

I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych na temat inicjatywy Królestwa Belgii, Republiki Bułgarii, Republiki Estońskiej, Królestwa Hiszpanii, Republiki Francuskiej, Republiki Włoskiej, Republiki Węgierskiej, Rzeczypospolitej Polskiej, Republiki Portugalskiej, Rumunii, Republiki Finlandii i Królestwa Szwecji w sprawie przyjęcia dyrektywy Parlamentu Europejskiego i Rady w sprawie europejskiego nakazu ochrony, oraz na temat inicjatywy Królestwa Belgii, Republiki Bułgarii, Republiki Estońskiej, Królestwa Hiszpanii, Republiki Austrii, Republiki Słowenii i Królestwa Szwecji dotyczącej dyrektywy Parlamentu Europejskiego i Rady w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych

(2010/C 355/01)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

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

uwzględniając Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 8,

uwzględniając dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych⁽¹⁾,

uwzględniając rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, w szczególności jego art. 41⁽²⁾,

uwzględniając decyzję ramową Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych⁽³⁾,

I. WPROWADZENIE

1. W ostatnich latach dokładano coraz usilniejszych starań na rzecz poprawy współpracy organów wymiaru sprawiedliwości w sprawach karnych. Kwestia ta zajmuje obecnie ważną pozycję w programie sztokholmskim⁽⁴⁾ i wiąże się ze szczególną wrażliwością danych osobowych oraz skutkami, jakie przetwarzanie danych może mieć dla osób, których te dane dotyczą.
2. Z tych powodów Europejski Inspektor Ochrony Danych (EIOD) poświęca tej kwestii szczególną uwagę⁽⁵⁾ i zamierza poprzez niniejszą opinię jeszcze raz podkreślić konieczność ochrony praw podstawowych jako podstawy przestrzeni wolności, bezpieczeństwa i sprawiedliwości, określonej w programie sztokholmskim.
3. Niniejsza opinia dotyczy dwóch inicjatyw w sprawie dyrektywy przedłożonych przez pewną liczbę państw członkowskich zgodnie z art. 76 TFUE, a mianowicie:

⁽¹⁾ Dz.U. L 281 z 23.11.1995, s. 31.

⁽²⁾ Dz.U. L 8 z 12.1.2001, s. 1.

⁽³⁾ Dz.U. L 350 z 30.12.2008, s. 60.

⁽⁴⁾ Rada Europejska, Program sztokholmski – Otwarta i bezpieczna Europa dla dobra i ochrony obywateli (2010/C 115/01), rozdział 3, „Ułatwienie życia obywatelom: Europa prawa i sprawiedliwości” (Dz.U. C 115 z 4.5.2010, s. 1); zob. również opinia EIOD w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady dotyczącego przestrzeni wolności, bezpieczeństwa i sprawiedliwości w służbie obywateli (Dz.U. C 276 z 17.11.2009, s. 8).

⁽⁵⁾ W ostatnich latach EIOD wydał wiele opinii i uwag w sprawie inicjatyw dotyczących przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Można je znaleźć na stronie internetowej EIOD.

- a) inicjatywy 12 państw członkowskich w sprawie przyjęcia dyrektywy Parlamentu Europejskiego i Rady w sprawie europejskiego nakazu ochrony („inicjatywa w sprawie europejskiego nakazu ochrony”), przedstawionej w styczniu 2010 r. ⁽⁶⁾; oraz
- b) inicjatywy 7 państw członkowskich dotyczącej dyrektywy Parlamentu Europejskiego i Rady w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych („inicjatywa w sprawie europejskiego nakazu dochodzeniowego”), przedstawionej w kwietniu 2010 r. ⁽⁷⁾
4. Doradzanie w sprawie tych inicjatyw wchodzi w zakres zadania powierzonego EIOD w art. 41 rozporządzenia (WE) nr 45/2001, polegającego na doradzaniu instytucjom i organom UE we wszystkich kwestiach dotyczących przetwarzania danych osobowych. Dlatego też niniejsza opinia zawiera uwagi na temat inicjatyw w zakresie, w jakim odnoszą się one do przetwarzania danych osobowych. EIOD wydaje niniejszą opinię z własnej inicjatywy, ponieważ nie otrzymał żadnego wniosku o udzielenie porady ⁽⁸⁾.
5. EIOD przypomina, że zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 Komisja ma obowiązek konsultować się z EIOD, gdy przyjmuje wnioski ustawodawcze odnoszące się do ochrony praw i wolności osoby fizycznej w odniesieniu do przetwarzania danych osobowych. W przypadku inicjatywy państw członkowskich obowiązek ten nie stosuje się *stricto sensu*. Jednakże od chwili wejścia w życie Traktatu z Lizbony zwykła procedura ustawodawcza ma zastosowanie również do obszaru współpracy policyjnej i wymiarów sprawiedliwości, przy czym w art. 76 TFUE przewidziano szczególny wyjątek, a mianowicie że jedna czwarta państw członkowskich może wystąpić z inicjatywą w sprawie środków UE. Zgodnie z Traktatem z Lizbony inicjatywy te są dostosowane, na ile to możliwe, do wniosków Komisji i w razie możliwości należy zastosować gwarancje proceduralne. Z tego względu wspomnianym inicjatywom towarzyszy ocena skutków.
6. W tym kontekście EIOD nie tylko żałuje, że nie skonsultowano się z nim przy wydawaniu inicjatyw, ale również zaleca Komisji, aby ustanowiła procedurę konsultacji z EIOD, w przypadku gdy inicjatywa przedstawiona przez państwa członkowskie wiąże się z przetwarzaniem danych osobowych.
7. Mimo że dwie wspomniane inicjatywy mają różne cele, tj. poprawę ochrony ofiar oraz współpracę transgraniczną

w sprawach karnych poprzez transgraniczne gromadzenie materiału dowodowego, występują między nimi ważne podobieństwa:

- a) obie opierają się na zasadzie wzajemnego uznawania orzeczeń i decyzji sądowych ⁽⁹⁾;
- b) mają swoje źródło w programie sztokholmskim ⁽¹⁰⁾, oraz
- c) przewidują wymianę danych osobowych między państwami członkowskimi (zob. pkt 10 i 13 oraz sekcja II.4).

Z tych powodów EIOD uważa, że stosowne jest zbadanie obu wspomnianych inicjatyw razem.

8. W tym kontekście należy wspomnieć, że również Komisja Europejska niedawno zajmowała się kwestią gromadzenia materiału dowodowego w celu przedłożenia ich właściwym organom w innych państwach członkowskich (co stanowi określony cel inicjatywy w sprawie europejskiego nakazu dochodzeniowego). Pod koniec 2009 r. opublikowano zieloną księgę ⁽¹¹⁾ – konsultacje nad którą są obecnie zakończone ⁽¹²⁾ – przy czym celem Komisji (opartym na „Planie działań służącym realizacji programu sztokholmskiego” ⁽¹³⁾) było przedłożenie w 2011 r. wniosku ustawodawczego dotyczącego kompleksowego systemu pozyskiwania dowodów w sprawach karnych opartego o zasadę wzajemnego uznawania i obejmującego wszystkie rodzaje dowodów ⁽¹⁴⁾.

⁽⁹⁾ Zasadę tę wprowadzono w wiedeńskim planie działania (Plan działania Rady i Komisji w sprawie optymalnego wykonania postanowień traktatu z Amsterdamu dotyczących przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Tekst przyjęty przez Radę ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w dniu 3 grudnia 1998 r. (Dz.U. C 19 z 23.1.1999, s. 1), pkt 45(f)) i jasno sformułowano w konkluzjach przyjętych przez Radę Europejską w Tampere w dniach 15 i 16 października 1999 r., pkt 33, 35–37.

⁽¹⁰⁾ Trzecia inicjatywa (w sprawie przyjęcia dyrektywy Parlamentu Europejskiego i Rady w sprawie prawa do tłumaczenia ustnego i pisanego w postępowaniu karnym, 22.1.2010, 2010/0801) ma takie samo źródło, lecz nie jest uwzględniona w niniejszej opinii, ponieważ nie dotyczy kwestii związanych z ochroną danych osobowych. W tym temacie zob. także wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie prawa do tłumaczenia ustnego i pisanego w postępowaniu karnym, 9.3.2010, COM(2010) 82 wersja ostateczna.

⁽¹¹⁾ Zielona księga w sprawie wzajemnego udostępniania przez państwa członkowskie materiału dowodowego w sprawach karnych oraz zapewnienia jego dopuszczalności, COM(2009) 624 wersja ostateczna, 11.11.2009.

⁽¹²⁾ Komisja Europejska rozpatruje różne i czasami kontrastujące ze sobą odpowiedzi. Można się z nimi zapoznać na stronie: http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0004_en.htm

⁽¹³⁾ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Przestrzeń wolności, bezpieczeństwa i sprawiedliwości dla europejskich obywateli. Plan działań służący realizacji programu sztokholmskiego, Bruksela, 20.4.2010, COM(2010) 171 wersja ostateczna, s. 18.

⁽¹⁴⁾ Na razie nie jest jeszcze jasne, jak potencjalny przyszły instrument będzie powiązany z inicjatywą w sprawie europejskiego nakazu dochodzeniowego.

⁽⁶⁾ Dz.U. C 69 z 18.3.2010, s. 5.

⁽⁷⁾ Dz.U. C 165 z 24.6.2010, s. 22.

⁽⁸⁾ W przeszłości EIOD także przyjmował opinie w sprawie inicjatyw państw członkowskich: zob. np. opinia EIOD z dnia 4 kwietnia 2007 r. na temat inicjatywy 15 państw członkowskich w celu przyjęcia decyzji Rady w sprawie intensywniejszej współpracy transgranicznej, szczególnie w walce z terroryzmem i przestępczością transgraniczną (Dz.U. C 169 z 21.7.2007, s. 2) oraz opinia EIOD w sprawie inicjatywy 14 państw członkowskich mającej na celu przyjęcie decyzji Rady w sprawie wzmocnienia Eurojustu i zmiany decyzji 2002/187/WSiSW (Dz.U. C 310 z 5.12.2008, s. 1).

II. WSPÓŁPRACA WYMIARÓW SPRAWIEDLIWOŚCI W SPRAWACH KARNYCH I PRZETWARZANIE DANYCH OSOBOWYCH W RAMACH INICJATYW W SPRAWIE EUROPEJSKIEGO NAKAZU OCHRONY I EUROPEJSKIEGO NAKAZU DOCHODZENIOWEGO

II.1. Kontekst inicjatyw

9. Wspomniane inicjatywy wpasowują się w tendencję działań UE w przestrzeni wolności, bezpieczeństwa i sprawiedliwości w ostatnich latach. Od września 2001 r. doszło do znaczącego nasilenia gromadzenia i wymiany informacji w obrębie Unii Europejskiej (oraz z państwami trzecimi), również dzięki rozwojowi TIK i ułatwieniom ze strony wielu instrumentów prawnych UE. Inicjatywy w sprawie europejskiego nakazu ochrony i europejskiego nakazu dochodzeniowego również mają na celu poprawę wymiany informacji odnoszących się do osób fizycznych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości.

II.2. Inicjatywa w sprawie europejskiego nakazu ochrony

10. Inicjatywa w sprawie europejskiego nakazu ochrony – oparta na art. 82 ust. 1 lit. d) TFUE – skupia się na ochronie ofiar przestępstw, w szczególności kobiet, i ma na celu zagwarantowanie im skutecznej ochrony w obrębie Unii Europejskiej. Aby osiągnąć ten cel, inicjatywa w sprawie europejskiego nakazu ochrony umożliwia rozszerzenie środków ochronnych wymienionych w art. 2 ust. 2 i przyjętych zgodnie z prawem jednego z państw członkowskich („państwo wydające”) w innym państwie członkowskim, do którego przemieszcza się osoba podlegająca ochronie („państwo wykonujące”) bez potrzeby rozpoczynania przez ofiarę nowego postępowania lub ponownego przedstawiania dowodów w państwie wykonującym.

11. Dlatego też środki ochronne nałożone (na wniosek ofiary) na osobę będącą przyczyną niebezpieczeństwa mają na celu ochronę życia, nietykalności fizycznej i psychicznej, wolności lub nietykalności seksualnej ofiary w granicach UE, niezależnie od granic krajowych, a także próbę zapobieżenia nowym przestępstwom wobec tej samej ofiary.

12. Europejski nakaz ochrony powinien być wydany na wniosek ofiary w „państwie (członkowskim) wydającym” przez dowolny organ sądowy (lub równoważny). Proces ten obejmuje następujące kroki:

a) „państwo wydające” składa wniosek o europejski nakaz ochrony;

b) otrzymawszy europejski nakaz ochrony, „państwo wykonujące” przyjmuje na mocy swojego prawa krajowego decyzję o kontynuowaniu ochrony danej osoby.

13. Do osiągnięcia tego celu trzeba wprowadzić środki administracyjne. Będą one częściowo obejmowały wymianę informacji osobowych pomiędzy państwem członkowskim „wydającym” i „wykonującym”, dotyczących danej osoby („ofiary”) i osoby będącej przyczyną niebezpieczeństwa. Wymiana danych osobowych jest przewidziana w następujących przepisach:

a) w art. 6 przewiduje się, że sam europejski nakaz ochrony zawiera wiele elementów informacji osobowych, określonych w lit. a), e), f), g) i h) oraz w załączniku I;

b) obowiązki właściwego organu państwa wykonującego, określone w art. 8 ust. 1, wymagają przetwarzania danych osobowych, w szczególności obowiązek powiadomienia o wszelkich naruszeniach środka ochronnego (art. 8 ust. 1 lit. d) i załącznik II);

c) obowiązki właściwego organu państwa członkowskiego wydającego i wykonującego dotyczące zmiany, wygaśnięcia lub odwołania nakazu lub środków ochronnych (art. 14).

14. Informacje wspomniane w poprzednim punkcie wyraźnie wchodzą w zakres danych osobowych, szeroko definiowanych w prawodawstwie w dziedzinie ochrony danych jako „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej”⁽¹⁵⁾ i dalej wyjaśnionych przez grupę roboczą art. 29. Inicjatywa w zakresie europejskiego nakazu ochrony jest związana z informacjami o osobie fizycznej (oferze lub osobie będącej przyczyną niebezpieczeństwa) lub informacjami, które są lub mogą zostać wykorzystane do oceny i określonego traktowania statusu osoby fizycznej lub wpływania na ten status (w szczególności w przypadku osoby będącej przyczyną niebezpieczeństwa)⁽¹⁶⁾.

II.3. Inicjatywa w sprawie europejskiego nakazu dochodzeniowego

15. Inicjatywa w sprawie europejskiego nakazu dochodzeniowego – oparta na art. 82 ust. 1 lit. a) TFUE – wymaga od państw członkowskich gromadzenia, przechowywania i przekazywania materiałów dowodowych, nawet jeżeli nie są one jeszcze dostępne w jurysdykcji krajowej. Dlatego też inicjatywa wykracza poza zasadę dostępności, przedstawioną w programie haskim z 2004 r. jako innowacyjne

⁽¹⁵⁾ Zob. art. 2 lit. a) decyzji ramowej Rady 2008/977/WSiSW w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych oraz art. 2 lit. a) dyrektywy 95/46/WE i art. 2 lit. a) rozporządzenia (WE) nr 45/2001.

⁽¹⁶⁾ Zob. opinia grupy roboczej art. 29 4/2007 w sprawie pojęcia danych osobowych, WP 136, przyjęta w dniu 20 czerwca 2007 r., s. 10.

podejście do transgranicznej wymiany informacji organów ścigania⁽¹⁷⁾. Wykracza również poza decyzję ramową Rady 2008/978/WSiSW z dnia 18 grudnia 2008 r. w sprawie europejskiego nakazu dowodowego, która ma zastosowanie wyłącznie do (danych) dowodów, które już istnieją⁽¹⁸⁾.

16. Europejski nakaz dochodzeniowy ma być wydawany na potrzeby prowadzenia jednej lub więcej określonych czynności dochodzeniowych w państwie wykonującym w celu zgromadzenia materiału dowodowego (potencjalnie nieistniejącego w chwili wydania nakazu) i jego przekazania (art. 12). Stosuje się do niemal wszystkich czynności dochodzeniowych (zob. motywy 6 i 7 inicjatywy).
17. Celem inicjatywy w sprawie europejskiego nakazu dochodzeniowego jest utworzenie pojedynczego, skutecznego i elastycznego instrumentu uzyskiwania materiału dowodowego znajdującego się w innym państwie członkowskim w ramach postępowania karnego, zamiast aktualnych, bardziej złożonych instrumentów prawnych stosowanych przez organy sądowe (w oparciu z jednej strony o wzajemną pomoc prawną, a z drugiej – o wzajemne uznawanie)⁽¹⁹⁾.
18. Najwyraźniej materiał dowodowy zgromadzony poprzez europejski nakaz dochodzeniowy (zob. także załącznik A do inicjatywy) może zawierać dane osobowe, podobnie jak w przypadku informacji o rachunkach bankowych (art. 23), informacji o transakcjach bankowych (art. 24) i monitorowania transakcji bankowych (art. 25), lub może obejmować przekazywanie danych osobowych (jak w przypadku wideokonferencji i telekonferencji, o czym mowa w art. 21 i 22).
19. Z tych powodów inicjatywa w sprawie europejskiego nakazu dochodzeniowego ma znaczący wpływ na prawo do ochrony danych osobowych. Biorąc także pod uwagę fakt, że termin wdrożenia decyzji ramowej 2008/978/WSiSW jeszcze nie upłynął (i dlatego trudno ocenić skuteczność tego instrumentu oraz potrzebę dodat-

kowych środków prawnych)⁽²⁰⁾, EIOD przypomina o potrzebie okresowej weryfikacji w świetle zasad ochrony danych, skuteczności i proporcjonalności środków prawnych przyjętych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości⁽²¹⁾. Dlatego też EIOD zaleca dodanie klauzuli oceny do inicjatywy w sprawie europejskiego nakazu dochodzeniowego, która od państw członkowskich wymagałaby regularnego składania sprawozdań dotyczących stosowania tego instrumentu, a od Komisji wymagałaby dokonywania syntezy tych sprawozdań i, w stosownych przypadkach, wydawania odpowiednich wniosków w sprawie zmian.

II.4. Przetwarzanie danych osobowych przewidziane w inicjatywach w sprawie europejskiego nakazu ochrony i europejskiego nakazu dochodzeniowego

20. Jak wyjaśniono powyżej w pkt 13, 14 i 18, jest oczywiste, że na mocy proponowanych dyrektyw dane osobowe będą przetwarzane i wymieniane przez właściwe organy różnych państw członkowskich. W tym okolicznościach osoba, której dane dotyczą, jest chroniona podstawowym prawem do ochrony danych, uznanym w art. 16 TFUE i art. 8 Karty praw podstawowych Unii Europejskiej.
21. Mimo tego w „Informacjach szczegółowych” towarzyszących inicjatywie w sprawie europejskiego nakazu ochrony szacowane „ryzyko naruszenia praw podstawowych” określono jako „0” (zerowe)⁽²²⁾, a w ocenie skutków zawartej w „Informacjach szczegółowych” towarzyszących inicjatywie w sprawie europejskiego nakazu dochodzeniowego nie uwzględniono kwestii związanych z ochroną danych⁽²³⁾.
22. EIOD wyraża żal z powodu tych wniosków i podkreśla znaczenie ochrony danych w określonym kontekście, w którym dane osobowe są przetwarzane, a mianowicie z uwagi na:
 - a) szeroki obszar współpracy wymiarów sprawiedliwości w sprawach karnych;
 - b) fakt, że dane często zaliczają się do kategorii szczególnie chronionych i zazwyczaj pozyskiwane są przez policję i organy sądowe w wyniku dochodzenia;
 - c) możliwą treść danych, szczególnie w odniesieniu do inicjatywy w sprawie europejskiego nakazu dochodzeniowego, która obejmowałaby dowolny rodzaj materiału dowodowego; oraz

⁽¹⁷⁾ Zasada zapisana w Programie Haskim: wzmocnienie wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej, pkt 2.1, oznacza, „że na obszarze całej Unii urzędnik organu ścigania w jednym państwie członkowskim, który potrzebuje informacji w celu wykonania swoich obowiązków, może je uzyskać od drugiego państwa członkowskiego oraz że organ ścigania w tym drugim państwie członkowskim, który posiada informacje, udostępni je we wskazanym celu, uwzględniając wymagania toczących się dochodzeń w tamtym państwie”. W tej kwestii zob. opinia EIOD na temat wniosku dotyczącego decyzji ramowej Rady w sprawie wymiany informacji w ramach zasady dostępności (COM(2005) 490 wersja ostateczna), Dz.U. C 116 z 17.5.2006, s. 8.

⁽¹⁸⁾ Decyzja ramowa Rady 2008/978/WSiSW z dnia 18 grudnia 2008 r. w sprawie europejskiego nakazu dowodowego dotyczącego przedmiotów, dokumentów i danych, które mają zostać wykorzystane w postępowaniach w sprawach karnych, Dz.U. L 350 z 30.12.2008, s. 72.

⁽¹⁹⁾ Obecnie istnieją dwa instrumenty wzajemnego uznawania mające zastosowanie do uzyskiwania dowodów: decyzja ramowa Rady 2003/577/WSiSW z dnia 22 lipca 2003 r. w sprawie wykonania w Unii Europejskiej postanowień o zabezpieczeniu mienia i środków dowodowych (Dz.U. L 196 z 2.8.2003, s. 45) oraz decyzja ramowa 2008/978/WSiSW, przywołana w przypisie 18.

⁽²⁰⁾ Artykuł 23 ust. 1 decyzji ramowej 2008/978/WSiSW stanowi, że „państwa członkowskie podejmują niezbędne działania w celu wykonania przepisów niniejszej decyzji ramowej do dnia 19 stycznia 2011 r.”.

⁽²¹⁾ Również pkt 1.2.3 programu sztokholmskiego zawiera wymóg, że nowe inicjatywy prawodawcze należy przedkładać wyłącznie po sprawdzeniu, czy przestrzega się w nich zasady proporcjonalności.

⁽²²⁾ Informacje szczegółowe umożliwiające ocenę zgodności z zasadami pomocniczości i proporcjonalności zgodnie z art. 5 protokołu (nr 2) do Traktatu z Lizbony z dnia 6 stycznia 2010 r.

⁽²³⁾ Informacje szczegółowe z dnia 23 czerwca 2010 r., dokument międzyinstytucjonalny: 2010/0817 (COD) odnoszą się wyraźnie jedynie do prawa do wolności i bezpieczeństwa oraz do prawa do dobrej administracji (zob. s. 25 i p. 41).

- d) możliwe przekazywanie materiału dowodowego poza UE zgodnie z art. 13 decyzji ramowej Rady 2008/977/WSiSW w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych⁽²⁴⁾.
23. Ten kontekst sprawia, że operacje przetwarzania danych mają szczególne skutki i mogą znacząco wpływać na podstawowe prawa osoby, której dane dotyczą, w tym na prawo do ochrony danych osobowych.
24. W związku z powyższymi okolicznościami EIOD zastanawia się, dlaczego inicjatywy ani nie poruszają kwestii ochrony danych osobowych (z wyjątkiem odniesienia do obowiązku poufności narzuconego podmiotom uczestniczącym w dochodzeniu przez art. 18 inicjatywy w sprawie europejskiego nakazu dochodzeniowego), ani nie odnoszą się wyraźnie do decyzji ramowej 2008/977/WSiSW. Wspomniana decyzja ramowa rzeczywiście miałyby zastosowanie do operacji przetwarzania przewidzianych w obu inicjatywach (zob. art. 1 ust. 2 lit. a)).
25. Z tego względu EIOD z zadowoleniem przyjmuje fakt, że w trakcie prac przygotowawczych Rady związanych z europejskim nakazem ochrony wprowadzono odesłanie do decyzji ramowej 2008/977/WSiSW⁽²⁵⁾ i jest przekonany, że Parlament Europejski potwierdzi tę zmianę pierwotnej inicjatywy⁽²⁶⁾.
26. EIOD żałuje, że podobny motyw nie został jeszcze wprowadzony do inicjatywy w sprawie europejskiego nakazu dochodzeniowego, która wiąże się ze znacznie bardziej intensywną wymianą danych osobowych. W tym kontekście EIOD z zadowoleniem przyjmuje fakt, że Komisja Europejska w uwagach do inicjatywy w sprawie europejskiego nakazu dochodzeniowego sugeruje, że należy wprowadzić odniesienie (zarówno w motywie, jak i w treści wniosku) do stosowania decyzji ramowej 2008/977/WSiSW⁽²⁷⁾.

⁽²⁴⁾ Dalej: decyzja ramowa 2008/977/WSiSW.

⁽²⁵⁾ Zob. motyw 27 ostatniego projektu inicjatywy w sprawie europejskiego nakazu ochrony (28.5.2010, nr dok. Rady 10384/2010): „Dane osobowe przetwarzane w związku z wdrożeniem niniejszej decyzji ramowej powinny być chronione zgodnie z decyzją ramową Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych oraz zgodnie z zasadami określonymi w Konwencji Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, która została ratyfikowana przez wszystkie państwa członkowskie”.

⁽²⁶⁾ W tym znaczeniu zob. poprawka 21 zawarta w projekcie sprawozdania dotyczącego inicjatywy w sprawie przyjęcia dyrektywy Parlamentu Europejskiego i Rady w sprawie europejskiego nakazu ochrony (00002/2010 – C7-0006/2010 – 2010/0802 (COD)), 20.5.2010, Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych – Komisja Praw Kobiet i Równouprawnienia, sprawozdawcy: Teresa Jiménez-Becerril Barrio, Carmen Romero López, dostępny pod adresem: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/femm/pr/817/817530/817530en.pdf

⁽²⁷⁾ Zob. uwagi Komisji na temat proponowanego europejskiego nakazu dochodzeniowego w sprawach karnych, 24.8.2010, JUST/B/1/AA-et D(2010) 6815, s. 9 i 38, dostępny pod adresem: http://ec.europa.eu/justice/news/intro/doc/comment_2010_08_24_en.pdf

27. Dlatego też, bez uszczerbku dla sekcji III poniżej, obie inicjatywy powinny zawierać szczegółowe przepisy wyjaśniające, że decyzja ramowa 2008/977/WSiSW ma zastosowanie do przetwarzania danych przewidzianego w tych inicjatywach.

III. SZCZEGÓLNE ZASADY POTRZEBNE OPRÓCZ ISTNIEJĄCYCH RAM PRAWNYCH W DZIEDZINIE DANYCH OSOBOWYCH, DOTYCZĄCE WSPÓŁPRACY WYMIARÓW SPRAWIEDLIWOŚCI W SPRAWACH KARNYCH

28. W obu inicjatywach ponownie porusza się zasadniczą kwestię niepełnego i niespójnego stosowania zasad ochrony danych w obszarze współpracy wymiarów sprawiedliwości w sprawach karnych⁽²⁸⁾.
29. EIOD zdaje sobie sprawę ze znaczenia, jakie ma zwiększenie skuteczności współpracy wymiarów sprawiedliwości między państwami członkowskimi, także w obszarach objętych inicjatywami w sprawie europejskiego nakazu ochrony i europejskiego nakazu dochodzeniowego⁽²⁹⁾. EIOD rozumie ponadto konieczność i korzyści z dzielenia się informacjami, ale pragnie podkreślić, że przetwarzanie takich danych musi odbywać się w sposób zgodny m.in.⁽³⁰⁾ z przepisami UE dotyczącymi ochrony danych. Jest to jeszcze bardziej oczywiste w świetle Traktatu z Lizbony wprowadzającego art. 16 TFUE i nadającego wiążący charakter art. 8 Karty praw podstawowych Unii Europejskiej.
30. Sytuacje wiążące się z transgraniczną wymianą informacji w UE zasługują na szczególną uwagę, ponieważ przetwarzanie danych osobowych w ramach więcej niż jednej jurysdykcji prowadzi do większego zagrożenia praw i interesów osób fizycznych. Dane osobowe będą przetwarzane w wielu jurysdykcjach, gdzie wymogi prawne oraz ramy technicznej niekoniecznie są takie same.
31. Ponadto prowadzi to do niepewności prawa w odniesieniu do osób, których dotyczą dane – możliwy jest udział stron z innych państw członkowskich, może mieć zastosowanie prawo krajowe różnych państw członkowskich i może się ono różnić od prawa, jakie znają osoby, których dotyczą dane, lub mieć zastosowanie w systemie prawnym, który nie jest znany osobie, której dotyczą dane. Wymaga to podjęcia większych starań w celu zapewnienia zgodności z wymogami prawodawstwa UE dotyczącego ochrony danych⁽³¹⁾.

⁽²⁸⁾ Zob. także sekcja V niniejszej opinii.

⁽²⁹⁾ Zob. m.in. poparcie konieczności poprawienia dostępu do wymiaru sprawiedliwości, usprawnienia współpracy między europejskimi organami prawnymi i zwiększenia skuteczności samego systemu sądownictwa, wrazone w opinii EIOD w sprawie europejskiej strategii w dziedzinie e-sprawiedliwości (Dz.U. C 128 z 6.6.2009, s. 13, pkt 9 i 21).

⁽³⁰⁾ W odniesieniu do aspektu związanego z poszanowaniem zasad procedury karnej w państwach członkowskich, szczególnie w obszarze wniosku dotyczącego europejskiego nakazu dochodzeniowego, można odnieść się do spostrzeżeń i uwag zawartych w odpowiedziach przesłanych Komisji Europejskiej podczas konsultacji społecznej dotyczącej *zielonej księgi* (zob. przypisy 11 i 12).

⁽³¹⁾ Zob. także Rada, Program Haski: wzmacnianie wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej (2005/C 53/01), (Dz.U. C 53 z 3.3.2005, s. 17 i następane).

32. Zdaniem EIOD wyjaśnienie stosowania decyzji ramowej 2008/977/WSiSW, jak zaproponowano w pkt 27, stanowi zaledwie pierwszy krok.
33. Szczególne wyzwania w zakresie skutecznej ochrony w obszarze współpracy wymiarów sprawiedliwości w sprawach karnych, w połączeniu z nie całkiem zadowalającą decyzją ramową 2008/977/WSiSW (zob. pkt 52–56), mogą wymagać przepisów szczegółowych dotyczących ochrony danych, w przypadku gdy określone instrumenty prawne UE wymagają wymiany danych osobowych.

IV. WYZWANIA W ZAKRESIE SKUTECZNEJ OCHRONY DANYCH PRZY WSPÓLPRACY W SPRAWACH KARNYCH: ZALECENIA DOTYCZĄCE INICJATYW W SPRAWIE EUROPEJSKIEGO NAKAZU OCHRONY I EUROPEJSKIEGO NAKAZU DOCHODZENIOWEGO

IV.1. Uwagi wstępne

34. Skuteczna ochrona danych osobowych (jak podkreślono w pkt 29) jest ważna nie tylko dla osoby, której dotyczą dane, ale też przyczynia się do powodzenia samej współpracy wymiarów sprawiedliwości. W rzeczywistości gotowość do wymiany tych danych z organami innych państw członkowskich zwiększy się, jeżeli dany organ będzie miał pewność co do poziomu ochrony, dokładności i wiarygodności danych osobowych w tym innym państwie członkowskim⁽³²⁾. Krótko mówiąc, ustalenie (wysokich) wspólnych norm ochrony danych w tym wrażliwym obszarze będzie sprzyjało wzajemnemu zaufaniu i pewności pomiędzy państwami członkowskimi i wzmocni współpracę wymiarów sprawiedliwości opartą na wzajemnym uznawaniu, poprawiając jakość danych objętych wymianą informacji.
35. W tym określonym kontekście EIOD zaleca, oprócz ogólnego odniesienia do decyzji ramowej 2008/977/WSiSW (jak zaproponowano w pkt 27), uwzględnienie w inicjatywach w sprawie europejskiego nakazu ochrony i europejskiego nakazu dochodzeniowego konkretnych zabezpieczeń dotyczących danych osobowych.
36. Niektóre z tych zabezpieczeń mają bardziej ogólny charakter i powinny zostać uwzględnione w obu inicjatywach, w szczególności zabezpieczenia mające na celu poprawę dokładności danych, a także bezpieczeństwa i poufności. Inne zabezpieczenia odnoszą się do przepisów szczegółowych zawartych w inicjatywie w sprawie europejskiego nakazu ochrony lub w sprawie europejskiego nakazu dochodzeniowego.

IV.2. Zabezpieczenia o bardziej ogólnym charakterze

Dokładność

37. W przewidzianych w inicjatywach sytuacjach, w których dochodzi do wymiany danych pomiędzy państwami, należy

⁽³²⁾ Zob. opinia EIOD w sprawie wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (COM(2005) 475 wersja ostateczna), (Dz.U. C 47 z 25.2.2006, s. 27, pkt 5–7).

położyć szczególny nacisk na zapewnienie dokładności informacji. W tej kwestii EIOD z zadowoleniem stwierdza, że inicjatywa w sprawie europejskiego nakazu ochrony zawiera w art. 14 jasne obowiązki właściwego organu państwa wydającego w zakresie informowania właściwego organu państwa wykonującego o każdej zmianie, wygaśnięciu, lub odwołaniu nakazu ochrony.

38. EIOD zauważa także, że konieczność tłumaczenia może wpływać na dokładność informacji, szczególnie dlatego że inicjatywy dotyczą określonych instrumentów prawnych, które mogą mieć różne znaczenie w różnych językach i różnych systemach prawnych. Chociaż w tym kontekście EIOD z zadowoleniem przyjmuje fakt, że inicjatywa w sprawie europejskiego nakazu ochrony uwzględnia kwestię tłumaczenia (art. 16), to sugeruje włączenie podobnego przepisu do inicjatywy w sprawie europejskiego nakazu dochodzeniowego.

Bezpieczeństwo, świadomość i odpowiedzialność

39. Rozwój współpracy transgranicznej, który może być wynikiem przyjęcia obu wspomnianych inicjatyw, wymaga dokładnego rozważenia aspektów bezpieczeństwa transgranicznego przekazywania danych osobowych związanego z wykonywaniem europejskich nakazów ochrony i europejskich nakazów dochodzeniowych⁽³³⁾. Jest to konieczne nie tylko w celu spełnienia standardów bezpieczeństwa w odniesieniu do przetwarzania danych osobowych, wymaganych zgodnie z art. 22 decyzji ramowej 2008/977/WSiSW, ale również w celu zapewnienia tajemnicy dochodzenia i poufności postępowania karnego, co jest uregulowane w art. 18 inicjatywy w sprawie europejskiego nakazu dochodzeniowego oraz, jako ogólna zasada dotycząca danych osobowych wynikająca z wymiany transgranicznej, w art. 21 decyzji ramowej 2008/977/WSiSW.
40. EIOD podkreśla konieczność zabezpieczenia systemów telekomunikacyjnych stosowanych w procedurach przesyłania danych. Dlatego też z zadowoleniem przyjmuje przepis dotyczący stosowania europejskiej sieci sądowej⁽³⁴⁾ jako narzędzia, które gwarantuje, że europejski nakaz ochrony i europejski nakaz dochodzeniowy są właściwie kierowane do odpowiednich organów krajowych, i w ten sposób zapobiega ryzyku zaangażowania niewłaściwych organów w wymianę danych osobowych lub je minimalizuje (zob. art. 7 ust. 2 i 3 inicjatywy w sprawie europejskiego nakazu ochrony oraz art. 6 ust. 3 i 4 inicjatywy w sprawie europejskiego nakazu dochodzeniowego).
41. Dlatego też inicjatywy powinny zawierać przepisy wymagające od państw członkowskich dopilnowania, aby:

⁽³³⁾ Zob. ogólnie komunikat Komisji do Rady, Parlamentu Europejskiego i Europejskiego Komitetu ekonomiczno-społecznego – Droga do europejskiej strategii w dziedzinie e-sprawiedliwości, Bruksela, 30.5.2008, COM(2008)329 wersja ostateczna, s. 8: „Organom sądowym należy zapewnić możliwość całkowicie bezpiecznej wymiany poufnych danych”.

⁽³⁴⁾ Decyzja Rady 2008/976/WSiSW z dnia 16 grudnia 2008 r. w sprawie Europejskiej Sieci Sądowej (Dz.U. L 348 z 24.12.2008, s. 130).

- a) właściwe organy posiadały wystarczające zasoby na potrzeby stosowania proponowanych dyrektyw;
- b) właściwi funkcjonariusze przestrzegali norm zawodowych i podlegali odpowiednim procedurom wewnętrznym, które zapewniają w szczególności ochronę osób fizycznych w odniesieniu do przetwarzania danych osobowych, uczciwość proceduralną i stosowne przestrzeganie przepisów dotyczących poufności oraz tajemnicy służbowej (jak przewiduje się w art. 18 inicjatywy w sprawie europejskiego nakazu dochodzeniowego).
42. Ponadto EIOD zaleca wprowadzenie przepisów zapewniających przestrzeganie istotnych zasad ochrony danych podczas przetwarzania tych danych i nakładających obowiązek posiadania niezbędnych mechanizmów wewnętrznych na potrzeby wykazywania zgodności zainteresowanym stronom zewnętrznym. Takie przepisy byłyby instrumentami obciążającymi odpowiedzialnością administratorów danych (zgodnie z „zasadą odpowiedzialności”, która jest omawiana w kontekście obecnego przeglądu ram prawnych w dziedzinie ochrony danych⁽³⁵⁾). Wymaga to podejmowania przez nich niezbędnych środków dla zapewnienia zgodności. Przepisy te powinny obejmować:
- a) systemy uwierzytelniania, które zezwalają na dostęp do baz danych zawierających dane osobowe lub pomieszczeń, w których znajduje się materiał dowodowy, wyłącznie upoważnionym osobom fizycznym;
- b) monitorowanie korzystania z dostępu do danych osobowych i operacji wykonywanych na tych danych;
- c) wprowadzenie kontroli audytowej.

IV.3. Zabezpieczenia w ramach inicjatywy w sprawie europejskiego nakazu dochodzeniowego

43. Biorąc pod uwagę szczególnie inwazyjny charakter określonych czynności dochodzeniowych, EIOD wzywa do gruntownej refleksji nad dopuszczalnością dowodów zgromadzonych w celach innych niż działania prewencyjne, czynności dochodzeniowo-śledcze lub prokuratorskie w przypadkach przestępstw lub wykonywanie sankcji karnych oraz egzekwowanie prawa do obrony. Ze szczególną uwagą należy rozważyć wykorzystanie dowodów uzyskanych na mocy art. 11 ust. 1 lit. d) decyzji ramowej 2008/977/WSiSW⁽³⁶⁾.

⁽³⁵⁾ Zob. grupa robocza art. 29 oraz grupa robocza ds. policji i wymiaru sprawiedliwości, Przyszłość prywatności (The Future of Privacy), s. 20 i następnę.

⁽³⁶⁾ Przepis ten dopuszcza wykorzystanie dowodów również „w innym celu – wyłącznie za uprzednią zgodą państwa członkowskiego przekazującego dane lub za zgodą osoby, której dotyczą dane, udzieloną zgodnie z prawem krajowym”.

44. Dlatego też w inicjatywie w sprawie europejskiego nakazu dochodzeniowego należy uwzględnić wyjątek od stosowania przepisów art. 11 ust. 1 lit. d). Wyjątek ten powinien przewidywać, że materiał dowodowy zgromadzony na mocy europejskiego nakazu dochodzeniowego nie może zostać wykorzystany w celach innych niż działania prewencyjne, czynności dochodzeniowo-śledcze lub prokuratorskie w przypadkach przestępstw lub wykonywanie sankcji karnych oraz egzekwowanie prawa do obrony.

IV.4. Zabezpieczenia w ramach inicjatywy w sprawie europejskiego nakazu ochrony

45. W odniesieniu do inicjatywy w sprawie europejskiego nakazu ochrony EIOD uznaje, że dane osobowe wymieniane pomiędzy właściwymi organami i wymienione w załączniku I inicjatywy (odnoszące się zarówno do ofiary, jak i osoby będącej przyczyną niebezpieczeństwa) są prawidłowe, stosowne oraz nienadmierne w stosunku do celów, dla których są gromadzone i przetwarzane dalej.
46. Jednakże niewystarczająco wyraźnie wynika z inicjatywy – szczególnie w art. 8 ust. 1 lit. b) – które dane osobowe dotyczące ofiary będą przekazywane osobie będącej przyczyną niebezpieczeństwa przez właściwy organ państwa wykonującego.
47. EIOD uważa, że przed udzieleniem informacji osobie będącej przyczyną niebezpieczeństwa właściwe będzie rozważenie okoliczności i treści środków ochronnych wydanych przez organ sądowy wydającego państwa członkowskiego. Z tego względu osobie tej należy udostępniać tylko te dane osobowe ofiary (co w niektórych przypadkach może obejmować dane kontaktowe), które są ściśle istotne dla pełnego wykonania środka ochronnego.
48. EIOD zdaje sobie sprawę, że przekazanie informacji kontaktowych (np. numerów telefonów, adresu ofiary oraz innych miejsc regularnie odwiedzanych, takich jak miejsce pracy lub szkoła dzieci) może w rzeczywistości zagrozić fizycznemu i psychicznemu samopoczuciu ofiary, a także wpłynąć na jej prawo do prywatności i do ochrony danych osobowych. Z drugiej strony w niektórych przypadkach wskazanie odpowiednich adresów może być konieczne do ostrzeżenia osoby będącej przyczyną niebezpieczeństwa o miejscach, w których nie wolno jej przebywać. Ma to na celu umożliwienie zgodności z nakazem i zapobieganie potencjalnym karom za jego naruszenie. Ponadto, w zależności od okoliczności, określenie jednej lub wielu lokalizacji, w których nie wolno przebywać osobie będącej przyczyną niebezpieczeństwa, może być konieczne, aby niepotrzebnie nie ograniczać jej swobody przemieszczania się.

49. W świetle tych rozważań EIOD podkreśla wagę tego zagadnienia i zaleca, żeby inicjatywa w sprawie europejskiego nakazu ochrony wyraźnie przewidywała, że, w zależności od okoliczności sprawy, osoba będąca przyczyną niebezpieczeństwa powinna otrzymać tylko te dane osobowe ofiary

(które w niektórych przypadkach mogą obejmować dane kontaktowe), które mają ścisły związek z pełnym wykonaniem środka ochronnego⁽³⁷⁾).

50. Na koniec EIOD prosi o wyjaśnienie wyrażenia „metody elektroniczne”, zawartego w motywie 10 inicjatywy w sprawie europejskiego nakazu ochrony. W szczególności należy wyjaśnić, czy dane osobowe są przetwarzane z użyciem „metod elektronicznych” i jakie gwarancje są zapewniane w takim przypadku.

V. ZASADY OCHRONY DANYCH I WSPÓLPRACA WYMIARÓW SPRAWIEDLIWOŚCI W SPRAWACH KARNYCH: KWESTIE ZWIĄZANE Z INICJATYWAMI W SPRAWIE EUROPEJSKIEGO NAKAZU OCHRONY I EUROPEJSKIEGO NAKAZU DOCHODZENIOWEGO

51. Decyzja Ramowa 2008/977/WSiSW stosuje się do każdej wymiany danych osobowych na mocy inicjatyw w sprawie europejskiego nakazu ochrony i europejskiego nakazu dochodzeniowego.
52. Mimo że EIOD uznaje, iż decyzja ramowa 2008/977/WSiSW – po wdrożeniu przez państwa członkowskie – stanowi znaczące działanie na rzecz ochrony danych w obszarze współpracy policyjnej i sądowej⁽³⁸⁾, to sama decyzja ramowa nie jest w pełni zadowalająca⁽³⁹⁾. Główna nierozwiązana kwestia odnosi się do jej ograniczonego zakresu stosowania. Stosowanie decyzji ramowej jest ograniczone do wymiany danych osobowych w obszarze policji i organów sądowych pomiędzy organami i systemami w różnych państwach członkowskich i na szczeblu UE⁽⁴⁰⁾.
53. Nawet jeżeli nie można rozstrzygnąć tej kwestii w kontekście inicjatyw w sprawie europejskiego nakazu ochrony i europejskiego nakazu dochodzeniowego, EIOD nalega na podkreślenie, że brak (wysokich) wspólnych norm ochrony danych we współpracy wymiarów sprawiedliwości może oznaczać, iż organ sądowy na szczeblu krajowym lub na szczeblu UE, gdy zajmuje się aktami sprawy zawierającymi dane pochodzące z innego państwa członkowskiego (w tym np. materiał dowodowy zgromadzony w oparciu o europejski nakaz dochodzeniowy), będzie musiał stosować inne zasady ochrony danych: niezależne przepisy krajowe (które muszą być zgodne

z konwencją nr 108 Rady Europy) w odniesieniu do danych pochodzących z tego samego państwa członkowskiego oraz przepisy wdrażające decyzję ramową 2008/977/WSiSW w odniesieniu do danych pochodzących z innego państwa członkowskiego. Tym samym różne „fragmenty informacji” mogłyby podlegać różnym systemom prawnym.

54. Skutki stosowania „podwójnych” norm ochrony danych w odniesieniu do każdego akt sprawy zawierających elementy transgraniczne jest istotne dla codziennej praktyki (np. zatrzymanie informacji przewidziane w obowiązujących przepisach każdego z organów przekazujących; dalsze ograniczenia dotyczące przetwarzania żądane przez każdy z organów przekazujących; w razie wniosku ze strony państwa trzeciego każdy z organów przekazujących dane wydawałby zgodę na podstawie własnej oceny tego państwa trzeciego pod kątem zapewnienia odpowiedniego poziomu ochrony lub zgodnie ze zobowiązaniami międzynarodowymi; różnice w przepisach dotyczących prawa dostępu osobę, której dane dotyczą, do tych danych). Ponadto poziom ochrony obywateli i ich prawa mogą być ogromnie różnicowane i podlegać różnym szerokim odstępstwom, w zależności od państwa członkowskiego, w którym odbywa się przetwarzanie⁽⁴¹⁾.
55. Dlatego też EIOD korzysta z okazji, aby powtórzyć swoją opinię na temat konieczności stosowania szerokich ram prawnych w dziedzinie ochrony danych, obejmujących wszystkie obszary kompetencji UE, w tym policję i wymiar sprawiedliwości, w odniesieniu zarówno do danych osobowych przekazywanych lub udostępnianych przez właściwe organy innego państwa członkowskiego, jak i do krajowego przetwarzania w przestrzeni wolności, bezpieczeństwa i sprawiedliwości⁽⁴²⁾.
56. Wreszcie EIOD zwraca uwagę, że zasady ochrony danych powinny stosować się do wszystkich sektorów i do wykorzystywania danych w każdym celu⁽⁴³⁾. Oczywiście właściwie uzasadnione i jasno sformułowane wyjątki powinny być możliwe, szczególnie w odniesieniu do danych osobowych przetwarzanych dla celów egzekwowania prawa⁽⁴⁴⁾. Luki w ochronie danych osobowych są

⁽³⁷⁾ Wydaje się to być celem poprawek 13 i 55 zawartych w projekcie sprawozdania dotyczącego inicjatywy w sprawie przyjęcia dyrektywy Parlamentu Europejskiego i Rady w sprawie europejskiego nakazu ochrony (00002/2010 – C7-0006/2010 – 2010/0802 (COD)), 20.5.2010, Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych – Komisja Praw Kobiety i Równouprawnienia.

⁽³⁸⁾ Zob. opinia EIOD w sprawie komunikatu Komisji do Parlamentu Europejskiego, Rady i Europejskiego Komitetu Ekonomiczno-Społecznego: Droga do europejskiej strategii w dziedzinie e-sprawiedliwości (2009/C 128/02) (Dz.U. C 128 z 6.6.2009, s. 13, pkt 17).

⁽³⁹⁾ Zob. trzy opinie EIOD w sprawie wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (COM (2005) 475 wersja ostateczna) (Dz.U. C 47 z 25.2.2006, s. 27, Dz.U. C 91 z 26.4.2007, s. 9, Dz.U. C 139 z 23.6.2007, s. 1). Zob. także opinia EIOD w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady dotyczącego przestrzeni wolności, bezpieczeństwa i sprawiedliwości w służbie obywateli (Dz.U. C 276 z 17.11.2009, s. 8, pkt 19, 29 i 30).

⁽⁴⁰⁾ Zob. art. 2 decyzji ramowej 2008/977/WSiSW.

⁽⁴¹⁾ Zob. trzecia opinia EIOD w sprawie wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.U. C 139 z 23.6.2007, s. 41), wspomniana w przypisie 39, pkt 46.

⁽⁴²⁾ To stanowisko EIOD jest wyraźnie poparte w opinii grupy roboczej art. 29 oraz grupy roboczej ds. policji i wymiaru sprawiedliwości Przyszłość prywatności. Wspólny wkład w konsultacje Komisji Europejskiej w sprawie ram prawnych dotyczących podstawowego prawa do ochrony danych osobowych (The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data), WP 168, przyjętej w dniu 1 grudnia 2009 r., s. 4, 7 i następane oraz s. 24 i następane.

⁽⁴³⁾ Zob. komunikat Komisji do Parlamentu Europejskiego i Rady – Przestrzeń wolności, bezpieczeństwa i sprawiedliwości w służbie obywateli, Bruksela, 10.6.2009, COM(2009) 262 wersja ostateczna, s. 30: „Unia powinna przyjąć pełny system ochrony danych osobowych, obejmujący wszystkie obszary, w których przysługuje jej właściwość”.

⁽⁴⁴⁾ Takie podejście byłoby również zgodne z celem deklaracji 21 w sprawie ochrony danych osobowych w dziedzinie współpracy sądowej w sprawach karnych i współpracy policyjnej, załączonej do Traktatu z Lizbony.

sprzeczne z obecnymi (odnowionymi) ramami prawnymi Unii Europejskiej. Artykuł 3 ust. 2 dyrektywy 95/46/WE – wyłączający z zakresu stosowania dyrektywy obszar policji i wymiaru sprawiedliwości – nie spełnia założeń art. 16 TFUE. Ponadto konwencja nr 108 Rady Europy⁽⁴⁵⁾, która jest wiążąca dla wszystkich państw członkowskich, w niewystarczającym stopniu pokrywa te luki.

VI. WNIOSKI I ZALECENIA

57. W odniesieniu do inicjatyw w sprawie europejskiego nakazu ochrony i europejskiego nakazu dochodzeniowego EIOD zaleca:

- uwzględnienie przepisów szczegółowych przewidujących, że instrumenty te stosują się, nie naruszając decyzji ramowej Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych,
- uwzględnienie przepisów wymagających od państw członkowskich dopilnowania, aby:
 - właściwe organy posiadały zasoby niezbędne do stosowania proponowanych dyrektyw,
 - właściwi funkcjonariusze przestrzegali norm zawodowych i podlegali odpowiednim procedurom wewnętrznym, które zapewniają w szczególności ochronę osób fizycznych w odniesieniu do przetwarzania danych osobowych, uczciwość proceduralną i stosowne przestrzeganie przepisów dotyczących poufności oraz tajemnicy służbowej,
 - systemy uwierzytelniania zezwalały na dostęp do baz danych zawierających dane osobowe lub pomieszczeń, w których znajduje się materiał dowodowy, wyłącznie upoważnionym osobom fizycznym,
 - prowadzono monitorowanie korzystania z dostępu do danych oraz operacji,
 - wprowadzono kontrolę audytową.

58. W odniesieniu do inicjatywy w sprawie europejskiego nakazu ochrony EIOD zaleca:

- zawarcie w niej jasnego stwierdzenia, że, w zależności od okoliczności sprawy, osoba będąca przyczyną niebezpieczeństwa powinna otrzymać tylko te dane osobowe ofiary (które w niektórych przypadkach

mogą obejmować dane kontaktowe), które mają ścisły związek z pełnym wykonaniem środka ochronnego,

- wyjaśnienie wyrażenie „metody elektroniczne”, zawartego w motywie 10 inicjatywy w sprawie europejskiego nakazu ochrony.

59. W odniesieniu do inicjatywy w sprawie europejskiego nakazu dochodzeniowego EIOD zaleca:

- wprowadzenie do niej przepisu dotyczącego tłumaczeń, podobnego do art. 16 inicjatywy w sprawie europejskiego nakazu ochrony,
- włączenie do niej przepisu zapobiegającego wykorzystaniu materiału dowodowego w celach innych niż działania prewencyjne, czynności dochodzeniowo-śledcze lub prokuratorskie w przypadkach przestępstw lub wykonywanie sankcji karnych oraz egzekwowanie z prawa do obrony, stanowiącego wyjątek od art. 11 ust. 1 lit. d) decyzji ramowej 2008/977/WSiSW,
- dodanie klauzuli oceny do inicjatywy w sprawie europejskiego nakazu dochodzeniowego, która od państw członkowskich wymagałaby regularnego składania sprawozdań dotyczących stosowania tego instrumentu, a od Komisji wymagałaby dokonywania syntezy tych sprawozdań i, w stosownych przypadkach, wydawania odpowiednich wniosków w sprawie zmian.

60. Ponadto ogólnie EIOD:

- zaleca Komisji, aby ustanowiła procedurę konsultacji z EIOD, w przypadku gdy inicjatywa przedstawiona przez państwa członkowskie wiąże się z przetwarzaniem danych osobowych,
- po raz kolejny podkreśla konieczność stosowania szerokich ram prawnych w dziedzinie ochrony danych, obejmujących wszystkie obszary kompetencji UE, w tym policję i wymiar sprawiedliwości, w odniesieniu zarówno do danych osobowych przekazywanych lub udostępnianych przez właściwe organy innego państwa członkowskiego, jak i do krajowego przetwarzania w przestrzeni wolności, bezpieczeństwa i sprawiedliwości.

Sporządzono w Brukseli dnia 5 października 2010 r.

Peter HUSTINX
Europejski Inspektor Ochrony Danych

⁽⁴⁵⁾ Konwencja Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, 28.1.1981, nr 108.