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