Projekt opinii Europejskiego Inspektora Ochrony Danych na temat wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie stosowania praw pacjenta w transgranicznej opiece zdrowotnej

(2009/C 128/03)

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,

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

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

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. **WPROWADZENIE**

Wniosek dotyczący dyrektywy w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej

1. Dnia 2 lipca 2008 r. Komisja przyjęła wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej (dalej zwany „wnioskiem") [1]. Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 Komisja przesłała wniosek EIOD do konsultacji.

2. Celem wniosku jest ustanowienie wspólnotowych ram udzielania transgranicznej opieki zdrowotnej w UE w przypadkach gdy forma opieki poszukiwanej przez pacjentów świadczona jest w państwie członkowskim innym niż ich własne państwo. Wniosek obejmuje trzy główne obszary:

— ustanowienie we wszystkich systemach zdrowotnych UE wspólnych zasad jasno definiujących obowiązki państw członkowskich;

— opracowanie szczegółowych ram transgranicznej opieki zdrowotnej, dostarczanie jasnych informacji na temat praw pacjentów do otrzymania opieki zdrowotnej w innym państwie członkowskim;

— promowanie współpracy na szczeblu UE w dziedzinie opieki zdrowotnej w obszarach takich jak uznawanie recept wystawionych w innych państwach, europejskie sieci referencyjne, ocena technologii medycznych, gromadzenie danych, jakość i bezpieczeństwo.

3. Cele niniejszych ram są dwojakiego rodzaju: zagwarantowanie dostatecznej jasności na temat prawa do zwrotu kosztów opieki zdrowotnej udzielonej w innych państwach członkowskich oraz dopilnowanie, by w przypadku transgranicznej opieki zdrowotnej spełnione zostały konieczne wymagania w zakresie wysokiej jakości, bezpieczeństwa i skuteczności opieki zdrowotnej.

4. Wdrożenie systemu transgranicznej opieki zdrowotnej niesie ze sobą konieczność wymiany odpowiednich danych osobowych dotyczących zdrowia pacjentów (dalej zwanych „danymi na temat zdrowia") między upoważnionymi organizacjami oraz pracownikami służby zdrowia w różnych państwach członkowskich. Dane te uważane są za dane wrażliwe i podlegają ściślejszym zasadom ochrony danych zgodnie z art. 8 dyrektywy 95/46/WE, który dotyczy szczególnych kategorii danych.

Konsultacje z EIOD

5. EIOD z zadowoleniem przyjmuje fakt, że zwrócono się do niego z prośbą o konsultacje w tej kwestii oraz że w preambule przedmiotowego wniosku zawarto odniesienie do tych konsultacji zgodnie z art. 28 rozporządzenia (WE) nr 45/2001.

6. Po raz pierwszy formalnie zasięga się opinii EIOD w sprawie wniosku dotyczącego dyrektywy w dziedzinie opieki zdrowotnej. W związku z tym w niniejszej opinii zawarto pewne uwagi o szerszym zakresie, poruszając ogólne zagadnienia ochrony danych osobowych w sektorze opieki zdrowotnej, które mogą mieć zastosowanie do innych odpowiednich instrumentów prawnych (wiążących lub nie).

[1] COM(2008) 414 wersja ostateczna. Należy zwrócić uwagę, że tego samego dnia został również przyjęty uzupełniający komunikat dotyczący wspólnotowych ram stosowania praw pacjenta w transgranicznej opiece zdrowotnej (COM (2008) 415 wersja ostateczna). Ponieważ komunikat ten ma raczej charakter ogólny, EIOD postanowił skupić się na proponowanej dyrektywie.

7. Już na wstępie EIOD chciałby wyrazić swoje poparcie dla inicjatyw, które mają na celu poprawę warunków transgranicznej opieki zdrowotnej. Przedmiotowy wniosek należałoby w istocie rozpatrywać w kontekście ogólnego programu WE na rzecz poprawy zdrowia obywateli w społeczeństwie informacyjnym. Innymi inicjatywami w tym zakresie są planowana przez Komisję dyrektywa i komunikat w sprawie dawstwa i przeszczepów organów ([1]), zalecenie w sprawie interoperacyjności elektronicznych kart zdrowia ([2]), jak również planowany komunikat w sprawie telemedycyny ([3]). EIOD jest jednak zaniepokojony faktem, że wszystkie tego typu powiązane ze sobą inicjatywy nie są ściśle związane lub nie łączą się z dziedziną bezpieczeństwa danych i prywatności, opóźniając tym samym przyjęcie ujednoliconego podejścia do ochrony danych w dziedzinie ochrony zdrowia, zwłaszcza w odniesieniu do wykorzystania nowych technologii informacyjno-komunikacyjnych. Przykładowo w obecnym wniosku w motywie 10 wymienia się wyraźnie telemedycynę, nie ma jednak odniesienia do wymiaru ochrony danych w odpowiednim komunikacie Komisji. Oprócz tego, chociaż elektroniczne karty zdrowia są jednym z możliwych sposobów transgranicznego przekazywania danych medycznych, nie nawiązano do kwestii prywatności poruszonych w odpowiednim zaleceniu Komisji ([4]). Stwarza to wrażenie, że ogólna perspektywa prywatności w opiece zdrowotnej w dalszym ciągu nie jest jasno zdefiniowana, a w niektórych przypadkach całkowicie jej brakuje.

8. Jest to również widoczne w obecnym wniosku, w związku z czym EIOD ubolewa nad faktem, że nie zajęto się w nim w sposób konkretny skutkami, jakie wniosek ten będzie miał dla ochrony danych. Oczywiście, można we wniosku tym znaleźć odniesienia do ochrony danych, mają one jednak charakter ogólny i nie odzwierciedlają w odpowiedni sposób specyficznych potrzeb i wymogów transgranicznej opieki zdrowotnej związanych z prywatnością.

9. EIOD pragnie podkreślić, że ujednolicone i zdecydowane podejście do ochrony danych zastosowane w proponowanych instrumentach w dziedzinie opieki zdrowotnej nie tylko zagwarantuje podstawowe prawo obywateli do ochrony ich danych, ale przyczyni się również do dalszego rozwoju transgranicznej opieki zdrowotnej w UE.

II. **OCHRONA DANYCH W TRANSGRANICZNEJ OPIECE ZDROWOTNEJ**

Kontekst ogólny

10. Najważniejszym celem Wspólnoty Europejskiej było ustanowienie rynku wewnętrznego, który stanowi przestrzeń bez granic wewnętrznych i na którym zapewniony jest swobodny przepływ towarów, osób, usług i kapitału. Umożliwienie obywatelom łatwiejszego przemieszczania się i osiedlania w państwach członkowskich innych niż ich państwo pochodzenia nieuchronnie pociągnęło za sobą kwestie związane z ochroną zdrowia. Z tego powodu w latach 90. Trybunał Sprawiedliwości zmierzył się w kontekście rynku wewnętrznego z zagadnieniami ewentualnego zwrotu kosztów leczenia poniesionych w innym państwie członkowskim. Trybunał Sprawiedliwości uznał, że swoboda świadczenia usług, o której mowa w art. 49 Traktatu WE, obejmuje swobodę przemieszczania się osób do innego państwa członkowskiego, aby poddać się leczeniu ([5]). W konsekwencji pacjenci, którzy poszukiwali opieki zdrowotnej poza granicami kraju, nie mogli być traktowani inaczej niż obywatele w ich własnym kraju, którzy otrzymywali takie samo leczenie bez przekraczania granicy.

11. Te wyroki Trybunału dotykają meritum obecnego wniosku. Ponieważ orzecznictwo Trybunału opiera się na poszczególnych przypadkach, w obecnym wniosku planowano poprawić jasność, aby zagwarantować ogólniejsze i skuteczniejsze stosowanie swobody otrzymywania i świadczenia usług zdrowotnych. Jak już jednak wspomniano, przedmiotowy wniosek jest także częścią ambitniejszego programu, którego celem jest poprawa zdrowia obywateli w społeczeństwie informacyjnym i w którym UE widzi możliwość znacznego rozszerzenia transgranicznej opieki zdrowotnej dzięki wykorzystaniu technologii informacyjnych.

12. Z oczywistych względów ustalenie zasad transgranicznej opieki zdrowotnej jest delikatną kwestią. Dotyka ona delikatnego obszaru, w którym państwa członkowskie stworzyły systemy krajowe różniące się między sobą na przykład pod względem ubezpieczenia i zwrotu kosztów leczenia lub organizacją infrastruktury opieki zdrowotnej, w tym sieci i zastosowań w zakresie informacji o opiece zdrowotnej. Chociaż w przedmiotowym wniosku prawodawca wspólnotowy skupia się wyłącznie na *transgranicznej* opiece zdrowotnej, zasady te przynajmniej wpłyną na sposób, w jaki są zorganizowane krajowe systemy opieki zdrowotnej.

13. Poprawa warunków świadczenia trangranicznych usług opieki zdrowotnej przyniesie korzyść obywatelom. Jednocześnie będzie ze sobą niosła jednak również pewne ryzyko dla obywateli. Rozwiązania będzie wymagało wiele problemów natury praktycznej, które nieodmiennie łączą się z transgraniczną współpracą między ludźmi z innych państw posługującymi się różnymi językami. Ponieważ dobry stan zdrowia ma największe znaczenie dla każdego obywatela, należy wykluczyć wszelkie ryzyko niezrozumienia i wynikających z niego nieścisłości. Rozumie się samo przez się, że rozbudowanie transgranicznej opieki zdrowotnej w połączeniu z wykorzystaniem osiągnięć technologicznych ma ogromne znaczenie dla ochrony danych osobowych. Skuteczniejsza, a więc coraz szersza wymiana danych

([1]) Ogłoszone w programie prac Komisji.
([2]) Zalecenie Komisji z dnia 2 lipca 2008 r. w sprawie transgranicznej interoperacyjności systemów elektronicznych kart zdrowia (notyfikowane jako dokument nr C(2008) 3282), Dz.U. L 190 z 18.7.2008, s. 37.
([3]) Ogłoszone w programie prac Komisji.
([4]) Dobrą ilustracją w tym zakresie jest fakt, że w przywoływanym w pierwszym przypisie komunikacie, którego celem jest ustalenie wspólnotowych ram stosowania praw pacjentów w transgranicznej opiece zdrowotnej, nie ma odniesienia do ochrony danych lub prywatności.
([5]) Sprawa C-158/96 *Kohll*, [1998] Rec. I-1931, pkt 34. Zob. m.in. sprawa C-147/99, *Smits and Peerbooms* [2001] Rec. I-5473 oraz sprawa C-385/99, *Müller-Fauré and Van Riet* [2003] Rec. I-12403.

medycznych, rosnące odległości między osobami i konkretnymi instytucjami, różnice w krajowych przepisach wykonawczych dotyczących zasad ochrony danych rodzą problemy związane z bezpieczeństwem danych i pewnością prawną.

Ochrona danych medycznych

14. Należy podkreślić, że dane medyczne należą do specjalnej kategorii danych, która zasługuje na szczególną ochronę. Jak niedawno orzekł Europejski Trybunał Praw Człowieka w kontekście art. 8 Europejskiej konwencji praw człowieka: „Ochrona danych osobowych, w szczególności danych medycznych ma podstawowe znaczenie, aby osoby prywatne mogły się cieszyć swoim prawem do poszanowania życia prywatnego i rodzinnego, które zostało zagwarantowane w art. 8 konwencji" ([1]). Zanim przejdziemy do wyjaśnienia bardziej rygorystycznych zasad przetwarzania danych medycznych, które zostały określone w dyrektywie 95/46/WE, poświęcimy kilka słów terminowi „dane na temat zdrowia".

15. W dyrektywie 95/46/WE nie ma bezpośredniej definicji danych na temat zdrowia. Powszechnie stosuje się szeroką interpretację, zgodnie z którą dane na temat zdrowia to najczęściej „dane osobowe, które mają wyraźny i ścisły związek z opisem stanu zdrowia osoby ([2])". W tym zakresie dane na temat zdrowia zwykle obejmują dane medyczne (np. skierowania i recepty lekarskie, wyniki badań medycznych, testów laboratoryjnych, prześwietleń itp.), jak również administracyjne i finansowe dane dotyczące zdrowia (np. dokumenty dotyczące przyjęcia do szpitala, numer ubezpieczenia społecznego, plany wizyt lekarskich, faktury za usługi opieki medycznej itp.). Należy zauważyć, że termin „dane medyczne" ([3]) jest również czasami stosowany w odniesieniu do danych na temat zdrowia; występuje również termin „dane dotyczące opieki zdrowotnej" ([4]). W niniejszej opinii będziemy się posługiwać terminem „dane na temat zdrowia".

16. Przydatna definicja „danych na temat zdrowia" znajduje się w normie ISO 27799: „wszelkie informacje, które dotyczą zdrowia fizycznego lub psychicznego danej osoby lub świadczenia danej osobie usług zdrowotnych, i które mogą obejmować: a) informacje na temat rejestracji danej osoby w celu świadczenia jej usług zdrowotnych; b) informacje na temat płatności lub kwalifikowalności danej osoby do otrzymania opieki zdrowotnej; c) liczbę, symbol lub oznaczenie przypisane do danej osoby, które pozwala na jej jednoznaczną identyfikację do celów opieki zdrowotnej; d) wszelkie informacje na temat danej osoby zebrane w procesie udzielania usług zdrowotnych tej osobie; e) informacje uzyskane podczas przeprowadzania testów lub badań części ciała lub płynów ustrojowych oraz f) identyfikację osoby (pracownika służby zdrowia), która udziela opieki medycznej danej osobie".

17. EIOD zdecydowanie opowiada się za przyjęciem w kontekście obecnego wniosku szczegółowej definicji terminu „dane dotyczące zdrowia", która to definicja mogłaby również być wykorzystywana w innych odnośnych tekstach prawnych UE (zob. sekcja III poniżej).

18. W art. 8 dyrektywy 95/46/WE ustalono zasady przetwarzania szczególnych kategorii danych. Zasady te są bardziej surowe, niż zasady dotyczące przetwarzania danych określone w art. 7 dyrektywy 95/46/WE. Jest to widoczne już w art. 8 ust. 1, w którym stwierdza się bezpośrednio, że państwa członkowskie *zabraniają* przetwarzania – między innymi – danych dotyczących zdrowia. W dalszych ustępach tego artykułu wymienia się kilka wyjątków od tego zakazu, ale są one węższe niż podstawy przetwarzania zwykłych danych określone w art. 7. Na przykład zakaz nie obowiązuje, jeżeli osoba, której dane dotyczą, udzieliła *wyraźnej* zgody (art. 8 ust. 2 lit. a)), w przeciwieństwie do wymogu wyrażenia *jednoznacznej* zgody zawartego w art. 7 lit. a) dyrektywy 95/46/WE. Ponadto w prawie państw członkowskich może zostać określone, że w pewnych przypadkach nawet wyrażenie zgody przez osobę, której dane dotyczą, nie może znieść tego zakazu. Art. 8 ust. 3 dotyczy wyłącznie przetwarzania danych dotyczących zdrowia. Zgodnie z tym ustępem zakaz, o którym mowa w ust. 1, nie ma zastosowania, w przypadku gdy przetwarzanie danych wymagane jest do celów medycyny prewencyjnej, diagnostyki medycznej, świadczenia opieki lub leczenia lub też zarządzania opieką zdrowotną, jak również w przypadkach, gdy dane są przetwarzane przez pracownika służby zdrowia, zgodnie z przepisami prawa krajowego lub zasadami określonymi przez właściwe krajowe instytucje, podlegającego obowiązkowi zachowania tajemnicy zawodowej lub przez inną osobę również zobowiązaną do zachowania tajemnicy.

19. W art. 8 dyrektywy 95/46/WE położono nacisk na fakt, że państwa członkowskie powinny stworzyć odpowiednie lub adekwatne zabezpieczenia. W art. 8 ust. 4 pozwala się na przykład państwom członkowskim ustalić dodatkowe wyłączenia od zakazu przetwarzania danych wrażliwych – ze względu na istotny interes publiczny – pod warunkiem ustanowienia odpowiednich środków zabezpieczających. Podkreśla się tym samym ogólnie odpowiedzialność, jaką państwa członkowskie ponoszą za dołożenie szczególnych starań przy przetwarzaniu danych wrażliwych, takich jak dane dotyczące zdrowia.

Ochrona danych dotyczących zdrowia w kontekście transgranicznym

Wspólna odpowiedzialność państw członkowskich

20. Państwa członkowskie powinny zdawać sobie szczególnie sprawę z wyżej wymienionej odpowiedzialności, w przypadku gdy chodzi o zagadnienie transgranicznej wymiany danych na temat zdrowia. Jak wspomniano

([1]) Zob. wyrok Europejskiego Trybunału Praw Człowieka z dnia 17 lipca 2008 r. *I vs. Finland* (sprawa nr 20511/03), pkt 38.

([2]) Zob. dokument roboczy Grupy Roboczej, art. 29 w sprawie przetwarzania danych osobowych dotyczących zdrowia w elektronicznych kartach zdrowia, luty 2007, WP 131, ust. II.2. Zob. również wyjaśnienie szerszego znaczenia „danych osobowych": Opinia 4/2007 Grupy Roboczej, art. 29 w sprawie pojęcia danych osobowych, WP 136.

([3]) Rada Europy, Zalecenie nr R(97)5 w sprawie ochrony danych medycznych

([4]) ISO 27799:2008 „Informatyka w ochronie zdrowia – Zarządzanie bezpieczeństwem informacji w ochronie zdrowia przy użyciu ISO/IEC 27002".

powyżej, transgraniczna wymiana danych na temat zdrowia zwiększa ryzyko nieprecyzyjnego lub nieuprawnionego przetwarzania danych. Może to oczywiście pociągać za sobą ogromne negatywne skutki dla osoby, której dane dotyczą. W procesie tym biorą udział zarówno państwo członkowskie ubezpieczenia (w którym pacjent jest osobą ubezpieczoną) oraz państwo członkowskie leczenia (w którym faktycznie udzielono transgranicznej opieki zdrowotnej), a co za tym idzie wspólnie ponoszą one odpowiedzialność.

21. W tym kontekście ważnym zagadnieniem jest bezpieczeństwo danych na temat zdrowia. W przywoływanym wyżej niedawnym orzeczeniu Europejski Trybunał Praw Człowieka położył szczególny nacisk na poufność danych na temat zdrowia: „Poszanowanie poufności danych na temat zdrowia jest ważną zasadą w systemach prawnych wszystkich umawiających się stron konwencji. Kluczowe znaczenie ma nie tylko poszanowanie poczucia prywatności pacjenta, ale również ochrona jego zaufania do zawodów związanych ze służbą zdrowia oraz ogólnie do usług zdrowotnych" ([1]).

22. Zasady dotyczące ochrony danych określone w dyrektywie 95/46/WE wymagają ponadto, by państwo członkowskie ubezpieczenia dostarczało pacjentowi odpowiednich, dokładnych i aktualnych informacji na temat przekazywania jego danych osobowych do innego państwa członkowskiego, przy jednoczesnym zagwarantowaniu bezpiecznego przekazania danych do tego państwa członkowskiego. Państwo członkowskie leczenia powinno również dopilnować, by dane te zostały w bezpieczny sposób przyjęte, oraz zgodnie z własnym prawem zagwarantować odpowiedni stopień ochrony w momencie ich faktycznego przetwarzania.

23. EIOD chciałby, aby we wniosku wyraźnie podkreślono wspólną odpowiedzialność państw członkowskich, także z uwzględnieniem przekazywania danych drogą elektroniczną, zwłaszcza w kontekście nowych aplikacji TIK, jak omówiono poniżej.

Przekazywanie danych na temat zdrowia drogą elektroniczną

24. Poprawę w dziedzinie transgranicznej wymiany danych na temat zdrowia osiąga się głównie dzięki wykorzystaniu technologii informacyjnych. Chociaż wymiana danych w systemie transgranicznej opieki zdrowotnej w dalszym ciągu może odbywać się w formie papierowej (np. pacjent przenosi się do innego państwa członkowskiego, przywożąc ze sobą wszystkie istotne dane na temat swojego zdrowia, np. wyniki badań laboratoryjnych, skierowania lekarskie itp.), to jednak wyraźnie planowane jest wykorzystywanie w tym celu środków elektronicznych. Przekazywanie danych na temat zdrowia drogą elektroniczną będą wspierały utworzone (lub mające zostać utworzone) w państwach członkowskich (w szpitalach, klinikach itp.) systemy informacji o opiece zdrowotnej, jak również wykorzystanie nowych technologii, jak np. aplikacji do prowadzenia elektronicznych kart zdrowia (działających w miarę możliwości w Internecie), a także innych narzędzi, takich jak karty pacjenta i lekarza. Oczywiście, w zależności od systemów opieki zdrowotnej w państwach członkowskich, możliwe jest również łączne wykorzystanie formy papierowej i elektronicznej w przypadku wymiany danych.

25. Aplikacje w zakresie e-zdrowia i telemedycyny, które wchodzą w zakres zastosowania proponowanej dyrektywy, będą polegały wyłącznie na wymianie elektronicznych danych na temat zdrowia (np. danych na temat funkcji życiowych, wyników obrazowania itp.) zwykle w połączeniu z innymi istniejącymi elektronicznymi systemami informacji o opiece zdrowotnej zlokalizowanymi w państwie członkowskim leczenia i w państwie członkowskim ubezpieczenia. Uwzględnia się tutaj systemy typu pacjent – lekarz (np. zdalne monitorowanie i diagnoza) oraz systemy typu lekarz – lekarz (np. telekonsultacje między pracownikami służby zdrowia w zakresie specjalistycznych porad na temat konkretnych przypadków zdrowotnych). Inne bardziej szczegółowe aplikacje wspomagające ogólne udzielanie opieki zdrowotnej w kontekście transgranicznym również mogą zależeć wyłącznie od elektronicznej wymiany danych, np. wystawianie elektronicznych recept (e-recepty – ang. *ePrescription*) lub elektronicznych skierowań (e-skierowań – ang. *eReferral*), które w niektórych państwach członkowskich są już wprowadzane na szczeblu krajowym ([2]).

Problematyczne obszary w transgranicznej wymianie danych na temat zdrowia

26. Mając na uwadze powyższe rozważania oraz istniejące zróżnicowanie między systemami opieki zdrowotnej w poszczególnych państwach członkowskich, jak również coraz intensywniejszy rozwój aplikacji w zakresie e-zdrowia, należy wyróżnić dwa główne problematyczne obszary w odniesieniu do ochrony danych osobowych w transgranicznej opiece zdrowotnej: a) różne stopnie bezpieczeństwa, które państwa członkowskie mogą stosować w odniesieniu do ochrony danych osobowych (pod kątem środków technicznych i organizacyjnych); oraz b) uwzględnienie prywatności w aplikacjach w zakresie e-zdrowia, zwłaszcza w przypadku nowych rozwiązań. Ponadto szczególnej uwagi mogą wymagać inne aspekty, takie jak wtórne wykorzystanie danych na temat zdrowia, zwłaszcza w dziedzinie tworzenia statystyk. Zagadnienia te zostały dokładniej przeanalizowane w dalszej części niniejszej sekcji.

Bezpieczeństwo danych w państwach członkowskich

27. Niezależnie od faktu, że dyrektywy 95/46/WE i 2002/58/WE są jednolicie stosowane w Europie, interpretacja i wdrożenie niektórych elementów może być różna w poszczególnych państwach, zwłaszcza w tych obszarach, w których przepisy są ogólne i pozostawione do dalszej regulacji państwom członkowskim. W tym sensie głównym obszarem zainteresowania jest bezpieczeństwo przetwarzania, tj. środki (techniczne i organizacyjne), które państwa członkowskie podejmują, aby zagwarantować bezpieczeństwo danych na temat zdrowia.

([1]) Zob. wyrok Europejskiego Trybunału Praw Człowieka z dnia 17 lipca 2008 r. *I vs. Finland* (sprawa nr 20511/03), pkt 38.

([2]) eHealth ERA Report, Towards the Establishment of a European eHealth Research Area, European Commission, Information Society and Media (Sprawozdanie ERA na temat e-zdrowia, W kierunku ustanowienia europejskiej przestrzeni badawczej w dziedzinie e-zdrowia, Komisja Europejska, Społeczeństwo Informacyjne i Media,) marzec 2007, http://ec.europa.eu/information_society/activities/health/docs/policy/ehealth-era-full-report.pdf

28. Chociaż w zakresie odpowiedzialności wszystkich państw członkowskich leży ścisła ochrona danych na temat zdrowia, w UE nie ma obecnie powszechnie przyjętej definicji „odpowiedniego" poziomu bezpieczeństwa w przypadku opieki zdrowotnej, którą można by zastosować w przypadku transgranicznej opieki zdrowotnej. Przykładowo więc szpital w jednym państwie członkowskim może być zobowiązany krajowymi przepisami dotyczącymi ochrony danych osobowych do przyjęcia szczególnych środków bezpieczeństwa (np. do określenia polityki bezpieczeństwa i kodeksów postępowania, szczegółowych zasad zlecania prac na zewnątrz i zatrudniania zewnętrznych wykonawców, wymagań dotyczących audytu itp.), natomiast w innym państwie członkowskim takie wymagania mogą nie istnieć. Tego typu niespójność może mieć wpływ na wymianę danych w kontekście transgranicznym, zwłaszcza w przypadku elektronicznej formy wymiany, ponieważ nie można zagwarantować, że w różnych państwach członkowskich dane będą chronione na tym samym poziomie (z technicznego i organizacyjnego punktu widzenia).

29. W tej dziedzinie istnieje więc potrzeba dalszej harmonizacji definiowania wspólnego zestawu wymagań w zakresie bezpieczeństwa danych w opiece zdrowotnej, który powinien zostać powszechnie przyjęty przez podmioty świadczące usługi zdrowotne w państwach członkowskich. Potrzeba ta jest jak najbardziej zgodna z ogólną potrzebą zdefiniowania wspólnych zasad dotyczących systemów zdrowotnych UE, co określono w przedmiotowym wniosku.

30. Należy tego dokonać w sposób ogólny, bez nakładania na państwa członkowskie specyficznych rozwiązań technicznych, ustalając jednak podstawy wzajemnego uznawania i zatwierdzania, np. w dziedzinie określenia polityki bezpieczeństwa, identyfikacji i uwierzytelniania pacjentów i pracowników służby zdrowia itp. Jako punkty odniesienia w tym zakresie można wykorzystywać istniejące normy europejskie i międzynarodowe (np. ISO i CEN) dotyczące opieki zdrowotnej i bezpieczeństwa, jak również powszechnie przyjęte i mające podstawy prawne rozwiązania techniczne (np. podpis elektroniczny ([1])).

31. EIOD popiera ideę harmonizacji bezpieczeństwa w służbie zdrowia na szczeblu UE i jest zdania, że Komisja powinna podjąć odpowiednie inicjatywy już w ramach przedmiotowego wniosku (zob. sekcja III poniżej).

Prywatność w aplikacjach w zakresie e-zdrowia

32. Prywatność i bezpieczeństwo powinny być częścią projektu i wdrożenia każdego systemu opieki zdrowotnej, zwłaszcza – jak wspomniano w przedmiotowym wniosku – w aplikacjach w zakresie e-zdrowia („domyślna ochrona prywatności"). Ten bezdyskusyjny wymóg został już uzasadniony w innych odpowiednich dokumentach dotyczących kierunków polityki ([2]), zarówno ogólnych, jak i dotyczących konkretnie opieki zdrowotnej ([3]).

33. W ramach interoperacyjności systemów e-zdrowia omówionej w przedmiotowym wniosku należy jeszcze raz podkreślić koncepcję „domyślnej ochrony prywatności", jako podstawę wszystkich przewidzianych rozwiązań. Koncepcję tę można zastosować na kilku różnych poziomach: organizacyjnym, semantycznym, technicznym.

— Na poziomie organizacyjnym należy uwzględnić ochronę prywatności w określaniu procedur niezbędnych przy wymianie danych na temat zdrowia między placówkami opieki zdrowotnej w poszczególnych państwach członkowskich. Może mieć to bezpośredni wpływ na rodzaj wymiany i obejmować również rodzaj danych, które są przekazywane (np. stosowanie w miarę możliwości numerów identyfikacyjnych zamiast nazwisk pacjentów).

— Na poziomie semantycznym wymagania dotyczące prywatności i bezpieczeństwa należy uwzględnić w nowych normach i systemach, np. przy ustalaniu elektronicznego wzoru recepty, jak omówiono w przedmiotowym wniosku. Można wykorzystać istniejące w tej dziedzinie normy techniczne, np. normy dotyczące poufności danych i podpisu cyfrowego, oraz zwrócić uwagę na potrzeby związane konkretnie z opieką zdrowotną, takie jak uwierzytelnianie wykwalifikowanych pracowników służby zdrowia w oparciu o pełnioną przez nich funkcję.

— Na poziomie technicznym architektura systemów i aplikacji dla użytkowników powinna obejmować technologie zwiększające prywatność i wdrażać wspomnianą wcześniej definicję semantyczną.

34. EIOD jest przekonany, że jako punkt wyjścia do integracji wymagań prywatności i bezpieczeństwa w początkowej fazie może posłużyć elektroniczne wystawianie recept (zob. sekcja III poniżej).

Inne zagadnienia

35. Dodatkowym zagadnieniem, które można rozważać w ramach transgranicznej wymiany danych na temat zdrowia, jest wtórne wykorzystanie tych danych, zwłaszcza do celów statystycznych, jak określono w przedmiotowym wniosku.

36. Jak już wspomniano w pkt 18, w art. 8 ust. 4 dyrektywy 95/46 przewidziano możliwość wtórnego wykorzystania danych na temat zdrowia. Jednak takie dalsze przetwarzanie powinno się odbywać tylko ze względu na „istotny interes publiczny" i pod warunkiem ustanowienia na mocy ustawy krajowej lub decyzji organu nadzorczego „odpowiednich środków zabezpieczających" ([4]). Ponadto

([1]) Dyrektywa 1999/93/WE Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie ram wspólnotowych w zakresie podpisów elektronicznych (Dz.U. L 13 z 19.1.2000, s. 12–20).

([2]) The EDPS and EU Research and Technological Development, Policy Paper, EDPS (EIOD a badania i rozwój technologiczny w UE, dokument dotyczący kierunków polityki, EIOD), kwiecień 2008, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf

([3]) Zalecenie Komisji z dnia 2 lipca 2008 r. w sprawie transgranicznej interoperacyjności systemów elektronicznych kart zdrowia (notyfikowane jako dokument nr C(2008) 3282), Dz.U. L 190 z 18.7.2008, s. 37.

([4]) Zob. również motyw 34 dyrektywy 95/46. Zob. również na ten temat opinia Grupy Roboczej Art. 29 w sprawie elektronicznej dokumentacji zdrowotnej s. 16, wspomniana powyżej w przypisie 8.

w przypadku przetwarzania danych do celów statystycznych, jak wspomniano w opinii EIOD na temat proponowanego rozporządzenia w sprawie statystyk Wspólnoty w zakresie zdrowia publicznego oraz bezpieczeństwa i higieny pracy ([1]), dodatkowe ryzyko może wynikać z faktu, że pojęcia „poufność" i „ochrona danych" mogą mieć inne znaczenie w stosowaniu prawodawstwa dotyczącego ochrony danych, a inne – w prawodawstwie dotyczącym statystyki.

37. EIOD pragnie zwrócić uwagę na powyższe elementy w kontekście przedmiotowego wniosku. Należy uwzględnić wyraźniejsze odniesienia do wymagań dotyczących ochrony danych w kontekście dalszego wykorzystywania danych na temat zdrowia (zob. sekcja III poniżej).

III. **SZCZEGÓŁOWA ANALIZA WNIOSKU**

Przepisy dotyczące ochrony danych zawarte we wniosku

38. We wniosku w różnych jego częściach zawarto szereg odniesień do ochrony danych i prywatności, mianowicie:

— w motywie 3 stwierdza się między innymi, że przedmiotową dyrektywę należy wdrażać i stosować z należytym poszanowaniem praw do życia prywatnego i rodzinnego oraz ochrony danych osobowych;

— w motywie 11 odwołano się do podstawowego prawa do prywatności w odniesieniu do przetwarzania danych osobowych i do poufności, jako dwóch zasad funkcjonowania systemów zdrowotnych w całej Wspólnocie;

— w motywie 17 opisano prawo do ochrony danych osobowych jako prawo podstawowe jednostki, które należy chronić, skupiając się zwłaszcza na prawie obywateli do dostępu do danych dotyczących ich zdrowia – również w kontekście transgranicznej opieki zdrowotnej – jak ustanowiono w dyrektywie 95/46/WE;

— w art. 3, w którym określono stosunek przedmiotowej dyrektywy do innych przepisów prawa wspólnotowego, ust. 1 lit. a) odwołano się do dyrektyw 95/46/WE i 2002/58/WE;

— w art. 5 dotyczącym obowiązków państwa członkowskiego leczenia w ust. 1 lit. f) jako jeden z tych obowiązków ustalono ochronę prawa do prywatności zgodnie z krajowymi przepisami wdrażającymi dyrektywy 95/46/WE i 2002/58/WE;

— w art. 6 dotyczącym opieki zdrowotnej w innym państwie członkowskim w ust. 5 pacjentom udającym się do innego państwa członkowskiego z zamiarem uzyskania tam opieki zdrowotnej lub poszukującym możliwości uzyskania opieki zdrowotnej świadczonej w innym państwie członkowskim zagwarantowano prawo dostępu do ich dokumentacji medycznej, również zgodnie z krajowymi środkami wdrażającymi dyrektywy 95/46/WE i 2002/58/WE;

— w art. 12 dotyczącym krajowych punktów kontaktowych do spraw transgranicznej opieki zdrowotnej w ust. 2 lit. a) stwierdza się, że punkty te powinny być również odpowiedzialne – między innymi – za dostarczanie i rozpowszechnianie wśród pacjentów informacji w zakresie zagwarantowania ochrony danych osobowych udostępnionych w innym państwie członkowskim;

— w art. 16 dotyczącym e-zdrowia stwierdza się, że środki niezbędne do osiągnięcia interoperacyjności w zakresie systemów technologii informacyjno-komunikacyjnych powinny respektować podstawowe prawo do ochrony danych osobowych zgodnie z odpowiednimi przepisami;

— na koniec w art. 18 ust. 1 wspomniano – między innymi – że gromadzenie danych do celów statystycznych i do celów monitorowania powinno odbywać się zgodnie z prawem krajowym i wspólnotowym dotyczącym ochrony danych osobowych.

39. EIOD z zadowoleniem przyjmuje fakt, że przy przygotowywaniu wniosku uwzględniono zagadnienie ochrony danych i że podjęto starania, aby wykazać ogólną potrzebę zachowania prywatności w kontekście transgranicznej opieki zdrowotnej. Jednak zawarte we wniosku przepisy dotyczące ochrony danych są albo zbyt ogólne, albo odnoszą się do obowiązków państw członkowskich w dość wybiórczy i rozproszony sposób:

— w szczególności motywy 3 i 11 oraz art. 3 ust. 1 lit. a), art. 16 i art. 18 ust. 1 odwołują się w istocie do ogólnych ram prawnych w zakresie ochrony danych (dwa ostatnie w kontekście e-zdrowia i gromadzenia statystyk, ale bez ustalenia konkretnych wymagań dotyczących prywatności);

— w odniesieniu do obowiązków państw członkowskich w art. 5 ust. 1 lit. f) umieszczono ogólne odwołanie;

— motyw 17 i art. 6 ust. 5 zawierają bardziej szczegółowe odniesienie do prawa pacjentów do dostępu do danych osobowych w państwie członkowskim leczenia;

— na koniec art. 12 ust. 2 lit. a) zawiera przepis o prawie pacjentów do informacji w państwie członkowskim ubezpieczenia (w ramach funkcjonowania krajowych punktów kontaktowych).

Ponadto, jak już wspomniano we wprowadzeniu do niniejszej opinii, brakuje powiązania lub odniesienia do aspektów związanych z prywatnością poruszonych w innych instrumentach prawnych UE (wiążących lub nie) obowiązujących w dziedzinie opieki zdrowotnej, zwłaszcza w odniesieniu do stosowania nowych aplikacji TIK (takich jak telemedycyna lub elektroniczne karty zdrowia).

([1]) Dz.U. C 295 z 7.12.2007, s. 1.

40. W ten sposób, chociaż ogólnie stwierdza się, że ochrona prywatności jest wymaganiem związanym z transgraniczną opieką zdrowotną, nadal brakuje obrazu całości zarówno w kontekście zobowiązań państw członkowskich, jak i szczegółów związanych z transgranicznym charakterem udzielania opieki zdrowotnej (w przeciwieństwie do udzielania opieki zdrowotnej w kraju). Konkretniej:

— obowiązków państw członkowskich nie przedstawiono w sposób zintegrowany, ponieważ niektóre zobowiązania (prawo do dostępu i informacji) podkreślono – chociaż w różnych częściach wniosku – natomiast inne, jak bezpieczeństwo przetwarzania, całkowicie pominięto;

— nie odwołano się do zastrzeżeń dotyczących braku spójności między środkami bezpieczeństwa stosowanymi przez państwa członkowskie oraz do konieczności zharmonizowania na szczeblu europejskim bezpieczeństwa danych na temat zdrowia w kontekście transgranicznej opieki zdrowotnej;

— nie odniesiono się do kwestii zintegrowania prywatności w aplikacjach w zakresie e-zdrowia. Zagadnienie to nie zostało również odpowiednio odzwierciedlone w przypadku wystawiania elektronicznych recept (*ePrescription*).

41. Ponadto pewne konkretne obawy budzi art. 18 dotyczący gromadzenia danych do celów statystycznych i do celów monitorowania. W pierwszym ustępie mówi się o „danych statystycznych i *innych dodatkowych danych*"; ponadto wspomina się w nim w liczbie mnogiej o „celach monitorowania", a następnie wymienia obszary, których to monitorowanie dotyczy, tj. świadczenie transgranicznej opieki zdrowotnej, przeprowadzone leczenie, podmioty świadczące opiekę, pacjentów, koszty oraz rezultaty. W tym kontekście – i tak już dość niejasnym – dokonuje się ogólnego odniesienia do prawa w zakresie ochrony danych, nie ustanawia się jednak żadnych konkretnych wymagań dotyczących dalszego wykorzystania danych dotyczących zdrowia, o których mowa w art. 8 ust. 4 dyrektywy 95/46/WE. Dodatkowo w ust. 2 zawarto bezwarunkowe zobowiązanie do przekazywania Komisji dużej ilości danych przynajmniej raz w roku. Ponieważ nie dokonano wyraźnego odniesienia do oceny konieczności takiego przekazania, wydaje się, że sam prawodawca wspólnotowy już ustanowił konieczność dokonywania takiego przekazania do Komisji.

Zalecenia EIOD

42. EIOD przedstawia szereg zaleceń – w postaci opisanych poniżej pięciu podstawowych kroków do dokonania zmian – które pozwolą w odpowiedni sposób odnieść się do wspomnianych wyżej elementów.

Krok 1 – definicja danych na temat zdrowia

43. W art. 4 zdefiniowano podstawowe terminy stosowane w przedmiotowym wniosku. EIOD zdecydowanie zaleca wprowadzenie w tym artykule definicji danych na temat zdrowia. Należy przyjąć szeroką interpretację danych na temat zdrowia, podobną do opisanej w sekcji II niniejszej opinii (pkt 14 i 15).

Krok 2 – wprowadzenie szczegółowego artykułu dotyczącego ochrony danych

44. EIOD zdecydowanie zaleca również wprowadzenie do wniosku szczegółowego artykułu dotyczącego ochrony danych, w którym w jasny i zrozumiały sposób będzie można całościowo określić wymiar prywatności. W artykule tym należy a) opisać obowiązki państw członkowskich ubezpieczenia i leczenia, w tym – między innymi – konieczność zagwarantowania bezpieczeństwa przetwarzania; oraz b) określić główne obszary dalszych prac, np. harmonizację bezpieczeństwa i integrację zagadnienia prywatności w dziedzinie e-zdrowia. W tym celu można przygotować (w ramach proponowanego artykułu) szczegółowe przepisy, o których mowa w krokach 3 i 4 poniżej.

Krok 3 – szczegółowy przepis dotyczący harmonizacji bezpieczeństwa

45. W następstwie zmiany zaproponowanej w kroku 2 EIOD zaleca, aby Komisja przyjęła mechanizm pozwalający na ustalenie powszechnie akceptowalnego poziomu bezpieczeństwa danych dotyczących opieki zdrowotnej na poziomie krajowym, z uwzględnieniem norm technicznych obowiązujących w tej dziedzinie. Powinno to znaleźć odzwierciedlenie we wniosku. Ewentualnego wdrożenia można dokonać w drodze procedury komitetowej, która została już opisana w art. 19 i ma zastosowanie do pozostałych części wniosku. Ponadto można wykorzystać dodatkowe instrumenty służące stworzeniu odpowiednich wytycznych; można także skorzystać z pomocy wszystkich stron zainteresowanych, takich jak Grupa Robocza Art. 29 i EIOD.

Krok 4 – integracja ochrony prywatności we wzorze elektronicznej recepty (*ePrescription*)

46. W art. 14 dotyczącym uznawania recept wystawionych w innym państwie członkowskim przewidziano opracowanie wspólnotowego wzoru recepty przyczyniającego się do interoperacyjności e-recept. Środek ten przyjmuje się w ramach procedury komitetowej, o której mowa w art. 19 ust. 2 przedmiotowego wniosku.

47. EIOD zaleca, aby w proponowanym wzorze e-recepty uwzględnić zagadnienia prywatności i bezpieczeństwa już w momencie podstawowego definiowania semantycznego tego wzoru. Należy wyraźnie wspomnieć o tym w art. 14 ust. 2 lit. a). Ponownie duże znaczenie ma zaangażowanie wszystkich zainteresowanych stron. W związku z tym EIOD chciałby być informowany o dalszych działaniach podejmowanych w tej dziedzinie w ramach proponowanej procedury komitetowej oraz brać udział w tych działaniach.

Krok 5 – dalsze wykorzystanie danych na temat zdrowia do celów statystycznych i do celów monitorowania

48. Aby uniknąć nieporozumień, EIOD zaleca wyjaśnienie pojęcia „innych dodatkowych danych", które pojawia się w art. 18 ust. 1. Artykuł ten należałoby ponadto zmienić, tak aby w bardziej jednoznaczny sposób odnosił się do wymagań związanych z dalszym wykorzystaniem danych dotyczących zdrowia, o którym mowa w art. 8 ust. 4 dyrektywy 95/46/WE. Dodatkowo zawarty w drugim ustępie obowiązek przekazywania wszystkich danych Komisji powinien podlegać ocenie konieczności takiego przekazania do uzasadnionych celów, które należy zawczasu należycie określić.

IV. **PODSUMOWANIE**

49. EIOD chciałby wyrazić poparcie dla inicjatyw, które mają na celu poprawę warunków transgranicznej opieki zdrowotnej. Wyraża jednak zaniepokojenie faktem, że inicjatywy WE w zakresie opieki zdrowotnej nie zawsze są należycie skoordynowane pod względem wykorzystania TIK, prywatności i bezpieczeństwa, co opóźnia przyjęcie ogólnego podejścia w zakresie ochrony danych w dziedzinie opieki zdrowotnej.

50. EIOD z zadowoleniem przyjmuje odniesienie do prywatności, które uwzględniono w przedmiotowym wniosku. Konieczna jest jednak pewna liczba zmian – jak wyjaśniono w sekcji III niniejszej opinii – aby przedstawić jasne wymagania wobec państw członkowskich leczenia i ubezpieczenia, jak również w odpowiedni sposób odnieść się do wymiaru ochrony danych w kontekście transgranicznej opieki zdrowotnej:

— w art. 4 należy umieścić definicję danych dotyczących zdrowia, która będzie obejmowała wszelkie dane osobowe mające wyraźny i ścisły związek z opisem stanu zdrowia danej osoby. Powinna ona zasadniczo objąć dane medyczne, jak również dane administracyjne i finansowe dotyczące zdrowia;

— zdecydowanie zaleca się wprowadzenie konkretnego artykułu dotyczącego ochrony danych. W artykule tym należy jasno uwzględnić pełen obraz, opisując zobowiązania państw członkowskich ubezpieczenia i leczenia oraz określając główne obszary dalszych prac, np. harmonizację bezpieczeństwa i integrację zagadnienia prywatności zwłaszcza w aplikacjach dotyczących e-zdrowia;

— zaleca się, aby w ramach przedmiotowego wniosku Komisja przyjęła mechanizm pozwalający na ustalenie powszechnie akceptowalnego poziomu bezpieczeństwa danych dotyczących opieki zdrowotnej na poziomie krajowym, z uwzględnieniem norm technicznych obowiązujących w tej dziedzinie. Należy również zachęcać do podejmowania dodatkowych lub uzupełniających inicjatyw, w których będą uczestniczyć wszystkie zainteresowane strony, Grupa Robocza Art. 29 i EIOD.

— zaleca się, aby w proponowanym wspólnotowym wzorze e-recepty uwzględnić koncepcję „domyślnej ochrony prywatności" (również na poziomie semantycznym). Należy wyraźnie wspomnieć o tym w art. 14 ust. 2 lit. a). EIOD chciałby być informowany o dalszych działaniach podejmowanych w tej dziedzinie w ramach proponowanej procedury komitetowej oraz brać udział w tych działaniach;

— zaleca się doprecyzowanie brzmienia art. 18 oraz zawarcie w nim wyraźniejszego odniesienia do konkretnych wymagań dotyczących dalszego wykorzystania danych dotyczących zdrowia, o którym mowa w art. 8 ust. 4 dyrektywy 95/46/WE.

Sporządzono w Brukseli, dnia 2 grudnia 2008 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych