ust. 2 wniosku, w którym przedstawiono potrzebę systemu identyfikacji dawców, stanowi, że *„państwa członkowskie zapewniają wdrożenie systemu identyfikacji dawców, umożliwiającego zidentyfikowanie każdego aktu dawstwa i każdego pobranego w ten sposób narządu*. Państwa członkowskie zapewniają opracowanie i dobór wspomnianego systemu identyfikacji dawców w taki sposób, aby wykluczyć lub zminimalizować gromadzenie, przetwarzanie lub wykorzystywanie danych osobowych. W szczególności należy wykorzystywać możliwości stosowania pseudonimów lub metod zapewniających anonimowość poszczególnych osób" ([2]). EIOD jest zdania, że podkreślone wyrażenia w tym konkretnym ustępie kłócą się z pojęciem identyfikowalności, ponieważ nie można dysponować danymi umożliwiającymi śledzenie i identyfikację, jeśli zapewnia się anonimowość dawcom i biorcom. Poza tym godny uwagi jest fakt, że w ustępie tym mowa jest o identyfikacji dawców, nie ma zaś wzmianki o identyfikacji biorców (która również jest częścią procesu).

24. Wspomniana wcześniej sprzeczność jest jeszcze lepiej widoczna w art. 17, dotyczącym zapewniania anonimowości dawców i biorców, w którym stwierdza się, że: „państwa członkowskie podejmują wszelkie niezbędne środki w celu zapewnienia anonimowości wszystkich danych osobowych dawców i biorców, przetwarzanych w zakresie objętym niniejszą dyrektywą, tak aby uniemożliwić ustalenie tożsamości dawców i biorców". Artykuł ten stoi w całkowitej sprzeczności z artykułami wniosku dotyczącymi identyfikowalności.

Poufność zamiast anonimowości

25. EIOD rozumie, że terminu „anonimowość" użyto, by podkreślić potrzebę zwiększonej *poufności* ([3]) danych dawców i biorców, co oznacza, że dostęp do tych informacji miałyby wyłącznie osoby do tego uprawnione. EIOD zakłada, że wyrażenie „anonimizacja" jest domyślnie, bardziej konkretnie stosowane dla określenia systemu pośredniej identyfikacji dawców i biorców ([4]), co również może się różnić od sposobu, w jaki termin ten jest stosowany w dyrektywie 2004/23/WE w sprawie tkanek i komórek. Jak jednak stwierdzono wcześniej, zastosowanie terminu „anonimowość" nie jest poprawne.

26. Przykład rozwiązania kwestii ochrony danych i identyfikowalności w ramach działań związanych z przeszczepem można znaleźć w Protokole dodatkowym Rady Europy do Konwencji o prawach człowieka i biomedycynie ([5]). W protokole zamiast pojęcia anonimowości stosowane jest pojęcie poufności. I tak art. 23 ust. 1 protokołu stanowi, że „wszystkie dane osobowe odnoszące się do osoby, od której pobrano narządy lub tkanki, oraz dane odnoszące się do biorcy są traktowane jako poufne. Zbieranie, przetwarzanie lub przekazywanie takich danych może mieć miejsce jedynie zgodnie z przepisami dotyczącymi tajemnicy służbowej i ochrony danych osobowych". Ust. 2 w tym samym artykule stanowi, że: „przepisy ust. 1 są interpretowane bez uszczerbku dla przepisów umożliwiających – pod warunkiem zachowania odpowiednich gwarancji – zbieranie, przetwarzanie i przekazywanie niezbędnych informacji o osobie, od której pobrano narządy lub tkanki, lub o biorcy narządów i tkanek, o ile jest to konieczne do celów medycznych, w tym dla potrzeb identyfikowalności, przewidzianych w art. 3 niniejszego protokołu".

27. Na podstawie powyższych rozważań EIOD zaleca zmianę brzmienia niektórych części wniosku, aby uniknąć dwuznaczności i jednoznacznie wyrazić fakt, że dane nie są anonimowe, ale powinny być przetwarzane w myśl rygorystycznych przepisów dotyczących poufności i bezpieczeństwa. Mówiąc ściślej, EIOD zaleca następujące zmiany:

([1]) EIOD zawarł podobny komentarz w swoich uwagach z dnia 19.9.2006 r. dotyczących publicznych konsultacji na temat przyszłych działań UE w dziedzinie dawstwa i przeszczepiania organów.

([2]) Podkreślenie dodane.

([3]) Dopilnowanie, by informacja była udostępniana jedynie podmiotom do tego uprawnionym (definicja ISO, źródło: http://www.wikipedia.org).

([4]) Termin „anonimizacja", w zależności od kontekstu, w jakim został użyty, czasem jest stosowany domyślnie dla określenia pośrednio identyfikowalnych danych, np. w przypadku statystyk. Nie jest to jednak zastosowanie poprawne z punktu widzenia ochrony danych, jak już wyjaśnił EIOD w swojej opinii na temat wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie statystyk Wspólnoty w zakresie zdrowia publicznego oraz bezpieczeństwa i higieny pracy (COM(2007) 46 wersja ostateczna) i w opinii na temat wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie statystyk europejskich (COM(2007) 625 wersja ostateczna).

([5]) Rada Europy, Protokół dodatkowy do Konwencji o prawach człowieka i biomedycynie dotyczący przeszczepiania narządów i tkanek pochodzenia ludzkiego, Strasburg, 24.1.2002; aby sprawdzić stan ratyfikacji, zob. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=186&CM=8&DF=2/13/2009&CL=ENG
Zob. również: Rada Europy, Konwencja o ochronie praw człowieka i godności istoty ludzkiej w kontekście zastosowań biologii i medycyny: konwencja o prawach człowieka i biomedycynie, Oviedo, 4.4.1997; aby sprawdzić stan ratyfikacji zob. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=164&CM=8&DF=2/13/2009&CL=ENG

— w motywie 16, zdanie ostatnie: „Zgodnie z Kartą oraz biorąc w stosownych przypadkach pod uwagę konwencję o prawach człowieka i biomedycynie programy przeszczepiania narządów powinny opierać się na zasadzie dobrowolnego i nieodpłatnego dawstwa, altruizmu dawcy oraz solidarności między dawcą i biorcą, oraz anonimowości zmarłego dawcy oraz biorcy, a jednocześnie zawierać rygorystyczne przepisy dotyczące poufności i bezpieczeństwa w celu ochrony danych osobowych dawców i biorców”;

— w art. 10 ust. 2: „Państwa członkowskie zapewniają wdrożenie systemu identyfikacji dawców i biorców, umożliwiającego zidentyfikowanie każdego aktu dawstwa i każdego pobranego w ten sposób narządu. Państwa członkowskie zapewniają opracowanie i dobór wspomnianego systemu identyfikacji dawców i biorców w taki sposób, aby zminimalizować gromadzenie, przetwarzanie lub wykorzystywanie danych osobowych, w szczególności stosując metody polegające na opatrywaniu danych pseudonimami, a także zapewniają istnienie koniecznych środków technicznych i organizacyjnych, aby zapewnić bezpieczeństwo tych danych”;

— art. 17 jako taki można by skreślić, a jego treść (jeśli chodzi o potrzebę poufności) przenieść do nowego ustępu w art. 16, dotyczącym ochrony danych osobowych, poufności i bezpieczeństwa przetwarzania danych (zob. pkt 36 poniżej).

28. Ponadto – jak zostało to omówione w dalszej części niniejszej opinii – EIOD sugeruje, by silniej naświetlić potrzebę *wzmocnionej ochrony* danych dawców i biorców poprzez stosowanie *zdecydowanych środków bezpieczeństwa*, zarówno na szczeblu krajowym, jak i w stosunkach transgranicznych.

III. **POŁOŻENIE NACISKU NA KRAJOWE ŚRODKI BEZPIECZEŃSTWA DANYCH**

Podstawowe potrzeby i wymogi w zakresie bezpieczeństwa

29. Jak wynika z wniosku, przetwarzanie danych osobowych dawców i biorców odbywa się przede wszystkim na szczeblu krajowym, tj. w instytucjach pobierających narządy i ośrodkach transplantacyjnych państw członkowskich. To właśnie na tym szczeblu prowadzony jest również rejestr żywych dawców. Choć mechanizm śledzenia nie został jeszcze określony, można oczekiwać, że wszelkie działania związane z kodowaniem również prowadzone będą na szczeblu krajowym, nawet jeśli stosowany będzie europejski system kodowania, ponieważ zidentyfikowanie dawców i biorców możliwe jest wyłącznie za pośrednictwem właściwych organów krajowych.

30. Sprawą najwyższej wagi jest zatem wprowadzenie polityki w zakresie bezpieczeństwa informacji, której podstawą będą *rygorystyczne i solidne środki bezpieczeństwa* podjęte przez odpowiednie służby krajowe, zwłaszcza aby sprostać określonym we wniosku wymogom poufności w odniesieniu do dawców i biorców, a także by zagwarantować *integralność* ([1]), *rzetelność* ([2]) i *dostępność* ([3]) tych danych. W tym względzie wspomniana polityka w zakresie bezpieczeństwa powinna obejmować elementy bezpieczeństwa fizycznego i logicznego, skupiając się m.in. na kontrolowaniu wprowadzanych danych, dostępu do nich, ich zapisu, transferu i przekazywania, a także na kontrolowaniu nośników danych i urządzeń do ich przechowywania.

31. Jeśli chodzi o poufność, dane medyczne biorców ([4]), a także dane wykorzystane przy tworzeniu charakterystyki dawców i w dalszych działaniach (również w odniesieniu do dawców zakwalifikowanych na podstawie rozszerzonych kryteriów ([5])) mogą ujawniać sensytywne dane osobowe dotyczące tych osób, co może mieć również wpływ na ich życie społeczne, zawodowe lub prywatne. Ochrona danych umożliwiających identyfikację dawców jest również istotna, ponieważ żywi dawcy lub osoby, które wyraziły zgodę na oddanie narządów po swojej śmierci, mogliby paść ofiarą handlu ludzkimi narządami i tkankami, gdyby informacje te zostały ujawnione. Kluczowe znaczenie ma także integralność danych odnoszących się do narządów, jako że najmniejszy błąd w przekazywanych informacjach może stanowić zagrożenie dla życia biorcy. To samo dotyczy dokładności danych o stanie zdrowia dawcy przed przeszczepem, ponieważ dane te służą stwierdzeniu, czy narząd nadaje się do przeszczepu czy też nie. Jeśli chodzi o rzetelność, to z uwagi na fakt, że tak wiele różnych organizacji zaangażowanych jest w cały mechanizm dawstwa i transplantacji, powinien istnieć sposób sprawienia, by wszystkie zaangażowane podmioty były świadome swoich działań i brały za nie odpowiedzialność, np. w przypadku gdy okazało się, że dane umożliwiające identyfikację

([1]) Zadbanie o to, by dane były „w całości” lub kompletne, sytuacja, w której dane zachowują tę samą postać podczas każdej operacji (np. transferu, przechowywania lub pobierania), zachowanie danych do planowanego użytku, lub, w przypadku określonych operacji, uprzednie założenie odpowiedniej jakości danych. Mówiąc po prostu, integralność danych to pewność, że dane są spójne i poprawne (źródło: http://www.wikipedia.org); dopilnowanie, by dostęp do informacji i możliwość ich modyfikowania miały tylko podmioty do tego uprawnione (źródło: http://searchdatacenter.techtarget.com).

([2]) Odpowiedzialność za swoje działania; niezaprzeczalność: dopilnowanie, by dane zostały przesłane i otrzymane przez strony, które twierdzą, że je przesłały i otrzymały; dopilnowanie, by strona sporu nie mogła zaprzeczyć ważności oświadczenia lub go obalić (źródło: http://www.wikipedia.org).

([3]) Stopień, do jakiego dane są natychmiastowo dostępne (źródło: http://www.pcmag.com).

([4]) Należy zauważyć, że sam fakt, iż biorca otrzymuje przeszczep, stanowi sensytywną daną osobową na temat zdrowia tej osoby.

([5]) Potencjalni dawcy, którzy nie są dawcami idealnymi, ale których kandydatura może być rozważana w pewnych okolicznościach, np. dla biorców w podeszłym wieku. Zob.: dokument roboczy służb Komisji dołączony do wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie norm jakości i bezpieczeństwa narządów ludzkich do przeszczepów oraz komunikat Komisji: „Plan działania dotyczący dawstwa i przeszczepiania narządów (2009-2015): zacieśnianie współpracy między państwami członkowskimi”, ocena skutków, 8.12.2008.

dawców zostały ujawnione nieuprawnionym osobom lub że dane medyczne narządów nie są prawidłowe. Ponadto, ponieważ cały system opiera się na transferze danych odnoszących się do narządów i na mechanizmie śledzenia począwszy od etapu dawcy na biorcy kończąc, w razie potrzeby dane te powinny być do dyspozycji uprawnionych osób niezwłocznie (w przeciwnym razie niedostępność danych zagroziłaby prawidłowemu funkcjonowaniu systemu).

32. Z tego względu powinny istnieć stosowne *mechanizmy autoryzacji*, wynikające ze szczegółowych *polityk w zakresie kontroli dostępu*, zarówno w przypadku krajowych baz danych, jak i transgranicznej wymiany narządów. Polityki te należy najpierw określić na szczeblu organizacji, zwłaszcza co się tyczy procedur identyfikacji dawców i biorców (np. kto ma dostęp do jakich informacji i w jakich okolicznościach). W ten sposób określone zostaną *prawa dostępu*, a także *scenariusze dostępu*, w ramach których można korzystać z tych praw (np. okoliczności i procedura ujawnienia właściwemu organowi danych przez instytucję pobierającą narządy, ewentualne przypadki, w których konieczne jest ujawnienie biorcy tożsamości dawcy, i procedury, których należy przy tym przestrzegać). Aby te polityki były skuteczne, osoby zaangażowane w przetwarzanie powinny być związane szczegółowymi *przepisami dotyczącymi poufności*.

33. Po określeniu polityk można je wdrożyć na szczeblu technicznym, tj. kontrolować dostęp użytkowników do systemów i programów zgodnie z wcześniej określonymi prawami dostępu. Można w tym celu skorzystać ze sprawdzonych technologii, takich jak *szyfrowanie* lub *certyfikaty cyfrowe* ([1]) (np. wykorzystujących *infrastrukturę klucza publicznego* ([2]). W celu ograniczenia użytkownikom praw dostępu w zależności od pełnionej przez nich funkcji można też zastosować *mechanizmy uwierzytelnienia na podstawie pełnionej funkcji* (np. wyłącznie lekarze powinni móc modyfikować dane medyczne biorców i dawców w krajowych bazach danych).

34. Kontroli dostępu powinny towarzyszyć możliwości *rejestrowania* działań użytkowników (np. dostępu do danych medycznych w celu ich odczytywania i zapisywania), zwłaszcza gdy stosowane są systemy elektroniczne. Powinny również istnieć fizyczne i logiczne środki bezpieczeństwa, które posłużą zapewnieniu *pełnej operacyjności* baz danych dawców i narządów jako centralnego elementu proponowanego systemu dawstwa i transplantacji. Za kamień węgielny systemu należy uważać dostępność danych. W tym względzie podstawą polityki w zakresie bezpieczeństwa informacji powinny być *prawidłowa analiza i ocena ryzyka*; polityka ta powinna również obejmować elementy takie jak incydenty i zarządzanie ciągłością działania. Wszystkie te elementy należy utrzymywać i usprawniać w ramach regularnego procesu monitorowania i przeglądu. Skuteczność i usprawnianie systemu można również zwiększyć przez *niezależne audyty*, poświęcone szczególnie praktykom w zakresie opatrywania pseudonimem, identyfikowalności i transferu danych.

35. EIOD chciałby, by w proponowanej dyrektywie więcej nacisku położono na potrzebę stosowania takich środków.

Udoskonalenie przepisów dotyczących bezpieczeństwa zawartych we wniosku

36. Art. 16 wniosku, dotyczący ochrony danych osobowych, poufności i bezpieczeństwa przetwarzania, stanowi, że „państwa członkowskie dopilnowują pełnego i skutecznego przestrzegania podstawowego prawa do ochrony danych osobowych we wszystkich działaniach związanych z przeszczepianiem narządów, zgodnie z przepisami Wspólnoty w zakresie ochrony danych osobowych, w tym z dyrektywą 95/46/WE, a w szczególności z jej art. 8 ust. 3, art. 16, art. 17 i art. 28 ust. 2". EIOD zaleca, by do artykułu dodać *drugi akapit*, w którym opisane zostaną podstawowe zasady służące zapewnieniu bezpieczeństwa na szczeblu państwa członkowskiego; powinny one co najmniej zawierać odniesienie do następujących zagadnień:

— Należy wprowadzić politykę w zakresie bezpieczeństwa informacji, realizującą środki techniczne i organizacyjne, które zapewnią poufność, integralność, rzetelność i dostępność danych osobowych dawców i biorców.

— Należy określić konkretną politykę w zakresie poufności i kontroli dostępu, która będzie realizowana we wszystkich państwach członkowskich i która określa prawa dostępu, funkcje i obowiązki wszystkich zaangażowanych stron (dawcy, instytucji pobierającej narządy, ośrodka transplantacyjnego, biorcy, właściwego organu krajowego, organu posiadającego właściwość na szczeblu transgranicznym) na wszystkich etapach łańcucha identyfikowalności. Osoby zaangażowane w przetwarzanie powinny być zobowiązane do zapewnienia konkretnych gwarancji poufności danych, szczególnie jeśli osoby te nie są związane tajemnicą lekarską (np. powinny istnieć kodeksy postępowania w zakresie poufności i środki podnoszenia świadomości).

— Należy podkreślić potrzebę zajęcia się kwestią mechanizmów bezpieczeństwa (takich jak szyfrowanie i certyfikaty cyfrowe) w krajowych bazach danych. Zwłaszcza co się tyczy rejestrów dawców, powinna obowiązywać zasada „poszanowania prywatności od samego początku", tak by już na początkowych etapach wdrażania takich rozwiązań uwzględnić wszelkie niezbędne wymogi bezpieczeństwa.

— Należy również wprowadzić procedury, które pozwolą zagwarantować dawcom i biorcom prawa w zakresie ochrony danych, zwłaszcza prawo dostępu i poprawiania, a także prawo do otrzymania informacji. Szczególną uwagę należy poświęcić przypadkom dawców, którzy chcą wycofać swoją zgodę lub (po przeprowadzeniu charakterystyki dawcy i narządu) nie zostali zaakceptowani jako dawcy. W takim przypadku należy określić specjalną procedurę i limity czasowe zatrzymywania ich danych.

([1]) Elektroniczny odpowiednik dokumentu tożsamości, który uwierzytelnia autora podpisu elektronicznego (źródło: http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_04_appx_b_glossary.html).

([2]) Infrastruktura klucza publicznego to połączenie sprzętu, oprogramowania, osób, polityk i procedur niezbędnych by stworzyć, przechowywać, upowszechniać i unieważniać certyfikaty cyfrowe oraz nimi zarządzać (źródło: http://www.wikipedia.org).

— Polityka w zakresie bezpieczeństwa informacji powinna również zawierać środki, które mają zagwarantować integralność i niezakłóconą dostępność danych. Ocenie ryzyka dla bezpieczeństwa informacji powinny towarzyszyć elementy dotyczące incydentów i zarządzania ciągłością działania.

— Polityki w zakresie bezpieczeństwa informacji powinny być regularnie monitorowane i podlegać regularnym przeglądom, w tym w ramach niezależnych audytów.

37. EIOD zaleca, by wyżej wymienione elementy zostały włączone do art. 16, a następnie bardziej szczegółowo omówione jako część środków wykonawczych zawartych w art. 25, zwłaszcza w ust. 1 lit. a), b) i c).

IV. **GWARANCJE DOTYCZĄCE TRANSGRANICZNEJ WYMIANY NARZĄDÓW**

Harmonizacja środków bezpieczeństwa w państwach członkowskich

38. Transgraniczna wymiana narządów w praktyce zawsze będzie oznaczać przetwarzanie danych osobowych, ponieważ – nawet zakodowane – narządy pozostają (pośrednio) możliwe do zidentyfikowania za pośrednictwem właściwych organów krajowych.

39. EIOD wyraził już swoją opinię na temat potrzeb w zakresie bezpieczeństwa dotyczących ochrony danych osobowych w ramach transgranicznej opieki zdrowotnej w Europie; podkreślił m.in. potrzebę dokonania harmonizacji polityk w zakresie bezpieczeństwa informacji w państwach członkowskich, tak by osiągnąć odpowiedni poziom ochrony danych ([1]). EIOD zaleca, by element ten pojawił się również w omawianym wniosku, a konkretnie – w motywie 17, gdzie znajduje się wzmianka o przepisie dyrektywy 95/46/WE dotyczącym bezpieczeństwa przetwarzania.

Ustanowienie systemu śledzenia

40. W tym szczególnym przypadku istotnym czynnikiem w zapewnieniu transgranicznego bezpieczeństwa danych jest planowany mechanizm śledzenia. W tym względzie, poza środkami bezpieczeństwa stosowanymi na szczeblu państw członkowskich, szczególną uwagę należy poświęcić możliwościom związanym z opatrywaniem pseudonimem, które zostaną wykorzystane przy identyfikowaniu dawców i biorców (np. typowi kodowania, możliwości podwójnego kodowania itd.), oraz utrzymaniu interoperacyjności z systemem identyfikacji tkanek i komórek.

41. EIOD zaleca, by w art. 25 proponowanej dyrektywy, dotyczącym środków wykonawczych, zamieścić konkretne odniesienie do tego zagadnienia, zmieniając ust. 1 lit. b) w następujący sposób: „procedury służące zapewnieniu pełnej identyfikowalności narządu, w tym wymogi dotyczące oznakowywania, zapewniające przy tym dawcom i biorcom poufność na każdym etapie procesu śledzenia i zachowujące interoperacyjność z systemem identyfikacji tkanek i komórek".

Wymiana narządów z państwami trzecimi

42. Potrzeby w zakresie bezpieczeństwa jeszcze wzrastają, gdy dane są wymieniane z państwami trzecimi, w których nie zawsze możliwe jest zagwarantowanie odpowiedniego poziomu ochrony danych. Konkretne ustalenia dotyczące transferu danych osobowych do państw trzecich są określone w art. 25 i 26 dyrektywy 95/46/WE. EIOD jest świadomy faktu, że wymogi ochrony danych nie mogą przeszkadzać w szybkim i efektywnym transferze narządów, co jest warunkiem koniecznym w systemie dawstwa narządów i często może być kwestią życia i śmierci. Należy zatem zbadać możliwości dopuszczenia transferów nawet w przypadkach ogólnie niezadowalającego poziomu ochrony danych w danym państwie trzecim. Należy przy tym wziąć pod uwagę, że w związku z faktem, że dane osoby są identyfikowane na szczeblu transgranicznym tylko pośrednio i że właściwe organy krajowe sprawują ogólny nadzór nad systemem, ewentualne zagrożenia są najprawdopodobniej mniejsze niż zagrożenia, które mogą się pojawić na szczeblu krajowym ([2]).

43. Z tego względu EIOD jest zdania, że właściwy organ, który odpowiedzialny jest za wydawanie zezwoleń na takie transfery, powinien zasięgnąć opinii krajowego organu ochrony danych i na tej podstawie opracować – w świetle ewentualnych odstępstw wskazanych w art. 26 dyrektywy 95/46/WE – przepisy niezbędne do zapewnienia bezpiecznego, lecz również szybkiego i efektywnego transferu danych na temat narządów do państw trzecich i w kierunku przeciwnym. EIOD zaleca, by odniesienie na ten temat zamieścić w art. 21, dotyczącym wymiany narządów z państwami trzecimi, lub w odpowiadającym mu motywie 15.

Środki wykonawcze

44. Na zakończenie EIOD apeluje do prawodawcy o zadbanie o to, by w odniesieniu do art. 25, we wszystkich przypadkach, w których rozważane są środki wykonawcze mające wpływ na ochronę danych i ich bezpieczeństwo, zasięgnięto opinii wszystkich zainteresowanych stron, w tym EIOD i Grupy Roboczej Art. 29.

V. **PODSUMOWANIE**

45. EIOD odnotował inicjatywę na rzecz zapewnienia wysokich norm jakości i bezpieczeństwa ludzkich narządów do przeszczepu, która może być postrzegana jako część ogólnego podejścia WE do kwestii ustanowienia wspólnych norm służących promowaniu transgranicznej dostępności usług opieki zdrowotnej w całej Europie.

46. We wniosku zajęto się już potrzebami dawców i biorców narządów w zakresie ochrony danych, zwłaszcza w odniesieniu do wymogu zachowania poufności, jeśli chodzi o ich tożsamość. EIOD z żalem zauważa jednak, że niektóre z tych przepisów są niejasne, niejednoznaczne lub ogólne, i z tego względu zaleca szereg zmian, które posłużą poprawie jakości przepisów dotyczących ochrony danych zawartych we wniosku.

([1]) Opinia EIOD z dnia 2 grudnia 2008 r. na temat wniosku dotyczącego dyrektywy w sprawie stosowania praw pacjenta w transgranicznej opiece zdrowotnej.

([2]) Zob. opinię 4/2007 Grupy Roboczej Art. 29 (ds. ochrony danych), s. 18 – dane opatrzone pseudonimem i zakodowane za pomocą klucza.

47. Po pierwsze, EIOD odnotowuje istnienie sprzeczności między pojęciem identyfikowalności a pojęciem anonimowości, które są używane we wniosku. W tym względzie zaleca wprowadzenie konkretnych zmian w sformułowaniu niektórych części wniosku (tj. motywie 16, art. 10 ust. 2 i art. 17), tak by uniknąć niejednoznaczności i jasno odzwierciedlić fakt, że dane nie są anonimowe, lecz powinny być przetwarzane z zachowaniem rygorystycznych przepisów dotyczących poufności i bezpieczeństwa.

48. Ponadto zaleca położenie większego nacisku na potrzebę przyjęcia rygorystycznych środków bezpieczeństwa na szczeblu krajowym. Można to uczynić, dodając w art. 16 drugi akapit, w którym opisane zostaną podstawowe zasady zapewnienia bezpieczeństwa na szczeblu państw członkowskich, a następnie precyzując te zasady jako część środków wykonawczych zawartych w art. 25 ust. 1. Proponowane zasady bezpieczeństwa powinny obejmować:

a) przyjęcie polityki w zakresie bezpieczeństwa informacji, aby zapewnić poufność, integralność, rzetelność i dostępność danych osobowych dawców i biorców;

b) określenie konkretnej polityki w zakresie poufności i kontroli dostępu, a także gwarancji zachowania poufności danych przez osoby biorące udział w przetwarzaniu;

c) zajęcie się kwestią mechanizmów bezpieczeństwa w krajowych bazach danych, w oparciu o zasadę „poszanowania prywatności od samego początku";

d) wprowadzenie procedur służących zagwarantowaniu dawcom i biorcom praw w zakresie ochrony danych, zwłaszcza prawa dostępu i poprawiania oraz prawa do otrzymania informacji; należy przy tym zwrócić szczególną uwagę na przypadki dawców, którzy chcą wycofać swoją zgodę lub którzy nie zostali zaakceptowani jako dawcy;

e) wprowadzenie środków służących zagwarantowaniu integralności i niezakłóconej dostępności danych;

f) zapewnienie regularnego monitorowania i niezależnych audytów stosowanych polityk w zakresie bezpieczeństwa.

49. Jeśli chodzi o transgraniczną wymianę narządów, EIOD zaleca, by w motywie 17 wniosku zawrzeć wzmiankę o potrzebie zharmonizowania polityk w zakresie bezpieczeństwa informacji w państwach członkowskich. Należy ponadto zwrócić szczególną uwagę na możliwości związane z opatrywaniem pseudonimem, które zostaną wykorzystane do identyfikacji dawców i biorców; należy także zwrócić uwagę na zachowanie interoperacyjności z systemem identyfikacji tkanek i komórek. EIOD zaleca, by w art. 25 ust. 1 lit. b) zawrzeć konkretne odniesienie do tego zagadnienia.

50. Co się tyczy wymiany narządów z państwami trzecimi, EIOD zaleca, by w art. 21 wniosku lub odpowiadającym mu motywie 15 zawrzeć informację, że właściwy organ zasięga opinii krajowego organu ochrony danych, by opracować niezbędne ramy bezpiecznego, ale również szybkiego i efektywnego transferu danych o narządach do państw trzecich i w kierunku przeciwnym.

51. EIOD zaleca ponadto, by we wszystkich przypadkach, gdy rozważane są środki wykonawcze mające wpływ na ochronę i bezpieczeństwo danych, zasięgano opinii wszystkich zainteresowanych podmiotów, w tym EIOD i Grupy Roboczej Art. 29.

Sporządzono w Brukseli dnia 5 marca 2009 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych