

Opinia Europejskiego Inspektora Ochrony Danych w sprawie zmienionego wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (WE) nr (.../...) (ustanawiającego kryteria i mechanizmy ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca)

(2011/C 101/03)

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 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 11 października 2010 r. Komisja Europejska przyjęła zmieniony wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (WE) nr (.../...) (ustanawiającego kryteria i mechanizmy ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca) (zwany dalej „wnioskiem”) ⁽³⁾. Tego samego dnia wniosek przyjęty przez Komisję przesłano EIOD do konsultacji zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001. EIOD z zadowoleniem przyjmuje fakt, że Komisja pragnie się z nim skonsultować i prosi, aby odniesiono się do wspomnianych konsultacji w motywach wniosku.
2. Eurodac ustanowiono rozporządzeniem (WE) nr 2725/2000 dotyczącym ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania konwencji dublińskiej ⁽⁴⁾. Komisja przyjęła wniosek dotyczący przekształcenia zmierzający do zmiany rozpo-

ządzenia Eurodac w grudniu 2008 r. ⁽⁵⁾ (zwany dalej „wnioskiem z grudnia 2008 r.”). EIOD przedstawił opinię w sprawie tego wniosku w lutym 2009 r. ⁽⁶⁾.

3. Wniosek z grudnia 2008 r. miał zapewnić skuteczniejsze wspieranie stosowania rozporządzenia dublińskiego oraz odpowiednie zaradzenie problemom związanym z ochroną danych. We wniosku dostosowano także strukturę zarządzania aspektami informacyjno-komunikacyjnymi do rozwiązań przyjętych w rozporządzeniach dotyczących SIS II i VIS, przewidując przejęcie zadań związanych z zarządzaniem operacyjnym systemu Eurodac przez mającą powstać agencję do spraw zarządzania operacyjnego wielkoskalowymi systemami informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości ⁽⁷⁾ (zwaną dalej „agencją ds. TI”) ⁽⁸⁾.
4. We wrześniu 2009 r. Komisja przyjęła zmieniony wniosek, aby umożliwić organom ścigania państw członkowskich oraz Europolowi dostęp do centralnej bazy danych Eurodac na potrzeby prewencji, wykrywania i dochodzenia przestępstw terrorystycznych oraz innych poważnych przestępstw kryminalnych.

⁽⁵⁾ Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (WE) nr (.../...) (ustanawiającego kryteria i mechanizmy ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca), COM(2008) 825 wersja ostateczna.

⁽⁶⁾ Opinia z dnia 18 lutego 2009 r. dotycząca wniosku w sprawie rozporządzenia dotyczącego ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (WE) nr (.../...) (ustanawiającego kryteria i mechanizmy ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela kraju trzeciego lub bezpaństwowca) (COM(2008) 825), Dz.U. C 229 z 23.9.2009, s. 6.

⁽⁷⁾ Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego agencję do spraw zarządzania operacyjnego wielkoskalowymi systemami informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości (COM(2009) 292 wersja ostateczna) został przyjęty dnia 24 czerwca 2009 r. Zmieniony wniosek został przyjęty dnia 19 marca 2010 r.: zmieniony wniosek rozporządzenie (UE) nr.../... Parlamentu Europejskiego i Rady ustanawiające agencję do spraw zarządzania operacyjnego wielkoskalowymi systemami informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, COM(2010) 93.

⁽⁸⁾ EIOD wydał opinię dotyczącą utworzenia agencji ds. TI (Opinia z dnia 7 grudnia 2009 r. dotycząca wniosku rozporządzenia ustanawiającego agencję do spraw zarządzania operacyjnego wielkoskalowymi systemami informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz dotyczącą wniosku w sprawie decyzji Rady powierzającej tej agencji zadania dotyczące zarządzania operacyjnego systemami SIS II i VIS w zastosowaniu tytułu VI Traktatu UE, Dz.U. C 70 z 19.3.2010, s. 13).

⁽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) 555 wersja ostateczna.

⁽⁴⁾ Dz.U. L 62 z 5.3.2002, s. 1.

5. W szczególności we wniosku wprowadzono klauzulę pomostową umożliwiającą taki dostęp na potrzeby ochrony porządku publicznego wraz z niezbędnymi przepisami towarzyszącymi oraz zmieniono wniosek z grudnia 2008 r. Został on przedstawiony jednocześnie z wnioskiem dotyczącym decyzji Rady w sprawie składania przez organy ścigania państw członkowskich oraz Europol wniosków o porównanie z danymi Eurodac na potrzeby ochrony porządku publicznego⁽¹⁾ (zwanej dalej „decyzją Rady”), określającym dokładnie tryby takiego dostępu. EIOD przedstawił opinię w sprawie tego wniosku w grudniu 2009 r.⁽²⁾
6. Wskutek wejścia w życie traktatu lizbońskiego oraz zniesienia systemu filarów wniosek dotyczący decyzji Rady stracił ważność; musiał on zostać formalnie wycofany i zastąpiony nowym wnioskiem, by uwzględnić nowe ramy TFUE.
7. W uzasadnieniu wniosku stwierdzono, że aby uzyskać postępy w negocjacjach dotyczących pakietu azylowego⁽³⁾ oraz ułatwić zawarcie porozumienia w sprawie rozporządzenia Eurodac, Komisja uznaje za właściwsze wycofanie z rozporządzenia Eurodac tych przepisów, które dotyczą dostępu do celów ochrony porządku publicznego.
8. Komisja jest zdania, że wycofanie tej (dość kontrowersyjnej) części wniosku i umożliwienie w ten sposób szybszego przyjęcia nowego rozporządzenia Eurodac ułatwi także szybkie ustanowienie agencji do spraw zarządzania operacyjnego wielkoskalowymi systemami informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, ponieważ planuje się, że agencja ta odpowiadać będzie także za zarządzanie systemem Eurodac.
9. Wskutek tego obecny zmieniony wniosek wprowadza dwa przepisy techniczne, jednak jego głównym celem jest zmiana poprzedniego wniosku (tzn. z września 2009 r.) poprzez skreślenie w nim wariantu dotyczącego dostępu do celów ochrony porządku publicznego. Dlatego też uznano, że nie ma potrzeby przeprowadzenia nowej oceny skutków na potrzeby niniejszego wniosku.

⁽¹⁾ COM(2009) 344.

⁽²⁾ Opinia Europejskiego Inspektora Ochrony Danych dotycząca zmienionego wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia systemu „Eurodac” do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (WE) nr (.../...) (ustanawiającego kryteria i mechanizmy ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca) oraz dotycząca wniosku w sprawie decyzji Rady w sprawie składania przez organy ścigania państw członkowskich oraz Europol wniosków o porównanie z danymi Eurodac na potrzeby ochrony porządku publicznego, Dz.U. C 92 z 10.4.2010, s. 1.

⁽³⁾ „Pakiet azylowy” ma na celu poprawę funkcjonowania unijnego systemu azylowego i wzmocnienie praw osób ubiegających się o azyl. Zawiera on poprawki do dyrektywy w sprawie warunków przyjmowania (RCD), rozporządzenia dublińskiego i Eurodac. Pakiet przewiduje także utworzenie Europejskiego Urzędu Wsparcia w dziedzinie Azylu (EASO), któremu towarzyszyć ma decyzja ułatwiająca finansowanie tego organu poprzez przesunięcie części środków przeznaczanych obecnie na Europejski Fundusz na rzecz Uchodźców.

II. CEL OPINII EIOD

10. Jak wspomniano powyżej, EIOD wydał już kilka opinii w tej sprawie. Celem niniejszej opinii jest przedstawienie zalecanych poprawek do wniosku, które oparte są na bieżących zmianach sytuacji lub też na wcześniejszych zaleceniach, których nie wzięto pod uwagę, lecz EIOD uznał, że jego argumenty nie spotkały się z dostatecznym zrozumieniem lub ma na ich poparcie nowe argumenty.
11. Niniejsza opinia koncentruje się na następujących kwestiach:
- wycofanie postanowień dotyczących dostępu wymiaru sprawiedliwości do systemu Eurodac,
 - sytuacja osoby, której odcisków palców nie można wykorzystać,
 - informacje o podmiocie danych,
 - wykorzystanie najlepszych dostępnych technik celem wdrożenia koncepcji „uwzględnienia ochrony prywatności w fazie projektowania”,
 - konsekwencje zlecenia podwykonawcom będącym osobami trzecimi (części) prac związanych z tworzeniem lub zarządzaniem systemem.

III. WYCOFANIE POSTANOWIEŃ DOTYCZĄCYCH DOSTĘPU WYMIARU SPRAWIEDLIWOŚCI

12. EIOD z zadowoleniem przyjmuje fakt, że możliwość udzielenia wymiarowi sprawiedliwości dostępu do systemu EURODAC została z bieżącego wniosku usunięta. Choć EIOD nie kwestionuje faktu, że rządy potrzebują odpowiednich narzędzi by zagwarantować obywatelom bezpieczeństwo, miał on wiele zastrzeżeń co do zasadności tego wniosku, opartych na poniższych kwestiach.
13. Działania mające na celu zwalczanie przestępstw o charakterze terrorystycznym i innych poważnych przestępstw mogą stanowić przesłankę uzasadniającą zgodę na przetwarzanie danych osobowych – nawet jeśli byłoby to niezgodne z celem, w jakim dane te były gromadzone – pod warunkiem jednak, że konieczność ta zostanie poparta jasnymi i niedającymi się podważyć argumentami oraz wykazana zostanie proporcjonalność ich przetwarzania. Jest to niezbędne tym bardziej, że wnioski dotyczą grupy szczególnie podatnej, wymagającej większej ochrony ze względu na to, iż osoby te uciekają przed prześladowaniami. Ich niepewna sytuacja musi zostać uwzględniona przy dokonywaniu oceny konieczności i proporcjonalności proponowanych działań. EIOD w sposób bardziej konkretny podkreślił, że konieczność musi zostać udowodniona poprzez wskazanie solidnych dowodów na istnienie powiązań pomiędzy osobą ubiegającą się o azyl a terroryzmem lub poważnym przestępstwem. Wnioski pomijają tę kwestię.

14. Na wyższym poziomie ogólności EIOD podkreśla potrzebę oceny wszystkich istniejących narzędzi wymiany informacji przed zaproponowaniem nowych w ramach licznych opinii i uwag, zwłaszcza w wydanej niedawno opinii zatytułowanej „Przegląd zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości”⁽¹⁾ oraz „Unijna polityka przeciwdziałania terroryzmowi: najważniejsze osiągnięcia i nadchodzące wyzwania”⁽²⁾.
15. Ocena skuteczności istniejących działań w kontekście wpływu nowych planowanych środków na prywatność jest kwestią zasadniczą, powinna też odgrywać istotną rolę w działaniach Unii Europejskiej w tej dziedzinie, zgodnie z podejściem postulowanym w ramach programu sztokholmskiego. W tym przypadku szczególną uwagę należy poświęcić na przykład wdrożeniu wymiany danych w ramach mechanizmu wprowadzonego na mocy konwencji z Prüm. W tym kontekście przewidywana jest wymiana odcisków palców, należy więc wspomnieć o poważnych niedociągnięciach systemu, co uzasadnia dostęp do takiej bazy danych jak np. Eurodac.
16. W bieżących opiniach, jak i w wielu wcześniejszych, EIOD zaleca zwrócenie szczególnej uwagi na wnioski, wskutek których powstają zbiory danych osobowych szerokich grup obywateli, nie tylko osób podejrzanych. Szczególnej rozważli i uzasadnienia wymagają te przypadki, w których przetwarzanie danych osobowych przewiduje się do celów innych niż te, w których dane zostały zebrane, jak choćby Eurodac.
17. Konkludując EIOD z zadowoleniem przyjmuje usunięcie tego elementu z bieżącego wniosku.

IV. SYTUACJA OSÓB NIEMOGĄCYCH DOKONAĆ WPISU DO SYSTEMU

18. Pobieranie i dalsze przetwarzanie odcisków palców zajmuje centralne miejsce w systemie Eurodac. Należy podkreślić, że przetwarzanie danych biometrycznych, takich jak odciski palców, wiąże się z określonymi wyzwaniami i stwarza pewne rodzaje ryzyka, wobec których należy podjąć działania. W kontekście wniosku EIOD pragnie szczególnie podkreślić problem tzw. „niepowodzenia rejestracji”, czyli sytuacji, w której znajduje się osoba, której odcisków palców z jakiegoś powodu nie można wykorzystać.
19. Niepowodzenie rejestracji może nastąpić, gdy dana osoba ma tymczasowo lub trwale zniszczone opuszki palców lub dłoń wskutek działania rozmaitych czynników, takich jak

choroba, niepełnosprawność, rany czy oparzenia. W niektórych przypadkach może się to wiązać z pochodzeniem etnicznym lub wykonywanym zawodem. Zwłaszcza duża liczba robotników rolnych i budowlanych ma odciski palców tak zniszczone, że nie są one czytelne. W innych przypadkach, których częstotliwość trudno jest ocenić, uchodźcy mogą dokonywać samookaleczenia celem uniknięcia pobrania odcisków palców.

20. EIOD przyznaje, że trudno jest odróżnić przypadki obywateli państw trzecich, którzy z własnej woli dokonali zniszczenia odcisków palców celem utrudnienia procesu ustalania ich tożsamości, od tych, których odciski palców są rzeczywiście nieczytelne.
21. Bardzo ważne jest jednak by zagwarantować, aby sam fakt niepowodzenia rejestracji nie prowadził do odmowy przyznania praw osobom ubiegającym się o azyl. Byłoby to nie do zaakceptowania, gdyby na przykład niepowodzenie rejestracji było interpretowane przez system jako próba oszustwa i prowadziło do odmowy rozpatrzenia wniosku o azyl lub nieudzielenie dalszej pomocy osobie starającej się o przyznanie azylu. Gdyby tak się stało, oznaczałoby to, że możliwość zdjęcia odcisków palców stanowi jedno z kryteriów ustalenia statusu osoby ubiegającej się o azyl. Celem systemu Eurodac jest ułatwienie stosowania postanowień konwencji dublińskiej, a nie ustanowienie dodatkowego kryterium („posiadanie odcisków palców, które można wykorzystać”) w ramach przyznawania statusu osoby ubiegającej się o azyl. Stanowiłoby to naruszenie zasady celowości, a przede wszystkim sprzeniewierzenie się idei prawa do azylu.
22. EIOD podkreśla również, że niniejszy wniosek powinien być zgodny z innymi odnośnymi dyrektywami. Zwłaszcza dyrektywa dotycząca kwalifikowania wymaga, aby każdy wniosek rozpatrywany był indywidualnie, i nie wspomina o tym, aby nieudany wpis do systemu miał stanowić jedno z kryteriów oceny⁽³⁾.
23. Bieżący wniosek częściowo obejmuje już kwestię niepowodzenia rejestracji w art. 6.1 i 6.2⁽⁴⁾.

⁽³⁾ Zob. zwłaszcza art. 4 ust. 3 dyrektywy Rady 2004/83/WE z dnia 29 kwietnia 2004 r. w sprawie minimalnych norm dla kwalifikacji i statusu obywateli państw trzecich lub bezpaństwowców jako uchodźców lub jako osoby, które z innych względów potrzebują międzynarodowej ochrony oraz zawartości przyznawanej ochrony, Dz.U. L 304 z 30.9.2004, s. 2.

⁽⁴⁾ „1. Jeżeli stan opuszków palców wnioskodawcy nie pozwala na pobranie odcisków palców o jakości gwarantującej właściwe porównanie na podstawie art. 18 niniejszego rozporządzenia, państwo członkowskie pochodzenia pobiera powtórnie jego odciski palców i przesyła je powtórnie jak najszybciej, lecz nie później niż 48 godzin po ich skutecznym pobraniu.”

„2. Na zasadzie odstępowania od ust. 1, jeżeli pobranie odcisków palców wnioskodawcy nie jest możliwe z powodu środków podjętych w celu zabezpieczenia zdrowia wnioskodawcy lub ochrony zdrowia publicznego, państwa członkowskie pobierają i przesyłają odciski palców wnioskodawcy jak najszybciej, lecz nie później niż 48 godzin po ustaniu tych powodów.”

⁽¹⁾ Opinia Europejskiego Inspektora Ochrony Danych z dnia 30 września 2010 r. w sprawie Komunikatu Komisji do Parlamentu Europejskiego i Rady – „Przegląd zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości”, dostępna na stronie internetowej EIOD.

⁽²⁾ Opinia Europejskiego Inspektora Ochrony Danych z dnia 24 listopada 2010 r. w sprawie Komunikatu Komisji do Parlamentu Europejskiego i Rady – „Unijna polityka przeciwdziałania terroryzmowi: najważniejsze osiągnięcia i nadchodzące wyzwania”, dostępna na stronie internetowej EIOD.

24. Postanowienia te jednak uwzględniają jedynie hipotezę o tymczasowym niepowodzeniu rejestracji, podczas gdy w znacznej liczbie przypadków niemożność dokonania wpisu do systemu będzie trwała. Artykuł 1 rozporządzenia zmieniającego wspólne instrukcje konsularne⁽¹⁾ przewiduje tego typu przypadki. Stanowi on, że: (...) Państwa członkowskie zapewniają wprowadzenie odpowiednich procedur gwarantujących poszanowanie godności osoby ubiegającej się o wizę w sytuacji, gdy wystąpią problemy z pobraniem danych. Fakt, że pobranie odcisków palców jest fizycznie niemożliwe, nie ma wpływu na przyznanie lub odmowę przyznania wizy.

25. Aby rozwiązać ten problem w kontekście systemu Eurodac, EIOD zaleca dodanie w art. 6 zapisu inspirowanego powyższym, który mógłby brzmieć następująco: „Czasowa lub trwała niemożność pobrania odcisków palców, które można wykorzystać, nie wpływa negatywnie na sytuację prawną danej osoby. W żadnym razie nie może to stanowić wystarczającej przesłanki do odmowy rozpatrzenia ani do odrzucenia wniosku o udzielenie azylu”.

V. PRAWO PODMIOTU DANYCH DO INFORMACJI

26. EIOD pragnie zwrócić uwagę, że skuteczna realizacja prawa do informacji jest kluczowa z punktu widzenia poprawnego funkcjonowania systemu Eurodac. Należy przede wszystkim zagwarantować, aby informacje udzielane były w taki sposób, by osoba ubiegająca się o azyl mogła w pełni zrozumieć swoją sytuację jak i prawa jej przysługujące, łącznie z krokami proceduralnymi, jakie może podjąć, gdy zostaną w jej sprawie wydane decyzje administracyjne. EIOD przypomina również, że prawo dostępu stanowi fundament ochrony danych, o którym mowa zwłaszcza w art. 8 Karty praw podstawowych Unii Europejskiej.

27. EIOD podkreślił tę kwestię w poprzedniej opinii dotyczącej systemu Eurodac. Ponieważ proponowana zmiana nie została przyjęta, EIOD pragnie podkreślić wagę tej kwestii.

28. Artykuł 24 wniosku brzmi:

Państwo członkowskie pochodzenia podaje osobie objętej zakresem niniejszego rozporządzenia na piśmie lub w odpowiednich przypadkach ustnie, w języku, który ta osoba rozumie lub co do którego można w uzasadniony sposób przypuszczać, że jest dla niej zrozumiałą następujące informacje:

(...)

⁽¹⁾ Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 390/2009 z dnia 23 kwietnia 2009 r. zmieniające wspólne instrukcje konsularne dla misji dyplomatycznych i urzędów konsularnych dotyczące wiz w związku z wprowadzeniem danych biometrycznych oraz zmieniające przepisy dotyczące systemu przyjmowania i przetwarzania wniosków wizowych, Dz.U. L 131 z 28.5.2009, s. 1.

e) o prawie do dostępu do danych dotyczących tej osoby oraz prawie do żądania poprawienia nieprawidłowych danych dotyczących tej osoby lub usunięcia danych dotyczących tej osoby przetwarzanych niezgodnie z prawem, a także prawie otrzymywania informacji o procedurach korzystania z tych praw, w tym o danych kontaktowych administratora danych oraz krajowych organów nadzorczych, o których mowa w art. 25 ust. 1.

29. EIOD proponuje zmianę brzmienia art. 24 celem objaśnienia praw przysługujących wnioskującemu. Proponowane brzmienie jest niejasne, gdyż może zostać zinterpretowane jako „prawo do otrzymywania informacji o procedurach korzystania z tych praw (...)” oprócz prawa dostępu do danych lub prawa do żądania poprawienia nieprawidłowych danych (...). Ponadto zgodnie z aktualnym brzmieniem wspomnianego zapisu, państwa członkowskie muszą informować osobę podlegającą rozporządzeniu nie o treści ich praw, lecz o ich „istnieniu”. Ponieważ to ostatnie zagadnienie wydaje się jedynie kwestią stylistyczną, EIOD sugeruje, aby art. 24 otrzymał następujące brzmienie: Państwo członkowskie pochodzenia podaje osobie objętej zakresem niniejszego rozporządzenia (...) informację o (...) g) prawie do dostępu do danych dotyczących tej osoby oraz do ich sprostowania oraz prawie do żądania poprawienia nieprawidłowych danych dotyczących tej osoby lub usunięcia danych dotyczących tej osoby przetwarzanych niezgodnie z prawem.

VI. NAJLEPSZE DOSTĘPNE TECHNIKI

30. Artykuł 4 ust. 1 wniosku mówi: Po okresie przejściowym odpowiedzialność za zarządzanie operacyjne systemem Eurodac spoczywać będzie na organie zarządzającym, finansowanym z budżetu ogólnego Unii Europejskiej. Organ zarządzający zapewnia, we współpracy z państwami członkowskimi, by w systemie centralnym stosowane były zawsze, gdy przemawiają za tym wyniki analizy kosztów i korzyści, najlepsze z dostępnych technologii. Choć EIOD z zadowoleniem przyjmuje wymóg ustanowiony na mocy art. 4 ust. 1, pragnie jednak podkreślić, że występujące we wspomnianym zapisie wyrażenie „najlepsze z dostępnych technologii” należy zastąpić sformułowaniem „najlepsze z dostępnych technik”, co obejmuje zarówno zastosowaną technologię, jak i sposób, w jaki instalacja jest zaprojektowana, zbudowana, utrzymywana i obsługiwana.

31. Kwestia ta jest istotna, ponieważ sformułowanie „najlepsze z dostępnych technik” jest szersze i obejmuje różne czynniki mające wkład w „uwzględnienie ochrony prywatności w fazie projektowania”, które uważane jest za kluczową zasadę w ramach przeglądu unijnych ram prawnych dotyczących ochrony danych. Podkreśla to, że ochronę danych można wdrażać w różny sposób, nie tylko za pomocą technologii. Ważne jest, aby badać nie tylko technologię, lecz również sposób, w jaki jest ona używana jako narzędzie do osiągnięcia celu, czyli przetwarzania danych na miejscu. Procesy biznesowe muszą być zorientowane na osiągnięcie tego celu, który przekłada się na procedury i struktury organizacyjne.

32. W tym celu i na bardziej ogólnym poziomie EIOD pragnie powtórzyć zalecenie zawarte we wcześniejszych opiniach⁽¹⁾ dotyczące konieczności, aby Komisja zdefiniowała i promowała wraz z zainteresowanymi przedstawicielami przemysłu „najlepsze z dostępnych technik” w oparciu o tę samą procedurę, jaka została zastosowana przez Komisję w dziedzinie ochrony środowiska⁽²⁾. „Najlepsze z dostępnych technik” oznaczałyby najskuteczniejszy i najbardziej zaawansowany etap rozwoju technologii oraz metody stosowania, które wskazują praktyczną przydatność poszczególnych technik z punktu widzenia zdefiniowanej granicy wykrywalności, zgodnie z unijnymi ramami ochrony prywatności i danych. „Najlepsze z dostępnych technik” będą zaprojektowane tak, by zapobiegać różnym rodzajom ryzyka związanego z bezpieczeństwem przetwarzania danych, gdy nie jest to możliwe – ograniczać ryzyko do odpowiedniego poziomu oraz w jak najwyższym stopniu minimalizować wpływ ryzyka na prywatność.
33. W procesie tym dostępne powinny być również dokumenty referencyjne dotyczące „najlepszych z dostępnych technik”, oferujące przydatne wytyczne co do zarządzania innymi unijnymi wielkoskalowymi systemami informatycznymi. Wpłynęłyby to również na zwiększenie harmonizacji tego typu działań w całej UE. Zdefiniowanie „najlepszych z dostępnych technik” sprzyjających prywatności i bezpieczeństwu ułatwiłoby także sprawowanie nadzoru organom ochrony danych, gdyż otrzymałyby one w ten sposób odniesienia techniczne zgodne z polityką prywatności i ochrony danych przyjęte przez administratorów danych.

VII. ZLECANIE PODWYKONAWSTWA

34. EIOD pragnie zauważyć, że Wniosek nie obejmuje kwestii zlecenia podwykonania części zadań Komisji⁽³⁾ innym organizacjom lub podmiotom (np. firmom prywatnym). Pomimo to zlecenie podwykonawstwa jest często wykorzystywane przez Komisję przy tworzeniu systemu i infrastruktury komunikacyjnej oraz zarządzaniu nimi. Choć zlecenie podwykonawstwa samo w sobie nie stoi w sprzeczności z wymogami ochrony danych, należy stworzyć istotne zabezpieczenia celem zagwarantowania, że podwykonawstwo nie będzie miało żadnego negatywnego wpływu na stosowanie rozporządzenia (WE) nr 45/2001, łącznie z nadzorowaniem ochrony danych przez EIOD. Należy ponadto wprowadzić dodatkowe zabezpieczenia o charakterze technicznym.
35. W tym względzie EIOD sugeruje, że zabezpieczenia podobne do istniejących w ramach instrumentów prawnych SIS II należałoby wprowadzić *mutatis mutandis* w ramach przeglądu rozporządzenia w sprawie Eurodac. Gdy Komisja zleca podwykonawstwo części swoich zadań

innemu organowi lub organizacji, musi ona zagwarantować inspektorowi prawo i możliwość pełnej realizacji jego zadań, w tym również przeprowadzenia kontroli na miejscu i skorzystania z wszelkich innych uprawnień nadanych mu na mocy art. 47 rozporządzenia (WE) nr 45/2001.

VIII. WNIOSKI

36. EIOD z zadowoleniem przyjmuje fakt, że Komisja pragnie się z nim skonsultować i prosi, aby w motywach wniosku odniesiono się do wspomnianych konsultacji.
37. EIOD z zadowoleniem przyjmuje fakt, że możliwość udzielenia wymiarowi sprawiedliwości dostępu do systemu Eurodac została z bieżącego wniosku usunięta.
38. Pobieranie i dalsze przetwarzanie odcisków palców zajmuje centralne miejsce w systemie Eurodac. EIOD podkreśla, że przetwarzanie danych biometrycznych, takich jak odciski palców, wiąże się z określonymi wyzwaniem i stwarza pewne rodzaje ryzyka, wobec których należy podjąć działania. EIOD pragnie zwłaszcza podkreślić problem tzw. nieudanego wpisu do systemu, czyli sytuacji, w której znajduje się osoba, której odcisków palców z jakiegoś powodu nie można wykorzystać. Sam fakt nieudanego wpisu do systemu nie powinien prowadzić do odmowy przyznania praw osobom ubiegającym się o azyl.
39. EIOD zaleca dodanie w art. 6a wniosku zapisu, który mógłby brzmieć następująco: „Czasowa lub trwała niemożność pobrania odcisków palców, które można wykorzystać, nie wpływa negatywnie na sytuację prawną danej osoby. W żadnym razie nie może to stanowić wystarczającej przesłanki do odmowy rozpatrzenia ani do odrzucenia wniosku o udzielenie azylu”.
40. EIOD stoi na stanowisku, że skuteczna realizacja prawa do informacji jest kwestią zasadniczą z punktu widzenia poprawnego funkcjonowania systemu Eurodac, należy więc zagwarantować, aby informacje udzielane były w taki sposób, by osoba ubiegająca się o azyl mogła w pełni zrozumieć swoją sytuację jak i prawa jej przysługujące, łącznie z krokami proceduralnymi, jakie może podjąć, gdy zostaną w jej sprawie podjęte decyzje administracyjne. EIOD proponuje zmianę brzmienia art. 24 wniosku celem objaśnienia praw przysługujących osobie wnioskującej o azyl.
41. EIOD zaleca zmianę art. 4 ust. 1 wniosku i użycie sformułowania „najlepsze z dostępnych technik” zamiast „najlepsze z dostępnych technologii”. Wyrażenie „najlepsze z dostępnych technik” obejmuje zarówno zastosowaną technologię, jak i sposób, w jaki instalacja jest zaprojektowana, zbudowana, utrzymywana i obsługiwana.

⁽¹⁾ Opinia EIOD dotycząca systemów transportu inteligentnego, lipiec 2009 r.; Opinia EIOD dotycząca komunikatu RFID, grudzień 2007 r.; Raport roczny EIOD z 2006 r., str. 48–49.

⁽²⁾ <http://eippcb.jrc.es/>

⁽³⁾ Lub w przyszłości organowi zarządzającemu, jak wspomniano powyżej. W tym ustępie odwołania do Komisji należy rozumieć jako odwołania do instytucji lub organu Unii, który pełni funkcję administratora danych Eurodac.

42. Co się tyczy zlecenia podwykonania części zadań Komisji innym organizacjom lub podmiotom (np. firmom prywatnym), EIOD zaleca stworzenie zabezpieczeń celem zagwarantowania, że podwykonawstwo nie będzie miało żadnego negatywnego wpływu na stosowanie rozporządzenia (WE) nr 45/2001, łącznie z nadzorowaniem ochrony danych przez EIOD. Należy ponadto wprowadzić dodatkowe zabezpieczenia o charakterze technicznym.

Sporządzono w Brukseli dnia 15 grudnia 2010 r.

Peter HUSTINX
Europejski Inspektor Ochrony Danych
