KOMISJA EUROPEJSKA

Bruksela, dnia 22.4.2010
KOM(2010)170 wersja ostateczna

SPRAWOZDANIE KOMISJI

w sprawie stanu ochrony danych w Systemie Wymiany Informacji na Rynku Wewnętrznym

SPRAWOZDANIE KOMISJI

w sprawie stanu ochrony danych w Systemie Wymiany Informacji na Rynku Wewnętrznym

1. STRESZCZENIE

Komisja jest zadowolona ze sposobu, w jaki w Systemie Wymiany Informacji na Rynku Wewnętrznym (systemie IMI) zapewnia się prawa i wolności osobiste w odniesieniu do ochrony danych osobowych (zwanej dalej „ochroną danych"). System IMI jest bezpiecznym i wielojęzycznym internetowym systemem wymiany informacji, który wspiera państwa członkowskie w wykonywaniu ich obowiązków związanych ze współpracą administracyjną. Komisja jest również zadowolona z wdrażania zalecenia w sprawie wytycznych w zakresie ochrony danych dla systemu IMI.

Państwa członkowskie nie zgłosiły żadnych problemów w zakresie ochrony danych. Ten stan rzeczy uzasadnia podejście krok po kroku uzgodnione z Europejskim Inspektorem Ochrony Danych i mające na celu stworzenie ram prawnych dla systemu IMI w odpowiedzi na rozwój technologiczny i rozszerzenie zakresu systemu na inne obszary prawodawstwa w ramach rynku wewnętrznego.

W 2010 r. Komisja zbada możliwość rozszerzenia zakresu systemu IMI na inne obszary rynku wewnętrznego i zdobędzie większe doświadczenie w zakresie praktycznego stosowania systemu w obszarze usług. W pierwszym kwartale 2011 r. Komisja opublikuje dokument roboczy służb Komisji w sprawie funkcjonowania i rozwoju systemu IMI w 2010 r., który obejmie również kwestię ochrony danych.

2. CEL NINIEJSZEGO SPRAWOZDANIA

Niniejsze sprawozdanie, przewidziane w zaleceniu Komisji w sprawie wytycznych w zakresie ochrony danych dla Systemu Wymiany Informacji na Rynku Wewnętrznym[1] („zalecenie"), zawiera przegląd realizacji zalecenia przez państwa członkowskie i przez Komisję oraz ocenę stanu ochrony danych w systemie IMI. Obejmuje ono również nowe kwestie, którymi nie zajęto się w zaleceniu, w szczególności objęcie systemem nowej dyrektywy o usługach.

Podczas sporządzania niniejszego sprawozdania Komisja uwzględniła informacje zwrotne przedstawione przez państwa członkowskie zarówno w ramach konsultacji *ad hoc* rozpoczętych w listopadzie 2009 r.[2], jak i regularnego kontaktu z

---

1 C(2009) 2041 wersja ostateczna. Dz.U. L 100 z 18.4.2009, s. 12–28.

2 W ramach konsultacji siedemnaście państw członkowskich odpowiedziało na następujące pytania:
- Czy kontaktowali się Państwo z krajowym organem ochrony danych? Czy wypowiedział się on na temat krajowego wdrażania wytycznych?
- Czy sporządzili Państwo ogólne oświadczenie o polityce ochrony prywatności dla wszystkich użytkowników systemu IMI czy też jest ono przygotowywane lokalnie przez właściwe organy?

koordynatorami systemu IMI i przedstawicielami państw członkowskich na posiedzeniach IMAC-IMI (rynek wewnętrzny – Komitet Doradczy ds. Rynku Wewnętrznego w ramach systemu IMI).

3. ROZWÓJ SYSTEMU IMI W 2009 R.

Rok 2009 był decydujący dla rozwoju systemu IMI. Zakres stosowania systemu IMI w odniesieniu do prawodawstwa dotyczącego kwalifikacji zawodowych rozszerzono na 20 nowych zawodów, a większość zasobów przeznaczono na rozszerzenie zakresu systemu IMI w celu objęcia nim dyrektywy o usługach[3].

Krajowi koordynatorzy systemu IMI uczestniczyli w projekcie pilotażowym mającym na celu wymianę informacji w zakresie dyrektywy o usługach (w oparciu o przypadki rzeczywiste i fikcyjne) i w szkoleniach, które odbyły się w Brukseli[4]. Komisja wydała nową wersję oprogramowania (1.7), aby umożliwić właściwym organom samodzielną rejestrację. Pod koniec roku Komisja wydała również tymczasową wersję 2.0, która zawierała oddzielną aplikację komputerową dla mechanizmu ostrzegania[5]. Nowa wersja oprogramowania zaczęła w pełni działać w pierwszym kwartale 2010 r.

Dzięki wspólnym wysiłkom Komisji i państw członkowskich do końca stycznia 2010 r. w systemie IMI zarejestrowano 4 508 właściwych organów, z których 3 689 miało dostęp do nowego obszaru usług. Oczekuje się jednak, że w ciągu kilku następnych miesięcy liczba ta znacznie wzrośnie. Średnia dzienna liczba różnych zalogowanych użytkowników wzrosła z 40 w styczniu 2009 r. do 180 w grudniu.

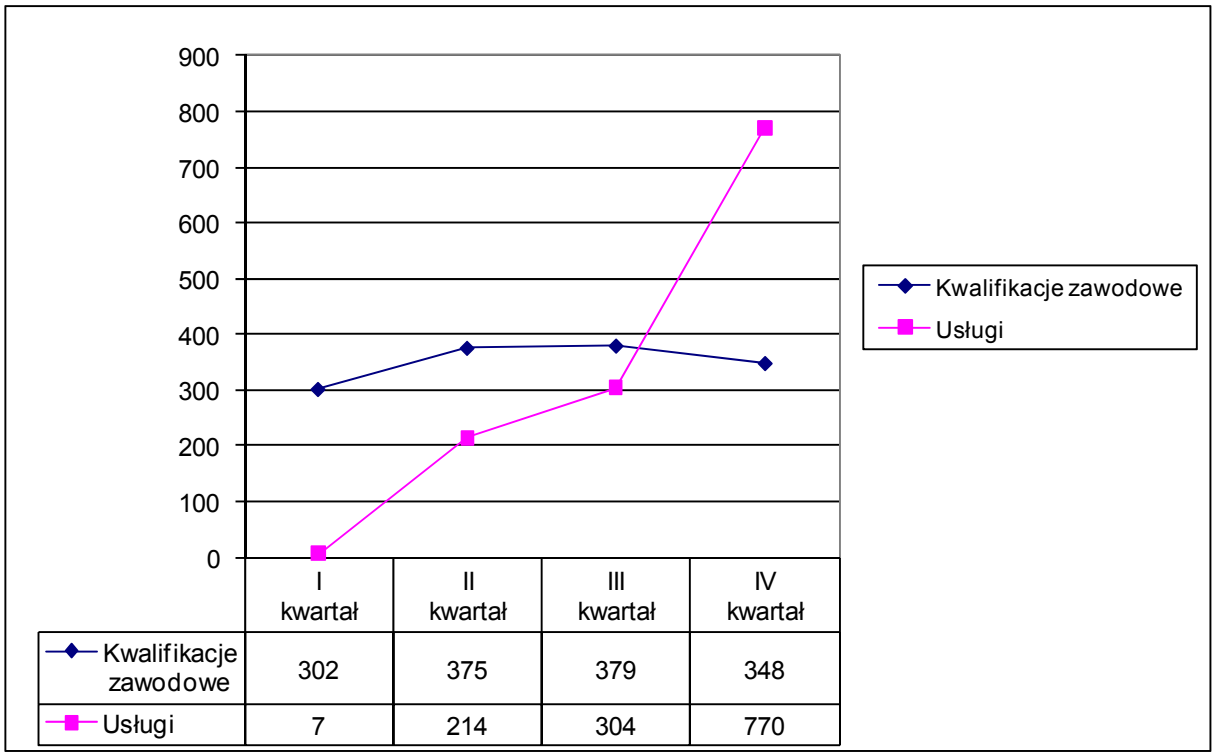
- Czy właściwe organy doświadczyły jakichkolwiek problemów w związku z ochroną danych podczas wysyłania wniosków lub odpowiedzi na wnioski w systemie IMI?
- Czy właściwe organy zgłosiły jakiekolwiek problemy w rozpatrywaniu pytań w sprawie rejestrów karnych?
- Czy właściwe organy otrzymały od osób, których dotyczą dane, jakiekolwiek wnioski dotyczące dostępu do danych, ich anulowania lub poprawiania?
- Czy właściwe organy są świadome możliwości szybkiego anulowania danych osobowych w systemie? Czy korzystają z tej możliwości?
- Czy uwzględnili Państwo kwestię ochrony danych w szkoleniach w zakresie systemu IMI?

[3] Dyrektywa 2006/123/WE Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. dotycząca usług na rynku wewnętrznym, Dz.U. L 376 z 27.12.2006, s. 36–68.

[4] W 2009 r. Komisja zorganizowała w Brukseli trzy jednodniowe szkolenia dla koordynatorów systemu IMI, każde dla około 60 uczestników. W tym samym czasie państwa członkowskie zorganizowały w sumie ponad 100 szkoleń dla właściwych organów na szczeblu lokalnym, regionalnym i krajowym.

[5] Zob. art. 32 dyrektywy o usługach.

Łączna liczba wysłanych wniosków na kwartał i w podziale na obszary prawodawstwa w 2009 r.



	I kwartał	II kwartał	III kwartał	IV kwartał
Kwalifikacje zawodowe	302	375	379	348
Usługi	7	214	304	770

W dziedzinie kwalifikacji zawodowych system rozwinął się w pełni, a jego niezaprzeczalny sukces obrazuje możliwości systemu IMI jako narzędzia dla współpracy administracyjnej w UE. W każdym kwartale wysłano średnio 350 wniosków. Ponad 90 % wszystkich wniosków dotyczących kwalifikacji zawodowych wysłanych w 2009 r. pochodziło z UE-15, tj. państw członkowskich, które przystąpiły do UE przed 2004 r., co odzwierciedla kierunek migracji zarobkowej. Polska i Rumunia były odbiorcami 32 % wszystkich wniosków.

Przyglądając się tym liczbom, należy zauważyć, że na 56 % wniosków odpowiedziano w ciągu jednego tygodnia.

Czas potrzebny na odpowiedź na wniosek w ramach dyrektywy o kwalifikacjach zawodowych w 2009 r.

	Wnioski przyjęte	**Narastająco %**	**Wnioski, na które udzielono odpowiedzi**	**Narastająco %**
W ciągu 3 dni	**741**	**57,0 %**	**518**	**43,0 %**
W ciągu 1 tygodnia	**216**	**73,7 %**	**167**	**56,8 %**
W ciągu 2 tygodni	**166**	**86,5 %**	**170**	**71,0 %**

W ciągu 4 tygodni	**120**	**95,7 %**	**164**	**84,6 %**
W ciągu 8 tygodni	**35**	**98,4 %**	**106**	**93,4 %**
Powyżej 8 tygodni	**21**	**100,0 %**	**80**	**100,0 %**
Ogółem:	**1 299**		**1 205**	

(* Rozbieżność między liczbą wniosków przyjętych a liczbą wniosków, na które udzielono odpowiedzi, jest spowodowana wnioskami wycofanymi lub nadal rozpatrywanymi w grudniu 2009 r.)

4. POPRAWA OCHRONY DANYCH W SYSTEMIE IMI, PODEJŚCIE KROK PO KROKU

System IMI działa zgodnie z tzw. podejściem „poszanowania prywatności od samego początku", w którym przestrzeganie ochrony danych jest wpisane w systemy zawierające informacje od samego początku. Względy dotyczące ochrony danych są również częścią codziennego stosowania systemu i zostały zawarte w materiałach szkoleniowych, co stanowi podejście wychodzące poza formalną lub teoretyczną ochronę. Wydaje się, że jest to korzystne podejście, skoro żadne państwo członkowskie nie zgłosiło ani jednego incydentu związanego z ochroną danych w systemie IMI, ani żadna osoba, której dotyczą dane, nie złożyła skargi.

W ciągu dwóch ostatnich lat Komisja włączyła się w dialog z organami ochrony danych i z Europejskim Inspektorem Ochrony Danych. W myśl głównej zasady podejścia krok po kroku – biorąc pod uwagę, że system zapewnia wysoki poziom technicznej i proceduralnej ochrony danych, a Komisja jest wyraźnie zaangażowana w jego stałe ulepszanie – ramy prawne dla systemu IMI powinny być dostosowane do rozwoju technologicznego i rozszerzenia zakresu systemu na inne obszary prawodawstwa w ramach rynku wewnętrznego.

Podejście krok po kroku – w oparciu o ograniczone doświadczenie w korzystaniu z systemu – umożliwiło Komisji odniesienie się do wszystkich problemów zasygnalizowanych przez Europejskiego Inspektora Ochrony Danych w opinii z dnia 12 grudnia 2007 r. oraz przyjęcie trzech aktów prawnych dotyczących kwestii ochrony danych w systemie IMI:

a) decyzji Komisji z dnia 12 grudnia 2007 r. w sprawie wdrożenia systemu wymiany informacji rynku wewnętrznego (IMI) pod względem ochrony danych osobowych[6];

b) zalecenia Komisji z dnia 26 marca 2009 r. w sprawie wytycznych w zakresie ochrony danych dla systemu wymiany informacji na rynku wewnętrznym (IMI)[7];

c) decyzji Komisji z dnia 2 października 2009 r. określającej praktyczne ustalenia dotyczące wymiany informacji drogą elektroniczną między

[6] C(2007) 6306, Dz.U. L 13 z 16.1.2008, s. 13-23.
[7] C(2009) 2041 wersja ostateczna, Dz.U. L 100 z 18.4.2009, s. 12-28.

państwami członkowskimi na mocy rozdziału VI dyrektywy 2006/123/WE Parlamentu Europejskiego i Rady dotyczącej usług na rynku wewnętrznym[8].

W sekcji 6 niniejszego sprawozdania omówione zostaną wszelkie pozostałe kwestie oraz treść i stosowność wszelkich przyszłych środków, w tym ewentualne przyjęcie aktu prawnego.

5. REALIZACJA ZALECENIA KOMISJI

5.1. Ulepszenia wprowadzone przez państwa członkowskie

5.1.1. Kontakty z organami ochrony danych

Zalecenie obejmuje „zachęcenie koordynatorów systemu IMI, aby zwrócili się do krajowych urzędów ochrony danych o wskazówki i pomoc w określeniu najlepszego sposobu realizacji niniejszych wytycznych zgodnie z prawem krajowym". W sprawozdaniach przedstawianych Komisji państwa członkowskie stwierdziły w większości, że przeprowadziły konsultacje z krajowymi organami ochrony danych. Konsultacje te upewniły użytkowników systemu IMI, że dane osobowe można wymieniać za pomocą systemu IMI zgodnie z przepisami o ochronie danych, i jednocześnie umożliwiły krajowym organom regulacyjnym ustanowienie relacji roboczych z przedstawicielami administracji publicznej, dla których ochrona danych ma duże znaczenie i którzy są zaangażowani w zapewnienie powodzenia tego prawdziwie europejskiego projektu.

5.1.2. Oświadczenia o ochronie prywatności

Zgodnie z sugestią ze strony Europejskiego Inspektora Ochrony Danych w zaleceniu zachęcono koordynatorów systemu IMI do dyskusji na temat treści oświadczeń o ochronie prywatności również z lokalnymi organami ochrony danych. Zalecenie nie mogło być bardzo szczegółowe w tej kwestii, ponieważ mimo pełnej harmonizacji dyrektywy o ochronie danych państwa członkowskie mają margines swobody uznania w odniesieniu do wdrażania niektórych przepisów. Sprawozdania państw członkowskich potwierdzają, że istnieją różne praktyki krajowe w zakresie treści i formy oświadczeń o ochronie prywatności. Nieznaczna większość państw członkowskich uważa, że o odpowiedniej formie i treści informacji, które należy zapewnić osobom fizycznym, powinien decydować każdy właściwy organ na szczeblu lokalnym zgodnie z lokalnymi przepisami. W niektórych państwach członkowskich proponuje się natomiast możliwe do dostosowywania wzory dla całego państwa członkowskiego[9].

---

[8] C(2009) 7493, Dz.U. L 263 z 7.10.2009, s. 32-34.

[9] Dobrym przykładem krajowego wzoru opracowanego z pomocą techniczną ze strony krajowego organu ochrony danych jest oświadczenie o ochronie prywatności (*cláusula de privacidad*) udostępnione przez hiszpański zespół ds. systemu IMI: http://www.mpt.es/documentacion/sistema_IMI/documentos/protec_datos/ClausulaIMI_ES/document_es/Clausula_IMI.pdf.

5.1.3. Świadomość i szkolenie

Jednym z najważniejszych osiągnięć zalecenia jest fakt, że przyczyniło się do zwiększenia świadomości w zakresie ochrony danych wśród uczestników i użytkowników systemu IMI, którzy obecnie znają ogólne zasady ochrony danych, oraz zapewniło praktyczne sugestie w celu zagwarantowania wysokiego poziomu ochrony danych w systemie IMI. Dzięki zaleceniu odesłania do wytycznych w zakresie ochrony danych zostały zawarte również w materiałach szkoleniowych dotyczących systemu IMI opracowanych dla właściwych organów.

5.2. Ulepszenia wprowadzone przez Komisję

5.2.1. Plan bezpieczeństwa systemu IMI

Bezpieczeństwo i poufność danych są regulowane przez decyzję Komisji z dnia 16 sierpnia 2006 r. dotyczącą bezpieczeństwa systemów informacyjnych wykorzystywanych przez Komisję Europejską[10]. Decyzję tę zaktualizowano przepisami wykonawczymi przyjętymi w 2009 r. oraz niedawnymi wytycznymi i normami, które zasadniczo są takie same, jak normy międzynarodowe. W 2009 r. dokonano przeglądu środków bezpieczeństwa w systemie IMI i odpowiednio je zaktualizowano oraz sporządzono szczegółowy plan bezpieczeństwa, którego przegląd nastąpi w 2010 r.

5.2.2. Ulepszenia techniczne

W przypadku gdy wymiana informacji dotyczy danych szczególnie chronionych, na ekranie pojawia się obecnie przypomnienie, że informacje są szczególnie chronione, a osoba zajmująca się daną sprawą powinna zwrócić się o takie informacje jedynie, gdy jest to niezbędnie konieczne i bezpośrednio związane z wykonywaniem zawodu lub świadczeniem danej usługi. Względy dotyczące ochrony danych wzięto również w pełni pod uwagę przy opracowywaniu i wdrażaniu nowego mechanizmu ostrzegania (zob. część 5.2.3.2 poniżej).

Stronę internetową systemu IMI również ulepszono, tak aby znalezienie przez użytkowników odpowiednich dokumentów było bardziej intuicyjne. Część dotycząca ochrony danych[11] została zaktualizowana z uwzględnieniem wszystkich aktów prawnych związanych z ochroną danych, korespondencji z Europejskim Inspektorem Ochrony Danych i zestawów pytań stosowanych w systemie. Dla celów przejrzystości i w odpowiedzi na sugestię ze strony Europejskiego Inspektora Ochrony Danych zidentyfikowano kwestie dotyczące danych szczególnie chronionych.

5.2.3. Nowy obszar prawodawstwa związany z dyrektywą o usługach

5.2.3.1. Stosowanie systemu IMI na potrzeby dyrektywy o usługach

Dyrektywa o usługach nie odnosi się w szczególności do systemu IMI (ale bardziej ogólnie do elektronicznego systemu wymiany informacji). Konieczne było zatem

---

[10] C(2006) 3602.

[11] http://ec.europa.eu/internal_market/imi-net/data_protection_pl.html.

formalne określenie, że do tego celu stosowany będzie system IMI. Uczyniono to w drodze decyzji[12] przyjętej przez Komisję zgodnie z procedurą przewidzianą w dyrektywie o usługach („decyzja w ramach procedury komitetowej").

Decyzja przyjęta w ramach procedury komitetowej określa praktyczne ustalenia dotyczące wymiany informacji w obszarze usług w systemie IMI. Przyczynia się ona do wysokiego poziomu ochrony danych w systemie i zapewnia dodatkową przejrzystość i dokładność ogólnych przepisów wynikających z decyzji 2008/49/WE i wytycznych w zakresie ochrony danych zawartych w zaleceniu. Przewiduje w razie potrzeby możliwość podjęcia w późniejszym terminie decyzji o wszelkich dodatkowych środkach ochrony danych w świetle doświadczenia zdobytego w stosowaniu systemu[13].

5.2.3.2. Projekt mechanizmu ostrzegania sprzyjający ochronie danych

Mechanizm ostrzegania jest mechanizmem ostrzegającym ustanowionym zgodnie z art. 29 ust. 3 i art. 32 dyrektywy o usługach, uzupełniającym system RAPEX dla produktów. Pomaga on uniknąć odbiorcom usług ryzyka wynikającego z tych usług.

Mechanizm ostrzegania umożliwia państwom członkowskim przestrzeganie obowiązku prawnego dotyczącego wymiany informacji i jest tym samym w pełni zgodny z prawem z punktu widzenia ochrony danych. Komisja jest jednak świadoma skutków stosowania takiego systemu w zakresie ochrony danych. Dlatego też starannie zaprojektowała system, zapewniając jego sprzyjający ochronie danych charakter, oraz zachęca państwa członkowskie, które są odpowiedzialne za ochronę danych przy wysyłaniu i otrzymywaniu ostrzeżeń, do zachowania czujności w celu prawidłowego stosowania przepisów.

Mechanizm ostrzegania obejmuje szereg środków ochrony danych, które stanowią ogólne cechy systemu IMI, oraz kilka szczególnych środków ochrony mających na celu zagwarantowanie, że:

a) **Dostęp do danych jest ograniczony tylko do określonych właściwych organów/użytkowników**

Zgodnie z ogólnym podejściem w ramach systemu IMI dostęp do informacji objętych mechanizmem ostrzegania jest ściśle ograniczony w oparciu o zasadę ograniczonego dostępu. Właściwe organy i użytkownicy systemu IMI mają dostęp do ostrzeżeń jedynie w przypadku, w którym państwa członkowskie udzieliły im szczególnego dostępu nie tylko ogólnie do systemu IMI, ale również do specjalnej aplikacji dla ostrzeżeń. Właściwe organy i użytkownicy systemu IMI nie mogą wysyłać ani odbierać ostrzeżeń w ramach ustawień domyślnych. Funkcję tę należy uruchomić oddzielnie.

b) **Nie wysyła się niepotrzebnych ostrzeżeń**

---

[12] Decyzja Komisji z dnia 2 października 2009 r. określająca praktyczne ustalenia dotyczące wymiany informacji drogą elektroniczną między państwami członkowskimi na mocy rozdziału VI dyrektywy 2006/123/WE Parlamentu Europejskiego i Rady dotyczącej usług na rynku wewnętrznym.

[13] Zob. pkt. 13 załącznika do zalecenia, „Prace w toku", lit. d).

Nie można wysłać żadnego ostrzeżenia bez wypełnienia listy kontrolnej w celu zapewnienia spełnienia kryteriów; na przykład wykazania, że mają miejsce szczególne poważne działania lub okoliczności związane z działalnością usługową, które mogłyby spowodować znaczne szkody. Jeżeli organ inicjujący nie spełni wszystkich właściwych kryteriów, system nie zezwoli mu na wysłanie ostrzeżenia.

Ponadto ostrzeżeń nie wysyła się bezpośrednio do innych państw członkowskich, lecz przedkłada się je koordynatorowi ds. ostrzeżeń w tym samym państwie członkowskim. Koordynator ds. ostrzeżeń powinien ponownie rozważyć, czy dane ostrzeżenie należy rozpowszechnić w innych państwach członkowskich.

c) **Ostrzeżeń nie wysyła się do większej liczby odbiorców niż jest to konieczne w celu zapewnienia zgodności z wymogami informacyjnymi określonymi w przepisach**

Jeżeli ostrzeżenia wysyła się do innych państw członkowskich, organ inicjujący i koordynator ds. ostrzeżeń muszą ocenić, które państwa członkowskie powinny otrzymać ostrzeżenie. Jeżeli państwo członkowskie, w którym świadczona jest usługa, chce wysłać ostrzeżenie, z założenia ostrzeżenie otrzyma jedynie państwo członkowskie prowadzenia działalności przez usługodawcę i Komisja. Powyższa domyślna konfiguracja gwarantuje, że dodanie innego państwa członkowskiego do listy odbiorców podlega decyzjom podejmowanym w każdym indywidualnym przypadku w oparciu o zasadę ograniczonego dostępu.

Co więcej, jeżeli ostrzeżenie rozpowszechnia się w innych państwach członkowskich, nie wysyła się go do wszystkich właściwych organów w państwach członkowskich otrzymujących ostrzeżenie, ale jedynie do skrzynki pocztowej do odbioru ostrzeżeń (zazwyczaj krajowego koordynatora ds. ostrzeżeń). Odbiorca decyduje, których właściwych organów w jego państwie członkowskim dotyczy ostrzeżenie i które organy muszą zostać zaangażowane.

d) **Chociaż Komisja otrzymuje ostrzeżenia zgodnie z dyrektywą o usługach, nie ma dostępu do danych osobowych**

Dyrektywa o usługach przewiduje, że wszystkie ostrzeżenia są wysyłane do Komisji, ale Komisja, w przeciwieństwie do państw członkowskich, nie potrzebuje mieć dostępu do danych osobowych. Komisja otrzymuje zatem ostrzeżenia bez danych osobowych.

e) **Jeżeli mimo podjętych środków ostrożności nieuzasadnione ostrzeżenia zostaną wysłane, można je szybko wycofać a nieprawidłowe dane można poprawić lub usunąć**

System IMI umożliwia właściwemu organowi, który wysłał nieuzasadnione ostrzeżenie, natychmiastowe wycofanie go, co spowoduje, że stanie się ono niewidoczne dla wszystkich użytkowników systemu IMI. Jeżeli ostrzeżenie było uzasadnione, ale konieczne jest poprawienie niektórych informacji, właściwy organ inicjujący może uczynić to w każdej chwili. System IMI umożliwia ponadto innym właściwym organom, które otrzymały ostrzeżenie, wskazanie, że niektóre informacje przedstawione w ostrzeżeniu są nieprawidłowe.

f) **Ostrzeżenia zamyka się w chwili, gdy nie ma już ryzyka; dane natychmiast stają się niewidoczne dla wszystkich użytkowników, a dane osobowe usuwa się sześć miesięcy po zamknięciu ostrzeżenia**

Kiedy zniknie ryzyko, które doprowadziło do wysłania ostrzeżenia, ostrzeżenie należy zamknąć. System IMI umożliwia wtedy państwu członkowskiemu prowadzenia działalności zamknięcie ostrzeżenia, a do odpowiedzialnych organów wysyła się powiadomienia pocztą elektroniczną. Kiedy ostrzeżenie zostaje zamknięte, staje się niewidoczne. Najpóźniej sześć miesięcy po zamknięciu ostrzeżenia wszystkie dane osobowe są automatycznie usuwane i eliminowane z systemu.

6. KWESTIE DO DALSZEGO ROZWAŻENIA

Mimo że większość państw członkowskich wyraziła pozytywną opinię na temat ochrony danych w systemie IMI, kilka państw członkowskich podniosło pewne kwestie, których przegląd znajduje się w niniejszej części sprawozdania.

6.1. Obowiązujące przepisy dotyczące bezpieczeństwa i poufności danych

Przetwarzanie danych osobowych w systemie IMI obejmuje wspólne przetwarzanie danych (między Komisją i państwami członkowskimi), współadministrację (między różnymi użytkownikami i podmiotami) i wspólny nadzór (przez krajowe organy ochrony danych i Europejskiego Inspektora Ochrony Danych). Przydzielenie obowiązków w tak złożonej sytuacji nie zawsze jest łatwe.

Zdaniem duńskich i niemieckich organów ochrony danych w związku z tym, że właściwe organy znajdujące się na ich terytorium muszą spełniać wymogi krajowe (np. lepszy mechanizm uwierzytelniający, o którym mowa w następnej części), powinny one nalegać, aby system IMI również spełniał te wymogi krajowe, a w przeciwnym razie zaprzestać korzystania z systemu. Właściwe organy przekazały te wnioski Komisji, która jest odpowiedzialna za bezpieczeństwo systemu.

Komisja uważa, że system IMI jest systemem bezpiecznym i że prawdziwie europejska sieć, taka jak system IMI, po prostu nie mogłaby działać, gdyby każde państwo członkowskie wymagało, żeby przestrzegano jego krajowych norm bezpieczeństwa. Przyjęcie dyrektywy o ochronie danych prawie dwadzieścia lat temu miało dwojaki cel: z jednej strony ochronę podstawowego prawa do ochrony danych, a z drugiej zapewnienie swobodnego przepływu danych osobowych między państwami członkowskimi i między państwami członkowskimi a instytucjami UE[14].

Na tej podstawie Komisja stwierdza stanowczo, że w świetle wysokiego poziomu gwarancji w odniesieniu do ochrony danych w systemie IMI i zasady lojalnej współpracy zawartej w art. 4 ust. 3 Traktatu o Unii Europejskiej krajowe organy

[14] Zasada ta jest wyraźnie określona w art. 1 ust. 2 dyrektywy o ochronie danych, w art. 1 ust. 1 i w motywie 13 rozporządzenia o ochronie danych: „Celem jest zapewnienie zarówno efektywnej zgodności z regułami rządzącymi ochroną podstawowych praw i wolności osób fizycznych oraz swobodnego przepływu danych osobowych między państwami członkowskimi a instytucjami i organami wspólnotowymi, jak i między instytucjami i organami wspólnotowymi do celów związanych z wykorzystaniem ich kompetencji".

ochrony danych nie powinny stwarzać przeszkód dla stosowania systemu przez właściwe organy.

6.2. W kierunku lepszego uwierzytelniania w systemie IMI

System uwierzytelniania w systemie IMI stanowi zaawansowaną wersję uwierzytelniania jednoskładnikowego, ponieważ łączy nazwę użytkownika i hasło z kodem PIN. Kiedy użytkownik chce wejść do systemu, jest proszony o podanie losowo wybranej kombinacji znaków z kodu PIN.

Niemieckie i duńskie organy ochrony danych wyraziły pewne obawy co do systemu uwierzytelniania w systemie IMI. Komisja uważa, że obecny mechanizm uwierzytelniania jest właściwy, biorąc pod uwagę aktualny stan wiedzy w tej dziedzinie i koszty wdrożenia, ale zgadza się, że w perspektywie długoterminowej lepsze uwierzytelnianie jest pożądane. Ponieważ państwa członkowskie wprowadziły różne systemy uwierzytelniania, które nie zawsze są interoperacyjne, zalecanym rozwiązaniem mającym na celu osiągnięcie lepszego uwierzytelniania w systemie IMI są e-tożsamości zarządzane na szczeblu państwa członkowskiego, które stałyby się interoperacyjne dzięki oprogramowaniu pośredniczącemu.

Jedną z możliwości jest projekt STORK, opracowywany obecnie przez konsorcjum, w którym uczestniczą niektóre państwa członkowskie i które jest finansowane w ramach programu na rzecz wspierania polityki w zakresie technologii informacyjnych i komunikacyjnych stanowiącego część programu ramowego na rzecz konkurencyjności i innowacji. Komisja będzie ściśle monitorować postępy projektu w ciągu następnych miesięcy, które będą przełomowe dla podjęcia decyzji o tym, czy zostanie on zastosowany w systemie IMI.

Dalsze odniesienia do kwestii bezpieczeństwa danych znajdują się w części 7.2.

6.3. Zatrzymywanie danych

Polityka zatrzymywania danych w systemie IMI jest bardzo surowa[15]. Niektóre podmioty i niektórzy użytkownicy uważają, że należy dokonać jej przeglądu. Szybkie usuwanie danych w systemie nie zawsze leży w interesie osoby, której dotyczą dane i która mogłaby chcieć, aby jej dane były przechowywane w systemie IMI przez dłuższy czas, np. w związku z postępowaniem sądowym.

W niedawnym wyroku[16] Europejski Trybunał Sprawiedliwości stwierdził, że prawo dostępu do informacji[17] ma zastosowanie nie tylko do bieżących danych, ale również do danych przechowywanych w przeszłości. Trybunał uznaje zatem, że ograniczanie dostępu do danych przez ich usuwanie może być niezgodne z prawem, chyba że można wykazać, że dłuższe przechowywanie informacji stanowiłoby nadmierne obciążenie dla administratora danych. Komisja nie uważa, aby przechowywanie danych osobowych w systemie IMI przez dłuższy okres stanowiło nadmierne

---

15 Szybkie usuwanie danych osobowych jest możliwe za pomocą zaledwie dwóch kliknięć, a w każdym przypadku wszystkie dane osobowe są automatycznie usuwane sześć miesięcy po zamknięciu wniosków o informacje.

16 C-553/07, *Rotterdam przeciwko Rijkeboer*.

17 Zob. art. 12 lit. a) dyrektywy 95/46/WE.

obciążenie i dlatego zamierza rozważyć dłuższy okres przechowywania informacji, który mógłby obejmować również etap przejściowy blokowania danych sprawiający, że dane staną się niewidoczne dla wszystkich użytkowników, zanim zostaną ostatecznie usunięte. Ewentualne skutki blokowania, łącznie z tym, kto będzie miał dostęp do blokowanych danych i w jakim celu, zostaną uważnie przeanalizowane.

Jest to dobry przykład na to, że należy się uważnie zastanowić przed podjęciem decyzji dotyczącej pakietu przepisów regulujących funkcjonowanie systemu IMI w drodze prawnie wiążącego aktu. Istotne jest, aby Komisja i państwa członkowskie, zapewniając należytą ochronę danych i zaangażowanie organów ochrony danych w ten proces, mogły skorzystać z wystarczającego doświadczenia w stosowaniu systemu w celu uniknięcia ustanawiania przepisów dotyczących ochrony danych, które byłyby nieskuteczne lub nawet przynosiły skutki odwrotne do zamierzonych.

6.4. Krajowe stosowanie systemu IMI

Transpozycja dyrektywy o usługach w Królestwie Niderlandów przewiduje stosowanie systemu IMI na potrzeby krajowe, tj. w celu wymiany informacji również między holenderskimi organami administracji. Komisja Europejska popiera takie podejście, ponieważ ilustruje ono potencjał systemu IMI w zastosowaniu między organami administracji. Krajowe wykorzystanie systemu IMI przez państwa członkowskie podlega jednak trzem warunkom:

a) przetwarzanie danych osobowych i przechowywanie informacji na serwerach Komisji jest uznawane za zgodne z prawem krajowym;

b) system stosuje się w takiej samej postaci, z tymi samymi zestawami pytań i funkcjami; oraz

c) państwo członkowskie przyjmuje pełną odpowiedzialność za wszelkie kwestie (dotyczące ochrony danych lub inne) w związku ze stosowaniem systemu na potrzeby krajowe.

Dlatego też, jeżeli państwa członkowskie są zainteresowane krajowym stosowaniem systemu IMI, zaleca się, aby najpierw przeprowadziły konsultacje z krajowymi organami ochrony danych, a następnie nawiązały kontakt z Komisją w celu omówienia tej kwestii i upewnienia się, że nie powoduje ona żadnych problemów z punktu widzenia przepisów o ochronie danych.

6.5. Szczególne środki ochrony danych w prawnie wiążących przepisach wspólnotowych

W opinii z dnia 12 grudnia 2007 r. i w formie wymiany listów z Komisją Europejski Inspektor Ochrony Danych wezwał do ustanowienia w prawodawstwie UE szczególnych, prawnie wiążących środków ochrony danych w związku z rozszerzeniem zakresu systemu IMI poza dyrektywę o usługach i dyrektywę o kwalifikacjach zawodowych. Niemieckie organy ochrony danych wyraziły podobną opinię.

W 2010 r. nowa Komisja przyjrzy się od nowa funkcjonowaniu jednolitego rynku i możliwości zwiększenia wkładu systemu IMI w poprawę wdrażania prawodawstwa rynku wewnętrznego w państwach członkowskich. Rozważy ona w ten sposób, w

jakich innych obszarach polityki możliwe byłoby odniesienie korzyści ze stosowania systemu IMI.

Wprowadzono już solidny pakiet środków ochrony danych, a informacje zwrotne otrzymane od państw członkowskich są pozytywne. Dlatego też Komisja uważa, że nierozsądne byłoby prowadzenie dalszych działań w związku z wnioskiem ustawodawczym przed określeniem zakresu systemu IMI i przed skorzystaniem z doświadczenia w praktycznym stosowaniu systemu w odniesieniu do usług. Wszelkie przyszłe wnioski muszą być dostosowane do tych zmian w celu zapewnienia pewnej, uwzględniającej przyszłe potrzeby podstawy systemu IMI i ochrony danych.

W międzyczasie Komisja będzie nadal ulepszać ochronę danych w systemie IMI w ścisłej współpracy z państwami członkowskimi i Europejskim Inspektorem Ochrony Danych, jak przedstawiono poniżej.

7. PRZYSZŁE ULEPSZENIA

7.1. Ulepszenia techniczne

Automatyczne powiadomienia i ponaglenia do przyjęcia odpowiedzi (tak aby wnioski nie były otwarte dłużej niż jest to konieczne) zostaną włączone do nowej wersji oprogramowania. Jeśli chodzi o procedurę on-line dotyczącą poprawiania, blokowania lub usuwania danych, ponieważ dotychczas nie pojawiły się wnioski i jest mało prawdopodobne, aby pojawiła się ich znaczna liczba w przyszłości, Komisja uważa, że bardziej stosowne będzie wprowadzenie lżejszej procedury, która zostanie odpowiednio udokumentowana z pomocą urzędnika Komisji ds. ochrony danych i Europejskiego Inspektora Ochrony Danych.

7.2. Bezpieczeństwo danych

Zgodnie z nowymi wytycznymi i normami przyjętymi niedawno przez Komisję przeprowadzi ona nową ocenę ryzyka dla systemu IMI w 2010 r. i odpowiednio zaktualizuje plan bezpieczeństwa, określając części systemu, które należy rozważyć, ewentualne zagrożenia i konieczną infrastrukturę oraz środki w zakresie oprogramowania. Jeżeli ocena ryzyka wykaże potrzebę wprowadzenia dodatkowych środków bezpieczeństwa, będą one stopniowo wprowadzane do przyszłych wersji oprogramowania.

Na początku 2011 r. zostanie przeprowadzony audyt zewnętrzny, który skoncentruje się głównie na wynikach i stabilności systemu, ale może również objąć niektóre kwestie z zakresu ochrony i bezpieczeństwa danych.

7.3. Przegląd dyrektywy o kwalifikacjach zawodowych

Ocena dyrektywy o kwalifikacjach zawodowych zostanie przeprowadzona w latach 2010-2011; obejmie ona ocenę współpracy administracyjnej i wykorzystanie systemu IMI, w tym kwestie ochrony danych.

8. WNIOSKI

Komisja jest zadowolona z wdrażania zalecenia oraz ze stanu ochrony danych w systemie IMI. Będzie jednak nadal pracowała nad dalszymi ulepszeniami systemu, szczególnie nad ulepszeniami technicznymi i poprawą bezpieczeństwa danych.

Komisja zamierza również zbadać możliwość rozszerzenia zakresu systemu IMI na inne obszary rynku wewnętrznego, korzystając jednocześnie z dalszego praktycznego doświadczenia w jego stosowaniu w obszarze usług. Wszelkie przyszłe wnioski ustawodawcze na szczeblu UE uwzględnią te zmiany i refleksje w celu zapewnienia pewnej i uwzględniającej przyszłe potrzeby podstawy systemu IMI i ochrony danych.

W pierwszym kwartale 2011 r. zostanie opublikowany dokument roboczy służb Komisji w sprawie funkcjonowania i rozwoju systemu IMI w 2010 r. Obejmie on również kwestię ochronę danych.