# OPINIE

# EUROPEJSKI INSPEKTOR OCHRONY DANYCH

## Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku Komisji dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie współpracy administracyjnej za pośrednictwem systemu wymiany informacji na rynku wewnętrznym („IMI")

(2012/C 48/02)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16,

uwzględniając Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 7 i 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]),

uwzględniając wniosek o wydanie opinii zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

### 1. WPROWADZENIE

#### 1.1. Konsultacje z EIOD

1. Dnia 29 sierpnia 2011 r. Komisja przyjęła wniosek dotyczący rozporządzenia (zwany dalej „wnioskiem" lub „wnioskowanym rozporządzeniem") Parlamentu Europejskiego i Rady w sprawie współpracy administracyjnej za pośrednictwem systemu wymiany informacji na rynku wewnętrznym („IMI") ([3]). Tego samego dnia wniosek przesłano EIOD do konsultacji.

2. Przed przyjęciem wniosku EIOD miał możliwość zgłoszenia nieformalnych uwag na temat wniosku, wcześniej zaś na temat komunikatu Komisji „Lepsze zarządzanie jednolitym rynkiem dzięki ściślejszej współpracy administracyjnej: Strategia rozszerzania i rozwoju systemu wymiany informacji na rynku wewnętrznym („IMI")" („komunikatu w sprawie strategii IMI") ([4]), który poprzedził wniosek. Wiele z tych uwag uwzględniono we wniosku, w wyniku czego zabezpieczenia związane z ochroną danych zawarte we wniosku zostały udoskonalone.

3. EIOD z zadowoleniem przyjmuje fakt przeprowadzenia z nim formalnych konsultacji przez Komisję oraz zamieszczenia odniesienia do obecnej opinii w preambule wniosku.

#### 1.2. Cele i zakres wniosku

4. System IMI jest narzędziem informatycznym umożliwiającym właściwym organom w państwach członkowskich wzajemną wymianę informacji podczas stosowania prawodawstwa dotyczącego rynku wewnętrznego. System ten umożliwia władzom krajowym, regionalnym i lokalnym państw członkowskich UE szybką oraz łatwą komunikację z odpowiednikami w pozostałych krajach europejskich. Wiąże się to również z przetwarzaniem stosownych danych osobowych, w tym danych szczególnie chronionych.

5. System IMI powstał pierwotnie jako narzędzie komunikacyjne służące bezpośredniej wymianie informacji na mocy dyrektywy w sprawie uznawania kwalifikacji zawodowych ([5]) i dyrektywy usługowej ([6]). Pomaga on użytkownikom znaleźć właściwy organ, z którym należy się skontaktować w innym państwie, oraz skomunikować się z nim za pomocą już przetłumaczonych zestawów standardowych pytań i odpowiedzi ([7]).

([1]) Dz.U. L 281 z 23.11.1995, s. 31.
([2]) Dz.U. L 8 z 12.1.2001, s. 1.
([3]) COM(2011) 522 wersja ostateczna.
([4]) COM(2011) 75.
([5]) Dyrektywa 2005/36/WE Parlamentu Europejskiego i Rady z dnia 7 września 2005 r. w sprawie uznawania kwalifikacji zawodowych (Dz.U. L 255 z 30.9.2005, s. 22).
([6]) 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).
([7]) Dla ilustracji, typowym pytaniem zawierającym dane szczególnie chronione byłoby na przykład: „Czy załączony dokument zgodnie z prawem poświadcza, że w odniesieniu do następującej osoby: (migrujący pracownik) nie zawieszono prawa do wykonywania zawodu ani nie zakazano wykonywania właściwej działalności zawodowej z powodu poważnego wykroczenia zawodowego lub przestępstwa?".

6. IMI jest jednak w założeniu elastycznym, horyzontalnym systemem, który można dostosować do potrzeb wielu obszarów prawodawstwa dotyczącego rynku wewnętrznego. Przewiduje się, że jego zastosowanie będzie w przyszłości stopniowo rozszerzane na dodatkowe obszary prawodawstwa.

7. Planuje się również rozszerzenie funkcji IMI. Oprócz wymiany informacji między dwiema stronami planuje się także, lub też wdrożono już, inne funkcje takie jak „procedury powiadamiania, mechanizmy ostrzegania, procedury wzajemnej pomocy oraz rozwiązywania problemów" ([8]), jak też „repozytorium informacji do późniejszego wykorzystania przez uczestników IMI" ([9]). Wiele, choć nie wszystkie, z tych funkcji może się także wiązać z przetwarzaniem danych osobowych.

8. Celem wniosku jest zapewnienie IMI jednoznacznej podstawy prawnej i kompleksowych ram ochrony danych.

### 1.3. **Ogólne informacje o wniosku: proces stopniowego tworzenia kompleksowych ram ochrony danych dla IMI**

9. Wiosną 2007 r. Komisja poprosiła o opinię Grupy Roboczej Art. 29 dotyczącą implikacji IMI z punktu widzenia ochrony danych. Grupa Robocza wydała opinię dnia 20 września 2007 r. ([10]). W opinii zalecono, aby Komisja zapewniła bardziej jednoznaczną podstawę prawną i konkretne zabezpieczenia związane z ochroną danych przy ich wymianie w ramach IMI. EIOD wziął aktywny udział w pracach podgrupy zajmującej się IMI i poparł wnioski zawarte w opinii Grupy Roboczej Art. 29.

10. Na późniejszym etapie EIOD nadal przedstawiał Komisji wskazówki dotyczące sposobu stopniowego zapewnienia IMI bardziej kompleksowych ram ochrony danych ([11]). W ramach tej współpracy od chwili wydania w dniu 22 lutego 2008 r. opinii w sprawie wdrożenia IMI ([12]) EIOD konsekwentnie opowiada się za stworzeniem nowego instrumentu prawnego w ramach zwykłej procedury ustawodawczej w celu ustanowienia w odniesieniu do IMI bardziej kompleksowych ram ochrony danych i zagwarantowania pewności prawa. Obecnie przedstawiono wniosek dotyczący takiego instrumentu prawnego ([13]).

([8]) Zob. motyw 10.
([9]) Zob. art. 13 ust. 2.
([10]) Opinia nr 7/2007 Grupy Roboczej Art. 29 w sprawie kwestii ochrony danych w związku z systemem informacji na temat rynku wewnętrznego (IMI), WP140. Dokument ten jest dostępny pod adresem: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp140_pl.pdf
([11]) Najważniejsze dokumenty związane z tą współpracą są dostępne na stronie internetowej Komisji poświęconej IMI pod adresem: http://ec.europa.eu/internal_market/imi-net/data_protection_pl.html, jak również na stronie internetowej EIOD pod adresem: http://www.edps.europa.eu
([12]) Opinia EIOD dotycząca decyzji 2008/49/WE Komisji z dnia 12 grudnia 2007 r. w sprawie wdrożenia systemu wymiany informacji rynku wewnętrznego (IMI) pod względem ochrony danych osobowych (Dz.U. C 270 z 25.10.2008, s. 1).
([13]) Grupa Robocza Art. 29 również planuje zgłosić uwagi dotyczące wniosku. EIOD śledzi prace stosownej podgrupy Grupy Roboczej i zgłasza uwagi.

## 2. **ANALIZA WNIOSKU**

### 2.1. **Ogólny pogląd EIOD na temat wniosku oraz na temat najważniejszych wyzwań związanych z uregulowaniem IMI**

11. EIOD ogólnie pozytywnie ocenia IMI. Popiera on cele Komisji polegające na ustanowieniu elektronicznego systemu wymiany informacji oraz uregulowaniu jego aspektów dotyczących ochrony danych. Usprawniony system nie tylko zwiększy efektywność współpracy, ale może też pomóc w zapewnieniu trwałej zgodności ze stosownymi przepisami dotyczącymi ochrony danych. Będzie to możliwe dzięki określeniu jasnych zasad, jakie informacje można wymieniać, z kim i pod jakimi warunkami.

12. EIOD z zadowoleniem przyjmuje również fakt, że Komisja proponuje horyzontalny instrument prawny dla IMI w postaci rozporządzenia Rady i Parlamentu. Z zadowoleniem stwierdza, że we wniosku kompleksowo wskazano najistotniejsze kwestie dotyczące ochrony danych w związku z IMI. Jego uwagi należy zatem interpretować w tym pozytywnym kontekście.

13. EIOD ostrzega niemniej, że ustanowienie jednego scentralizowanego systemu elektronicznego dla większej liczby obszarów współpracy administracyjnej wiąże się także z ryzykiem. Najważniejszym rodzajem ryzyka jest możliwość udostępniania większej ilości danych szerszej grupie odbiorców, niż jest to konieczne do celów efektywnej współpracy, oraz fakt, że dane, w tym również potencjalnie dane nieaktualne i niedokładne, mogą pozostawać w systemie elektronicznym dłużej, niż jest to niezbędne. Wrażliwą kwestią jest też bezpieczeństwo systemu informacyjnego dostępnego w 27 państwach członkowskich, gdyż cały system będzie tylko tak bezpieczny, jak najsłabsze ogniwo łańcucha.

Najważniejsze wyzwania

14. W odniesieniu do ram prawnych IMI, które mają zostać ustanowione we wnioskowanym rozporządzeniu, EIOD zwraca uwagę na dwa główne wyzwania:

— potrzebę zapewnienia spójności przy poszanowaniu różnorodności oraz

— potrzebę wyważenia pomiędzy elastycznością a pewnością prawa.

15. Te główne wyzwania stanowią ważne punkty odniesienia i w znacznej mierze decydują o podejściu przyjętym przez EIOD w obecnej opinii.

Zapewnienie spójności przy poszanowaniu różnorodności

16. Po pierwsze, system IMI jest wykorzystywany w 27 państwach członkowskich. Na obecnym etapie harmonizacji przepisów europejskich między krajowymi procedurami administracyjnymi oraz krajowymi przepisami dotyczącymi ochrony danych występują znaczące różnice. System IMI trzeba skonstruować w taki sposób, aby użytkownicy w każdym z 27 państw członkowskich mieli możliwość przestrzegania swojego prawa krajowego,

w tym krajowych przepisów dotyczących ochrony danych, przy wymianie danych osobowych za jego pośrednictwem. Jednocześnie osoby, których dane dotyczą, muszą również mieć pewność, że ich dane będą podlegać spójnej ochronie niezależnie od ich przekazywania za pośrednictwem IMI do innego państwa członkowskiego. Zapewnienie spójności przy poszanowaniu różnorodności jest jednym z głównych wyzwań z punktu widzenia budowy infrastruktury zarówno technicznej, jak i prawnej systemu IMI. Należy unikać nadmiernej złożoności i rozdrobnienia. Czynności przetwarzania danych w ramach IMI muszą być przejrzyste, a odpowiedzialność za podejmowanie decyzji dotyczących konstrukcji systemu, jego bieżącego utrzymywania i wykorzystania, jak również nadzoru nad nim musi być określona w jednoznaczny sposób.

Wyważenie pomiędzy elastycznością a pewnością prawa

17. Po drugie, w przeciwieństwie do niektórych innych wielkoskalowych systemów informatycznych takich jak system informacyjny Schengen, wizowy system informacyjny, system informacji celnej czy Eurodac, które skupiają się bez wyjątku na współpracy w konkretnych, wyraźnie określonych obszarach, system IMI jest horyzontalnym narzędziem wymiany informacji i może być wykorzystywany w celu jej ułatwienia w wielu różnych obszarach polityki. Oczekuje się również, że zakres IMI ulegnie stopniowemu rozszerzeniu o dodatkowe obszary polityki, a jego funkcje mogą także ulec zmianie, obejmując nieokreślone jak dotąd rodzaje współpracy administracyjnej. Te szczególne cechy systemu IMI utrudniają jednoznaczne określenie jego funkcji oraz rodzajów wymiany danych, które mogą następować w ramach systemu. Dlatego też trudniej jest jednoznacznie określić stosowne zabezpieczenia związane z ochroną danych.

18. EIOD przyznaje, że niezbędna jest elastyczność i dostrzega pragnienie Komisji, aby uczynić rozporządzenie odpornym na upływ czasu. Nie powinno to jednak skutkować brakiem jasności lub pewności prawa, jeżeli chodzi o funkcje systemu oraz wdrażane zabezpieczenia związane z ochroną danych. Z tego powodu, gdy tylko jest to możliwe, wniosek powinien mieć bardziej szczegółowy charakter, wychodząc poza powtórzenie najważniejszych zasad ochrony danych określonych w dyrektywie 95/46/WE i rozporządzeniu (WE) nr 45/2011 ([14]).

### 2.2. **Zakres IMI i jego przewidywane rozszerzenie (art. 3 i 4)**

#### 2.2.1. *Wprowadzenie*

19. EIOD z zadowoleniem przyjmuje jednoznaczne określenie we wniosku obecnego zakresu systemu IMI; w załączniku I wymieniono stosowne akty unijne, na podstawie których może dochodzić do wymiany informacji. Przewidziano tam współpracę na mocy konkretnych przepisów dyrektywy w sprawie uznawania kwalifikacji zawodowych, dyrektywy usługowej oraz dyrektywy w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej ([15]).

20. Przewidywane jest rozszerzenie zakresu IMI, więc potencjalne obszary jego rozszerzenia wymieniono w załączniku II. Pozycje z załącznika II mogą być przenoszone do załącznika I aktem delegowanym przyjmowanym przez Komisję po ocenie skutków ([16]).

21. EIOD przyjmuje tę zasadę z zadowoleniem, gdyż (i) wyraźnie określa ona zakres IMI oraz (ii) zapewnia przejrzystość; a zarazem (iii) umożliwia elastyczność w przypadkach, w których system IMI będzie w przyszłości wykorzystywany do dodatkowej wymiany informacji. Gwarantuje ona również, że za pośrednictwem systemu IMI nie będą mogły być dokonywane wymiany informacji bez (i) właściwej podstawy prawnej w konkretnym prawodawstwie w sprawie rynku wewnętrznego umożliwiającym lub nakazującym wymianę informacji ([17]) oraz (ii) zamieszczenia odniesienia do tej podstawy prawnej w załączniku I do rozporządzenia.

22. Mimo tego nadal występuje niepewność w odniesieniu do zakresu IMI, w odniesieniu do obszarów polityki, które może objąć system oraz w odniesieniu do funkcji, które zawiera on lub może zawierać.

23. Po pierwsze, nie można wykluczyć, że zakres IMI zostanie rozszerzony poza obszary polityki wymienione w załączniku I i II. Może tak się stać, jeżeli wykorzystanie IMI zostanie zapisane w odniesieniu do pewnych rodzajów wymiany informacji nie w akcie delegowanym Komisji, ale w akcie przyjętym przez Parlament i Radę w przypadku, którego nie przewidziano w załączniku II ([18]).

([14]) W tym kontekście zob. też nasze uwagi w sekcji 2.2 dotyczące przewidywanego rozszerzenia IMI.

([15]) Dyrektywa 2011/24/WE Parlamentu Europejskiego i Rady z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej (Dz.U. L 88 z 4.4.2011, s. 45).

([16]) W samym projekcie rozporządzenia nie wspomniano o ocenie skutków. Na stronie 8 uzasadnienia towarzyszącego wnioskowi wyjaśniono jednak, że Komisja będzie upoważniona do przenoszenia pozycji z załącznika II do załącznika I poprzez przyjęcie aktu delegowanego „po przeprowadzeniu oceny wykonalności technicznej, opłacalności oraz łatwości obsługi i ogólnego wpływu proponowanych rozwiązań na system oraz, w stosownych przypadkach, oceny wyników ewentualnej fazy testowej".

([17]) Wyjątkiem jest SOLVIT (zob. sekcja I pkt 1 załącznika II), w przypadku którego dostępne jest jedynie „prawo miękkie" w postaci zalecenia Komisji. Z punktu widzenia ochrony danych zdaniem EIOD w konkretnym przypadku SOLVIT-u podstawą prawną przetwarzania może być „zgoda" osób, których dane dotyczą.

([18]) Może tak się stać z inicjatywy Komisji, ale nie można też wykluczyć, że pomysł wykorzystania IMI w konkretnym obszarze polityki pojawi się na późniejszym etapie procesu ustawodawczego – może to zaproponować Parlament lub Rada. W przeszłości miało to już miejsce w odniesieniu do dyrektywy w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej. W takim przypadku potrzebna byłaby większa jasność co do „procedury" rozszerzenia, w której, jak się wydaje, skupiono się wyłącznie na rozszerzeniu poprzez akty delegowane (zob. przepisy dotyczące oceny skutków, aktów delegowanych, aktualizacji załącznika I).

24. Po drugie, chociaż rozszerzenie zakresu na nowe obszary polityki może w pewnych przypadkach wymagać niewielkich lub nie wymagać żadnych zmian istniejących funkcji systemu ([19]), inne rozszerzenia mogą wymagać nowych i innych funkcji lub też znaczących zmian funkcji istniejących:

— chociaż we wniosku odniesiono się do kilku istniejących lub planowanych funkcji, odniesienia te są często niewystarczająco jasne lub szczegółowe. Dotyczy to w różnym stopniu odniesień do ostrzeżeń, podmiotów zewnętrznych, repozytoriów, procedur wzajemnej pomocy i rozwiązywania problemów ([20]). Dla ilustracji, odnoszące się do kluczowej istniejącej funkcji słowo „ostrzeganie" pojawia się tylko raz – w motywie 10,

— na mocy wnioskowanego rozporządzenia możliwe jest wprowadzenie nowych rodzajów funkcji, o których w ogóle nie wspomniano we wniosku,

— jak dotąd system IMI określany jest jako narzędzie informatyczne służące wymianie informacji, a więc innymi słowy narzędzie komunikacyjne (zob. np. art. 3 wniosku). Niektóre spośród funkcji, o których jest mowa we wniosku, w tym funkcja „repozytorium informacji", wydają się wszakże wychodzić poza ten zakres. Wnioskowane wydłużenie okresów zatrzymywania danych do pięciu lat również sugeruje przejście w stronę „bazy danych". W fundamentalny sposób zmieniłoby to charakter IMI ([21]).

2.2.2. *Zalecenia*

25. Aby zaradzić tym niejasnościom, EIOD zaleca dwojakie podejście. Proponuje po pierwsze, aby jasno opisać i konkretnie wskazać możliwe już teraz do przewidzenia funkcje; po drugie, aby zastosować odpowiednie zabezpieczenia proceduralne zapewniające wnikliwe uwzględnienie kwestii ochrony danych również podczas przyszłego rozwoju systemu IMI.

Wyjaśnienia dotyczące już dostępnych lub możliwych do przewidzenia funkcji (np. wymian między dwiema stronami, ostrzeżeń, repozytoriów, rozwiązywania problemów i podmiotów zewnętrznych)

26. EIOD zaleca, aby w rozporządzeniu bardziej szczegółowo opisać te funkcje, które są już znane, na przykład wymiany informacji, o których mowa w załącznikach I i II.

27. Można na przykład przewidzieć bardziej szczegółowe i wyraźne środki związane z integracją SOLVIT-u ([22]) z systemem IMI (przepisy dotyczące „podmiotów zewnętrznych" i „rozwiązywania problemów") oraz z wykazami specjalistów i dostawców usług (przepisy dotyczące „repozytoriów").

28. Należy też zamieścić dodatkowe wyjaśnienia odnoszące się do „ostrzeżeń", które są już wykorzystywane na mocy dyrektywy usługowej i mogą zostać wprowadzone w dodatkowych obszarach polityki. W szczególności „ostrzeżenie" jako funkcję należy wyraźnie zdefiniować w art. 5 (wraz z innymi funkcjami takimi jak wymiana informacji między dwiema stronami i repozytoria). Należy też zamieścić wyjaśnienia dotyczące praw dostępu i okresów zatrzymywania w odniesieniu do ostrzeżeń ([23]).

Zabezpieczenia proceduralne (ocena skutków z punktu widzenia ochrony danych i konsultacje z organami ochrony danych)

29. Jeżeli zamierzeniem jest zapewnienie rozporządzeniu odporności na upływ czasu w odniesieniu do dodatkowych funkcji, które mogą być niezbędne w perspektywie długookresowej, a tym samym dopuszczenie dodatkowych funkcji niezdefiniowanych jeszcze w rozporządzeniu, powinny temu towarzyszyć odpowiednie zabezpieczenia proceduralne zapewniające podjęcie stosownych działań na rzecz wdrożenia niezbędnych zabezpieczeń związanych z ochroną danych przed wprowadzeniem nowych funkcji. Powinno to też dotyczyć rozszerzania systemu na nowe obszary polityki, gdy ma to skutki z punktu widzenia ochrony danych.

30. EIOD zaleca wprowadzenie jednoznacznego mechanizmu zapewniającego wnikliwą ocenę zagadnień związanych z ochroną danych przed każdym rozszerzeniem funkcjonalności lub objęciem nowego obszaru polityki zakresem IMI; w razie potrzeby w architekturze systemu należy uwzględnić dodatkowe zabezpieczenia lub środki techniczne. W szczególności:

— wymóg oceny skutków, o której mowa na stronie 8 uzasadnienia, powinien zostać zamieszczony w samym rozporządzeniu, i powinien obejmować również ocenę skutków z punktu widzenia ochrony danych, w której należy konkretnie wskazać, jakie ewentualne zmiany w strukturze IMI są konieczne w celu zagwarantowania, że zabezpieczenia związane z ochroną danych, obejmujące także nowe obszary polityki lub funkcje, pozostaną odpowiednie,

— w rozporządzeniu należy konkretnie wskazać, że przed każdym rozszerzeniem IMI wymagane są konsultacje z EIOD i krajowymi organami ochrony danych. Konsultacje te mogą odbywać się w ramach mechanizmu przewidzianego do celów skoordynowanego nadzoru w art. 20.

([19]) Na przykład wymiana informacji między dwiema stronami na mocy dyrektywy w sprawie uznawania kwalifikacji zawodowych oraz dyrektywy w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej opiera się zasadniczo na takiej samej strukturze i może następować przy wykorzystaniu podobnych funkcji oraz podobnych zabezpieczeń związanych z ochroną danych.

([20]) Zob. motywy 2, 10, 12, 13 i 15 oraz art. 5 lit. b), art. 5 lit. i), art. 10 ust. 7 i art. 13 ust. 2.

([21]) Nawiasem mówiąc, jeżeli system IMI ma zastąpić/uzupełnić istniejące systemy służące obsłudze i archiwizacji akt lub też ma być wykorzystywany jako baza danych, należy to wskazać wyraźniej w art. 3.

([22]) Zob. sekcja I pkt 1 załącznika II.

([23]) Zob. sekcje 2.4 i 2.5.5 poniżej.

31. Powyższe zabezpieczenia proceduralne (ocena skutków z punktu widzenia ochrony danych i konsultacje) powinny odnosić się do rozszerzenia zarówno za pośrednictwem aktu delegowanego Komisji (przeniesienia pozycji z załącznika II do załącznika I), jak i za pośrednictwem rozporządzenia Parlamentu i Rady uwzględniającego pozycję, której nie zawarto w załączniku II.

32. Wreszcie, EIOD zaleca, aby w rozporządzeniu wyjaśniono, czy zakres aktów delegowanych, które Komisja będzie mogła przyjmować na mocy art. 23, obejmie jakiekolwiek inne kwestie poza przenoszeniem pozycji z załącznika II do załącznika I. W miarę możliwości Komisja powinna na mocy rozporządzenia zyskać uprawnienia do przyjmowania konkretnych aktów wykonawczych lub delegowanych w celu sprecyzowania wszelkich dodatkowych funkcji systemu lub też odniesienia się do ewentualnych przyszłych kwestii związanych z ochroną danych.

### 2.3. **Role, kompetencje i obowiązki (art. 7–9)**

33. EIOD z zadowoleniem przyjmuje poświęcenie pełnego rozdziału (Rozdziału II) wyjaśnieniu kwestii funkcji i obowiązków poszczególnych podmiotów zaangażowanych w IMI. Przepisy te można dodatkowo udoskonalić w sposób opisany poniżej.

34. W art. 9 opisano obowiązki wynikające z roli Komisji jako administratora danych. EIOD zaleca ponadto zamieszczenie dodatkowego przepisu dotyczącego roli Komisji w dopilnowaniu, aby system zaprojektowano z uwzględnieniem zasad ochrony prywatności, jak też dotyczącego jej roli jako koordynatora kwestii związanych z ochroną danych.

35. EIOD z zadowoleniem odnotowuje fakt, że wśród zadań koordynatorów IMI określonych w art. 7 wymieniono konkretnie koordynację związaną z ochroną danych, w tym pełnienie roli punktu kontaktowego dla Komisji. Zaleca ponadto doprecyzowanie, że powyższe zadania związane z koordynacją obejmują też kontakty z krajowymi organami ochrony danych.

### 2.4. **Prawa dostępu (art. 10)**

36. W art. 10 zawarto zabezpieczenia dotyczące praw dostępu. EIOD z zadowoleniem przyjmuje fakt, że po zgłoszeniu przez niego uwag przepisy te znacząco udoskonalono.

37. Biorąc pod uwagę horyzontalny charakter IMI i rozszerzanie się systemu, ważne jest dopilnowanie, aby gwarantował on zastosowanie „chińskich murów" ograniczających przetwarzanie informacji w danym obszarze polityki wyłącznie do tego obszaru: użytkownicy IMI powinni: (i) mieć dostęp do informacji wyłącznie zgodnie z zasadą ograniczonego dostępu oraz (ii) mieć dostęp ograniczony do danego obszaru polityki.

38. Jeżeli nie da się uniknąć sytuacji, w której użytkownik IMI ma prawo dostępu do informacji dotyczących kilku obszarów polityki (może tak być na przykład w przypadku niektórych instytucji samorządowych), system powinien co najmniej zapobiegać łączeniu informacji pochodzących z różnych obszarów polityki. Ewentualne niezbędne wyjątki należy określić w przepisach wykonawczych lub w akcie Unii, ściśle przestrzegając zasady celowości.

39. Zasady te naszkicowano ogólnie w tekście rozporządzenia, ale można je dodatkowo wzmocnić i zapewnić ich realizację.

40. W odniesieniu do praw dostępu przyznanych Komisji EIOD z zadowoleniem przyjmuje fakt, że w art. 9 ust. 2, art. 9 ust. 4 i art. 10 ust. 6 wniosku czytanych łącznie stwierdza się, iż Komisja nie będzie miała dostępu do danych osobowych wymienianych między państwami członkowskimi z wyjątkiem przypadków, w których Komisję wskazano jako uczestnika procedury współpracy administracyjnej.

41. Należy również doprecyzować prawa dostępu podmiotów zewnętrznych oraz prawo dostępu do ostrzeżeń ([24]). Jeżeli chodzi o ostrzeżenia, EIOD zaleca, aby w rozporządzeniu znalazł się zapis, że nie należy ich domyślnie przesyłać wszystkim stosownym właściwym organom we wszystkich państwach członkowskich, ale jedynie organom, których one dotyczą – zgodnie z zasadą ograniczonego dostępu. Nie wyklucza to przesyłania ostrzeżeń wszystkim państwom członkowskim w konkretnych przypadkach lub konkretnych obszarach polityki, jeżeli dotyczą one wszystkich państw. Podobnie niezbędna jest analiza indywidualnych przypadków, aby zadecydować, czy Komisja powinna mieć dostęp do ostrzeżeń.

### 2.5. **Zatrzymywanie danych osobowych (art. 13 i 14)**

#### 2.5.1. *Wprowadzenie*

42. W art. 13 wniosku wydłużono okres przechowywania danych w IMI z obecnych sześciu miesięcy (liczonych od zamknięcia sprawy) do pięciu lat, przy czym dane są „blokowane" po 18 miesiącach. Podczas okresu „blokady" dane są dostępne jedynie przy zastosowaniu konkretnej procedury, którą można zainicjować tylko na wniosek osoby, której dane dotyczą, lub w przypadku, gdy dane są konieczne „do celów udostępnienia dowodu potwierdzającego przeprowadzenie wymiany informacji za pomocą IMI".

43. W rezultacie przechowywanie danych w IMI można więc podzielić na trzy okresy:

— od chwili ich przesłania do chwili zamknięcia sprawy,

— od chwili zamknięcia sprawy przez okres 18 miesięcy ([25]),

— od chwili upływu okresu 18 miesięcy – w zablokowanej formie przez dalsze trzy lata i sześć miesięcy (innymi słowy, do chwili upływu pięciu lat od zamknięcia sprawy).

([24]) Zob. również sekcję 2.2.2

([25]) W art. 13 ust. 1 sugeruje się, że 18 miesięcy jest okresem maksymalnym, możliwe jest zatem też ustanowienie okresu krótszego. Nie ma to jednak wpływu na całkowitą długość okresu zatrzymywania, który w każdym przypadku trwałby do chwili upływu pięciu lat od zamknięcia sprawy.

44. Oprócz tych zasad ogólnych w art. 13 ust. 2 dopuszcza się zatrzymanie danych w „repozytorium informacji" tak długo, jak są one potrzebne do tego celu, za zgodą osoby, której dane dotyczą, lub gdy „jest to konieczne, aby zastosować się do przepisów aktu Unii". Ponadto w art. 14 przewidziano podobny mechanizm blokowania w odniesieniu do zatrzymywania danych osobowych użytkowników IMI – przez pięć lat od daty, gdy przestają oni być użytkownikami IMI.

45. Innych konkretnych przepisów brak. Dlatego też ogólne zasady mają przypuszczalnie znaleźć zastosowanie nie tylko do wymian między dwiema stronami, ale też do ostrzeżeń, rozwiązywania problemów (jak w przypadku SOLVIT-u ([26])) oraz wszystkich innych funkcji związanych z przetwarzaniem danych osobowych.

46. EIOD ma kilka uwag w odniesieniu do okresów zatrzymywania danych w świetle art. 6 ust. 1 lit. e) dyrektywy 95/46/WE i art. 4 ust. 1 lit. e) rozporządzenia (WE) nr 45/2001, zgodnie z którymi dane osobowe nie mogą być przechowywane dłużej, niż jest to konieczne do celów, dla których dane były gromadzone lub dla których są przetwarzane dalej.

2.5.2. *Od przesłania do zamknięcia sprawy: potrzeba punktualnego zamknięcia sprawy*

47. W odniesieniu do pierwszego okresu – od przesłania informacji do zamknięcia sprawy – EIOD żywi obawy związane z ryzykiem, że pewne sprawy mogą nie zostać zamknięte nigdy lub zostać zamknięte dopiero po nieproporcjonalnie długim czasie. Może to skutkować pozostawieniem pewnych danych osobowych w bazie danych dłużej, niż jest to konieczne, lub nawet na czas nieokreślony.

48. EIOD zdaje sobie sprawę, że Komisja dokonała praktycznych postępów w redukcji zaległości w IMI, wdrożono też w odniesieniu do wymian między dwiema stronami system monitorujący punktualne zamykanie spraw i wysyłający regularne przypomnienia spóźniającym się podmiotom. Ponadto nowo wprowadzona zmiana funkcji systemu pozwala, zgodnie z zasadą „ochrony prywatności w fazie projektowania", zaakceptować odpowiedź, a zarazem zamknąć sprawę jednym wciśnięciem przycisku. Wcześniej wymagało to dwóch osobnych kroków, co mogło prowadzić do pozostania w systemie części nieaktywnych spraw.

49. EIOD z zadowoleniem przyjmuje te wysiłki o charakterze praktycznym. Zaleca jednak, aby w tekście samego rozporządzenia zawarto gwarancje, że sprawy w IMI będą zamykane punktualnie, a sprawy nieaktywne (w odniesieniu do których nie podejmowano ostatnio żadnych działań) zostaną usunięte z bazy danych.

([26]) Zob. sekcję I pkt 1 załącznika II.

2.5.3. *Od zamknięcia sprawy do upływu 18 miesięcy: czy wydłużenie sześciomiesięcznego okresu jest uzasadnione?*

50. EIOD zachęca do ponownego rozważenia, czy istnieje wystarczające uzasadnienie dla wydłużenia obecnego sześciomiesięcznego okresu do 18 miesięcy od chwili zamknięcia sprawy, a jeżeli tak, czy to uzasadnienie dotyczy jedynie wymian informacji między dwiema stronami, czy też innych funkcji. IMI istnieje już od kilku lat i należy wziąć pod uwagę praktyczne doświadczenia zgromadzone pod tym względem.

51. Jeżeli IMI pozostanie narzędziem wymiany informacji (a nie systemem obsługi dokumentów, bazą danych lub archiwum), i jeżeli właściwym organom udostępni się środki umożliwiające pobranie z systemu otrzymanych informacji (elektronicznie lub w formie papierowej, ale w każdym przypadku w sposób pozwalający wykorzystać pobrane informacje jako dowody ([27])), wydaje się, że w ogóle nie ma większej potrzeby przechowywania danych w IMI po zamknięciu sprawy.

52. W przypadku wymian informacji między dwiema stronami potencjalna potrzeba zadania dalszych pytań nawet po przyjęciu odpowiedzi, a więc po zamknięciu sprawy, może uzasadniać (rozsądnie krótki) okres zatrzymywania danych po zamknięciu sprawy. Na pierwszy rzut oka obecny sześciomiesięczny okres wydaje się wystarczająco długi w tym celu.

2.5.4. *Od 18 miesięcy do pięciu lat: dane „zablokowane"*

53. Zdaniem EIOD Komisja nie przedstawiła również wystarczającego uzasadnienia dla konieczności i proporcjonalności zatrzymywania „danych zablokowanych" przez okres do pięciu lat.

54. Na stronie 9 uzasadnienia znajduje się odniesienie do orzeczenia Trybunału Sprawiedliwości w sprawie Rijkeboer ([28]). EIOD zaleca Komisji ponowne rozważenie implikacji tej sprawy z punktu widzenia zatrzymywania danych w IMI. Jego zdaniem sprawa Rijkeboer nie pociąga za sobą konieczności takiej konfiguracji IMI, by dane były zatrzymywane przez pięć lat po zamknięciu sprawy.

55. EIOD nie uważa odniesienia do wyroku w sprawie Rijkeboer lub do praw osób, których dane dotyczą, do dostępu do tych danych, za wystarczające i odpowiednie uzasadnienie zatrzymywania danych w IMI przez pięć lat od chwili zamknięcia sprawy. Mniej naruszającą prywatność możliwością, która może zasługiwać na dalsze rozważenie, jest przechowywanie jedynie dzienników (ściśle określonych danych z wyłączeniem treści, w tym wszelkich załączników lub danych szczególnie chronionych). Na tym etapie EIOD nie jest wszakże przekonany, czy nawet taki środek byłby konieczny lub proporcjonalny.

([27]) W naszym rozumieniu podjęto wysiłki na rzecz osiągnięcia takiego stanu rzeczy w praktyce.

([28]) C-553/07 Rijkeboer [2009] Zb. Orz. s. I-3889.

56. Ponadto problematyczny jest także brak jasności co do tego, kto może uzyskać dostęp do „danych zablokowanych" i w jakich celach. Nie wystarcza tutaj po prostu odwołać się do wykorzystania „do celów udostępnienia dowodu potwierdzającego przeprowadzenie wymiany informacji" (jak w art. 13 ust. 3). Jeżeli przepis dotyczący „blokowania" zostanie utrzymany, należy w każdym razie dokładniej określić, kto może zwrócić się o dowód potwierdzający przeprowadzenie wymiany informacji i w jakim kontekście. Czy inne podmioty oprócz osoby, której dane dotyczą, również będą miały prawo wnioskować o dostęp? Jeżeli tak, czy chodzi wyłącznie o właściwe organy, i wyłącznie w celu udowodnienia, że doszło do konkretnej wymiany informacji o konkretnej treści (na wypadek, gdyby taką wymianę zakwestionowały właściwe organy, które wysłały lub otrzymały komunikat)? Czy przewidziano inne możliwe sposoby wykorzystania danych „do celów udostępnienia dowodu potwierdzającego przeprowadzenie wymiany informacji" ([29])?

2.5.5. *Ostrzeżenia*

57. EIOD zaleca dokonanie wyraźniejszego rozróżnienia między ostrzeżeniami a repozytoriami informacji. Wykorzystanie ostrzeżenia jako narzędzia komunikacji w celu zawiadomienia właściwych organów o konkretnym wykroczeniu lub podejrzeniu jest jedną rzeczą; zupełnie inną jest natomiast przechowywanie tego ostrzeżenia w bazie danych przez dłuższy lub wręcz nieokreślony czas. Przechowywanie informacji o ostrzeżeniach budziłoby dodatkowe obawy i wymagałoby konkretnych zasad oraz dodatkowych zabezpieczeń związanych z ochroną danych.

58. Dlatego też EIOD zaleca, aby w rozporządzeniu ustanowić następującą domyślną zasadę: (i) jeżeli prawodawstwo pionowe nie stanowi inaczej i pod warunkiem zastosowania odpowiednich dodatkowych zabezpieczeń, okres zatrzymywania ostrzeżeń powinien wynosić sześć miesięcy oraz, co ważne, (ii) okres ten powinien być liczony od chwili wysłania ostrzeżenia.

59. Alternatywnie EIOD zaleca ustanowienie we wnioskowanym rozporządzeniu szczegółowych zabezpieczeń w odniesieniu do ostrzeżeń. Jeżeli obrane zostałoby podejście drugie, EIOD jest gotowy wspomagać Komisję i prawodawców dalszymi poradami w tym zakresie.

2.6. **Szczególne kategorie danych (art. 15)**

60. EIOD z zadowoleniem przyjmuje rozróżnienie dokonane między danymi osobowymi, o których mowa w art. 8 ust. 1 dyrektywy 95/46/WE z jednej strony, a danymi osobowymi, o których mowa w art. 8 ust. 5 z drugiej strony. Z zadowoleniem przyjmuje też fakt, że w rozporządzeniu stwierdza się jednoznacznie, iż szczególne kategorie danych mogą być przetwarzane wyłącznie na szczególnych warunkach określonych w art. 8 dyrektywy 95/46/WE.

61. W tym kontekście EIOD sądzi, że IMI będzie przetwarzać znaczącą ilość danych szczególnie chronionych objętych art. 8 ust. 2 dyrektywy 95/46/WE. W istocie IMI od chwili pierwszego wdrożenia systemu do celów wspierania współpracy administracyjnej na mocy dyrektyw usługowej i w sprawie uznawania kwalifikacji zawodowych miał przetwarzać takie dane, a w szczególności dane odnoszące się do przestępstw i naruszeń administracyjnych, które mogą mieć wpływ na prawo specjalisty lub dostawcy usług do wykonywania pracy/świadczenia usług w innym państwie członkowskim.

62. Ponadto od chwili jego rozszerzenia o moduł SOLVIT ([30]) w IMI będzie również zapewne przetwarzana znacząca ilość danych szczególnie chronionych na mocy art. 8 ust. 1 (głównie związanych ze stanem zdrowia). Wreszcie, nie można wykluczyć, że dodatkowe dane szczególnie chronione będą też gromadzone za pośrednictwem IMI w przyszłości – w sposób doraźny lub systematyczny.

2.7. **Bezpieczeństwo (art. 16 i motyw 16)**

63. EIOD z zadowoleniem stwierdza, że art. 16 odnosi się konkretnie do obowiązku przestrzegania przez Komisję jej własnych zasad wewnętrznych przyjętych dla zapewnienia zgodności z art. 22 rozporządzenia (WE) nr 45/2001 oraz przyjęcia i stałej aktualizacji planu bezpieczeństwa dla IMI.

64. Aby dodatkowo udoskonalić te przepisy, EIOD zaleca, aby w rozporządzeniu zawarto wymóg oceny ryzyka oraz przeglądu planu bezpieczeństwa przed każdym rozszerzeniem IMI na nowy obszar polityki lub przed dodaniem nowych funkcji niosących skutki z punktu widzenia danych osobowych ([31]).

65. Ponadto EIOD zauważa także, że w art. 16 i motywie 16 znajdują się wyłącznie odniesienia do obowiązków Komisji i nadzorczej roli EIOD. Odniesienia te mogą być mylące. Chociaż prawdą jest, że operatorem systemu jest Komisja, w związku z czym jest ona w przeważającej mierze odpowiedzialna za zapewnienie bezpieczeństwa IMI, na właściwych organach również spoczywają obowiązki, których wypełnianie nadzorują z kolei krajowe organy ochrony danych. Dlatego też art. 16 i motyw 16 powinny odnosić się także do obowiązków związanych z bezpieczeństwem spoczywających na pozostałych podmiotach zaangażowanych w IMI na mocy dyrektywy 95/46/WE i do uprawnień nadzorczych krajowych organów ochrony danych.

2.8. **Informacje przekazywane osobom, których dane dotyczą, oraz przejrzystość (art. 17)**

2.8.1. *Informacje przekazywane w państwach członkowskich*

66. W odniesieniu do art. 17 ust. 1 EIOD zaleca zamieszczenie w rozporządzeniu bardziej szczegółowych przepisów, aby zapewnić pełne informowanie osób, których dane dotyczą, o przetwarzaniu ich danych w IMI. Biorąc pod uwagę, że IMI jest wykorzystywany przez wiele właściwych organów, w tym liczne niewielkie instytucje samorządowe bez wystarczających zasobów, zdecydowanie zaleca się, aby zapewnienie informacji koordynowano na szczeblu krajowym.

([29]) Chociaż zatrzymywanie danych osobowych stwarza stosunkowo mniejsze ryzyko z punktu widzenia prywatności, EIOD uważa niemniej, że zatrzymywania danych osobowych użytkowników IMI przez pięć lat od chwili utraty przez nich dostępu do systemu również nie uzasadniono w wystarczający sposób.

([30]) Zob. sekcję I pkt 1 załącznika II.

([31]) Zob. też zalecenia dotyczące kontroli w sekcji 12.

2.8.2. *Informacje przekazywane przez Komisję*

67. W art. 17 ust. 2 lit. a) wymaga się, aby Komisja przedstawiła informację o polityce prywatności w odniesieniu do przetwarzania przez nią danych na mocy art. 10 i 11 rozporządzenia (WE) nr 45/2011. Ponadto w art. 17 ust. 2 lit. b) wymaga się, aby Komisja przedstawiła również informacje na temat „aspektów procedur współpracy administracyjnej w ramach IMI, o których mowa w art. 12, związanych z ochroną danych". Wreszcie, w art. 17 ust. 2 lit. c) wymaga się, aby Komisja przedstawiła informacje na temat „przypadków, w których prawa osób, których dane dotyczą, podlegają wyłączeniu lub ograniczeniu, o czym mowa w art. 19".

68. EIOD z zadowoleniem przyjmuje te przepisy, które pomagają zapewnić przejrzystość czynności przetwarzania danych w IMI. Jak wskazano w sekcji 2.1, w przypadku systemu informatycznego wykorzystywanego w 27 różnych państwach członkowskich podstawową kwestią jest zapewnienie spójności w odniesieniu do funkcjonowania systemu, zastosowanych zabezpieczeń związanych z ochroną danych oraz informacji przedstawianych osobom, których dane dotyczą ([32]).

69. Mimo to przepisy art. 17 ust. 2 należy dodatkowo udoskonalić. Jako operator systemu, Komisja ma największe możliwości przyjęcia aktywnej roli w zakresie przedstawienia pierwszej „warstwy" informacji o polityce prywatności oraz innych stosownych informacji osobom, których dane dotyczą, na swojej wielojęzycznej stronie internetowej, również „w imieniu" właściwych organów, a więc informacji wymaganych na mocy art. 10 lub 11 dyrektywy 95/46/WE. W takim przypadku często wystarczałoby, aby informacje przedstawione przez właściwe organy w państwach członkowskich po prostu odnosiły się do informacji przedstawionych przez Komisję, uzupełniając je tylko w razie konieczności dostarczenia konkretnych dodatkowych informacji wymaganych na mocy prawa krajowego.

70. Ponadto w art. 17 ust. 2 lit. b) należy wyjaśnić, że informacje przedstawiane przez Komisję obejmują w kompleksowy sposób wszystkie obszary polityki, wszystkie rodzaje procedur współpracy administracyjnej i wszystkie funkcje IMI, jak też obejmują w szczególności kategorie danych, które mogą być przetwarzane. Powinny one też objąć publikację zestawów pytań wykorzystywanych we współpracy między dwiema stronami na stronie internetowej IMI, co obecnie ma miejsce w praktyce.

### 2.9. **Prawo do dostępu do danych oraz żądania ich sprostowania i usunięcia (art. 18)**

71. EIOD pragnie ponownie odnieść się do wskazanej w sekcji 2.1 konieczności zapewnienia spójności w odniesieniu do funkcjonowania systemu oraz zastosowanych zabezpieczeń związanych z ochroną danych. Z tego powodu EIOD zaleca uszczegółowienie przepisów dotyczących prawa do dostępu do danych oraz żądania ich sprostowania i usunięcia.

72. W art. 18 należy określić, do kogo osoby, których dane dotyczą, powinny zwracać się z wnioskiem o dostęp. Należy to jasno określić w odniesieniu do dostępu do danych w poszczególnych okresach:

— przed zamknięciem sprawy,

— po zamknięciu sprawy, ale przed upływem 18-miesięcznego okresu zatrzymywania danych,

— wreszcie, podczas okresu, gdy dane są „zablokowane".

73. W rozporządzeniu należy również zawrzeć wymóg, aby właściwe organy współpracowały w miarę potrzeb w odniesieniu do wniosków o dostęp. Sprostowania i usunięcia danych należy dokonywać „jak najszybciej, ale nie później niż w terminie 60 dni", nie zaś „w terminie 60 dni". Należy również zamieścić odniesienie do możliwości stworzenia modułu ochrony danych oraz możliwości wdrożenia rozwiązań z uwzględnieniem ochrony prywatności w fazie projektowania służących współpracy między organami w zakresie prawa dostępu, jak też „wzmocnienia uprawnień osób, których dane dotyczą", na przykład poprzez umożliwienie im w stosownych przypadkach bezpośredniego dostępu do ich danych, gdy jest to wykonalne.

### 2.10. **Nadzór (art. 20)**

74. W ostatnich latach powstał model „skoordynowanego nadzoru". Ten model nadzoru, wdrożony obecnie w Eurodac i częściowo w ramach systemu informacji celnej, przyjęto również w przypadku wizowego systemu informacyjnego (VIS) oraz systemu informacyjnego Schengen drugiej generacji (SIS-II).

75. Model ten składa się z trzech warstw:

— nadzór na szczeblu krajowym zapewniają krajowe organy ochrony danych,

— nadzór na szczeblu UE zapewnia EIOD,

— koordynację zapewniają regularne spotkania i inne skoordynowane działania wspierane przez EIOD, który stanowi sekretariat tego mechanizmu koordynacji.

76. Model ten dowiódł swojej przydatności i skuteczności, należy więc w przyszłości planować jego wdrażanie w odniesieniu do innych systemów informacyjnych.

77. EIOD z zadowoleniem przyjmuje fakt, że w art. 20 wniosku przewidziano skoordynowany nadzór z udziałem krajowych organów ochrony danych i EIOD oparty ogólnie na modelu ustanowionym w rozporządzeniach w sprawie VIS i SIS II ([33]).

([32]) To podejście do zapewnienia spójności powinno oczywiście uwzględniać w należyty sposób wszelkie różnice między krajami, gdy jest to niezbędne i uzasadnione.

([33]) Zob. rozporządzenie (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania systemu informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. L 381 z 28.12.2006, s. 4) oraz rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie wizowego systemu informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS) (Dz.U. L 218 z 13.8.2008, s. 60).

78. EIOD zaleca udoskonalenie przepisów o skoordynowanym nadzorze w pewnych aspektach; w tym celu zaleca wprowadzenie przepisów podobnych, jak np. obowiązujące w kontekście wizowego systemu informacyjnego (art. 41–43 rozporządzenia w sprawie VIS), systemu Schengen II (art. 44–46 rozporządzenia w sprawie SIS-II) oraz planowane w odniesieniu do Eurodac ([34]). W szczególności przydatne byłoby w odniesieniu do rozporządzenia:

— w art. 20 ust. 1 i 2 określenie oraz wyraźniejszy podział zadań nadzorczych należących odpowiednio do krajowych organów ochrony danych i EIOD ([35]),

— w art. 20 ust. 3 wskazanie, że krajowe organy ochrony danych i EIOD, działając w ramach swoich kompetencji, „współpracują czynnie" oraz „zapewniają skoordynowany nadzór nad systemem IMI" (zamiast odniesienia jedynie do skoordynowanego nadzoru bez wspomnienia o czynnej współpracy) ([36]) oraz

— bardziej szczegółowe określenie, co może obejmować współpraca, na przykład przez wprowadzenie wymogu, aby krajowe organy ochrony danych i EIOD, „działając w ramach swoich kompetencji, w miarę potrzeb dokonywali wymiany stosownych informacji, wspomagali się wzajemnie w przeprowadzaniu kontroli i inspekcji, analizowali trudności w interpretowaniu lub stosowaniu rozporządzenia w sprawie IMI, badali problemy związane ze sprawowaniem niezależnego nadzoru lub z wykonywaniem praw osób, których dane dotyczą, sporządzali uzgodnione wnioski w sprawie wspólnych rozwiązań problemów oraz upowszechniali wiedzę o prawach dotyczących ochrony danych" ([37]).

79. Mimo to EIOD ma świadomość mniejszej ilości przetwarzanych obecnie danych, ich odmiennego charakteru oraz zmieniającego się charakteru IMI. Dlatego też przyznaje, że w odniesieniu do częstotliwości spotkań i kontroli wskazana może być większa elastyczność. Krótko mówiąc, EIOD zaleca, aby w rozporządzeniu ustanowić zasady minimalne konieczne w celu zapewnienia skutecznej współpracy, ale nie nakładać zbędnych obciążeń administracyjnych.

80. W art. 20 ust. 3 wniosku nie wymaga się regularnych spotkań, stwierdzając po prostu, że EIOD może „w razie konieczności wystąpić do krajowych organów nadzorczych z zaproszeniem do udziału w spotkaniu". EIOD z zadowoleniem przyjmuje fakt, że w przepisach tych decyzję o częstotliwości i trybie przeprowadzania spotkań oraz o innych elementach proceduralnych współpracy pozostawiono zainteresowanym stronom. Kwestie te można uzgodnić w regulaminach, o których mowa we wniosku.

81. Jeżeli chodzi o regularne kontrole, skuteczniejsze może również być umożliwienie współpracującym organom samodzielnego określenia w ich regulaminach czasu i częstotliwości przeprowadzania takich kontroli. Mogą one zależeć od pewnych czynników i zmieniać się z czasem. Dlatego też EIOD popiera podejście Komisji, które umożliwia również w tym zakresie większą elastyczność.

### 2.11. **Krajowe wykorzystanie IMI**

82. EIOD z zadowoleniem przyjmuje fakt, że we wniosku ustanowiono jednoznaczną podstawę prawną krajowego wykorzystania IMI i podlega ono pewnym warunkom; między innymi zastrzeżono konieczność konsultacji z krajowym organem ochrony danych oraz zgodność wykorzystania z przepisami prawa krajowego.

### 2.12. **Wymiana informacji z państwami trzecimi (art. 22)**

83. EIOD z zadowoleniem przyjmuje wymogi ustanowione w art. 22 ust. 1 w odniesieniu do wymiany informacji, jak również fakt, że w art. 22 ust. 3 zapewniono przejrzystość rozszerzania mechanizmu poprzez publikację w Dzienniku Urzędowym zaktualizowanego wykazu państw trzecich korzystających z IMI (art. 22 ust. 3).

84. EIOD zaleca ponadto, aby Komisja zawęziła odniesienie poczynione do odstępstw na mocy art. 26 dyrektywy 95/46/WE jedynie do art. 26 ust. 2. Innymi słowy, właściwe organy lub inne podmioty zewnętrzne z państwa trzeciego, które nie zapewnia odpowiedniego stopnia ochrony, nie powinny uzyskać bezpośredniego dostępu do IMI, jeżeli nie obowiązują stosowne klauzule umowne. Negocjacja tych klauzul powinna przebiegać na szczeblu UE.

85. EIOD podkreśla, że nie należy stosować innych odstępstw takich jak „przekazanie danych jest konieczne lub wymagane przez prawo z ważnych względów publicznych lub w celu ustanowienia, wykonania lub obrony tytułu prawnego" w celu uzasadnienia przekazywania danych państwom trzecim przy wykorzystaniu bezpośredniego dostępu do IMI ([38]).

### 2.13. **Rozliczalność (art. 26)**

86. W związku z przewidywanymi działaniami na rzecz zwiększenia rozliczalności podczas przeglądu unijnych ram ochrony danych ([39]) EIOD zaleca ustanowienie w rozporządzeniu jednoznacznych ram dla odpowiednich mechanizmów kontroli wewnętrznej, zapewniających zgodność z zasadami ochrony danych i dowodzących tej zgodności, z uwzględnieniem co najmniej elementów wskazanych poniżej.

([34]) Rozporządzenie Rady (WE) nr 2725/2000 z dnia 11 grudnia 2000 r. dotyczące ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania Konwencji Dublińskiej, Dz.U. L 316 z 15.12.2000, s. 1, obecnie w trakcie przeglądu. W tym kontekście rozważane są przepisy podobne, jak w przypadku rozporządzeń w sprawie VIS i SIS II.

([35]) Zob. na przykład art. 41 i 42 rozporządzenia w sprawie VIS.

([36]) Zob. na przykład art. 43 ust. 1 rozporządzenia w sprawie VIS.

([37]) Zob. na przykład art. 43 ust. 2 rozporządzenia w sprawie VIS.

([38]) Podobne podejście przyjęto w art. 22 ust. 2 w odniesieniu do Komisji jako uczestnika IMI.

([39]) Zob. sekcję 2.2.4 komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej", COM(2010) 609 wersja ostateczna. Zob. też sekcję 7 opinii EIOD w sprawie powyższego komunikatu Komisji z dnia 14 stycznia 2011 r.

87. W tym kontekście EIOD z zadowoleniem przyjmuje zamieszczony w art. 26 ust. 2 rozporządzenia wymóg, aby Komisja raz na trzy lata przedstawiała EIOD sprawozdanie dotyczące aspektów związanych z ochroną danych, w tym bezpieczeństwa danych. Wskazane byłoby wyjaśnienie w rozporządzeniu, że EIOD ma z kolei obowiązek udostępnić sprawozdanie Komisji krajowym organom ochrony danych w ramach skoordynowanego nadzoru, o którym mowa w art. 20. Przydatne byłoby też wyjaśnienie, że w sprawozdaniu należy omówić w odniesieniu do poszczególnych obszarów polityki i poszczególnych funkcji sposób praktycznego uwzględnienia najważniejszych zasad oraz zagadnień związanych z ochroną danych (np. informacji przedstawianych osobom, których dane dotyczą, praw dostępu, bezpieczeństwa).

88. Ponadto w rozporządzeniu należy wyjaśnić, że mechanizmy kontroli wewnętrznej powinny w swoich ramach uwzględniać też oceny w zakresie prywatności (obejmujące także analizę ryzyka z punktu widzenia bezpieczeństwa), politykę ochrony danych (obejmującą plan bezpieczeństwa) przyjętą w oparciu o wyniki tych ocen, jak również okresowe przeglądy i kontrole.

### 2.14. **Ochrona prywatności w fazie projektowania**

89. EIOD z zadowoleniem przyjmuje odniesienie do tej zasady w motywie 6 rozporządzenia ([40]). Zaleca on, aby oprócz tego odniesienia w rozporządzeniu wprowadzono również konkretne zabezpieczenia związane z uwzględnieniem ochrony prywatności w fazie projektowania takie jak:

— moduł ochrony danych w celu umożliwienia osobom, których dane dotyczą, skuteczniejszego korzystania ze swoich praw ([41]),

— wyraźny rozdział poszczególnych obszarów polityki objętych IMI („chińskie mury") ([42]),

— konkretne rozwiązania techniczne mające na celu ograniczenie możliwości wyszukiwania w wykazach, informacjach o ostrzeżeniach i w innych danych, aby zapewnić zgodność z zasadą celowości,

— konkretne rozwiązania zapewniające zamknięcie spraw, co do których nie są podejmowane działania ([43]),

— odpowiednie zabezpieczenia proceduralne w kontekście przyszłych zmian ([44]).

## 3. **WNIOSKI**

90. EIOD ogólnie pozytywnie ocenia IMI. Popiera on cele Komisji polegające na ustanowieniu elektronicznego systemu wymiany informacji oraz uregulowaniu jego aspektów dotyczących ochrony danych. EIOD z zadowoleniem przyjmuje również fakt, że Komisja proponuje horyzontalny instrument prawny dla IMI w postaci rozporządzenia Parlamentu i Rady. Z radością stwierdza, że we wniosku kompleksowo wskazano najistotniejsze kwestie dotyczące ochrony danych w związku z IMI.

91. W odniesieniu do ram prawnych IMI, które mają zostać ustanowione we wnioskowanym rozporządzeniu, EIOD zwraca uwagę na dwa główne wyzwania:

— potrzebę zapewnienia spójności przy poszanowaniu różnorodności oraz

— potrzebę wyważenia pomiędzy elastycznością a pewnością prawa.

92. Możliwe już do przewidzenia funkcje IMI należy jasno opisać i konkretnie wskazać.

93. Należy zastosować odpowiednie zabezpieczenia proceduralne zapewniające wnikliwe uwzględnienie kwestii ochrony danych podczas przyszłego rozwoju IMI. Powinny one obejmować ocenę skutków i konsultacje z EIOD oraz krajowymi organami ochrony danych przed każdym rozszerzeniem zakresu IMI na nowy obszar polityki lub dodaniem nowych funkcji.

94. Należy doprecyzować prawa dostępu podmiotów zewnętrznych oraz prawo dostępu do ostrzeżeń.

95. W odniesieniu do okresów zatrzymywania danych:

— w rozporządzeniu należy zawrzeć gwarancje, że sprawy w IMI będą zamykane punktualnie, a sprawy nieaktywne (w odniesieniu do których nie podejmowano ostatnio żadnych działań) zostaną usunięte z bazy danych,

— należy ponownie rozważyć, czy istnieje wystarczające uzasadnienie dla wydłużenia obecnego sześciomiesięcznego okresu do 18 miesięcy od chwili zamknięcia sprawy,

— Komisja nie przedstawiła wystarczającego uzasadnienia dla konieczności i proporcjonalności zatrzymywania „danych zablokowanych" przez okres do pięciu lat, w związku z czym wniosek ten należy ponownie rozważyć,

— należy dokonać wyraźniejszego rozróżnienia między ostrzeżeniami a repozytoriami informacji: w rozporządzeniu należy ustanowić następującą domyślną zasadę: (i) jeżeli prawodawstwo pionowe nie stanowi inaczej i pod warunkiem zastosowania odpowiednich dodatkowych zabezpieczeń, okres zatrzymywania ostrzeżeń powinien wynosić sześć miesięcy oraz (ii) okres ten powinien być liczony od chwili wysłania ostrzeżenia.

96. W rozporządzeniu należy zawrzeć wymóg oceny ryzyka oraz przeglądu planu bezpieczeństwa przed każdym rozszerzeniem IMI na nowy obszar polityki lub przed dodaniem nowych funkcji niosących skutki z punktu widzenia danych osobowych.

97. Przepisy dotyczące informacji przedstawianych osobom, których dane dotyczą, oraz praw dostępu należy udoskonalić i powinny one zachęcać do bardziej spójnego podejścia.

([40]) Idem.
([41]) Zob. sekcję 2.9 powyżej.
([42]) Zob. sekcję 2.4 powyżej.
([43]) Zob. sekcję 2.5.2 powyżej.
([44]) Zob. sekcję 2.2.2 powyżej.

98. EIOD zaleca udoskonalenie przepisów o skoordynowanym nadzorze w pewnych aspektach; w tym celu zaleca wprowadzenie przepisów podobnych, jak np. obowiązujące w kontekście wizowego systemu informacyjnego i systemu Schengen II oraz planowane w odniesieniu do Eurodac. W odniesieniu do częstotliwości spotkań i kontroli EIOD popiera elastyczne podejście przyjęte we wniosku, którego celem jest ustanowienie w rozporządzeniu zasad minimalnych koniecznych dla zapewnienia skutecznej współpracy bez nakładania zbędnych obciążeń administracyjnych.

99. W rozporządzeniu należy zawrzeć gwarancje, że właściwe organy lub inne podmioty zewnętrzne z państwa trzeciego, które nie zapewnia odpowiedniego stopnia ochrony, nie uzyskają bezpośredniego dostępu do IMI, jeżeli nie obowiązują stosowne klauzule umowne. Negocjacja tych klauzul powinna przebiegać na szczeblu UE.

100. W rozporządzeniu należy ustanowić jasne ramy odpowiednich mechanizmów kontroli wewnętrznej, które zapewniają zgodność z zasadami ochrony danych i dowodzą tej zgodności, w tym ocen w zakresie prywatności (obejmujących także analizę ryzyka z punktu widzenia bezpieczeństwa), polityki ochrony danych (obejmującej plan bezpieczeństwa) przyjętej w oparciu o wyniki tych ocen, jak również okresowych przeglądów i kontroli.

101. W rozporządzeniu należy też wprowadzić konkretne zabezpieczenia związane z uwzględnieniem ochrony prywatności w fazie projektowania.

Sporządzono w Brukseli dnia 22 listopada 2011 r.

Giovanni BUTTARELLI

*Zastępca Europejskiego Inspektora Ochrony Danych*