ISSN 1725-5228

Dziennik Urzędowy C 229
Unii Europejskiej

Wydanie polskie

Tom 52

23 września 2009

Informacje i zawiadomienia

Powiadomienie nr | Spis treści | Strona

PL

(Ciąg dalszy na następnej stronie)

PL

I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady 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) 820 wersja ostateczna)

(2009/C 229/01)

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 [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,

uwzględniając wniosek o wydanie opinii złożony zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 i otrzymany od Komisji w dniu 3 grudnia 2008 r.,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. **WPROWADZENIE**

Konsultacje z Europejskim Inspektorem Ochrony Danych

1. Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady 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" lub „wnioskiem Komisji") został przedłożony przez Komisję Europejskiemu Inspektorowi Ochrony Danych do konsultacji w dniu 3 grudnia 2008 r., zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001. O konsultacjach tych należy wyraźnie wspomnieć w preambule rozporządzenia.

2. Europejski Inspektor Ochrony Danych zgłaszał na wcześniejszych etapach uwagi do proponowanego rozporządzenia i wiele kwestii, które w sposób nieformalny poruszył w czasie procesu przygotowawczego, zostało przez Komisję uwzględnionych w ostatecznej wersji wniosku.

Kontekst wniosku

3. Omawiany wniosek stanowi przekształcenie rozporządzenia Rady (WE) nr 343/2003/WE z dnia 18 lutego 2003 r. ustanawiającego kryteria i mechanizmy określania państwa członkowskiego właściwego dla rozpatrywania wniosku o azyl, wniesionego w jednym z państw członkowskich przez obywatela państwa trzeciego [3] (zwanego dalej „rozporządzeniem dublińskim"). Został on przedstawiony przez Komisję jako część pierwszego pakietu wniosków mających na celu zwiększenie harmonizacji w tej dziedzinie i wprowadzenie lepszych standardów ochrony dla celów wspólnego europejskiego systemu azylowego, do czego zachęca program haski z 4–5 listopada 2004 r. i co zostało ogłoszone w planie polityki azylowej Komisji z dnia 17 czerwca 2008 r. W programie haskim zachęca się Komisję do przeprowadzenia oceny instrumentów prawnych pierwszego etapu i przedstawienia Radzie i Parlamentowi Europejskiemu instrumentów i środków drugiego etapu do przyjęcia przed rokiem 2010.

[1] Dz.U. L 281 z 23.11.1995, s. 31.
[2] Dz.U. L 8 z 12.1.2001, s. 1.
[3] Dz.U. L 50 z 25.2.2003, s. 1.

4. Wniosek był przedmiotem gruntownych ocen i konsultacji. Uwzględnia on w szczególności wyniki sprawozdania Komisji z oceny systemu dublińskiego, które zostało przedstawione w dniu 6 czerwca 2007 r. ([1]) i w którym opisano szereg problemów natury praktycznej i prawnej występujących w aktualnym systemie, a także zawarto uwagi przedstawione Komisji przez poszczególne podmioty zainteresowane strony w odpowiedzi na zieloną księgę w sprawie przyszłości wspólnego europejskiego systemu azylowego ([2]).

5. Głównym celem wniosku jest poprawa wydajności systemu dublińskiego i zapewnienie lepszych standardów ochrony przyznawanej osobom występującym o międzynarodową ochronę zgodnie z procedurą dublińską. Ponadto ma on zwiększyć solidarność z tymi państwami członkowskimi, które spotykają się ze szczególną presją migracyjną ([3]).

6. Wniosek rozszerza zakres zastosowania rozporządzenia na osoby występujące o ochronę uzupełniającą (lub korzystające z takiej ochrony). Zmiana ta jest konieczna do zapewnienia spójności ze wspólnotowym dorobkiem prawnym, a w szczególności z dyrektywą 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 ([4]) (zwaną dalej „dyrektywą kwalifikacyjną"), w której to dyrektywie wprowadzono pojęcie ochrony uzupełniającej. Dodatkowo we wniosku uzgodniono terminologię i definicje zastosowane w rozporządzeniu dublińskim z terminami zawartymi w pozostałych aktach prawnych dotyczących azylu.

7. Z myślą o poprawie wydajności systemu we wniosku określono w szczególności termin składania wniosków o wtórne przyjęcie i skrócono termin udzielania odpowiedzi na wnioski o udzielenie informacji. We wniosku zawarto również bardziej precyzyjne klauzule wygaśnięcia odpowiedzialności oraz dokładniej opisano okoliczności i procedury dotyczące stosowania klauzul dyskrecjonalnych (klauzula humanitarna i klauzula suwerenności). We wniosku dodano również przepisy dotyczące przekazywania i rozszerzono aktualny mechanizm rozstrzygania sporów. Wniosek zawiera również przepis dotyczący organizowania obowiązkowych rozmów.

8. Ponadto, między innymi w celu zwiększenia poziomu ochrony przyznanej wnioskodawcom, wniosek Komisji przewiduje prawo odwołania się od decyzji o przekazaniu jak również zobowiązuje właściwe organy do rozstrzygania, czy wykonanie takiej decyzji należy zawiesić. Porusza on kwestię prawa do pomocy lub reprezentacji prawnej oraz do pomocy językowej. Wniosek odwołuje się także do zasady, zgodnie z którą nikt nie powinien być zatrzymany tylko dlatego, że ubiega się o ochronę międzynarodową. Rozszerza też prawo łączenia rodzin i wychodzi naprzeciw potrzebom nieletnich pozbawionych opieki i innych grup znajdujących się w szczególnie trudnej sytuacji.

Zakres opinii

9. Niniejsza opinia ma na celu głównie przeanalizowanie tych zmian w tekście, które są najważniejsze z punktu widzenia ochrony danych osobowych, a mianowicie:

— przepisów mających na celu usprawnienie wykonywania prawa do informacji, tj. zmian polegających na doprecyzowaniu treści i formy informacji oraz terminów ich przekazywania, a także zaproponowano przyjęcie wspólnej ulotki informacyjnej,

— nowego mechanizmu dzielenia się przez państwa członkowskie istotnymi informacjami przed przeprowadzeniem przekazania,

— wykorzystania bezpiecznego kanału łączności sieci DubliNet do wymiany informacji.

II. UWAGI OGÓLNE

10. Europejski Inspektor Ochrony Danych popiera cele wniosku Komisji, w szczególności te dotyczące poprawy wydajności systemu dublińskiego i zapewnienia lepszych standardów ochrony przyznawanej osobom występującym o ochronę międzynarodową zgodnie z procedurą dublińską. Rozumie także powody, dla których Komisja postanowiła przystąpić do modyfikacji systemu dublińskiego.

11. Wprowadzenie odpowiedniego poziomu ochrony danych osobowych jest warunkiem koniecznym do zapewnienia skutecznego wykonania i wysokiego poziomu ochrony innych praw podstawowych. Europejski Inspektor Ochrony Danych wydając niniejszą opinię jest w pełni świadomy, że istotnym elementem wniosku jest ochrona praw podstawowych, co dotyczy nie tylko przetwarzania danych osobowych, ale także wielu innych praw obywateli państw trzecich lub bezpaństwowców, w szczególności takich jak prawo do azylu, prawo do informacji w ogólnym rozumieniu tego pojęcia, prawo do łączenia rodzin, prawo do skutecznego środka prawnego, prawo do wolności i swoboda przemieszczania się, prawa dziecka lub prawa nieletnich pozbawionych opieki.

12. Zarówno w motywie 34. wniosku, jak i w uzasadnieniu podkreśla się działania podejmowane przez prawodawcę w celu zapewnienia zgodności wniosku z Kartą praw podstawowych. W tym kontekście uzasadnienie odnosi się w sposób wyraźny do ochrony danych osobowych i prawa do azylu. W uzasadnieniu podkreśla się również, że wniosek został złożony po gruntownej analizie, która miała wykazać, czy jego przepisy są w pełni zgodne z prawami podstawowymi jako ogólnymi zasadami prawa wspólnotowego i międzynarodowego. Z uwagi na zakres kompetencji Europejskiego Inspektora Ochrony Danych niniejsza opinia skupiać się będzie jednak głównie na aspektach wniosku dotyczących ochrony danych. Europejski Inspektor Ochrony Danych z zadowoleniem odnotowuje zatem, że temu prawu podstawowemu poświęca się we wniosku dużo uwagi i przypomina, że jest to niezbędne do zapewnienia sprawnego działania procedury dublińskiej przy pełnym poszanowaniu wymogów dotyczących praw podstawowych.

([1]) COM(2007) 299.
([2]) COM(2007) 301.
([3]) Zob. uzasadnienie wniosku.
([4]) Dz.U. L 304 z 30.9.2004, s. 12.

13. Europejski Inspektor Ochrony Danych zauważa też, że Komisja starała się, aby jej wniosek był spójny z innymi instrumentami prawnymi regulującymi tworzenie lub użytkowanie innych dużych systemów informatycznych. W szczególności Inspektor pragnie podkreślić, że zarówno podział obowiązków dotyczących bazy danych, jak i sposób określenia modelu nadzoru we wniosku zgodne są z ramami systemu informacyjnego Schengen drugiej generacji oraz wizowego systemu informacyjnego.

14. Europejski Inspektor Ochrony Danych z zadowoleniem odnotowuje, że jego rola w dziedzinie nadzoru została wyraźnie określona, czego z oczywistych względów brakowało w poprzedniej wersji tekstu.

III. **PRAWO DO INFORMACJI**

15. Artykuł 4 ust. 1 lit. f)–g) wniosku stanowi:

> Niezwłocznie po złożeniu przez osobę ubiegającą się o azyl wniosku o udzielenie ochrony procedury międzynarodowej, właściwe organy państwa członkowskiego informują ją o stosowaniu niniejszego rozporządzenia, a w szczególności o:
>
> f) „fakcie, że właściwe organy mogą wymieniać dane na jej temat, wyłącznie w celu wypełnienia zobowiązań wynikających z niniejszego rozporządzenia;
>
> g) istnieniu prawa dostępu do danych jej dotyczących oraz prawa do żądania poprawienia nieprawidłowych danych jej dotyczących lub usunięcia danych jej dotyczących przetwarzanych niezgodnie z prawem, w tym prawa do otrzymania informacji o procedurach służących wykonaniu tych praw oraz danych kontaktowych krajowych organów ochrony danych rozpatrujących skargi dotyczące ochrony danych osobowych."
>
> W art. 4 ust. 2 opisane są metody dostarczania wnioskodawcy informacji, o których mowa w ust. 1 tego przepisu.

16. Skuteczne wykonywanie prawa do informacji niezbędne jest do właściwego funkcjonowania procedury dublińskiej. W szczególności konieczne jest dostarczanie informacji w taki sposób, aby osoba ubiegająca się o azyl w pełni rozumiała swoją sytuację oraz przysługujące jej prawa, w tym procedury, z których może skorzystać w odpowiedzi na decyzje administracyjne podjęte w jej sprawie.

17. Jeśli chodzi o aspekty praktyczne wykonywania tego prawa, Europejski Inspektor Danych Osobowych pragnie przypomnieć, że zgodnie z art. 4 ust. 1 lit. g) i ust. 2 wniosku państwa członkowskie powinny stosować wspólną ulotkę dla wnioskodawców, która powinna zawierać m.in. „dane kontaktowe krajowych organów ochrony danych właściwych do rozpatrywania skarg dotyczących ochrony danych osobowych". W związku z tym Europejski Inspektor Ochrony Danych pragnie podkreślić, że chociaż krajowe organy ochrony danych, wymienione w art. 4 ust. 2 wniosku, są faktycznie organami właściwymi do rozpatrywania skarg dotyczących ochrony danych osobowych, to wniosek powinien być sformułowany tak, aby wnioskodawca (*osoba, której dane dotyczą*) miał możliwość skierowania wniosku przede wszystkim do administratora danych (w tym przypadku są to właściwe organy krajowe odpowiedzialne za współpracę dublińską). Treść art. 4 ust. 2 w obecnej formie zdaje się sugerować, że wnioskodawca powinien swój wniosek przedkładać – bezpośrednio i w każdym przypadku – krajowemu organowi ochrony danych, chociaż zgodnie ze standardowymi procedurami i praktykami przyjętymi w państwach członkowskich wnioskodawca składa skargę najpierw u administratora danych.

18. Europejski Inspektor Ochrony Danych zaleca także zmianę brzmienia art. 4 ust. 1 lit. g), tak aby doprecyzować, jakie prawa przyznane będą wnioskodawcy. Tekst w proponowanej wersji jest niejasny, ponieważ możliwa jest interpretacja, zgodnie z którą „prawo do otrzymywania informacji o procedurach służących wykonaniu tych praw (…)" jest we wniosku uznawane za część prawa dostępu do danych lub prawa do żądania poprawienia nieprawidłowych danych (…). Ponadto w obecnej wersji powyższego przepisu państwa członkowskie mają informować wnioskodawcę nie o treści jego praw, ale o ich „istnieniu". Ponieważ wydaje się, że ten drugi problem jest kwestią stylu, Europejski Inspektor Ochrony Danych zaleca, aby nadać art. 4 ust. 1 lit. g) następujące brzmienie:

> „Niezwłocznie po złożeniu przez osobę ubiegającą się o azyl wniosku o udzielenie ochrony międzynarodowej, właściwe organy państwa członkowskiego informują ją o (…):
>
> g) prawie dostępu do dotyczących jej danych oraz prawie do żądania poprawienia nieprawidłowych danych jej dotyczących lub usunięcia danych jej dotyczących przetworzonych niezgodnie z prawem, jak również procedurach służących wykonywaniu tych praw, co obejmuje również dane kontaktowe organów, o których mowa w art. 33 niniejszego rozporządzenia, oraz krajowych organów ochrony danych."

19. Jeśli chodzi o metody dostarczania informacji wnioskodawcom, Europejski Inspektor Ochrony Danych wskazuje na działania podejmowane przez grupę ds. koordynowania nadzoru nad systemem Eurodac [1] (w skład której wchodzą przedstawiciele organów ochrony danych każdego z uczestniczących państw oraz Europejski Inspektor Ochrony Danych). Grupa aktualnie analizuje tę kwestię w ramach systemu Eurodac w celu zaproponowania właściwych wskazówek, kiedy tylko zostaną opracowane i udostępnione wyniki krajowych postępowań wyjaśniających. Chociaż takie skoordynowane postępowanie wyjaśniające dotyczy w szczególności systemu Eurodac, wnioski z niego najprawdopodobniej będą też interesujące z punktu widzenia procedury dublińskiej, ponieważ dotyczą takich kwestii, jak języki/tłumaczenia oraz ocena faktycznego zrozumienia informacji przez osobę ubiegającą się o azyl itd.

[1] Wyjaśnienie dotyczące działań i statusu tej grupy dostępne jest pod następującym adresem: http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/79. Grupa zajmuje się skoordynowanym nadzorem systemu Eurodac. Z punktu widzenia ochrony danych jej prace będą jednak miały też ogólny wpływ na wymianę informacji w systemie dublińskim. Informacje te odnoszą się do tej samej osoby, której dane dotyczą i wymieniane są w ramach tej samej procedury z nią związanej.

IV. **PRZEJRZYSTOŚĆ**

20. Jeśli chodzi o organy, o których mowa w art. 33 wniosku, Europejski Inspektor Ochrony Danych z zadowoleniem odnotowuje, że Komisja opublikuje w *Dzienniku Urzędowym Unii Europejskiej* kompletny wykaz organów wymienionych w ust. 1 wymienionego wyżej przepisu. W przypadku pojawienia się zmian w tym wykazie Komisja będzie co roku publikować jego zaktualizowaną, kompletną wersję. Publikowanie kompletnego wykazu pomoże w utrzymaniu przejrzystości i ułatwi organom ochrony danych czynności nadzoru.

V. **NOWY MECHANIZM WYMIANY INFORMACJI**

21. Europejski Inspektor Ochrony Danych zwraca uwagę na wprowadzenie nowego mechanizmu wymiany istotnych informacji między państwami członkowskimi przed przeprowadzeniem przekazania (ustanowionego w art. 30 wniosku). Uznaje on, że taka wymiana informacji jest uzasadniona.

22. Europejski Inspektor Ochrony Danych zwraca także uwagę, że we wniosku przewidziano szczegółowe zabezpieczenia ochrony danych – zgodnie z art. 8 ust. 1–3 dyrektywy 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych – takie jak: a) wyraźna zgoda wnioskodawcy lub jego przedstawiciela, b) natychmiastowe usunięcie danych przez przekazujące państwo członkowskie po zakończeniu przekazania oraz c) „Przetwarzanie danych osobowych dotyczących zdrowia przeprowadzane jest wyłącznie przez pracowników służby zdrowia zobowiązanych do zachowania tajemnicy zawodowej na mocy przepisów krajowych lub reguł ustanowionych przez właściwe organy krajowe lub inną osobę, na której spoczywa równorzędny obowiązek zachowania tajemnicy." (posiadające odpowiednie przeszkolenie medyczne). Uznaje on również za słuszne to, że wymiana będzie prowadzona wyłącznie za pośrednictwem bezpiecznego systemu DubliNet i że właściwe organy będą powiadamiane z wyprzedzeniem.

23. Wybór struktury tego mechanizmu ma kluczowe znaczenie dla zapewnienia jego zgodności z systemem ochrony danych, w szczególności ze względu na to, że wymiana informacji dotyczyć będzie również szczególnie chronionych danych osobowych, na przykład informacji o „na temat szczególnych potrzeb wnioskodawcy, który ma zostać przekazany, które w określonych przypadkach obejmować mogą informacje na temat stanu zdrowia fizycznego i psychicznego wnioskodawcy, który ma zostać przekazany". W związku z tym Europejski Inspektor Ochrony Danych w pełni popiera umieszczenie we wniosku art. 36, który zobowiązuje państwa członkowskie do podejmowania niezbędnych kroków, tak aby wszystkie przypadki niewłaściwego korzystania z danych (…) podlegały sankcjom, w tym karom administracyjnym lub sankcjom karnym, zgodnie z przepisami prawa krajowego.

VI. **REGULACJA WYMIANY INFORMACJI W RAMACH SYSTEMU DUBLIŃSKIEGO**

24. Artykuł 32 wniosku Komisji reguluje *dzielenie się informacjami*. Europejski Inspektor Ochrony Danych zgłaszał wcześniej uwagi do tego przepisu i aprobuje jego treść w wersji aktualnie zaproponowanej przez Komisję.

25. Europejski Inspektor Ochrony Danych podkreśla, że ważne jest, aby organy państw członkowskich prowadziły wymianę danych osobowych za pomocą sieci DubliNet. Pozwala to nie tylko na zapewnienie lepszej ochrony, ale również umożliwia lepszą identyfikowalność transakcji. W związku z tym Europejski Inspektor Ochrony Danych wskazuje na dokument roboczy służb Komisji z dnia 6 czerwca 2007 r. „Dokument uzupełniający do sprawozdania Komisji do Parlamentu Europejskiego i Rady z oceny systemu dublińskiego", ([1]) w którym Komisja przypomina, że „stosowanie DubliNet jest zawsze obowiązkowe, z wyjątkiem przypadków określonych w art. 15 ust. 1 akapit drugi" rozporządzenia Komisji (WE) nr 1560/2003 z dnia 2 września 2003 r. ustanawiającego szczegółowe zasady stosowania rozporządzenia Rady (WE) nr 343/2003 ustanawiającego kryteria i mechanizmy określania państwa członkowskiego właściwego dla rozpatrywania wniosku o azyl, złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego ([2]) (zwanego dalej „dublińskim rozporządzeniem wykonawczym"). Europejski Inspektor Ochrony Danych obstaje przy stanowisku, że możliwość dopuszczenia odstępstw od stosowania systemu DubliNet, o której mowa w wyżej wymienionym art. 15 ust. 1, powinna być interpretowana w sposób zawężający.

26. Niektóre przepisy wniosku zostały właśnie w tym celu dodane lub zmienione, co Europejski Inspektor Ochrony Danych przyjmuje z zadowoleniem. Na przykład nowy art. 33 ust. 4 wniosku został przeformułowany tak, aby uściślić, że nie tylko wnioski, ale również odpowiedzi i cała korespondencja będzie podlegać przepisom dotyczącym ustanawiania bezpiecznych kanałów łączności elektronicznej (o których mowa w art. 15 ust. 1 dublińskiego rozporządzenia wykonawczego). Ponadto usunięcie ust. 2 w nowym art. 38, którego poprzednia wersja (art. 25) zobowiązywała państwa członkowskie do wysyłania wniosków i odpowiedzi „metodą, która zapewnia otrzymanie dowodu odbioru" ma na celu doprecyzowanie, że państwa członkowskie również i w tym zakresie powinny stosować DubliNet.

27. Europejski Inspektor Ochrony Danych zauważa, że jeśli chodzi o wymianę danych osobowych w ramach systemu dublińskiego wprowadzono relatywnie niewiele uregulowań. Chociaż niektóre aspekty wymiany zostały już poruszone w dublińskim rozporządzeniu wykonawczym, aktualne rozporządzenie nie obejmuje niestety, jak się wydaje, wszystkich aspektów wymiany danych osobowych ([3]).

28. W związku z tym należy wspomnieć, że kwestia wymiany informacji dotyczących osób ubiegających się o azyl była również omawiana na forum grupy ds. koordynowania nadzoru nad systemem Eurodac. Europejski Inspektor Ochrony Danych nie chce uprzedzać wyników prac grupy, jednak już teraz pragnie wspomnieć, że jednym z możliwych zaleceń mogłoby być przyjęcie zbioru przepisów podobnych do tych wprowadzonych w podręczniku Sirene Schengen.

([1]) SEC(2007) 742.
([2]) Dz.U. L 222 z 5.9.2003, s. 3.
([3]) Staje się to jeszcze bardziej widoczne przy porównaniu z zakresem, w jakim informacje uzupełniające zostały uregulowane w ramach systemu informacyjnego Schengen (SIRENE).

VII. **WNIOSKI**

29. Europejski Inspektor Ochrony Danych popiera wniosek Komisji w sprawie rozporządzenia 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. Rozumie on powody, dla których modyfikowany jest obecny system.

30. Europejski Inspektor Ochrony Danych z zadowoleniem odnotowuje, że wniosek Komisji jest spójny z innymi instrumentami prawnymi tworzącymi złożone ramy prawne w tym zakresie.

31. Europejski Inspektor Ochrony Danych jest również zadowolony, że we wniosku poświęcono dużo uwagi prawom podstawowym, w szczególności ochronie danych osobowych. Uznaje on takie podejście za ważny warunek udoskonalenia procedury dublińskiej. Szczególną uwagę prawodawców zwraca on na nowe mechanizmy wymiany danych, które będą stosowane m.in. w przypadku szczególnie chronionych danych osobowych osób ubiegających się o azyl.

32. Europejski Inspektor Ochrony Danych pragnie również zwrócić uwagę na istotne prace wykonane w tej dziedzinie przez grupę ds. koordynowania nadzoru nad systemem Eurodac i uważa, że wyniki prac grupy mogą być bardzo przydatne w lepszym określeniu elementów systemu.

33. Europejski Inspektor Ochrony Danych uznaje, że niektóre spośród obserwacji zawartych w niniejszej opinii mogą zostać rozwinięte po praktycznym wdrożeniu zmodyfikowanego systemu. W szczególności zamierza on zgłosić uwagi do określenia środków wykonawczych dotyczących wymiany informacji za pośrednictwem sieci DubliNet, jak wspomniano w art. 24–27 niniejszej opinii.

Sporządzono w Brukseli dnia 18 lutego 2009 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych

Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku na temat rozporządzenia Parlamentu Europejskiego i Rady 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)

(2009/C 229/02)

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 ([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,

uwzględniając wniosek o wydanie opinii złożony zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 i otrzymany od Komisji w dniu 3 grudnia 2008 r.,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. WPROWADZENIE

Konsultacje z Europejskim Inspektorem Ochrony Danych

1. Wniosek w sprawie rozporządzenia Parlamentu Europejskiego i Rady 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] (zwany dalej „wnioskiem" lub „wnioskiem Komisji") został w dniu 3 grudnia 2008 r. przekazany przez Komisję Europejskiemu Inspektorowi Ochrony Danych do konsultacji, zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001. O konsultacjach tych należy wyraźnie wspomnieć w preambule rozporządzenia.

2. Jak wspomniano w uzasadnieniu, Europejski Inspektor Ochrony Danych zgłaszał na wcześniejszych etapach uwagi do przedmiotowego wniosku i wiele z jego nieformalnych komentarzy zostało uwzględnionych w ostatecznej wersji wniosku Komisji.

Kontekst wniosku

3. Rozporządzenie Rady nr 2725/2000/WE ([3]) z dnia 11 grudnia 2000 r. dotyczące ustanowienia systemu Eurodac (zwane dalej „rozporządzeniem Eurodac") weszło w życie w dniu 15 grudnia 2000 r. Eurodac, ogólnowspólnotowy system informatyczny, został stworzony w celu ułatwienia stosowania konwencji dublińskiej, która miała na celu ustanowienie przejrzystego i sprawnego mechanizmu określania odpowiedzialności za wnioski o azyl składane w jednym z państw członkowskich. Konwencja dublińska została następnie zastąpiona wspólnotowym aktem prawnym – rozporządzeniem Rady (WE) nr 343/2003 z dnia 18 lutego 2003 r. ustanawiającym kryteria i mechanizmy określania państwa członkowskiego właściwego dla rozpatrywania wniosku o azyl, wniesionego w jednym z państw członkowskich przez obywatela państwa trzeciego ([4]) (zwanego dalej „rozporządzeniem dublińskim") ([5]). Eurodac zaczął działać w dniu 15 stycznia 2003 r.

4. Wniosek stanowi zmianę rozporządzenia Eurodac i jego rozporządzenia wykonawczego, którym jest rozporządzenie Rady nr 407/2002/WE; ma on na celu między innymi:

   — usprawnienie dotyczące stosowania rozporządzenia Eurodac,

   — zapewnienie spójności ze wspólnotowym dorobkiem prawnym dotyczącym azylu powstałym od czasu przyjęcia wyżej wymienionego rozporządzenia,

   — aktualizację szeregu przepisów z uwzględnieniem zmian stanu faktycznego, do których doszło od czasu przyjęcia rozporządzenia,

   — ustanowienie nowych ram dotyczących zarządzania.

5. Należy również podkreślić, że jednym z głównych celów wniosku jest zapewnienie pełniejszego poszanowania praw podstawowych, a w szczególności ochrony danych osobowych. Niniejsza opinia ma na celu przeanalizowanie, czy przepisy zawarte w przedmiotowym wniosku odpowiednio wypełniają ten cel.

([1]) Dz.U. L 281 z 23.11.1995, s. 31.
([2]) Dz.U. L 8 z 12.1.2001, s. 1.
([3]) Dz.U. L 316 z 15.12.2000, s. 1.
([4]) Dz.U. L 50 z 25.2.2003, s. 1.
([5]) Rozporządzenie dublińskie jest obecnie również przedmiotem zmian (COM(2008) 820 wersja ostateczna), 3.12.2008 (przekształcenie). Europejski Inspektor Ochrony Danych wydał również opinię dotyczącą wniosku dublińskiego.

6. Wniosek uwzględnia wyniki sprawozdania Komisji z oceny systemu dublińskiego z czerwca 2007 r. (zwanego dalej „sprawozdaniem z oceny"), która dotyczy pierwszych 3 lat funkcjonowania Eurodac C (lata 2003–2005).

7. W sprawozdaniu z oceny Komisja uznała, że system ustanowiony rozporządzeniem został w państwach członkowskich wdrożony w sposób na ogół zadowalający, jednak wskazała także na pewne problemy dotyczące wydajności aktualnych przepisów i określiła kwestie, które należy rozwiązać w celu usprawnienia systemu Eurodac i ułatwienia stosowania rozporządzenia dublińskiego. W sprawozdaniu w szczególności odnotowano, że niektóre państwa członkowskie nadal przekazują odciski palców z opóźnieniem. Rozporządzenie Eurodac przewiduje obecnie jedynie bardzo nieprecyzyjny termin przesyłania odcisków palców, co w praktyce może prowadzić do znacznych opóźnień. Kwestia ta ma kluczowe znaczenie dla skuteczności systemu, ponieważ zwłoka w przekazywaniu może powodować rezultaty sprzeczne z zasadami ustalania odpowiedzialności ustanowionymi w rozporządzeniu dublińskim.

8. W sprawozdaniu z oceny podkreślono też, że brak wydajnej metody pozwalającej państwom członkowskim wymieniać informacje na temat statusu osób ubiegających się o azyl prowadził wielokrotnie do nieefektywnego zarządzania procesem usuwania danych. Państwa członkowskie, które wprowadzają dane dotyczące konkretnych osób są często nieświadome faktu, że inne państwo członkowskie pochodzenia skasowało takie dane i dlatego nie zdają sobie sprawy, że powinny usunąć także swoje dane dotyczące tych osób. W rezultacie nie można w dostatecznym stopniu zapewnić przestrzegania zasady stanowiącej, że „żadne dane nie powinny być przechowywane w formie umożliwiającej identyfikację osób, których dane te dotyczą, przez okres dłuższy niż ten potrzebny do celów, do jakich dane zostały zgromadzone".

9. Ponadto, zgodnie z analizą zawartą w sprawozdaniu z oceny, brak jasnego określenia krajowych organów mających dostęp do systemu Eurodac utrudnia Komisji i Europejskiemu Inspektorowi Ochrony Danych pełnienie powierzonej im roli polegającej na monitorowaniu.

Zakres opinii

10. Z uwagi na swą aktualną rolę organu nadzorczego w stosunku do Eurodac, Europejski Inspektor Ochrony Danych jest szczególnie zainteresowany wnioskiem Komisji i pozytywnym wynikiem modyfikacji całego systemu Eurodac.

11. Europejski Inspektor Ochrony Danych zauważa, że wniosek obejmuje różne aspekty dotyczące praw podstawowych osób ubiegających się o azyl, takie jak prawo do azylu, prawo do informacji w szerokim rozumieniu tego pojęcia czy prawo do ochrony danych osobowych. Z uwagi na misję Europejskiego Inspektora Ochrony Danych niniejsza opinia skupia się głównie na poruszanych w zmienianym rozporządzeniu kwestiach, które związane są z ochroną danych. W tym kontekście Europejski Inspektor Ochrony Danych z zadowoleniem odnotowuje fakt, że we wniosku dużo uwagi poświęcono poszanowaniu i ochronie danych osobowych. Korzystając z okazji, Inspektor pragnie podkreślić, że zapewnienie wysokiego poziomu ochrony danych osobowych i sprawniejsze zastosowanie takiej ochrony w praktyce powinno być traktowane jako warunek wstępny niezbędny dla poprawy funkcjonowania systemu Eurodac.

12. Niniejsza opinia dotyczy przede wszystkich następujących zmian brzmienia, ponieważ są one najbardziej istotne z punktu widzenia ochrony danych osobowych:

— nadzór ze strony Europejskiego Inspektora Ochrony Danych, łącznie z przypadkami, w których zarządzanie systemem powierza się częściowo innemu podmiotowi (na przykład spółce prywatnej),

— procedura pobierania odcisków palców, łącznie z określeniem granic wieku,

— prawa osoby, której dane dotyczą.

II. **UWAGI OGÓLNE**

13. Europejski Inspektor Ochrony Danych z zadowoleniem odnotowuje, że autorzy wniosku starali się zachować spójność z innymi instrumentami prawnymi regulującymi tworzenie lub wykorzystywanie innych obszernych systemów informatycznych. W szczególności podział odpowiedzialności w zakresie bazy danych oraz sposób określenia modelu nadzoru we wniosku są spójne z instrumentami prawnymi ustanawiającymi system informacyjny Schengen II (SIS II) oraz wizowy system informacyjny (VIS).

14. Europejski Inspektor Ochrony Danych zauważa też spójność wniosku z dyrektywą 95/46/WE i rozporządzeniem (WE) nr 45/2001. W związku z tym Europejski Inspektor Ochrony Danych przyjmuje z zadowoleniem w szczególności nowe motywy 17, 18 i 19, które stanowią, że na mocy proponowanego rozporządzenia dyrektywa 95/46/WE i rozporządzenie (WE) nr 45/2001 mają zastosowanie do przetwarzania danych osobowych – odpowiednio – przez państwa członkowskie i przez odnośne instytucje i organy wspólnotowe.

15. Ponadto, Europejski Inspektor Ochrony Danych zwraca uwagę na potrzebę doprowadzenia do pełnej spójności między rozporządzeniem Eurodac i rozporządzeniem dublińskim i korzystając z okazji pragnie w niniejszej opinii przedstawić bardziej szczegółowe wskazówki dotyczące takiej zgodności. Zauważa on jednak, że w niektórych aspektach kwestia ta została już we wniosku uwzględniona, np. w uzasadnieniu, w którym wspomina się, że: „potrzeba zapewnienia spójności z rozporządzeniem dublińskim (oraz uwzględnienia problemów związanych z ochroną danych, w szczególności dotyczących przestrzegania zasady proporcjonalności) zostanie zaspokojona przez uzgodnienie okresu przechowywania danych na temat obywateli krajów trzecich oraz bezpaństwowców, od których pobrano odciski palców w związku z nielegalnym przekroczeniem granicy zewnętrznej, z okresem przez który, zgodnie z art. 14 ust. 1 rozporządzenia dublińskiego, państwo członkowskie pozostaje odpowiedzialne na podstawie tej informacji (tzn. okresem jednego roku)".

III. UWAGI SZCZEGÓŁOWE

III.1. Nadzór ze strony Europejskiego Inspektora Ochrony Danych

16. Europejski Inspektor Ochrony Danych z zadowoleniem przyjmuje model nadzoru ustanowiony we wniosku, jak również konkretne zadania, które zostały mu przydzielone na mocy art. 25 i 26 wniosku. Artykuł 25 powierza Europejskiemu Inspektorowi Ochrony Danych dwa zadania z zakresu nadzoru:

— „sprawdzanie, czy działania organu zarządzającego związane z przetwarzaniem danych osobowych przeprowadzane są zgodnie z niniejszym rozporządzeniem" (art. 25 ust. 1), oraz

— „zapewnianie, by audyt działań organu zarządzającego związanych z przetwarzaniem danych osobowych przeprowadzany był zgodnie z międzynarodowymi standardami audytu, co najmniej raz na cztery lata".

Artykuł 26 porusza kwestię współpracy między krajowymi organami nadzorczymi a Europejskim Inspektorem Ochrony Danych.

17. Europejski Inspektor Ochrony Danych zauważa także, że we wniosku zaproponowano podejście podobne do tego, które przyjęto w odniesieniu do systemów SIS II i VIS: wielowarstwowy system nadzoru, w ramach którego krajowe organy ds. ochrony danych i Europejski Inspektor Ochrony Danych sprawują nadzór odpowiednio na szczeblu krajowym i na szczeblu UE, a między tymi dwoma szczeblami funkcjonuje system współpracy. Model współpracy przewidziany we wniosku odzwierciedla również aktualne praktyki, które okazały się wydajne i doprowadziły do nawiązania ścisłej współpracy między Europejskim Inspektorem Ochrony Danych a krajowymi organami ds. ochrony danych. Dlatego też Europejski Inspektor Ochrony Danych z zadowoleniem przyjmuje fakt, że prawodawca w sposób formalny uwzględnił tę współpracę we wniosku, zapewniając jednocześnie spójność z systemami nadzoru innych obszernych systemów informatycznych.

III.2. Podwykonawstwo

18. Europejski Inspektor Ochrony Danych zauważa, że we wniosku nie poruszono kwestii powierzania części zadań Komisji innym organizacjom lub podmiotom (takim jak spółki prywatne). Mimo to Komisja powszechnie korzysta z usług podwykonawców w ramach zarządzania i rozwoju systemu oraz infrastruktury komunikacyjnej. Podwykonawstwo samo w sobie nie stoi w sprzeczności z wymogami ochrony danych, jednak należy wprowadzić odpowiednie zabezpieczenia, tak aby mieć pewność, że podwykonawstwo niektórych działań nie będzie miało żadnego wpływu na stosowanie rozporządzenia (WE) nr 45/2001, w tym na nadzór nad ochroną danych sprawowany przez Europejskiego Inspektora Ochrony Danych. Ponadto należy przyjąć dodatkowe zabezpieczenia bardziej technicznej natury.

19. W związku z tym Europejski Inspektor Ochrony Danych proponuje wprowadzenie w ramach zmiany rozporządzenia Eurodac podobnych zabezpieczeń prawnych do tych przewidzianych w instrumentach prawnych dotyczących systemu SIS II, tak aby jasno określić, że nawet w przypadku powierzenia przez Komisję zarządzania systemem innemu organowi, Komisja dokłada starań, aby to „*nie wpłynęło niekorzystnie na jakikolwiek system skutecznej kontroli ustanowiony prawem wspólnotowym, sprawowanej przez Trybunał Sprawiedliwości, Trybunał Obrachunkowy lub też przez Europejskiego Inspektora Ochrony Danych*" (art. 15 ust. 7 decyzji i rozporządzenia SIS II).

20. Przepisy art. 47 rozporządzenia SIS II są jeszcze bardziej szczegółowe i stanowią, że: „Jeżeli w okresie przejściowym Komisja deleguje swoje obowiązki innemu organowi lub organom (…), zapewnia ona Europejskiemu Inspektorowi Ochrony Danych prawo oraz możliwość pełnego wykonywania jego zadań, w tym przeprowadzania kontroli na miejscu oraz wykonywania wszelkich innych powierzonych mu uprawnień na mocy art. 47 rozporządzenia (WE) nr 45/2001".

21. Wyżej wymienione przepisy zapewniają należytą jasność co do konsekwencji powierzenia części zadań Komisji innym organom. Europejski Inspektor Ochrony Danych proponuje zatem dodanie do treści wniosku Komisji przepisów mających taki sam skutek.

III.3. Procedura pobierania odcisków palców (art. 3.5 i 6)

22. Artykuł 3 ust. 5 wniosku dotyczy procedury pobierania odcisków palców. Przepis ten stanowi, że procedurę tę „ustala się i stosuje zgodnie z praktyką obowiązującą w danym państwie członkowskim i zgodnie z gwarancjami ustanowionymi w Karcie praw podstawowych Unii Europejskiej, w Konwencji o ochronie praw człowieka i podstawowych wolności, jak również w europejskiej konwencji praw człowieka oraz w konwencji Organizacji Narodów Zjednoczonych o prawach dziecka". Artykuł 6 wniosku przewiduje, że minimalna granica wieku w przypadku wnioskodawców, od których pobiera się odciski palców, wynosi 14 lat, a odciski pobierane są nie później niż w ciągu 48 godzin od złożenia wniosku.

23. Przede wszystkim, jeśli chodzi o granicę wieku, Europejski Inspektor Ochrony Danych podkreśla potrzebę zapewnienia spójności wniosku z rozporządzeniem dublińskim. System Eurodac został ustanowiony w celu zapewnienia skutecznego wykonania rozporządzenia dublińskiego. Oznacza to, że jeśli wprowadzenie przedmiotowych zmian do rozporządzenia dublińskiego będzie miało wpływ na jego zastosowanie do małoletnich ubiegających się o azyl, powinno zostać to odzwierciedlone w rozporządzeniu Eurodac [1].

[1] W tym względzie Europejski Inspektor Ochrony Danych zwraca uwagę na fakt, że we wniosku Komisji dotyczącym zmiany rozporządzenia dublińskiego przedstawionym w dniu 3 grudnia 2008 r. (COM(2008) 825 wersja ostateczna) „małoletni" oznacza „obywatela kraju trzeciego lub bezpaństwowca w wieku poniżej 18 lat".

24. Po drugie, jeśli chodzi o określanie granic wieku dla potrzeb pobierania odcisków palców w ogóle, Europejski Inspektor Ochrony Danych pragnie pokreślić, że większość aktualnie dostępnych dokumentów zdaje się wskazywać, iż precyzja identyfikacji na podstawie odcisków palców maleje wraz z wiekiem danej osoby. W związku z tym zaleca się dokładne monitorowanie badań dotyczących odcisków palców prowadzonych w ramach wdrożenia systemu VIS. Europejski Inspektor Ochrony Danych nie chce uprzedzać wyników tych badań, jednak już teraz pragnie podkreślić, że we wszystkich sytuacjach, w których pobranie odcisków palców okaże się niemożliwe lub wyniki badania byłyby niewiarygodne, należy skorzystać z procedur awaryjnych, które powinny zapewniać pełne poszanowanie godności danej osoby.

25. Po trzecie, Europejski Inspektor Ochrony Danych odnotowuje działania podejmowane przez prawodawcę w celu zapewnienia zgodności przepisów dotyczących pobierania palców z wymogami międzynarodowych i europejskich przepisów dotyczących praw człowieka. Mimo to Inspektor zwraca uwagę na trudności, na które napotykają niektóre państwa członkowskie w związku z ustalaniem wieku młodych osób ubiegających się o azyl. Bardzo często osoby ubiegające się o azyl lub nielegalni imigranci nie mają dokumentów tożsamości, a w celu ustalenia, czy należy od nich pobrać odciski palców konieczne jest określenie ich wieku. Metody stosowane w tym celu są przedmiotem wielu dyskusji w poszczególnych państwach członkowskich.

26. W związku z tym Europejski Inspektor Ochrony Danych zwraca uwagę na fakt, że grupa ds. koordynowania nadzoru nad systemem Eurodac [1] rozpoczęła skoordynowaną kontrolę dotyczącą tej kwestii, a jej wyniki – których ogłoszenie przewidziane jest na pierwszą połowę 2009 r. – powinny ułatwić określenie wspólnych procedur w tym zakresie.

27. Reasumując, Europejski Inspektor Ochrony Danych dostrzega potrzebę lepszej koordynacji i harmonizacji na szczeblu UE procedur pobierania odcisków palców w jak największym możliwym zakresie.

III.4. **Najlepsze z dostępnych technik (art. 4)**

28. Artykuł 4 ust. 1 wniosku stanowi: „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". Chociaż Europejski Inspektor Ochrony Danych z zadowoleniem przyjmuje wymóg przewidziany w art. 4 ust. 1, pragnie zauważyć, że sformułowanie „najlepsze z dostępnych technologii" zastosowane w wyżej wymienionym przepisie powinno zostać zastąpione określeniem „najlepsze z dostępnych technik", które obejmuje zarówno stosowane technologie, jak i metody projektowania, budowy, konserwacji i eksploatacji instalacji.

III.5. **Wcześniejsze usunięcie danych (art. 9)**

29. Artykuł 9 ust. 1 wniosku porusza kwestię *wcześniejszego usunięcia danych*. Przepis ten zobowiązuje państwo członkowskie pochodzenia do usunięcia z systemu centralnego „danych odnoszących się do osoby, która uzyskała obywatelstwo któregokolwiek z państw członkowskich przed upływem okresu, o którym mowa w art. 8", zaraz po tym, gdy tylko państwo członkowskie pochodzenia uzyska informację, że dana osoba uzyskała takie obywatelstwo. Europejski Inspektor Ochrony Danych z zadowoleniem przyjmuje obowiązek usunięcia danych, ponieważ jest on zgodny z zasadą jakości danych. Ponadto, Europejski Inspektor Ochrony Danych uważa, że zmiana tego przepisu jest okazją, aby zachęcić państwa członkowskie do wprowadzenia procedur zapewniających rzetelne i terminowe (w miarę możliwości automatyczne) usunięcie danych odnoszących się do osoby, która uzyskała obywatelstwo któregokolwiek z państw członkowskich.

30. Co więcej, Europejski Inspektor Ochrony Danych pragnie podkreślić, że art. 9 ust. 2 dotyczący wcześniejszego usunięcia danych powinien zostać zmieniony, ponieważ w obecnym brzmieniu jest on niejasny. Tytułem poprawki stylistycznej Europejski Inspektor Ochrony Danych sugeruje zastąpienie sformułowania „to państwo" wyrażeniem „te państwa".

III.6. **Okres przechowywania danych obywateli krajów trzecich zatrzymanych w związku z nielegalnym przekroczeniem granicy (art. 12)**

31. Artykuł 12 wniosku dotyczy przechowywania danych. Europejski Inspektor Ochrony Danych pragnie zauważyć, że ustanowienie okresu przechowywania danych o długości do 1 roku (zamiast 2 lat przewidzianych w aktualnej wersji rozporządzenia) stanowi przykład dobrego zastosowania zasady jakości danych, która przewiduje, że dane nie powinny być przechowywane przez okres dłuższy niż potrzebny do realizacji celów, do jakich dane te są przetwarzane. Zmiana ta jest pożądana.

III.7. **Wykaz organów mających dostęp do Eurodac (art. 20)**

32. Przepis przewidujący publikowanie przez organ zarządzający wykazu organów mających dostęp do danych Eurodac stanowi pożądaną zmianę. Pozwoli to na poprawę przejrzystości i stanowić będzie praktyczne narzędzie umożliwiające lepszy nadzór nad systemem, np. przez organy ds. ochrony danych.

III.8. **Rejestr (art. 21)**

33. Artykuł 21 wniosku dotyczy prowadzenia rejestru wszystkich operacji związanych z przetwarzaniem danych w systemie centralnym. Artykuł 21 ust. 2 stanowi, że rejestr ten można wykorzystywać tylko do monitorowania, czy operacje przetwarzania są dopuszczalne w świetle zasad ochrony danych (…). W związku z tym wskazane byłoby wyjaśnienie, że obejmuje to także środki kontroli własnej.

[1] Wyjaśnienia dotyczące działalności i statusu grupy znajdują się pod adresem internetowym: http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/79. Grupa ta sprawuje skoordynowany nadzór nad systemem EURODAC.

III.9. **Prawa osoby, której dane dotyczą (art. 23)**

34. Artykuł 23 ust. 1 lit. e) wniosku stanowi:

„Państwo Członkowskie pochodzenia podaje osobie objętej zakresem niniejszego rozporządzenia (…) następujące informacje:

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 przetworzonych niezgodnie z prawem, łącznie z prawem otrzymania informacji na temat procedur korzystania z tych praw, jak również dane kontaktowe krajowych organów nadzorczych, o których mowa w art. 25 ust. 1, które rozpatrują skargi dotyczące ochrony danych osobowych".

35. Europejski Inspektor Ochrony Danych zauważa, że skuteczne stosowanie prawa do informacji jest bardzo ważne dla prawidłowego funkcjonowania systemu Eurodac. W szczególności konieczne jest dostarczanie informacji w taki sposób, aby osoba ubiegająca się o azyl w pełni rozumiała swoją sytuację oraz przysługujące jej prawa, w tym procedury, z których może skorzystać w następstwie decyzji administracyjnych podjętych w jej sprawie.

36. Jeśli chodzi o aspekty praktyczne wykonywania tego prawa, Europejski Inspektor Ochrony Danych pragnie podkreślić, że chociaż krajowe organy ds. ochrony danych, wymienione są faktycznie organami właściwymi do rozpatrywania skarg dotyczących ochrony danych osobowych, to wniosek powinien być sformułowany tak, aby wnioskodawca (*osoba, której dane dotyczą*) miał możliwość skierowania wniosku przede wszystkim do administratora danych. Zawarty w art. 23 ust. 1 lit. e) przepis w obecnym brzmieniu zdaje się sugerować, że wnioskodawca powinien swój wniosek przedkładać – bezpośrednio i w każdym przypadku – krajowemu organowi ds. ochrony danych, chociaż zgodnie ze standardowymi procedurami i praktykami przyjętymi w państwach członkowskich wnioskodawca składa skargę najpierw u administratora danych.

37. Europejski Inspektor Ochrony Danych zaleca także zmianę brzmienia art. 23 ust. 1 lit. e), tak aby doprecyzować, jakie prawa przyznane będą wnioskodawcy. Tekst w proponowanym brzmieniu jest niejasny, ponieważ możliwa jest interpretacja, zgodnie z którą „prawo otrzymania informacji na temat procedur korzystania z tych praw (…)" jest we wniosku uznawane za część prawa dostępu do danych lub prawa do żądania poprawienia nieprawidłowych danych (…). Ponadto zgodnie z obecnym brzmieniem powyższego przepisu państwa członkowskie mają informować osobę objętą zakresem rozporządzenia nie o treści jej praw, ale o ich „istnieniu". Ponieważ wydaje się, że ten drugi problem jest kwestią stylu, Europejski Inspektor Ochrony Danych zaleca, aby art. 23 ust. 1 lit. e) otrzymał następujące brzmienie

„Państwo Członkowskie pochodzenia podaje osobie objętej zakresem niniejszego rozporządzenia (…) następujące informacje:

g) o prawie dostępu danych dotyczących tej osoby oraz prawie do żądania poprawienia nieprawidłowych danych jej dotyczących lub usunięcia danych jej dotyczących przetworzonych niezgodnie z prawem, jak również o procedurach służących wykonywaniu tych praw, co obejmuje także dane kontaktowe krajowych organów nadzorczych, o których mowa w art. 25 ust. 1".

38. Na tej samej zasadzie art. 23 ust. 10 powinien otrzymać następujące brzmienie: „W każdym państwie członkowskim krajowy organ nadzorczy, w stosownych przypadkach (lub: na wniosek osoby, której dane dotyczą), wspiera osobę, której dane dotyczą, zgodnie z art. 28 ust. 4 dyrektywy 95/46/WE, w wykonywaniu jej praw". Europejski Inspektor Ochrony Danych pragnie ponownie podkreślić, że interwencja organu ds. ochrony danych nie powinna być zasadniczo konieczna; wręcz przeciwnie – należy zachęcać administratora danych, aby odpowiednio reagował na skargi osób, których dane dotyczą. To samo dotyczy przypadków, w których potrzebna jest współpraca między organami różnych państw członkowskich. To administratorzy danych powinni być przede wszystkim odpowiedzialni za rozpatrywanie wniosków i podejmowanie współpracy w tym zakresie.

39. Jeśli chodzi o art. 23 ust. 9, Europejski Inspektor Ochrony Danych z zadowoleniem przyjmuje nie tylko samo założenie tego przepisu (który przewiduje kontrolę korzystania z prawa do przeprowadzania „specjalnych przeszukiwań", zgodnie z zaleceniami organów ds. ochrony danych zawartymi w ich pierwszym sprawozdaniu w sprawie skoordynowanych kontroli), ale także z satysfakcją odnotowuje zaproponowaną w tym celu procedurę.

40. Jeśli chodzi o metody udzielania informacji wnioskodawcom, Europejski Inspektor Ochrony Danych wskazuje na działania podejmowane przez grupę ds. koordynowania nadzoru nad systemem Eurodac. Grupa ta aktualnie analizuje tę kwestię w ramach systemu Eurodac w celu zaproponowania właściwych wskazówek, kiedy tylko zostaną opracowane i udostępnione wyniki krajowych postępowań wyjaśniających.

IV. **KONKLUZJE**

41. Europejski Inspektor Ochrony Danych popiera wniosek w sprawie rozporządzenia Parlamentu Europejskiego i Rady 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.

42. Europejski Inspektor Ochrony Danych z zadowoleniem przyjmuje model nadzoru zaproponowany we wniosku, jak również rolę i zadania przydzielone mu w nowym systemie. Przewidziany model odzwierciedla aktualne praktyki, które okazały się wydajne.

43. Europejski Inspektor Ochrony Danych z zadowoleniem zauważa, że autorzy wniosku starali się zachować spójność z innymi instrumentami prawnymi regulującymi tworzenie lub wykorzystywanie innych obszernych systemów informatycznych.

44. Europejski Inspektor Ochrony Danych zauważa, że we wniosku dużo uwagi poświęcono poszanowaniu praw podstawowych, a w szczególności ochronie danych osobowych. Jak już wspomniano w opinii dotyczącej zmiany rozporządzenia dublińskiego, Europejski Inspektor Ochrony Danych uznaje to podejście za warunek wstępny niezbędny dla usprawnienia procedur udzielania azylu w Unii Europejskiej.

45. Europejski Inspektor Ochrony Danych zwraca uwagę na potrzebę doprowadzenia do pełnej spójności między rozporządzeniem Eurodac i rozporządzeniem dublińskim.

46. Europejski Inspektor Ochrony Danych dostrzega potrzebę lepszej koordynacji i harmonizacji na szczeblu UE procedur pobierania odcisków palców, zarówno w stosunku do osób ubiegających się o azyl jak i innych osób objętych procedurą Eurodac. Zwraca on szczególną uwagę na kwestię granic wieku w związku z pobieraniem odcisków palców, a w szczególności na problemy, jakie niektóre państwa członkowskie napotykają w związku z określeniem wieku młodych osób ubiegających się o azyl.

47. Europejski Inspektor Ochrony Danych obstaje przy stanowisku, że konieczne jest doprecyzowanie procedur dotyczących praw osób, których dane dotyczą i podkreśla w szczególności, że to przede wszystkim krajowi administratorzy danych odpowiedzialni są za zapewnienie wykonania takich praw.

Sporządzono w Brukseli dnia 18 lutego 2009 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych

Opinia Europejskiego Inspektora Ochrony Danych na temat inicjatywy Republiki Francuskiej na rzecz przyjęcia decyzji Rady w sprawie stosowania technologii informatycznych do potrzeb celnych

(2009/C 229/03)

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, ([1]).

uwzględniając decyzję ramową Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, ([2]).

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, ([3]). w szczególności jego art. 41,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. WPROWADZENIE

Konsultacje z Europejskim Inspektorem Ochrony Danych.

1. Inicjatywę Republiki Francuskiej mającą na celu przyjęcie decyzji Rady w sprawie wykorzystania technologii informatycznych dla potrzeb celnych opublikowano w Dzienniku Urzędowym z dnia 5 lutego 2009 r. ([4]) Ani państwo członkowskie, które wystąpiło z tą inicjatywą, ani Rada nie zasięgnęły w jej sprawie opinii Inspektora. Inspektor został jednak poproszony o uwagi co do inicjatywy – zgodnie z art. 41 rozporządzenia (WE) nr 45/2001 – przez parlamentarną Komisję Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych w kontekście opinii Parlamentu Europejskiego w sprawie tej inicjatywy. Choć w podobnych przypadkach ([5]) Inspektor wydawał opinie z własnej inicjatywy, niniejszą należy uznać za odpowiedź na wniosek Parlamentu Europejskiego.

2. Inspektor sądzi, że o niniejszej opinii należy wspomnieć w preambule do decyzji Rady, tak jak to zrobiono w przypadku innych jego opinii wspomnianych w różnych aktach prawnych przyjętych na podstawie wniosków Komisji.

3. Choć państwo członkowskie występujące z inicjatywą w sprawie środka prawnego na mocy tytułu VI Traktatu UE nie ma prawnego obowiązku zwracać się do Inspektora o opinię, stosowne zasady tego nie wykluczają. Inspektor ubolewa, że ani Republika Francuska, ani Rada nie wystąpiły do niego o poradę w tym przypadku.

4. Ponieważ prace Rady nad wnioskiem jeszcze trwają, Inspektor podkreśla, że uwagi przedstawione w niniejszej opinii odnoszą się do wersji z dnia 24 lutego 2009 r. (dok. 5903/2/09 REV 2) opublikowanej na stronie internetowej Parlamentu Europejskiego ([6]).

5. Inspektor sądzi, że należy lepiej wyjaśnić, czym uzasadniona jest sama inicjatywa i co oznaczają określone artykuły i mechanizmy w niej zawarte. Ubolewa również, że inicjatywie nie towarzyszą ocena skutków regulacji ani uzasadnienie. Są to niezbędne elementy zwiększające przejrzystość, a w szerszej perspektywie – jakość procesu legislacyjnego. Wyjaśnienia pomogłyby także ocenić szereg propozycji zawartych w projekcie, np. konieczność i zasadność udzielenia Europolowi i Eurojustowi dostępu do systemu informacji celnej.

6. Inspektor wziął pod uwagę opinię 09/03 Wspólnego Organu Nadzorczego ds. Ceł z dnia 24 marca 2009 r. dotyczącą projektu decyzji Rady w sprawie stosowania technologii informatycznych do potrzeb celnych.

Kontekst wniosku

7. System informacji celnej (zwany dalej „systemem") jest obecnie regulowany aktami zarówno pierwszego, jak i trzeciego filaru. Ramy prawne trzeciego filaru to głównie Konwencja z dnia 26 lipca 1995 r. sporządzona na podstawie artykułu K.3 Traktatu o Unii Europejskiej w sprawie wykorzystania technologii informatycznej dla potrzeb celnych (zwana dalej „konwencją" ([7]) oraz protokoły z dnia 12 marca 1999 r. i z dnia 8 marca 2003 r.

8. Obecne uzgodnienia dotyczące ochrony danych przewidują m.in. stosowanie Konwencji Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (zwanej dalej „konwencją nr 108 Rady Europy"). Ponadto na mocy projektu do systemu ma zastosowanie decyzja ramowa Rady 2008/977/WSiSW (zwana dalej „decyzją ramową 2008/977/WSiSW").

([1]) Dz.U. L 281 z 23.11.1995, s. 31.
([2]) Dz.U. L 350 z 30.12.2008, s. 60.
([3]) Dz.U. L 8 z 12.1.2001, s. 1.
([4]) Dz.U. C 29 z 5.2.2009, s. 6.
([5]) Zob. niedawna opinia Europejskiego Inspektora Ochrony Danych w sprawie inicjatywy 15 państw członkowskich mającej na celu przyjęcie decyzji Rady w sprawie wzmocnienia Eurojustu i zmiany decyzji 2002/187/WSiSW Dz.U. C 310 z 5.12.2008, s. 1.
([6]) http://www.europarl.europa.eu/meetdocs/2004_2009/organes/libe/libe_20090330_1500.htm
([7]) Dz.U. C 316 z 27.11.1995, s. 33.

9. Pierwszofilarowa część systemu jest regulowana rozporządzeniem Rady (WE) nr 515/97 dnia 13 marca 1997 r. w sprawie wzajemnej pomocy między organami administracyjnymi państw członkowskich i współpracy między państwami członkowskimi a Komisją w celu zapewnienia prawidłowego stosowania przepisów prawa celnego i rolnego ([1]).

10. Celem konwencji była – zgodnie z jej art. 2 ust. 2 – pomoc w zapobieganiu, prowadzeniu dochodzenia i ściganiu poważnych naruszeń przepisów krajowych poprzez zwiększenie, dzięki szybkiemu rozpowszechnianiu informacji, skuteczności współpracy i procedur kontroli administracji celnych państw członkowskich.

11. W myśl konwencji o CIS system informacji celnej składa się z centralnej bazy danych dostępnej z terminali umiejscowionych w każdym państwie członkowskim. Jego pozostałe główne cechy są następujące:

— konwencja przewiduje, że system będzie zawierał wyłącznie dane, w tym dane osobowe, niezbędne do realizacji jego celu; będą to dane z następujących kategorii: a) towary; b) środki transportu; c) przedsiębiorstwa; d) osoby; e) tendencje w dziedzinie nadużyć finansowych; f) dostępna wiedza specjalistyczna ([2]),

— państwa członkowskie określają pozycje, które należy wprowadzić do systemu, odpowiadające każdej z trzech ostatnich kategorii w zakresie niezbędnym do osiągnięcia celu systemu. W dwóch ostatnich kategoriach nie umieszcza się żadnej pozycji dotyczącej danych osobowych. Bezpośredni dostęp do danych zawartych w systemie informacji celnej jest zastrzeżony dla organów krajowych wyznaczonych przez każde państwo członkowskie. Tymi organami krajowymi są administracje celne, ale zgodnie z przepisami ustawowymi, wykonawczymi i procedurami danego państwa członkowskiego do działania dla osiągnięcia celu określonego w konwencji włączyć można również inne uprawnione organy,

— państwa członkowskie mogą korzystać z danych uzyskanych z systemu informacji celnej jedynie dla osiągnięcia celu konwencji; jednakże mogą one wykorzystywać je do celów administracyjnych lub innych po uprzednim uzyskaniu pozwolenia od państwa członkowskiego, które wprowadziło dane do systemu, i z zastrzeżeniem warunków nałożonych przez to państwo. Utworzono wspólny organ nadzorczy, którego zadaniem jest nadzorowanie części systemu podlegającej trzeciemu filarowi.

12. Francuska inicjatywa, oparta na art. 30 ust. 1 lit. a) i art. 34 ust. 2 Traktatu o Unii Europejskiej, ma na celu zastąpienie konwencji oraz protokołu z dnia 12 marca 1999 r. i protokół z dnia 8 marca 2003 r., po to by dostosować trzeciofilarową część systemu do instrumentów pierwszego filaru.

13. Jednak projekt przewiduje nie tylko zastąpienie konwencji decyzją Rady. Modyfikuje także znaczną liczbę przepisów konwencji i poszerza obecny dostęp do systemu, zapewniając go Europolowi i Eurojustowi. Zawiera ponadto przepisy o funkcjonowaniu systemu podobne do przepisów zawartych w wyżej wymienionym rozporządzeniu (WE) nr 766/2008, np. jeżeli chodzi o utworzenie identyfikującej bazy danych rejestru celnego (rozdział VI).

14. Projekt uwzględnia także nowe instrumenty prawne, takie jak decyzja ramowa 2008/977/WSiSW oraz decyzja ramowa 2006/960/WSiSW z dnia 13 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej ([3]).

15. Projekt ma z założenia między innymi:

— zacieśnić współpracę między administracjami celnymi i w tym celu ustanowić procedury, dzięki którym administracje celne będą mogły działać wspólnie oraz wymieniać dane osobowe i inne dane na temat nielegalnego handlu, wykorzystując nowe technologie do zarządzania takimi informacjami i ich przekazywania. Takie przetwarzanie podlega postanowieniom konwencji nr 108 Rady Europy, przepisom decyzji ramowej 2008/977/WSiSW, a także zasadom zawartym w zaleceniu R (87) 15 Komitetu Ministrów Rady Europy z dnia 17 września 1987 r. regulującym wykorzystanie danych osobowych przez policję,

— zwiększyć komplementarność względem działań prowadzonych w ramach współpracy z Europolem i Eurojustem, umożliwiając tym podmiotom dostęp do systemu informacji celnej.

16. Celem systemu jest zatem – zgodnie z art. 1 projektu – „pomagać w zapobieganiu poważnym naruszeniom przepisów krajowych, w prowadzeniu dochodzeń w sprawie tych naruszeń i w ich ściganiu i w tym celu ma możliwie szybko udostępniać dane, a przez to zwiększać skuteczność procedur współpracy i kontroli stosowanych przez administracje celne państw członkowskich". Przepis ten w dużej mierze opiera się na art. 2 ust. 2 konwencji.

17. Aby można było osiągnąć te cele, projekt rozszerza zakres wykorzystania danych z systemu oraz przewiduje kwerendy w systemach i możliwość analizy strategicznej lub operacyjnej. Inspektor odnotowuje, że rozszerzono cel i wykaz kategorii gromadzonych i przetwarzanych danych osobowych oraz wykaz osób, których dane dotyczą, mających bezpośredni dostęp do systemu.

([1]) Dz.U. L 82 z 22.3.1997, s. 1.

([2]) We wniosku dodano nową kategorię: g) przedmioty zatrzymane, zajęte lub skonfiskowane.

([3]) Dz.U. L 386 z 29.12.2006, s. 89.

Zakres opinii

18. Ponieważ Inspektor pełni obecnie rolę organu nadzorczego wobec najważniejszej części pierwszofilarowej części systemu, jest szczególnie zainteresowany przedmiotową inicjatywą i związanymi z jej treścią nowymi wydarzeniami w Radzie. Podkreśla, że dostosowanie do siebie pierwszo- i trzeciofilarowej części systemu wymaga spójnego i wszechstronnego podejścia.

19. Inspektor odnotowuje, że w projekcie pojawiają się różne aspekty związane z prawami podstawowymi, zwłaszcza ochrona danych osobowych, prawo do informacji oraz inne prawa osób, których dane dotyczą.

20. Jeżeli chodzi o obecny system ochrony danych przewidziany w konwencji, Inspektor nie może nie wspomnieć, że niektóre jej przepisy wymagają modyfikacji i uaktualnienia, ponieważ nie spełniają obecnych wymogów i standardów ochrony danych. Inspektor korzysta z okazji, by podkreślić, że od zwiększenia ochrony danych osobowych i jej skuteczniejszego wdrażania w praktyce w zasadniczym stopniu zależy, czy system będzie działać lepiej.

21. W niniejszej opinii przedstawiono najpierw kilka uwag ogólnych, a następnie poruszono przede wszystkim następujące kwestie ważne dla ochrony danych osobowych:

— gwarancje ochrony danych w systemie,

— baza danych rejestru celnego dla celów identyfikacyjnych,

— dostęp Eurojustu i Europolu do systemu (proporcjonalność i konieczność tego dostępu),

— model nadzoru nad całością systemu,

— wykaz organów mających dostęp do systemu.

II. **UWAGI OGÓLNE**

Spójność między pierwszo- a trzeciofilarową częścią systemu

22. Jak wspomniano we wprowadzeniu, Inspektor jest szczególnie zainteresowany nowymi wydarzeniami dotyczącymi trzeciofilarowej części systemu, ponieważ sprawuje już rolę nadzorczą wobec centralnej części jego części pierwszofilarowej – zgodnie z nowym rozporządzeniem (WE) nr 766/2008 zmieniającym rozporządzenie (WE) nr 515/97 w sprawie wzajemnej pomocy między organami administracyjnymi państw członkowskich i współpracy [1] w celu zapewnienia prawidłowego stosowania przepisów prawa celnego i rolnego.

23. Przy tej okazji Inspektor chciałby zwrócić uwagę prawodawcy na fakt, że kwestie związane z nadzorem nad pierwszofilarową częścią systemu poruszał już w niektórych dotychczasowych opiniach, zwłaszcza w opinii z dnia 22 lutego 2007 r. [2].

24. W opinii tej Inspektor podkreślił, że „tworzenie i ulepszanie różnych aktów służących zacieśnianiu współpracy we Wspólnocie, tj. SIC, FIDE oraz europejskiego zbioru danych, pociąga za sobą zwiększenie ilości danych osobowych, które będą gromadzone i wymieniane między organami administracyjnymi państw członkowskich, a w niektórych przypadkach także między państwami trzecimi. Przetwarzane i przekazywane dane osobowe mogą zawierać informacje o rzekomym lub udowodnionym udziale danych osób w działaniach niedozwolonych w obszarze celnym lub rolnym. (…) Ponadto jego znaczenie zwiększa się, jeśli wziąć pod uwagę rodzaj gromadzonych i przekazywanych danych, zwłaszcza podejrzenia o udział danych osób w działaniach niedozwolonych, jak również ogólny cel i wyniki przetwarzania".

Potrzeba strategicznego podejścia do całości systemu

25. Inspektor podkreśla, że projekt – inaczej niż poprawki wprowadzone rozporządzeniem (WE) nr 766/2008 do pierwszofilarowego instrumentu, któremu podlega system – przewiduje gruntowną modyfikację konwencji, co daje prawodawcy możliwość szerszego spojrzenia na cały system i zastosowania przy tym spójnego i wszechstronnego podejścia.

26. Zdaniem Inspektora podejście to musi być także zorientowane ku przyszłości. Podczas decydowania o treści projektu należy dokładnie rozważyć i uwzględnić nowe wydarzenia, takie jak przyjęcie decyzji ramowej 2008/977/WSiSW oraz (ewentualne) wejście w życie traktatu z Lizbony.

27. Jeśli chodzi o wejście w życie traktatu z Lizbony, Inspektor zwraca uwagę prawodawcy na fakt, że należy wnikliwie przeanalizować, jaki wpływ na system miałoby zniesienie struktury filarowej UE po wejściu w życie tego traktatu, gdyż obecnie system opiera się na kombinacji aktów pierwszo- i trzeciofilarowych. Inspektor ubolewa, że nie zamieszczono wyjaśnień na temat tego ważnego przyszłego wydarzenia mogącego znacznie wpłynąć na ramy prawne, którym podlega system. Mówiąc ogólniej, Inspektor stawia pytanie, czy nie byłoby właściwiej, gdyby prawodawca poczekał ze zmianą do czasu wejścia w życie traktatu z Lizbony, by uniknąć ewentualnej niepewności prawa.

Inspektor apeluje o uspójnienie systemu z innymi systemami o dużej skali

28. Inspektor jest zdania, że plan zastąpienia całości konwencji daje również dobrą okazję ku temu, by zapewnić spójność systemu z innymi systemami i mechanizmami wprowadzonymi od czasu jej przyjęcia. W związku z tym apeluje, by zadbać o spójność, także w kwestii modelu nadzoru, z innymi aktami prawnymi, zwłaszcza tymi, które ustanawiają system informacyjny Schengen II i wizowy system informacyjny.

[1] Dz.U. L 218 z 13.8.2008, s. 48.

[2] Opinia z dnia 22 lutego 2007 r. w celu zapewnienia prawidłowego stosowania przepisów prawa celnego i rolnego (COM(2006) 866 wersja ostateczna), Dz.U. C 94 z 28.4.2007, s. 3.

Powiązania z decyzją ramową 2008/977/WSiSW

29. Inspektor z zadowoleniem przyjmuje fakt, że z uwagi na wymianę danych, której w ramach systemu dokonują państwa członkowskie, projekt uwzględnia decyzję ramową o ochronie danych osobowych. Artykuł 20 projektu wyraźnie stwierdza, że „jeżeli niniejsza decyzja nie stanowi inaczej, ochrona danych wymienianych na podstawie niniejszej decyzji podlega przepisom decyzji ramowej 2008/977/WSiSW". Inspektor odnotowuje, że także inne przepisy projektu odwołują się do decyzji ramowej, np. art. 4 ust. 5 mówi o niewprowadzaniu danych wymienionych w art. 6 decyzji ramowej 2008/977/WSiSW; art. 8 – o wykorzystywaniu danych uzyskanych z systemu, by realizować cel wskazany w art. 1 ust. 2 decyzji; art. 22 – o prawach osób, których dane osobowe figurują w systemie, a art. 29 – o obowiązkach i odpowiedzialności.

30. Inspektor uważa, że koncepcje i zasady przyjęte w decyzji ramowej są odpowiednie w kontekście systemu, i dlatego powinny mieć zastosowanie – zarówno w interesie pewności prawa, jak i spójności systemów prawnych.

31. Inspektor zwraca jednak uwagę, że prawodawca powinien zadbać o niezbędne gwarancje, by przed pełnym wdrożeniem decyzji ramowej 2008/977/WSiSW, zgodnie z jej przepisami końcowymi, nie powstała luka w systemie ochrony danych. Innymi słowy, Inspektor chciałby podkreślić, że opowiada się za podejściem przewidującym zapewnienie niezbędnych i stosownych gwarancji, zanim wymieniane będą nowe dane.

III. **UWAGI SZCZEGÓŁOWE**

Gwarancje ochrony danych

32. Inspektor sądzi, że skuteczne wdrożenie prawa do ochrony danych i prawa do informacji to kluczowe elementy, od których zależy, czy system informacji celnej będzie właściwie funkcjonować. Gwarancje ochrony danych nie tylko są potrzebne, by zapewnić skuteczną ochronę osobom, których dane znajdują się w systemie, lecz także powinny pomóc we właściwym i wydajniejszym funkcjonowaniu tego systemu.

33. Inspektor zwraca uwagę prawodawcy na fakt, że zapotrzebowanie na zdecydowane i skuteczne gwarancje ochrony danych staje się jeszcze bardziej widoczne, gdy wziąć pod uwagę, że system jest bazą danych opartą raczej na „podejrzeniach" niż na wyrokach lub innych decyzjach sądowych bądź administracyjnych. Jest to odzwierciedlone w art. 5 projektu, który mówi, że „dane z kategorii, o których mowa w art. 3, wprowadza się do systemu informacji celnej jedynie do celów obserwacji, składania sprawozdań, niejawnego nadzoru, kontroli szczególnych oraz analizy strategicznej i operacyjnej. Dane osobowe (…) można wprowadzać na potrzeby proponowanych działań (…) do systemu informacji celnej jedynie wtedy, gdy istnieją faktyczne przesłanki, wynikające przede wszystkim z wcześniejszych nielegalnych działań, że dana osoba dopuściła się, dopuszcza się lub dopuści się poważnych naruszeń przepisów krajowych". Z uwagi na tę cechę systemu projekt wymaga wyważonych, skutecznych i uaktualnionych gwarancji, którymi są ochrona danych osobowych i mechanizmy kontrolne.

34. Jeżeli chodzi o szczegółowe przepisy projektu dotyczące ochrony danych osobowych, Inspektor odnotowuje starania prawodawcy, by zapewnić więcej zabezpieczeń niż w konwencji. Inspektor jest jednak zmuszony zgłosić kilka zasadniczych uwag dotyczacych tych przepisów, a zwłaszcza zastosowania zasady ograniczenia celu.

35. Przy tej okazji należy wspomnieć również o tym, że uwagi co do gwarancji ochrony danych zamieszczone w niniejszej opinii nie dotyczą wyłącznie przepisów modyfikujących lub rozszerzających zakres zastosowania konwencji, ale odnoszą się też do części tekstu skopiowanych z obowiązującej konwencji. Przyczyną tego jest fakt, że – jak wspomniano już w uwagach ogólnych – zdaniem Inspektora niektóre przepisy konwencji nie spełniają obecnych wymogów ochrony danych, a francuska inicjatywa jest dobrą okazją do przyjrzenia się na nowo całemu systemowi i zapewnienia odpowiedniej ochrony danych, równoważnej ochronie gwarantowanej w ramach pierwszofilarowej części systemu.

36. Inspektor z satysfakcją odnotowuje, że do systemu mogą zostać wprowadzone tylko dane osobowe z wyczerpującej i zamkniętej listy. Z zadowoleniem przyjmuje również fakt, że w projekcie znalazła się szersza niż w konwencji definicja terminu „dane osobowe". W myśl art. 2 ust. 2 projektu „dane osobowe" oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dotyczą dane"); osoba możliwa do zidentyfikowania to taka osoba, która może zostać zidentyfikowana bezpośrednio lub pośrednio, w szczególności na podstawie numeru identyfikacyjnego lub co najmniej jednego znaku szczególnego związanego z jej tożsamością fizyczną, psychologiczną, psychiczną, ekonomiczną, kulturową czy społeczną.

Ograniczenie celu

37. Przykładem przepisu, który budzi poważne wątpliwości związane z ochroną danych, jest art. 8 projektu stwierdzający, że „państwa członkowskie mogą wykorzystywać dane z systemu informacji celnej jedynie w celu, o którym mowa w art. 1 ust. 2. Mogą one jednak wykorzystywać te dane do celów administracyjnych lub innych za uprzednią zgodą państwa członkowskiego, które wprowadziło te dane do systemu, i pod warunkami postawionymi przez to państwo. Wykorzystanie danych do takich innych celów musi być zgodne z przepisami ustawowymi, wykonawczymi i procedurami państwa członkowskiego, które zamierza te dane wykorzystać zgodnie z art. 3 ust. 2 decyzji ramowej 2008/977/WSiSW". Przepis ten, dotyczący wykorzystania danych uzyskanych z systemu, jest bardzo istotny dla jego struktury, i dlatego wymaga szczególnej uwagi.

38. W art. 8 projektu odwołano się do art. 3 ust. 2 decyzji ramowej 2008/977/WSiSW, który mówi o „zasadach legalności, proporcjonalności i celowości". Artykuł 3 decyzji ramowej stwierdza, co następuje:

„1. Właściwe organy mogą gromadzić dane osobowe tylko do określonych, jednoznacznych i legalnych celów w ramach swoich zadań oraz przetwarzać je tylko do celów, w jakich zostały zgromadzone. Dane są przetwarzane zgodnie z prawem, adekwatnie do celu, w jakim są gromadzone, w związku z tym celem i w sposób niewykraczający poza ten cel.

2. Dane wolno przetwarzać dalej w innym celu, o ile:

a) nie jest to sprzeczne z celami, w jakich zostały zgromadzone;

b) właściwe organy są upoważnione do tego, by przetwarzać takie dane w takim innym celu zgodnie z obowiązującymi przepisami prawa; oraz

c) przetwarzanie jest konieczne i proporcjonalne względem tego innego celu".

39. Niezależnie od zastosowania art. 3 ust. 2 decyzji ramowej 2008/977/WSiSW, wskazującego ogólne warunki, na których można dopuścić przetwarzanie danych do innych celów, Inspektor zwraca uwagę na fakt, że istnieją wątpliwości, czy przepisy art. 8 projektu, umożliwiające wykorzystanie danych z systemu do ewentualnych niezdefiniowanych w projekcie celów administracyjnych lub innych, pozwolą przestrzegać wymogów ochrony danych, zwłaszcza zasady ograniczenia celu. Ponadto tak ogólnego zastosowania nie dopuszcza instrument pierwszofilarowy. Inspektor apeluje zatem o uszczegółowienie celów, w jakich można by wykorzystywać dane. Ma to zasadnicze znaczenie dla ochrony danych, ponieważ chodzi o istotę wykorzystywania danych z systemów o dużej skali: „dane należy wykorzystywać tylko w dobrze zdefiniowanych i wyraźnie ograniczonych celach wskazanych w ramach prawnych".

Przekazywanie danych państwom trzecim

40. Artykuł 8 ust. 4 projektu mówi o danych przekazywanych państwom trzecim lub organizacjom międzynarodowym. Przepis ten stwierdza, że „dane z systemu informacji celnej można – za uprzednią zgodą państwa członkowskiego, które wprowadziło dane do systemu, i pod warunkami postawionymi przez to państwo – przekazywać do użytku (…) państwom innym niż państwa członkowskie oraz organizacjom międzynarodowym lub regionalnym, które pragną wykorzystać te dane. Każde państwo członkowskie przedsiębierze specjalne środki, aby zapewnić bezpieczeństwo tych danych podczas ich przekazywania służbom znajdującym się poza jego terytorium. Szczegółowy opis takich środków należy przekazać wspólnemu organowi nadzorczemu, o którym mowa w art. 25".

41. Inspektor odnotowuje, że zastosowanie w tym kontekście ma art. 11 decyzji ramowej o ochronie danych osobowych. Należy jednak podkreślić, że biorąc pod uwagę bardzo ogólny charakter zastosowania przepisów art. 8 ust. 4 projektu, który zasadniczo daje państwom członkowskim możliwość przekazywania danych uzyskanych z systemu państwom innym niż państwa członkowskie oraz organizacjom międzynarodowym lub regionalnym, które pragną wykorzystać te dane, gwarancje ochrony danych osobowych przewidziane w tym przepisie są daleko niewystarczające. Inspektor apeluje, by ponownie przeanalizować art. 8 ust. 4 i zapewnić jednolity system oceny adekwatności o odpowiednim mechanizmie, np. z udziałem komitetu, o którym mowa w art. 26 projektu.

Inne gwarancje ochrony danych

42. Inspektor z satysfakcją odnotowuje przepisy o zmianie danych (rozdział IV, art. 13) będące ważnym elementem zasady jakości danych. Z zadowoleniem przyjmuje zwłaszcza szerszy niż w konwencji i zmodyfikowany w stosunku do niej zakres zastosowania tego przepisu, który mówi teraz także o korygowaniu i usuwaniu danych. Na przykład w myśl art. 13 ust. 3 jeżeli dostarczające państwo członkowskie lub Europol zauważą albo dowiedzą się, że wprowadzone przez nie dane są niezgodne ze stanem faktycznym albo zostały wprowadzone lub są przechowywane niezgodnie z przepisami decyzji, państwo to lub Europol odpowiednio zmieniają, uzupełniają, korygują lub usuwają takie dane i powiadamiają o tym odpowiednio pozostałe państwa członkowskie i Europol.

43. Inspektor odnotowuje przepisy rozdziału V o zachowywaniu danych, oparte głównie na konwencji i przewidujące między innymi ograniczony czas zachowywania danych pochodzących z systemu.

44. Rozdział IX (Ochrona danych osobowych) odzwierciedla wiele przepisów konwencji. Znajdują się w nim jednak także istotne zmiany, tzn. zastosowanie do systemu decyzji ramowej o ochronie danych osobowych oraz fragment art. 22 projektu mówiący, że „prawa osób, których dane osobowe figurują w systemie informacji celnej, w szczególności prawo dostępu do nich, prawo zażądania ich korekty, usunięcia lub zablokowania są wykonywane zgodnie z przepisami ustawowymi, wykonawczymi i procedurami państwa członkowskiego, które stosuje decyzję ramową 2008/977/WSiSW i w którym osoby te powołują się na te prawa". Przy tej okazji Inspektor chciałby szczególnie zaznaczyć, że ważne jest, by zachować procedurę pozwalającą osobom, których dotyczą dane, powoływać się na swoje prawa i występować o dostęp w każdym państwie członkowskim. Inspektor będzie uważnie obserwował, jak w praktyce wdrażane jest to ważne prawo przysługujące osobom, których dotyczą dane.

45. Projekt rozszerza także zakres zastosowania konwencji, jeżeli chodzi o zakaz kopiowania danych z systemu do innych archiwów z danymi krajowymi. Konwencja wyraźnie stwierdza w art. 14 ust. 2, że „danych osobowych wprowadzonych przez inne państwa członkowskie nie można kopiować z systemu informacji celnej do innych archiwów z danymi krajowymi". Artykuł 21 ust. 3 projektu dopuszcza kopiowanie „kopii przechowywanych w systemach zarządzania ryzykiem, które służą do bezpośrednich krajowych kontroli celnych, lub kopii przechowywanych w systemie analizy operacyjnej, który służy do koordynacji działań". Jeśli chodzi o ten przepis, Inspektor przychyla się do uwag Wspólnego Organu Nadzorczego ds. Ceł wyrażonych w opinii 09/03, zwłaszcza uwag o terminie „systemy zarządzania ryzykiem" oraz o potrzebie doprecyzowania, kiedy i w jakich okolicznościach kopiowanie dopuszczone w art. 21 ust. 3 byłoby możliwe.

46. Inspektor z zadowoleniem przyjmuje przepisy o bezpieczeństwie, które są podstawą sprawnego funkcjonowania systemu (rozdział XII).

Identyfikująca baza danych rejestru celnego

47. W projekcie dodano przepisy o identyfikującej bazie danych rejestru celnego (art. 16–19). Jest to reakcja na utworzenie takiej bazy w instrumencie pierwszofilarowym. Inspektor nie kwestionuje wprawdzie zapotrzebowania na takie nowe bazy w ramach systemu, ale zwraca uwagę, że należy zapewnić odpowiednie gwarancje ochrony danych. W związku z tym z zadowoleniem przyjmuje fakt, że do baz danych rejestru celnego dla celów identyfikacyjnych nie ma zastosowania odstępstwo przewidziane w art. 21 ust. 3.

Dostęp Europolu i Eurojustu do systemu

48. Projekt daje dostęp do systemu Europejskiemu Urzędowi Policji (Europolowi) i Europejskiej Jednostce Współpracy Sądowej (Eurojustowi).

49. Na wstępie Inspektor podkreśla, że należy jasno zdefiniować cel dostępu i ocenić proporcjonalność i konieczność jego rozszerzenia. Brak jest informacji o tym, dlaczego dostęp do systemu mają uzyskać Europol i Eurojust. Inspektor podkreśla także, że jeśli w grę wchodzi dostęp do baz danych i funkcji oraz przetwarzanie danych osobowych, zdecydowanie trzeba najpierw ocenić nie tylko użyteczność takiego dostępu, lecz także faktyczną i udokumentowaną potrzebę takiej propozycji. Inspektor zaznacza, że nie przedstawiono takiego uzasadnienia.

50. Inspektor apeluje także o jasne zdefiniowanie w tekście, w jakim dokładnie celu Europol i Eurojust mogą uzyskać dostęp do danych.

51. W myśl art. 11 „Europol ma – w granicach swojego mandatu i w celu realizacji swoich zadań – prawo dostępu do danych wprowadzonych do systemu informacji celnej (…), bezpośredniego ich przeszukiwania oraz wprowadzania danych do tego systemu".

52. Inspektor z zadowoleniem przyjmuje ograniczenia wprowadzone w projekcie, a zwłaszcza:

— uzależnienie wykorzystania informacji z systemu od zgody państwa członkowskiego, które wprowadziło te dane do systemu,

— ograniczenie możliwości przekazywania danych przez Europol państwom trzecim (także jedynie za zgodą państwa członkowskiego, które wprowadziło te dane do systemu),

— ograniczony dostęp do systemu (upoważnieni pracownicy),

— kontrolowanie działań Europolu przez jego wspólny organ nadzorczy.

53. Inspektor chciałby również wspomnieć, że tam, gdzie projekt odwołuje się do konwencji o Europolu, należy mieć na uwadze decyzję Rady, na mocy której od dnia 1 stycznia 2010 r. Europol stanie się agencją UE.

54. O dostępie Eurojustu do systemu mowa jest w art. 12. Przewiduje on, że „z zastrzeżeniem rozdziału IX przedstawiciele krajowi Europejskiej Jednostki Współpracy Sądowej (Eurojustu) oraz ich asystenci mają – w granicach swojego mandatu i w celu realizacji swoich zadań – prawo dostępu do danych wprowadzonych do systemu informacji celnej zgodnie z art. 1, 3, 4, 5 i 6 oraz do ich przeszukiwania". Podobnie jak w przypadku Europolu projekt przewiduje mechanizmy udzielania zgody przez państwo członkowskie, które wprowadziło dane. Powyższe uwagi o konieczności uzasadnienia dostępu, a w przypadku jego przyznania – jego odpowiedniego i niezbędnego ograniczenia dotyczą także Eurojustu.

55. Inspektor z zadowoleniem przyjmuje ograniczenie dostępu do systemu do krajowych przedstawicieli, ich zastępców i asystentów. Odnotowuje jednak, że art. 12 ust. 1 mówi jedynie o krajowych przedstawicielach i ich asystentach, gdy tymczasem pozostałe ustępy tego artykułu – także o zastępcach krajowych przedstawicieli. Prawodawca powinien w tym kontekście zadbać o precyzję i spójność.

Nadzór – ku spójnemu i wszechstronnemu modelowi

56. Jeżeli chodzi o proponowany nadzór nad trzeciofilarową częścią systemu, Inspektor zwraca uwagę prawodawcy na fakt, że należy zapewnić spójny i wszechstronny nadzór nad całym systemem. Należy mieć na uwadze skomplikowane ramy prawne, którym podlega system – oparte na dwóch podstawach prawnych – i dla jasności prawa oraz z powodów praktycznych powstrzymać się od tworzenia dwóch różnych modeli nadzoru.

57. Jak wspomniano już wcześniej, Inspektor jest obecnie odpowiedzialny za nadzór nad centralną częścią pierwszofilarowej części systemu. Jest to zgodne z art. 37 rozporządzenia Rady (WE) nr 515/97, zmienionego rozporządzeniem (WE) nr 766/2008, stwierdzającym, że „Europejski Inspektor Ochrony Danych nadzoruje zgodność SIC z rozporządzeniem (WE) nr 45/2001". Inspektor zauważa, że model nadzoru proponowany we francuskim projekcie nie uwzględnia tej roli. Model nadzoru opiera się na wspólnym organie nadzorczym systemu.

58. Inspektor docenia prace wspólnego organu nadzorczego, jednak chce zwrócić uwagę na dwa powody, dla których należałoby zastosować skoordynowany model nadzoru, spójny z obecną rolą nadzorczą Inspektora w przypadku innych systemów o dużej skali. Po pierwsze, taki model zapewniłby wewnętrzną spójność między trzecio- a pierwszofilarową częścią systemu. Po drugie, zapewniłby spójność z modelami ustanowionymi dla innych systemów o dużej skali. Dlatego Inspektor radzi, by do całego systemu zastosować podobny model jak do SIS II („skoordynowany nadzór" lub „model wielokierunkowy"). Jak wspomniał Inspektor w opinii o pierwszofilarowej części systemu „w ramach SIS II prawodawca europejski zdecydował się na racjonalizację modelu nadzoru, stosując ten sam wielokierunkowy model, który został opisany zarówno w częściach systemu działających w ramach pierwszego filara, jak i tych działających w ramach trzeciego".

59. Inspektor jest zdania, że najodpowiedniejszym rozwiązaniem w tym celu byłoby wprowadzenie bardziej jednolitego systemu nadzoru – już realizowanego modelu o strukturze trójkierunkowej: organy ochrony danych na szczeblu krajowym, Inspektor na szczeblu centralnym i koordynacja działań między obiema stronami. Inspektor jest przekonany, że plan zastąpienia konwencji stwarza niepowtarzalną okazję, by uprościć i uspójnić nadzór, w pełni dopasowując go do innych systemów o dużej skali (VIS, SIS II, Eurodac).

60. Ponadto skoordynowany model nadzoru bardziej uwzględnia zmiany, z którymi będzie się wiązać wejście w życie traktatu z Lizbony i zniesienie filarowej struktury UE.

61. Inspektor nie zajmuje stanowiska w sprawie tego, czy ustanowienie skoordynowanego modelu nadzoru wymagałoby wprowadzenia zmian do pierwszofilarowego instrumentu, któremu podlega system, mianowicie do rozporządzenia (WE) nr 766/2008 zmieniającego rozporządzenie (WE) nr 515/97, ale zwraca uwagę prawodawcy na fakt, że należy przeanalizować ten aspekt także z punktu widzenia spójności prawa.

Wykaz organów mających dostęp do systemu

62. W myśl art. 7 ust. 2 każde państwo członkowskie ma obowiązek przesłać pozostałym państwom członkowskim oraz komitetowi, o którym mowa w art. 26, wykaz właściwych organów wyznaczonych jako organy mające dostęp do systemu i określić, do jakich danych i w jakim celu każdy z tych organów może mieć dostęp.

63. Inspektor zwraca uwagę, że projekt przewiduje jedynie informowanie pozostałych państw członkowskich i komitetu, o którym mowa w art. 26, o organach mających dostęp do systemu, natomiast nie przewiduje publikacji wykazu takich organów. Należy nad tym ubolewać, ponieważ taka publikacja dałaby większą przejrzystość i stworzyła praktyczne narzędzie pozwalające skutecznie kontrolować system np. właściwym organom ochrony danych.

IV. **WNIOSKI**

64. Inspektor popiera projekt decyzji Rady w sprawie stosowania technologii informatycznych do potrzeb celnych. Podkreśla, że w związku z wciąż toczącymi się w Radzie pracami legislacyjnymi jego uwagi nie odnoszą się do ostatecznej wersji tego projektu.

65. Ubolewa z powodu braku dokumentów uzasadniających, które mogłyby dostarczyć pewnych niezbędnych wyjaśnień i informacji co do celów i specyfiki niektórych przepisów projektu.

66. Inspektor apeluje o to, by w projekcie więcej uwagi poświęcić zapotrzebowaniu na konkretne gwarancje ochrony danych. Widzi, że w pewnych kwestiach należy lepiej zadbać o praktyczne wdrożenie gwarancji ochrony danych; chodzi zwłaszcza o ograniczenie celu wykorzystywania danych wprowadzonych do systemu. Uważa, że od tego w zasadniczym stopniu zależy, czy system informacji celnej będzie lepiej funkcjonował.

67. Inspektor apeluje, by w projekcie wprowadzić skoordynowany model nadzoru. Należy zauważyć, że Inspektor pełni obecnie rolę nadzorczą wobec pierwszofilarowej części sytemu. Inspektor podkreśla, że dla spójności najlepiej byłoby zastosować skoordynowany model nadzoru także w przypadku trzeciofilarowej części systemu. Ten model zapewniłby także – tam gdzie jest to niezbędne i stosowne – spójność z innymi aktami prawnymi, którym podlega tworzenie i/lub stosowanie innych systemów informatycznych o dużej skali.

68. Inspektor apeluje, by lepiej wyjaśnić konieczność i proporcjonalność udostępnienia systemu Eurojustowi i Europolowi. Zwraca uwagę, że wyjaśnień na ten temat brakuje w projekcie.

69. Inspektor nalega także, by zaostrzyć przepisy art. 8 ust. 4 projektu dotyczące przekazywania danych państwom niebędącym państwami członkowskimi i organizacjom międzynarodowym. Należy m.in. zapewnić jednolity system oceny adekwatności.

70. Inspektor apeluje, by wprowadzić przepis o publikacji wykazu organów mających dostęp do systemu i w ten sposób zwiększyć przejrzystość i ułatwić nadzór nad systemem.

Sporządzono w Brukseli dnia 20 kwietnia 2009 r.

Peter HUSTINX

Europejski inspektor ochrony danych

Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (WE) nr 726/2004 ustanawiające wspólnotowe procedury wydawania pozwoleń dla produktów leczniczych stosowanych u ludzi i do celów weterynaryjnych i nadzoru nad nimi oraz ustanawiające Europejską Agencję Leków, odnośnie do nadzoru nad bezpieczeństwem farmakoterapii w odniesieniu do produktów leczniczych stosowanych u ludzi i do celów weterynaryjnych i nadzoru nad nimi oraz ustanawiające Europejską Agencję Leków, oraz w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywę 2001/83/WE w sprawie wspólnotowego kodeksu odnoszącego się do produktów leczniczych stosowanych u ludzi w zakresie nadzoru nad bezpieczeństwem farmakoterapii

(2009/C 229/04)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

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

uwzględniając Kartę praw podstawowych Unii Europejskiej, a 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]), a w szczególności jego art. 41,

WYDAŁ NASTĘPUJĄCĄ OPINIĘ:

I. WPROWADZENIE

Wnioski w sprawie zmiany aktualnego systemu nadzoru nad bezpieczeństwem farmakoterapii

1. W dniu 10 grudnia 2008 r. Komisja przyjęła dwa wnioski w sprawie zmiany – odpowiednio – rozporządzenia (WE) nr 726/2004 i dyrektywy 2001/83/WE ([3]). Rozporządzenie (WE) nr 726/2004 ustanawia wspólnotowe procedury wydawania pozwoleń dla produktów leczniczych stosowanych u ludzi i do celów weterynaryjnych i nadzoru nad nimi, a także Europejską Agencję Leków (zwaną dalej „EMEA") ([4]). Dyrektywa 2001/83/WE zawiera przepisy dotyczące wspólnotowego kodeksu odnoszącego się do produktów leczniczych stosowanych u ludzi, regulując określone procesy na szczeblu państw członkowskich ([5]). Wnioskowane zmiany dotyczą w obydwu dokumentach fragmentów związanych z *nadzorem nad bezpieczeństwem farmakoterapii* w odniesieniu do produktów leczniczych stosowanych u ludzi.

2. Nadzór nad bezpieczeństwem farmakoterapii definiuje się jako badania naukowe i działania związane z wykrywaniem, oceną i zrozumieniem niepożądanych działań produktów leczniczych oraz zapobieganiem tym niepożądanym działaniom ([6]). Stosowany obecnie w Europie system nadzoru nad bezpieczeństwem farmakoterapii umożliwia pacjentom i pracownikom ochrony zdrowia zgłaszanie niepożądanych działań leków odnośnym organom publicznym i prywatnym na szczeblu krajowym i europejskim. EMEA korzysta z ogólnoeuropejskiej bazy danych (baza *EudraVigilance*); jest to centralny punkt, w którym zgłasza się podejrzenia niepożądanych działań leków i zarządza takimi informacjami.

3. Nadzór nad bezpieczeństwem farmakoterapii jest postrzegany jako niezbędne uzupełnienie wspólnotowego systemu zezwoleń na produkty lecznicze; został on wprowadzony w 1965 roku wraz z przyjęciem dyrektywy Rady 65/65/EWG ([7]).

4. Jak wynika z uzasadnień oraz z oceny skutków regulacji dołączonej do wniosków, aktualny system nadzoru nad bezpieczeństwem farmakoterapii ma wiele słabych punktów, do których należy brak przejrzyście określonych ról i obowiązków poszczególnych podmiotów zainteresowanych, skomplikowane procedury zgłaszania przypadków niepożądanych działań leków, potrzeba zwiększenia przejrzystości i usprawnienia komunikacji w zakresie bezpieczeństwa leków, a także konieczność racjonalizacji planowania procesów zarządzania ryzykiem związanym z lekami.

5. Ogólnym celem obydwu wniosków jest usunięcie tych słabych punktów oraz usprawnienie i wzmocnienie wspólnotowego systemu nadzoru nad bezpieczeństwem farmakoterapii w celu poprawy ochrony zdrowia publicznego, zapewnienia właściwego funkcjonowania rynku wewnętrznego i uproszczenia aktualnych przepisów i procedur. ([8])

Dane osobowe w nadzorze nad bezpieczeństwem farmakoterapii i konsultacja z EIOD

6. Całościowe funkcjonowanie aktualnego systemu nadzoru nad bezpieczeństwem farmakoterapii opiera się na przetwarzaniu danych osobowych. Dane te są zawarte w sprawozdaniach dotyczących niepożądanych działań leków i mogą być uznane za dane dotyczące zdrowia („dane dotyczące zdrowia") osób zainteresowanych, ponieważ zawierają informacje na temat przyjmowanych leków i odnośnych problemów zdrowotnych. Przetwarzanie takich danych podlega ścisłym przepisom o ochronie danych określonym w art. 10 rozporządzenia (WE) nr 45/2001 oraz art. 8 dyrektywy 95/46/WE ([9]). Znaczenie ochrony takich danych wielokrotnie podkreślał

([1]) Dz.U. L 281 z 23.11.1995, s. 31.
([2]) Dz.U. L 8 z 12.1.2001, s. 1.
([3]) COM(2008) 664 wersja ostateczna i COM(2008) 665 wersja ostateczna.
([4]) Dz.U. L 136 z 30.4.2004, s. 1.
([5]) Dz.U. L 311 z 28.11.2001, s. 67.
([6]) Zob. uzasadnienia do obydwu wniosków na s. 3.
([7]) Dz.U. 22 z 9.2.1965, s. 369.
([8]) Zob. uzasadnienia, s. 2.
([9]) Zob. definicja danych dotyczących zdrowia w opinii Europejskiego Inspektora Ochrony Danych z dnia 2 grudnia 2008 r. dotyczącej proponowanej dyrektywy w sprawie praw pacjenta w transgranicznej opiece zdrowotnej, pkt 15–17, dostępna pod adresem http://www.edps.europa.eu

ostatnio Europejski Trybunał Praw Człowieka w związku z art. 8 europejskiej konwencji praw człowieka: „Ochrona danych osobowych, w szczególności danych medycznych, ma fundamentalne znaczenie w kontekście korzystania przez konkretną osobę z jej prawa do poszanowania życia prywatnego i rodzinnego, co gwarantuje art. 8 konwencji" ([10]).

7. Mimo to w aktualnej wersji rozporządzenia (WE) nr 726/2004 i dyrektywy 2001/83/WE brak jest jakichkolwiek odniesień do ochrony danych, za wyjątkiem jednego, konkretnego, zawartego w rozporządzeniu odniesienia, które zostanie omówione w pkt 21 i kolejnych.

8. Europejski Inspektor Ochrony Danych („EIOD") ubolewa nad tym, że proponowane zmiany nie uwzględniają aspektów dotyczących ochrony danych i że w sprawie tych dwóch wniosków dotyczących zmian nie podjęto z nim żadnych formalnych konsultacji, zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001. Obecna opinia opiera się więc zatem na art. 41 ust. 2 tego samego rozporządzenia. EIOD zaleca umieszczenie odniesienia do niniejszej opinii w preambule do obydwu wniosków.

9. EIOD zaznacza, że chociaż kwestie ochrony danych nie zostały w wystarczającym zakresie uwzględnione w aktualnych ramach prawnych ani we wnioskach dotyczących nadzoru nad bezpieczeństwem farmakoterapii, praktyczne zastosowanie centralnego wspólnotowego systemu EudraVigilance budzi oczywiste obawy związane z ochroną danych. Dlatego też EMEA w czerwcu 2008 roku poprosiła EIOD o kontrolę wstępną systemu EudraVigilance na podstawie art. 27 rozporządzenia (WE) nr 45/2001.

10. Niniejsza opinia i wnioski EIOD dotyczące kontroli wstępnej (których opublikowanie przewidziane jest na ten rok) z konieczności będą się w pewnym zakresie pokrywać. Jednakże główne cele tych dwóch instrumentów są inne: niniejsza opinia koncentruje się na ogólnych ramach prawnych, na których opiera się system ustanowiony rozporządzeniem (WE) nr 726/2004 i dyrektywą 2001/83/WE wraz z proponowanymi do niej zmianami, kontrola wstępna stanowi natomiast szczegółową analizę ochrony danych skupiającą się na tym, w jaki sposób aktualne przepisy zostały rozwinięte w późniejszych instrumentach (np. decyzjach i wytycznych) wydawanych przez EMEA lub wspólnie przez Komisję wraz z EMEA i jak system EudraVigilance funkcjonuje w praktyce.

11. W niniejszej opinii najpierw przedstawione zostanie uproszczone wyjaśnienie systemu nadzoru nad bezpieczeństwem farmakoterapii w UE ustanowionego rozporządzeniem (WE) nr 726/2004 i dyrektywą 2001/83/WE w ich obecnym kształcie. Następnie przeanalizowana zostanie potrzeba przetwarzania danych osobowych w związku z nadzorem nad bezpieczeństwem farmakoterapii. Potem omówione zostaną wnioski Komisji dotyczące poprawy aktualnych i przewidywanych ram prawnych i przedstawione zostaną zalecenia dotyczące zapewniania i ulepszania standardów ochrony danych.

II. SYSTEM NADZORU NAD BEZPIECZEŃSTWEM FARMAKOTERAPII W UE: PRZETWARZANIE DANYCH OSOBOWYCH I KWESTIE DOTYCZĄCE OCHRONY DANYCH

Podmioty biorące udział w zbieraniu i rozpowszechnianiu informacji

12. Zbieraniem i rozpowszechnianiem informacji na temat niepożądanych działań produktów leczniczych w Unii Europejskiej zajmuje się kilka różnych podmiotów. Na szczeblu krajowym dwa główne podmioty to posiadacze pozwoleń na dopuszczenie do obrotu (spółki posiadające pozwolenie na dopuszczenie produktów leczniczych do obrotu) oraz właściwe władze krajowe (organy odpowiedzialne za wydawanie pozwoleń na dopuszczenie do obrotu). Właściwe władze krajowe dopuszczają poszczególne produkty do obrotu na podstawie krajowych procedur, które obejmują procedurę wzajemnego uznawania i procedurę zdecentralizowaną ([11]). W przypadku produktów dopuszczanych do obrotu na podstawie tzw. procedury scentralizowanej organem właściwym może być również Komisja Europejska. Na szczeblu europejskim kolejnym istotnym podmiotem jest EMEA. Jednym z zadań tej agencji jest dbanie o rozpowszechnianie informacji na temat niepożądanych działań produktów leczniczych dopuszczanych do obrotu we Wspólnocie za pośrednictwem bazy danych, którą jest wymieniona wcześniej baza EudraVigilance.

Zbieranie i przechowywanie danych osobowych na szczeblu krajowym

13. Dyrektywa 2001/83/WE w ogólnym zarysie określa obowiązek posiadania przez państwa członkowskie systemu nadzoru nad bezpieczeństwem farmakoterapii, w którym zbierane są informacje „użyteczne w nadzorowaniu produktów leczniczych" (art. 102). Zgodnie z art. 103 i 104 dyrektywy 2001/83/WE (zob. także art. 23 i 24 rozporządzenia (WE) nr 726/2004, posiadacze pozwoleń na dopuszczenie do obrotu muszą posiadać własny system nadzoru nad bezpieczeństwem farmakoterapii, tak aby móc ponosić odpowiedzialność za swoje produkty wprowadzone na rynek i aby zapewnić możliwość podjęcia działań w razie potrzeby. Informacje zbierane są od pracowników ochrony zdrowia lub bezpośrednio od pacjentów. Posiadacz pozwolenia na dopuszczenie do obrotu zobowiązany jest zgłaszać właściwemu organowi w formie elektronicznej wszystkie informacje istotne z punktu widzenia bilansu ryzyka i korzyści produktu leczniczego.

14. Sama dyrektywa 2001/83/WE nie określa zbyt precyzyjnie, jakie informacje dotyczące działań niepożądanych należy zbierać na szczeblu krajowym, jak należy je przechowywać czy przekazywać. Artykuły 104 i 106 wspominają jedynie o obowiązku składania „sprawozdań". Bardziej szczegółowe przepisy dotyczące tych sprawozdań znajdują się w wytycznych opracowanych przez Komisję po konsultacjach z EMEA, państwami członkowskimi i stronami zainteresowanymi, na podstawie art. 106. W takich wytycznych

([10]) Zob. EKPC 17 lipca 2008 r., *I przeciwko Finlandii* (nr wniosku 20511/03), pkt 38 i EKPC 25 listopada 2008 r., *Armonas przeciwko Litwie* (nr wniosku 36919/02), pkt 40.

([11]) Zob. ocena skutków regulacji, s. 10.

dotyczących nadzoru nad bezpieczeństwem farmakoterapii w zakresie produktów leczniczych stosowanych u ludzi (zwanych dalej: „wytycznymi") znajduje się odniesienie do tzw. „indywidualnych sprawozdań dotyczących bezpieczeństwa przypadku" („ICSR"), czyli sprawozdań dotyczących niepożądanych działań produktów leczniczych odnoszących się do konkretnego pacjenta ([12]). Z wytycznych wynika, że jedną z informacji absolutnie wymaganych w sprawozdaniach ICSR jest „identyfikowalny pacjent" ([13]) Wytyczne stanowią, że pacjent może być zidentyfikowany na podstawie inicjałów, numeru pacjenta, daty urodzenia, wagi, wzrostu i płci, numeru szpitalnej karty pacjenta, informacji dotyczących historii chorób pacjenta oraz informacji dotyczących rodziców pacjenta ([14]).

15. Z uwagi na podkreślenie możliwości identyfikacji pacjenta, przetwarzanie takich danych w sposób oczywisty wchodzi w zakres przepisów o ochronie danych zawartych w dyrektywie 95/46/WE. Tak więc chociaż pacjent nie jest wymieniony z nazwiska, poprzez zestawienie różnych informacji (np. danych szpitala, daty urodzenia, inicjałów) i w określonych okolicznościach (np. w zamkniętych społecznościach lub niewielkich miejscowościach) możliwe jest jego zidentyfikowanie. Dlatego też informacje przetwarzane w związku z nadzorem nad bezpieczeństwem farmakoterapii powinny być zasadniczo traktowane jak informacje dotyczące identyfikowalnej osoby fizycznej w rozumieniu art. 2 lit. a) dyrektywy 95/46/WE ([15]). Chociaż ani dyrektywa, ani rozporządzenie nie określają tego jasno, jest to odzwierciedlone w wytycznych, które mówią, że „informacje powinny być na tyle pełne, na ile to możliwe, z uwzględnieniem prawodawstwa UE dotyczącego ochrony danych" ([16]).

16. Należy również podkreślić, że pomimo istnienia wytycznych procedury zgłaszania działań niepożądanych na szczeblu krajowym są w niewielkim stopniu ujednolicone. Kwestia ta zostanie dokładniej omówiona w pkt 24 i 25 poniżej.

Baza danych EudraVigilance

17. Kluczową rolę w systemie nadzoru nad bezpieczeństwem farmakoterapii w UE odgrywa baza danych EudraVigilance prowadzona przez EMEA. Jak już wspomniano, EudraVigilance to scentralizowana sieć przetwarzania danych i system zarządzania danymi służący do zgłaszania i oceny podejrzewanych działań niepożądanych w trakcie tworzenia produktów leczniczych i po uzyskaniu pozwolenia na dopuszczenie ich do obrotu we Wspólnocie Europejskiej i w krajach tworzących Europejski Obszar Gospodarczy. Podstawa prawna bazy danych EudraVigilance znajduje się w art. 57 ust. 1 lit. d) rozporządzenia (WE) nr 726/2004.

18. Obecna baza danych EudraVigilance składa się z dwóch działów, a mianowicie (1) informacji pochodzących z badań klinicznych (odbywających się przed dopuszczeniem leku do obrotu, w okresie zwanym „okresem przed dopuszczeniem") i (2) informacji pochodzących ze sprawozdań dotyczących niepożądanych działań (zebranych już potem, w okresie zwanym „okresem po dopuszczeniu"). Niniejsza opinia skupia się na „okresie po dopuszczeniu", ponieważ na nim koncentrują się proponowane zmiany.

19. Baza danych EudraVigilance zawiera dane na temat pacjentów pochodzące ze sprawozdań ICSR. EMEA otrzymuje sprawozdania ICSR od właściwych władz krajowych (zob. art. 102 dyrektywy 2001/83/WE i art. 22 rozporządzenia (WE) nr 726/2004), a w niektórych przypadkach także bezpośrednio od posiadaczy pozwoleń na dopuszczenie do obrotu (zob. art. 104 dyrektywy 2001/83/WE i art. 24 rozporządzenia (WE) nr 726/2004).

20. Niniejsza opinia skupia się na przetwarzaniu danych osobowych dotyczących pacjentów. Należy jednak pamiętać, że baza danych EudraVigilance zawiera także dane osobowe dotyczące osób pracujących we właściwych władzach krajowych lub u posiadaczy pozwoleń na dopuszczenie do obrotu, które dostarczają dane do bazy. W systemie przechowywane są imiona i nazwiska, adresy, informacje kontaktowe oraz dane dokumentów tożsamości tych osób. Kolejna kategoria danych osobowych to dane dotyczące tzw. wykwalifikowanych osób odpowiedzialnych za nadzór nad bezpieczeństwem farmakoterapii, które powoływane są przez posiadaczy pozwoleń na dopuszczenie do obrotu na podstawie art. 103 dyrektywy 2001/83/WE. Oczywistym jest więc, że prawa i obowiązki wynikające z rozporządzenia (WE) nr 45/2001 mają w pełni zastosowanie do przetwarzania takich informacji.

Dostęp do bazy danych EudraVigilance

21. Artykuł 57 ust. 1 lit. d) rozporządzenia (WE) nr 726/2004 stanowi, że baza danych powinna być stale dostępna dla wszystkich państw członkowskich. Pracownicy ochrony zdrowia, posiadacze pozwoleń na dopuszczenie do obrotu i obywatele muszą ponadto posiadać odpowiedni poziom dostępu do tej bazy danych przy jednoczesnym zapewnieniu ochrony danych osobowych. Jak już wspomniano w pkt 7, jest to jedyny przepis w rozporządzeniu i dyrektywie 2001/83/WE, który zawiera odniesienie do ochrony danych.

22. Artykuł 57 ust. 1 lit. d) wprowadził następujące zasady dostępu. Po otrzymaniu sprawozdania ICSR przez EMEA jest ono bezpośrednio wprowadzane do bramki EudraVigilance, do której pełny dostęp mają EMEA, właściwe władze krajowe oraz Komisja. Po zatwierdzeniu sprawozdania ICSR (sprawdzeniu jego autentyczności i niepowtarzalności) przez EMEA, informacje znajdujące się w sprawozdaniu ICSR przekazywane są do właściwej bazy danych. EMEA,

([12]) Zob. tom 9A Zasad dotyczących produktów leczniczych w Unii Europejskiej: Wytyczne dotyczące nadzoru nad bezpieczeństwem farmakoterapii z użyciem produktów leczniczych stosowanych u ludzi dostępne są pod adresem: http://ec.europa.eu/enterprise/pharmaceuticals/eudralex/vol-9/pdf/vol9a_09-2008.pdf

([13]) Zob. wytyczne, s. 57.

([14]) Zob. przypis 13.

([15]) Artykuł 2 lit. a) dyrektywy 95/46/WE definiuje „dane osobowe" jako „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dane dotyczą"); 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". Motyw 26 stanowi ponadto, że: „... w celu ustalenia, czy daną osobę można zidentyfikować, należy wziąć pod uwagę *wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba* w celu zidentyfikowania owej osoby". Dodatkowe omówienie znajduje się w art. 29 opinii grupy roboczej 4/2007 dotyczącej pojęcia danych osobowych (dokument WP 136) przyjętej dnia 20 czerwca 2007 r. i dostępnej pod adresem http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm Dotyczy to również rozporządzenia (WE) nr 45/2001.

([16]) Zob. przypis 13.

właściwe władze krajowe i Komisja mają pełny dostęp do bazy danych, natomiast posiadacze pozwoleń na dopuszczenie do obrotu mają jedynie dostęp do bazy z określonymi ograniczeniami, a mianowicie mogą mieć wgląd jedynie w dane, które sami przesłali do EMEA. Informacje zbiorcze dotyczące sprawozdań ICSR są następnie umieszczane na stronie internetowej EudraVigilance, do której dostęp ma ogół społeczeństwa, łącznie z pracownikami ochrony zdrowia.

23. W dniu 19 grudnia 2008 r. EMEA opublikowała na swojej stronie internetowej projekt polityki dostępu w celu jego konsultacji publicznej ([17]). Dokument ten pokazuje, w jaki sposób EMEA planuje wdrożyć art. 57 ust. 1 lit. d) rozporządzenia (WE) nr 726/2004. EIOD wróci pokrótce do tego zagadnienia w pkt 48 niniejszej opinii i kolejnych.

Słabe punkty obecnego systemu i brak zabezpieczeń ochrony danych

24. Opracowana przez Komisję ocena skutków regulacji przedstawia szereg słabych punktów obecnego systemu nadzoru nad bezpieczeństwem farmakoterapii w UE, który uznawany jest za zawiły i niejasny. Za jedną z najważniejszych wad uznaje się skomplikowany system zbierania i przechowywania danych oraz ich wymiany między poszczególnymi podmiotami na szczeblu krajowym i europejskim. Sytuację dodatkowo komplikują rozbieżności w sposobach wdrażania dyrektywy 2001/83/WE w poszczególnych państwach członkowskich ([18]). W związku z tym właściwe władze krajowe oraz EMEA często spotykają się z niepełnymi lub powtarzającymi się sprawozdaniami dotyczącymi przypadków niepożądanych działań produktów leczniczych ([19]).

25. Wynika to z tego, że wprawdzie opis zawartości sprawozdania ICSR został podany w wyżej wymienionych wytycznych, jednak decyzja o sposobie realizacji takich sprawozdań na szczeblu krajowym należy do państw członkowskich. Dotyczy to zarówno sposobu komunikacji zastosowanego do przesłania sprawozdania przez posiadaczy pozwoleń na dopuszczenie do obrotu właściwym władzom krajowym oraz faktycznych informacji zawartych w takich sprawozdaniach (w Europie brak jest ujednoliconego wzoru dla takich sprawozdań). Ponadto, niektóre właściwe władze krajowe mogą stosować szczegółowe kryteria jakości dotyczące dopuszczalności poszczególnych sprawozdań (na podstawie ich treści, kompletności itp.), podczas gdy w innych krajach takie praktyki mogą nie mieć miejsca. Oczywistym jest, że podejście zastosowane na szczeblu krajowym w zakresie przedkładania i oceny jakości sprawozdań ICSR przekłada się bezpośrednio na sposób przedstawiania takich sprawozdań w EMEA, tj. w bazie danych EudraVigilance.

26. EIOD pragnie podkreślić, że wspomniane słabe punkty nie tylko prowadzą do problemów natury praktycznej, ale stanowią również poważne zagrożenie dla ochrony danych dotyczących zdrowia obywateli. Mimo że, jak wykazano w poprzednich punktach, przetwarzanie danych dotyczących zdrowia odbywa się na kilku etapach nadzoru nad bezpieczeństwem farmakoterapii, nie istnieją obecnie żadne przepisy dotyczące ochrony takich danych. Jedyny wyjątek to ogólne odniesienie do ochrony danych zawarte w art. 57 ust. 1 lit. d) rozporządzenia (WE) nr 726/2004, które dotyczy jedynie ostatniego etapu przetwarzania danych, a mianowicie dostępności danych zawartych w bazie danych EudraVigilance. Ponadto, brak jasności w odniesieniu do ról i obowiązków poszczególnych podmiotów biorących udział w przetwarzaniu danych, a także brak określonych standardów samego przetwarzania zagraża poufności, a także spójności i rzetelności przetwarzanych danych osobowych.

27. EIOD pragnie zatem podkreślić, że brak dokładnej analizy ochrony danych, który widoczny jest w ramach prawnych stanowiących podstawę systemu nadzoru nad bezpieczeństwem farmakoterapii w UE, również należy postrzegać jako jedną ze słabości obecnego systemu. Można to poprawić zmieniając obowiązujące przepisy.

III. NADZÓR NAD BEZPIECZEŃSTWEM FARMAKOTERAPII I POTRZEBA DANYCH OSOBOWYCH

28. EIOD pragnie zająć się kwestią podstawową i ogólną, a mianowicie tym, czy przetwarzanie danych dotyczących zdrowia identyfikowalnych osób fizycznych jest faktycznie *konieczne* na wszystkich etapach systemu nadzoru nad bezpieczeństwem farmakoterapii (na szczeblu krajowym i europejskim).

29. Jak już wyjaśniono, w sprawozdaniach ICSR pacjent nie występuje z imienia ani nazwiska, a zatem nie jest zidentyfikowany. Jednakże identyfikacja pacjenta nadal mogłaby być w niektórych przypadkach możliwa na podstawie zestawienia różnych informacji figurujących w sprawozdaniu ICSR. Jak wynika z wytycznych, w niektórych przypadkach podany jest konkretny numer pacjenta, z czego wynika, że system jako całość pozwala na zidentyfikowanie danej osoby. Jednakże ani dyrektywa, ani rozporządzenie nie zawierają odniesień, z których wynikałoby, że możliwość identyfikowania osób jest częścią *celu* systemu nadzoru nad bezpieczeństwem farmakoterapii.

30. EIOD wzywa zatem prawodawcę do uściślenia, czy możliwość identyfikowania osób jest faktycznie jednym z celów nadzoru nad bezpieczeństwem farmakoterapii na poszczególnych etapach przetwarzania danych, a w szczególności w ramach bazy danych EudraVigilance.

31. W związku z tym pouczające byłoby porównanie z planowanym systemem dawstwa i przeszczepów narządów ([20]) W kontekście przeszczepów narządów możliwość przyporządkowania danego narządu do jego dawcy, jak również jego odbiorcy jest nadzwyczaj ważna, szczególnie w przypadku poważnych niepożądanych zdarzeń lub reakcji.

([17]) Zob. projekt polityki dostępu do bazy EudraVigilance w zakresie produktów leczniczych stosowanych u ludzi z dnia 19 grudnia 2008 r., który znajduje się pod adresem http://www.emea.europa.eu/pdfs/human/phv/18743906en.pdf

([18]) Zob. ocena skutków regulacji, s. 17.

([19]) Zob. przypis 18.

([20]) Zob. wniosek Komisji w sprawie dyrektywy Parlamentu Europejskiego i Rady w sprawie norm jakości i bezpieczeństwa narządów ludzkich do przeszczepu, COM(2008) 818 wersja ostateczna. Zob. opinia EIOD z dnia 5 marca 2009 r. dostępna pod adresem http://www.edps.europa.eu

32. Jednak w kontekście nadzoru nad bezpieczeństwem farmakoterapii EIOD nie ma wystarczających dowodów, aby stwierdzić, że możliwość identyfikacji jest faktycznie zawsze potrzebna. Nadzór nad bezpieczeństwem farmakoterapii polega na zgłaszaniu niepożądanych działań produktów leczniczych, które są i będą wykorzystywane przez (przeważnie) nieznaną liczbę ludzi. Istnieje zatem – przynajmniej w „okresie po dopuszczeniu" – mniej automatyczne i indywidualne powiązanie między informacjami dotyczącymi działań niepożądanych a daną osobą, tak jak w przypadku informacji dotyczących narządów i osób biorących udział w przeszczepie określonego narządu. Oczywistym jest, że pacjenci, którzy korzystali z określonego produktu leczniczego i zgłosili działania niepożądane, są zainteresowani wynikami ewentualnych późniejszych analiz. Nie oznacza to jednak, że zgłaszane informacje muszą być *w każdym przypadku* przyporządkowane do tej konkretnej osoby na wszystkich etapach nadzoru nad bezpieczeństwem farmakoterapii. W wielu przypadkach wystarczyłoby przyporządkowanie informacji dotyczących działań niepożądanych do samego produktu leczniczego, co pozwoliłoby zainteresowanym podmiotom, być może za pośrednictwem pracowników ochrony zdrowia, na informowanie pacjentów w ogólnym zakresie o konsekwencjach przyjmowania lub przyjęcia określonego produktu leczniczego.

33. Jeżeli w ogóle przewiduje się możliwość identyfikacji, EIOD pragnie przypomnieć analizę zawartą w jego opinii dotyczącej wniosku Komisji dotyczącego dyrektywy w sprawie norm jakości i bezpieczeństwa narządów ludzkich do przeszczepu. W tej opinii inspektor wyjaśnił powiązanie między możliwością śledzenia, możliwością identyfikacji, anonimowością i poufnością danych. Możliwość identyfikacji to termin kluczowy w prawodawstwie z zakresu ochrony danych ([21]). Przepisy dotyczące ochrony danych mają zastosowanie do danych dotyczących osób zidentyfikowanych lub *identyfikowalnych* ([22]). Możliwość przyporządkowania danych do konkretnej osoby – możliwość śledzenia – można przyrównać do możliwości identyfikacji. W prawodawstwie z zakresu ochrony danych anonimowość jest przeciwieństwem możliwości identyfikacji, a zatem możliwości śledzenia. Dane są uznawane za anonimowe, tylko jeśli niemożliwe jest zidentyfikowanie osoby, której dotyczą dane (lub przyporządkowanie jej do tych danych). Pojęcie „anonimowości" różni się zatem tu od definicji przyjętej zwyczajowo w życiu codziennym, zgodnie z którą osoby anonimowej nie można zidentyfikować na podstawie danych, na przykład dlatego że jej nazwisko zostało wymazane. W takich sytuacjach mówimy o poufności danych, co oznacza, że informacje są (w pełni) dostępne jedynie dla podmiotów upoważnionych do uzyskania do nich dostępu. Chociaż możliwość śledzenia i anonimowość nie mogą istnieć jednocześnie, jest to możliwe w przypadku możliwości śledzenia i poufności.

34. Oprócz możliwości śledzenia kolejnym uzasadnieniem zachowania możliwości identyfikacji pacjentów na wszystkich etapach nadzoru nad bezpieczeństwem farmakoterapii mogłoby być *dobre działanie* systemu. EIOD wie, że kiedy informacje dotyczą osoby identyfikowalnej, a zatem niepowtarzalnej, właściwym organom (np. właściwym władzom krajowym i EMEA) łatwiej jest monitorować i kontrolować treść sprawozdań ICSR (np. w celu ich sprawdzania pod kątem sprawozdań powtarzających się). Chociaż EIOD dostrzega potrzebę istnienia takiego mechanizmu kontroli, nie jest przekonany, że samo to uzasadniałoby przechowywanie identyfikowalnych danych na wszystkich etapach nadzoru nad bezpieczeństwem farmakoterapii, a zwłaszcza w bazie danych EudraVigilance. Powtarzającym się sprawozdaniom można by zapobiegać już na szczeblu krajowym poprzez lepsze ustrukturyzowanie i koordynację systemu sprawozdawczości, na przykład dzięki wprowadzeniu systemu zdecentralizowanego, co omówione zostało w pkt 42 i kolejnych.

35. EIOD uznaje, że w szczególnych okolicznościach niemożliwa jest anonimizacja danych. Jest tak na przykład w przypadku korzystania z określonych produktów leczniczych przez bardzo wąską grupę osób. W takich przypadkach należy wprowadzić określone zabezpieczenia, tak aby wypełniać zobowiązania, które nakłada prawodawstwo z zakresu ochrony danych.

36. Reasumując, EIOD ma poważne wątpliwości, czy możliwość śledzenia lub wykorzystywania danych dotyczących identyfikowalnych pacjentów jest konieczna na wszystkich etapach nadzoru nad bezpieczeństwem farmakoterapii. EIOD zdaje sobie sprawę, że zaniechanie przetwarzania na każdym etapie danych identyfikowalnych może nie być możliwe, zwłaszcza na szczeblu krajowym, na którym odbywa się właściwe zbieranie informacji dotyczących działań niepożądanych. Jednakże przepisy dotyczące ochrony danych wymagają, aby przetwarzanie danych dotyczących zdrowia zachodziło tylko wtedy, gdy jest absolutnie niezbędne. Wykorzystanie danych identyfikowalnych należy zatem możliwie jak najbardziej ograniczyć i zapobiegać mu lub powstrzymywać je na jak najwcześniejszym etapie w przypadkach, w których jest ono uznawane za niezbędne. EIOD wzywa zatem prawodawcę do ponownego zbadania konieczności wykorzystywania takich informacji na szczeblu europejskim oraz na szczeblu krajowym.

37. Zauważa się, że w przypadkach, w których faktycznie istnieje potrzeba przetwarzania identyfikowalnych danych lub kiedy niemożliwa jest anonimizacja danych (zob. pkt 35 powyżej), należy zbadać możliwości techniczne pośredniej identyfikacji osób, których dane dotyczą, np. przy zastosowaniu pseudonimizacji ([23]).

38. EIOD zaleca zatem wprowadzenie w rozporządzeniu (WE) nr 726/2004 i dyrektywie 2001/83/WE nowego artykułu, który stanowić będzie, że przepisy rozporządzenia (WE) nr 726/2004 i dyrektywy 2001/83/WE nie naruszają praw i obowiązków wynikających odpowiednio z przepisów rozporządzenia (WE) nr 45/2001 i dyrektywy 95/46/WE, ze szczególnym odniesieniem do art. 10 rozporządzenia (WE) nr 45/2001 i art. 8 dyrektywy 95/46/WE. Należy

([21]) Zob. opinia Europejskiego Inspektora Ochrony Danych, pkt 11–28.

([22]) Zob. art. 2 lit. a) dyrektywy 95/46/WE i art. 3 lit. a) rozporządzenia (WE) nr 45/2001 oraz dalsze wyjaśnienia w przypisie 13.

([23]) Pseudonimizacja to proces, który można zastosować do ukrycia tożsamości osoby, której dotyczą dane, przy jednoczesnym zachowaniu lokalizowalności tych danych. Istnieją różne możliwości techniczne, np. bezpieczne przechowywanie list prawdziwych tożsamości i przypisanych im pseudonimów, stosowanie dwukierunkowych algorytmów kryptograficznych itd.

tu jeszcze dodać, że identyfikowalne dane dotyczące zdrowia należy przetwarzać tylko wtedy, gdy będzie to absolutnie niezbędne, a podmioty biorące udział w tym przetwarzaniu powinny taką konieczność badać na każdym etapie nadzoru nad bezpieczeństwem farmakoterapii.

IV. **SZCZEGÓŁOWA ANALIZA WNIOSKU**

39. Chociaż ochrona danych jest praktycznie nieuwzględniona w proponowanych zmianach, wskazana wydaje się bardziej szczegółowa analiza wniosku, ponieważ pokazuje ona, że niektóre z przewidywanych zmian zwiększają skutki i późniejsze zagrożenia związane z ochroną danych.

40. Ogólnym założeniem tych dwóch wniosków jest poprawa spójności przepisów, precyzyjniejsze określenie obowiązków, uproszczenie systemu sprawozdawczości i wzmocnienie bazy danych EudraVigilance ([24]).

Dokładniejsze objaśnienie obowiązków

41. Komisja najwyraźniej próbowała dokładniej określić zakres obowiązków proponując zmianę aktualnych przepisów, tak aby z samego prawodawstwa wyraźniej wynikało, kto za co odpowiada. Oczywiście dokładniejsze określenie zainteresowanych podmiotów i ich zobowiązań w zakresie zgłaszania działań niepożądanych wpływa korzystnie na przejrzystość systemu, jest zatem zmianą na lepsze również z punktu widzenia ochrony danych. Pacjenci powinni być w stanie z lektury prawodawstwa w ogólnym zarysie zrozumieć jak, kiedy i przez kogo przetwarzane są ich dane osobowe. Jednakże proponowane wyjaśnienie zakresu obowiązków i odpowiedzialności powinno być także wyraźnie przedstawione w kontekście odpowiedzialności i obowiązków wynikających z prawodawstwa dotyczącego ochrony danych.

Uproszczenie systemu sprawozdawczości

42. Uproszczenie systemu sprawozdawczości powinno być osiągnięte poprzez wykorzystanie poświęconych bezpieczeństwu leków krajowych portali internetowych, które powiązane są z europejskim portalem internetowym poświęconym bezpieczeństwu leków (zob. nowo zaproponowany art. 106 dyrektywy 2001/83/WE oraz art. 26 rozporządzenia (WE) nr 726/2004). Krajowe portale internetowe zawierać będą ogólnodostępne formularze służące pracownikom ochrony zdrowia i pacjentom do zgłaszania podejrzewanych działań niepożądanych (zob. nowo zaproponowany art. 106 ust. 3 dyrektywy 2001/83/WE oraz art. 25 rozporządzenia (WE) nr 726/2004). Również europejskie portale internetowe zawierać będą informacje na temat przesyłania sprawozdań, w tym standardowe formularze do wysyłania sprawozdań przez Internet dla pacjentów i pracowników ochrony zdrowia.

43. EIOD pragnie podkreślić, że chociaż wykorzystanie takich portali internetowych i standardowych formularzy poprawi wydajność systemu sprawozdawczości, zwiększy jednak jednocześnie ryzyko związane z ochroną danych, na jakie narażony będzie system. EIOD wzywa prawodawcę do objęcia procesu tworzenia takiego systemu sprawozdawczości wymogami prawa o ochronie danych osobowych. Oznacza to, jak już wspomniano, że konieczność przetwarzania danych osobowych powinna być należycie badana w odniesieniu do każdego etapu procesu. Powinno to być odzwierciedlane w sposobie organizacji sprawozdań na szczeblu krajowym oraz w procesie przesyłania informacji do EMEA i do bazy danych EudraVigilance. W szerszej perspektywie EIOD zdecydowanie zaleca stworzenie na szczeblu krajowym jednolitych formularzy, które zapobiegłyby stosowaniu różnych praktyk skutkujących zróżnicowaniem poziomów ochrony danych.

44. Z planowanego systemu wynika zatem, jak się wydaje, że *pacjenci* mogą przesyłać sprawozdania bezpośrednio do EMEA lub nawet bezpośrednio do samej bazy danych EudraVigilance. Oznaczałoby to, że w przypadku aktualnej aplikacji bazy danych EudraVigilance informacje umieszczane w bramce EMEA, jak wyjaśniono w pkt 21–22 powyżej, byłyby w pełni dostępne również dla Komisji i właściwych władz krajowych.

45. Ogólnie rzecz biorąc, EIOD zdecydowanie popiera *zdecentralizowany system sprawozdawczości*. Komunikacja z europejskim portalem internetowym powinna być koordynowana przy pomocy krajowych portali internetowych, za które odpowiadają właściwe władze krajowe. Należy również wykorzystywać możliwość *pośredniego* nadsyłania sprawozdań przez pacjentów, tj. za pośrednictwem pracowników ochrony zdrowia (przy pomocy portali internetowych lub nie) zamiast możliwości *bezpośredniego* składania sprawozdań przez pacjentów, szczególnie w odniesieniu do bazy danych EudraVigilance.

46. W każdym razie, system nadsyłania sprawozdań za pośrednictwem portali internetowych wymaga ścisłych zasad bezpieczeństwa. W tym kontekście EIOD pragnie nawiązać do swej wcześniej wymienionej opinii dotyczącej proponowanej dyrektywy w sprawie transgranicznej opieki zdrowotnej, szczególnie do części dotyczącej bezpieczeństwa danych w państwach członkowskich i prywatności w aplikacjach w zakresie e-zdrowia ([25]). W opinii tej EIOD podkreślił już, że prywatność i bezpieczeństwo powinny być częścią projektu i realizacji wszystkich aplikacji w zakresie e-zdrowia (*domyślna ochrona prywatności*) ([26]). Ta sama kwestia dotyczy przewidywanych portali internetowych.

47. EIOD zaleca zatem zawarcie obowiązku uwzględniania odpowiednich środków ochrony prywatności i bezpieczeństwa w nowo zaproponowanych art. 25 i 26 rozporządzenia (WE) nr 726/2004 i art. 106 dyrektywy 2001/83/WE, które regulują kwestie związane z tworzeniem – w oparciu o portale internetowe – systemu sprawozdawczości działań niepożądanych. Zasady poufności, spójności, wiarygodności i dostępności danych mogłyby również zostać wymienione jako główne cele

([24]) Zob. uzasadnienia, s. 2–3.

([25]) Zob. wymieniona w przypisie 7 opinia Europejskiego Inspektora Ochrony Danych w sprawie praw pacjenta w transgranicznej opiece zdrowotnej, pkt 32–34.

([26]) Zob. pkt 32 opinii.

z zakresu bezpieczeństwa, które powinny być zagwarantowane na tym samym poziomie we wszystkich państwach członkowskich. Możliwe jest też uwzględnienie zastosowania właściwych standardów i środków technicznych, takich jak szyfrowanie i uwierzytelnianie przy pomocy podpisu cyfrowego.

Wzmocnienie bazy danych EudraVigilance: poprawa dostępu

48. Nowo zaproponowany art. 24 rozporządzenia (WE) nr 726/2004 dotyczy bazy danych EudraVigilance. Z artykułu jasno wynika, że wzmocnienie bazy danych oznacza zwiększenie jej wykorzystania przez poszczególne zainteresowane strony w zakresie dostarczania informacji do bazy i uzyskiwania do nich dostępu. Szczególnie interesujące są dwa ustępy art. 24.

49. Artykuł 24 ust. 2 mówi o dostępności bazy danych. Zastępuje on obecny art. 57 ust. 1 lit. d) rozporządzenia (WE) nr 726/2004, który był wymieniony wcześniej jako jedyny przepis aktualnie odnoszący się do ochrony danych. To odniesienie do ochrony danych zostało utrzymane, jednak zmniejszyła się liczba podmiotów nim objętych. Aktualna wersja stanowi, że pracownicy ochrony zdrowia, posiadacze pozwoleń na dopuszczenie do obrotu i obywatele uzyskają odpowiedni poziom dostępu do bazy danych przy jednoczesnej ochronie danych osobowych, Komisja natomiast proponuje teraz usunąć z tej listy posiadaczy pozwoleń na dopuszczenie do obrotu i udzielić im prawa dostępu „w zakresie umożliwiającym im przestrzeganie obowiązków związanych z nadzorem nad bezpieczeństwem farmakoterapii" bez żadnego odniesienia do ochrony danych. Przyczyny tego są niejasne.

50. Artykuł 24 ust. 3 ustanawia ponadto zasady dostępu do sprawozdań ICSR. Dostępu może zażądać każdy obywatel i będzie on mu przyznany w ciągu 90 dni, „o ile ujawnienie danych nie narusza anonimowości podmiotów sprawozdania". EIOD popiera zamysł tego przepisu, a mianowicie to, że możliwe jest tylko ujawnianie danych anonimowych. Pragnie jednak podkreślić, jak już wcześniej wyjaśniano, że anonimowość należy interpretować jako całkowity brak możliwości zidentyfikowania osoby, która zgłosiła wystąpienie działań niepożądanych (zob. także pkt 33).

51. Należy w ogólnym zakresie ponownie rozważyć dostęp do systemu EudraVigilance w świetle przepisów o ochronie danych. Ma to również bezpośrednie konsekwencje dla projektu polityki dostępu opublikowanego przez EMEA w grudniu 2008 roku i wymienionego w pkt 23 ([27]). O ile informacje zawarte w bazie danych EudraVigilance dotyczą identyfikowalnych osób fizycznych, dostęp do takich danych powinien możliwie jak najbardziej ograniczony.

52. EIOD zaleca zatem umieszczenie w proponowanym art. 24 ust. 2 rozporządzenia (WE) nr 726/2004 przepisu, z którego wynikać będzie, że dostęp do bazy danych EudraVigilance jest regulowany zgodnie z prawami i obowiązkami wynikającymi z prawodawstwa wspólnotowego dotyczącego ochrony danych.

([27]) Zob. też przypis 15.

Prawa osoby, której dotyczą dane

53. EIOD pragnie podkreślić, że po przetworzeniu danych identyfikowalnych strona odpowiedzialna za takie przetworzenie powinna spełnić wszystkie wymogi prawodawstwa wspólnotowego dotyczącego ochrony danych. Oznacza to m.in., że osoba zainteresowana jest świadoma tego, co będzie się działo z danymi i kto będzie je przetwarzał, oraz posiada wszelkie inne informacje wymagane zgodnie z art. 11 rozporządzenia (WE) nr 45/2001 lub art. 10 dyrektywy 95/46/WE. Osoba zainteresowana powinna ponadto mieć możliwość powołania się na przysługujące jej prawa na szczeblu krajowym i szczeblu europejskim, takie jak prawo dostępu do danych (art. 12 dyrektywy 95/46/WE i art. 13 rozporządzenia (WE) nr 45/2001), prawo sprzeciwu (art. 18 rozporządzenia (WE) nr 45/2001 i art. 14 dyrektywy 95/46/WE) itd.

54. EIOD zaleca zatem, aby do treści proponowanego art. 101 dyrektywy 2001/83/WE dodać ustęp, z którego wynikać będzie, że w przypadku przetwarzania danych osobowych danej osobie przekazane będą odpowiednie informacje, zgodnie z treścią art. 10 dyrektywy 95/46/WE.

55. Kwestia dostępu do własnych informacji zawartych w bazie danych EudraVigilance nie została poruszona ani w aktualnym ani w proponowanym prawodawstwie. Należy podkreślić, że w przypadkach, w których uznaje się za niezbędne przechowywanie danych osobowych w bazie, jak już wspominano, dany pacjent powinien mieć możliwość powołania się na prawo dostępu do swoich danych osobowych, zgodnie z art. 13 rozporządzenia (WE) nr 45/2001. EIOD zaleca zatem, aby do proponowanego art. 24 dodany został ustęp, z którego wynikać będzie, że podjęte zostaną środki gwarantujące, iż osoba, której dotyczą dane, będzie mogła wykonać przysługujące jej prawo dostępu do dotyczących jej danych osobowych, zgodnie z treścią art. 13 rozporządzenia (WE) nr 45/2001.

V. **WNIOSKI I ZALECENIA**

56. EIOD jest zdania, że brak odpowiedniej analizy konsekwencji nadzoru nad bezpieczeństwem farmakoterapii dotyczących ochrony danych stanowi jedną z największych słabości aktualnych ram prawnych ustanowionych rozporządzeniem (WE) nr 726/2004 i dyrektywą 2001/83/WE. Obecna zmiana rozporządzenia (WE) nr 726/2004 i dyrektywy 2001/83/WE powinna być postrzegana jako okazja do wprowadzenia kwestii ochrony danych jako pełnoprawnej i ważnej części nadzoru nad bezpieczeństwem farmakoterapii.

57. Kwestią ogólną, którą należy w tym kontekście rozważyć, jest faktyczna potrzeba przetwarzania danych osobowych dotyczących zdrowia na wszystkich etapach nadzoru nad bezpieczeństwem farmakoterapii. Jak już wyjaśniono w niniejszej opinii, EIOD wyraża poważne wątpliwości co do istnienia takiej potrzeby i wzywa prawodawcę do ponownego rozważenia tej kwestii na poszczególnych etapach nadzoru. Oczywistym jest, że cel nadzoru nad

bezpieczeństwem farmakoterapii może w wielu przypadkach zostać osiągnięty poprzez wymianę informacji, które dotyczą działań niepożądanych i które są anonimowe w rozumieniu przepisów o ochronie danych. Powtarzającym się sprawozdaniom można zapobiegać już na szczeblu krajowym poprzez lepsze ustrukturyzowanie procedur sprawozdawczości.

58. Proponowane zmiany przewidują uproszczenie systemu sprawozdawczości i wzmocnienie bazy danych EudraVigilance. EIOD wyjaśnił, że zmiany te powodują zwiększenie ryzyka związanego z ochroną danych, szczególnie w sytuacjach, kiedy w grę wchodzi bezpośrednie przesyłanie sprawozdań pacjentów do EMEA lub do bazy danych EudraVigilance. W związku z tym EIOD zdecydowanie popiera *zdecentralizowany i pośredni system sprawozdawczości*, w którym komunikacja z europejskim portalem internetowym koordynowana jest przy pomocy krajowych portali internetowych. EIOD podkreśla też, że prywatność i bezpieczeństwo powinny być częścią projektu i realizacji systemu sprawozdawczości wykorzystującego portale internetowe („*domyślna ochrona prywatności*").

59. EIOD podkreśla również, że w przypadku przetwarzania danych dotyczących zdrowia zidentyfikowanych lub identyfikowalnych osób fizycznych osoba odpowiedzialna za takie przetwarzanie powinna spełniać wszystkie wymogi prawodawstwa wspólnotowego dotyczącego ochrony danych.

60. Bardziej szczegółowo EIOD zaleca:

— zamieszczenie odniesienia do niniejszej opinii w preambule do obydwu wniosków,

— dodanie do rozporządzenia (WE) nr 726/2004 i dyrektywy 2001/83/WE motywu, w którym podkreślone będzie znaczenie ochrony danych w kontekście nadzoru nad bezpieczeństwem farmakoterapii, z odniesieniami do właściwego prawodawstwa wspólnotowego,

— dodanie do rozporządzenia (WE) nr 726/2004 i dyrektywy 2001/83/WE nowego artykułu o charakterze ogólnym, który stanowić będzie, że:

— przepisy rozporządzenia (WE) nr 726/2004 i dyrektywy 2001/83/WE nie naruszają praw i obowiązków wynikających odpowiednio z przepisów rozporządzenia (WE) nr 45/2001 i dyrektywy 95/46/WE, ze szczególnym odniesieniem do, odpowiednio, art. 10 rozporządzenia (WE) nr 45/2001 i art. 8 dyrektywy 95/46/WE,

— identyfikowalne dane dotyczące zdrowia należy przetwarzać tylko wtedy, gdy będzie to absolutnie niezbędne, a podmioty biorące udział w tym przetwarzaniu powinny taką konieczność badać na każdym etapie nadzoru nad bezpieczeństwem farmakoterapii,

— umieszczenie w proponowanym art. 24 ust. 2 rozporządzenia (WE) nr 726/2004 zdania, z którego wynikać będzie, że dostęp do bazy danych EudraVigilance jest regulowany zgodnie z prawami i obowiązkami wynikającymi z prawodawstwa wspólnotowego dotyczącego ochrony danych,

— dodanie do proponowanego art. 24 ustępu, z którego wynikać będzie, że podjęte zostaną środki gwarantujące, iż osoba, której dotyczą dane będzie mogła wykonać przysługujące jej prawo dostępu do dotyczących jej danych osobowych, zgodnie z treścią art. 13 rozporządzenia (WE) nr 45/2001,

— dodanie do proponowanego art. 101 dyrektywy 2001/83/WE ustępu, z którego wynikać będzie, że w przypadku przetwarzania danych osobowych danej osobie przekazane będą odpowiednie informacje, zgodnie z treścią art. 10 dyrektywy 95/46/WE,

— dodanie do nowo zaproponowanych art. 25 i 26 rozporządzenia (WE) nr 726/2004 i art. 106 dyrektywy 2001/83/WE, które dotyczyć będą stworzenia systemu sprawozdawczości w zakresie działań niepożądanych przy pomocy portali internetowych, obowiązku wprowadzenia odpowiednich środków dotyczących prywatności i bezpieczeństwa na takim samym poziomie we wszystkich państwach członkowskich, z uwzględnieniem podstawowych zasad poufności, spójności, rzetelności i dostępności danych.

Sporządzono w Brukseli dnia 22 kwietnia 2009 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych

IV

(Zawiadomienia)

ZAWIADOMIENIA INSTYTUCJI I ORGANÓW UNII EUROPEJSKIEJ

KOMISJA

Kursy walutowe euro [1]

22 września 2009 r.

(2009/C 229/05)

1 euro =

	Waluta	Kurs wymiany		Waluta	Kurs wymiany
USD	Dolar amerykański	1,4780	AUD	Dolar australijski	1,6922
JPY	Jen	135,09	CAD	Dolar kanadyjski	1,5787
DKK	Korona duńska	7,4422	HKD	Dolar hong kong	11,4552
GBP	Funt szterling	0,90470	NZD	Dolar nowozelandzki	2,0484
SEK	Korona szwedzka	10,0940	SGD	Dolar singapurski	2,0863
CHF	Frank szwajcarski	1,5149	KRW	Won	1 779,06
ISK	Korona islandzka		ZAR	Rand	10,9943
NOK	Korona norweska	8,6280	CNY	Yuan renminbi	10,0902
BGN	Lew	1,9558	HRK	Kuna chorwacka	7,2943
CZK	Korona czeska	25,131	IDR	Rupia indonezyjska	14 316,85
EEK	Korona estońska	15,6466	MYR	Ringgit malezyjski	5,1434
HUF	Forint węgierski	271,42	PHP	Peso filipińskie	70,238
LTL	Lit litewski	3,4528	RUB	Rubel rosyjski	44,5532
LVL	Łat łotewski	0,7055	THB	Bat tajlandzki	49,687
PLN	Złoty polski	4,1613	BRL	Real	2,6726
RON	Lej rumuński	4,2475	MXN	Peso meksykańskie	19,6500
TRY	Lir turecki	2,1882	INR	Rupia indyjska	70,8900

[1] *Źródło*: referencyjny kurs wymiany walut opublikowany przez ECB.

ZAWIADOMIENIA PAŃSTW CZŁONKOWSKICH

Aktualizacja wykazu przejść granicznych, o których mowa w art. 2 ust. 8 rozporządzenia (WE) nr 562/2006 Parlamentu Europejskiego i Rady ustanawiającego wspólnotowy kodeks zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen) (Dz.U. C 316 z 28.12.2007, s. 1; Dz.U. C 134 z 31.5.2008, s. 16; Dz.U. C 177 z 12.7.2008, s. 9; Dz.U. C 200 z 6.8.2008, s. 10; Dz.U. C 331 z 31.12.2008, s. 13; Dz.U. C 3 z 8.1.2009, s. 10; Dz.U. C 37 z 14.2.2009, s. 10; Dz.U. C 64 z 19.3.2009, s. 20; Dz.U. C 99 z 30.4.2009, s. 7)

(2009/C 229/06)

Publikacja wykazu przejść granicznych zgodnie z art. 2 ust. 8 rozporządzenia (WE) nr 562/2006 Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. ustanawiającego wspólnotowy kodeks zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen) opiera się na informacjach przekazanych Komisji przez państwa członkowskie zgodnie z art. 34 kodeksu granicznego Schengen.

Oprócz publikacji w Dzienniku Urzędowym, na stronie internetowej Dyrekcji Generalnej ds. Sprawiedliwości, Wolności i Bezpieczeństwa dostępne są aktualizowane co miesiąc informacje.

WĘGRY

Nowy wykaz zastępujący wykaz opublikowany w Dz.U. C 316 z 28.12.2007, s. 1.

WĘGRY–CHORWACJA

Granice lądowe

1. Barcs–Terezino Polje
2. Beremend–Baranjsko Petrovo Selo
3. Berzence–Gola
4. Drávaszabolcs–Donji Miholjac
5. Drávaszabolcs (rzeczne, na wniosek) (*)
6. Gyékényes–Koprivnica (kolejowe)
7. Letenye–Goričan I
8. Letenye–Goričan II (autostrada)
9. Magyarboly–Beli Manastir (kolejowe)
10. Mohács (rzeczne)
11. Murakeresztúr–Kotoriba (kolejowe)
12. Udvar–Dubosevica

(*) 07:00–19:00.

WĘGRY–SERBIA

Granice lądowe

1. Bácsalmás–Bajmok (**)
2. Hercegszántó–Bački Breg
3. Kelebia–Subotica (kolejowe)
4. Mohács (rzeczne)
5. Röszke–Horgoš (autostrada)
6. Röszke–Horgoš (autostrada)
7. Szeged (rzeczne) (**)
8. Tiszasziget–Đjala (Gyála) (**)
9. Tompa–Kelebija

(**) Zob. przypis (*).

WĘGRY–RUMUNIA

Granice lądowe

1. Ágerdőmajor (Tiborszállás)–Carei (kolejowe)
2. Ártánd–Borș
3. Battonya–Turnu
4. Biharkeresztes–Episcopia Bihorului (kolejowe)

5. Csengersima–Petea
6. Gyula–Vărşand
7. Kiszombor–Cenad
8. Kötegyán–Salonta (kolejowe)
9. Létavértes–Săcuieni (***)
10. Lökösháza–Curtici (kolejowe)
11. Méhkerék–Salonta
12. Nagylak–Nădlac
13. Nyírábrány–Valea Lui Mihai (kolejowe)
14. Nyírábrány–Valea Lui Mihai
15. Vállaj–Urziceni

(***) 06:00–22:00.

WĘGRY–UKRAINA

Granice lądowe

1. Barabás–Kosino (****)
2. Beregsurány–Luzhanka
3. Eperjeske–Salovka (kolejowe)
4. Lónya–Dzvinkove (*****)
5. Tiszabecs–Vylok
6. Záhony–Čop (kolejowe)
7. Záhony–Čop

(****) Zob. przypis (*).
(*****) 08:00–16:00.

Granice powietrzne

Międzynarodowe porty lotnicze:

1. Budapest Nemzetközi Repülőtér
2. Debrecen Repülőtér
3. Sármellék

Lądowiska (wyłącznie na wniosek):

1. Békéscsaba
2. Budaörs
3. Fertőszentmiklós
4. Győr–Pér
5. Kecskemét
6. Nyíregyháza
7. Pápa
8. Pécs–Pogány
9. Siófok–Balatonkiliti
10. Szeged
11. Szolnok

V

(Ogłoszenia)

PROCEDURY ZWIĄZANE Z REALIZACJĄ WSPÓLNEJ POLITYKI HANDLOWEJ

KOMISJA

Zawiadomienie o środkach antydumpingowych w odniesieniu do przywozu azotanu amonu pochodzącego z Rosji

(2009/C 229/07)

Sąd Pierwszej Instancji Wspólnot Europejskich, w następstwie wniosku złożonego przez JSC Kirovo-Chepetsky Khimichesky Kombinat, wyrokiem z dnia 10 września 2008 r. w sprawie T-348/05 unieważnił rozporządzenie Rady (WE) nr 945/2005 ([1]) z dnia 21 czerwca 2005 r. zmieniające (i) rozporządzenie (WE) nr 658/2002 ([2]) nakładające ostateczne cło antydumpingowe na przywóz azotanu amonu pochodzącego z Rosji i (ii) rozporządzenie (WE) nr 132/2001 ([3]) nakładające ostateczne cło antydumpingowe na przywóz azotanu amonu pochodzącego, między innymi, z Ukrainy. W następstwie wniosku o interpretację wymienionego wyżej wyroku Sąd Pierwszej Instancji, wyrokiem z dnia 9 lipca 2009 r., zdecydował, że sentencję wyroku z dnia 10 września 2008 r. należy interpretować w ten sposób, że rozporządzenie (WE) nr 945/2005 z dnia 21 czerwca 2005 r. jest unieważnione w zakresie, w którym dotyczy JSC Kirovo-Chepetsky Khimichesky Kombinat.

W rezultacie ostateczne cło antydumpingowe zapłacone zgodnie z rozporządzeniem Rady (WE) nr 658/2002 za przywóz produktów wytwarzanych i wywożonych do Unii Europejskiej przez JSC Kirovo-Chepetsky Khimichesky Kombinat, za wyjątkiem cła antydumpingowego nałożonego na przywóz produktów objętych kodami CN 3102 30 90 i 3102 40 90, powinno zostać zwrócone lub umorzone. Wnioski o zwrot lub umorzenie składa się do krajowych organów celnych zgodnie z obowiązującymi przepisami prawa celnego.

([1]) Dz.U. L 160 z 23.6.2005, s. 1.
([2]) Dz.U. L 102 z 18.4.2002, s. 1.
([3]) Dz.U. L 23 z 25.1.2001, s. 1.

CENY PRENUMERATY w 2009 r. (bez VAT, włącznie z normalną opłatą za dostawę przesyłki)

Dziennik Urzędowy UE, serie L i C, wyłącznie wersja papierowa	w 22 językach urzędowych UE	1 000 EUR/rok (*)
Dziennik Urzędowy UE, serie L i C, wyłącznie wersja papierowa	w 22 językach urzędowych UE	100 EUR/miesiąc (*)
Dziennik Urzędowy UE, serie L i C, wersja papierowa + roczne wydanie CD-ROM	w 22 językach urzędowych UE	1 200 EUR/rok
Dziennik Urzędowy UE, seria L, wyłącznie wersja papierowa	w 22 językach urzędowych UE	700 EUR/rok
Dziennik Urzędowy UE, seria L, wyłącznie wersja papierowa	w 22 językach urzędowych UE	70 EUR/miesiąc
Dziennik Urzędowy UE, seria C, wyłącznie wersja papierowa	w 22 językach urzędowych UE	400 EUR/rok
Dziennik Urzędowy UE, seria C, wyłącznie wersja papierowa	w 22 językach urzędowych UE	40 EUR/miesiąc
Dziennik Urzędowy UE, serie L i C, miesięczne wydanie CD-ROM (komplet)	w 22 językach urzędowych UE	500 EUR/rok
Suplement do Dziennika Urzędowego (seria S) – Ogłoszenia o przetargach, CD-ROM dwa razy w tygodniu	wielojęzyczny: w 23 językach urzędowych UE	360 EUR/rok (= 30 EUR/miesiąc)
Dziennik Urzędowy UE, seria C – Konkursy	w językach, których dotyczy konkurs	50 EUR/rok

(*) Pojedyncze egzemplarze: od 1 do 32 stron: 6 EUR
od 33 do 64 stron: 12 EUR
powyżej 64 stron: cena ustalana indywidualnie

Prenumerata *Dziennika Urzędowego Unii Europejskiej*, który jest wydawany w językach urzędowych Unii, dostępna jest w 22 wersjach językowych. Dziennik Urzędowy składa się z dwóch serii – L (Legislacja) oraz C (Informacje i zawiadomienia).

Dla każdej wersji językowej jest otwierana osobna prenumerata.

Zgodnie z rozporządzeniem Rady (WE) nr 920/2005, opublikowanym w Dzienniku Urzędowym L 156 z dnia 18 czerwca 2005 r., instytucje Unii Europejskiej nie mają obowiązku sporządzania wszystkich aktów prawnych w języku irlandzkim ani publikowania ich w tym języku. W związku z tym irlandzkie wydania Dziennika Urzędowego sprzedawane są osobno.

Prenumerata Suplementu do Dziennika Urzędowego (seria S – Ogłoszenia o przetargach) obejmuje wszystkie 23 wersje językowe na pojedynczym CD-ROM-ie.

Na żądanie prenumeratorzy *Dziennika Urzędowego Unii Europejskiej* mogą otrzymać różne załączniki do Dziennika Urzędowego. Prenumeratorzy informowani są o publikacji załączników poprzez zawiadomienia dołączane do *Dziennika Urzędowego Unii Europejskiej*.

Sprzedaż i prenumerata

Odpłatne publikacje, wydawane przez Urząd Publikacji, dostępne są u naszych dystrybutorów handlowych. Wykaz dystrybutorów handlowych znajduje się na stronie internetowej:

http://publications.europa.eu/others/agents/index_pl.htm

Portal EUR-Lex (http://eur-lex.europa.eu) zapewnia bezpośredni i bezpłatny dostęp do prawodawstwa Unii Europejskiej. EUR-Lex umożliwia dostęp do *Dziennika Urzędowego Unii Europejskiej* oraz traktatów, aktów prawnych, orzecznictwa oraz aktów przygotowawczych.

Dodatkowe informacje o Unii Europejskiej znajdują się na stronie: http://europa.eu

Urząd Publikacji Unii Europejskiej
2985 Luksemburg
LUKSEMBURG

PL