RADA UNII EUROPEJSKIEJ

Bruksela, 27 stycznia 2012 r. (13.02) (OR. en)

5834/12

DATAPROTECT 7
JAI 42
DAPIX 10
FREMP 9
COMIX 60

PISMO PRZEWODNIE

Od:	Sekretarz Generalny Komisji Europejskiej, podpisał dyrektor Jordi AYET PUIGARNAU
Data otrzymania:	27 stycznia 2012 r.
Do:	Uwe CORSEPIUS, Sekretarz Generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2012) 12 final
Dotyczy:	Sprawozdanie Komisji dla Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów na podstawie art. 29 ust. 2 decyzji ramowej Rady z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych.

Delegacje otrzymują w załączeniu dokument Komisji COM(2012) 12 final.

Zał.: COM(2012) 12 final

KOMISJA EUROPEJSKA

Bruksela, dnia 25.1.2012 r.
COM(2012) 12 final

SPRAWOZDANIE KOMISJI DLA PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW

na podstawie art. 29 ust. 2 decyzji ramowej Rady z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych.

{SEC(2012) 75 final}

SPRAWOZDANIE KOMISJI DLA PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW

na podstawie art. 29 ust. 2 decyzji ramowej Rady z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych.

1. WPROWADZENIE

1.1. Kontekst

Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r.[1] (zwana dalej „decyzją ramową") w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych stworzyła ogólne ramy prawne ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych. Weszła w życie w dniu 19 stycznia 2009 r.[2]

Przyjęcie decyzji ramowej było niezbędne, ponieważ w tym czasie nie istniał żaden ogólny instrument na poziomie europejskim, obejmujący przetwarzanie danych osobowych w ramach współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych[3]. Artykuł 3 dyrektywy 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych stanowi, że dyrektywa „nie ma zastosowania do przetwarzania danych osobowych w ramach działalności wykraczającej poza zakres prawa Wspólnoty, takiej jak działalność określona w tytule VI Traktatu o Unii Europejskiej, a w żadnym razie do działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa oraz działalności państwa w obszarach prawa karnego".

Celem decyzji ramowej jest zapewnienie na poziomie UE wysokiego poziomu ochrony praw podstawowych i wolności osób fizycznych w toku przetwarzania danych osobowych w ramach współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych. Jednocześnie należy zagwarantować wysoki poziom bezpieczeństwa publicznego[4]. Nie stanowi to dla państw członkowskich przeszkody w ustanawianiu wyższych gwarancji ochrony bezpieczeństwa danych osobowych zbieranych lub przetwarzanych na szczeblu krajowym[5].

Zakres[6] decyzji ramowej ogranicza się do przetwarzania danych osobowych w celu zapobiegania przestępstwom, wykrywania przestępstw, ich ścigania lub karania lub

---

1 Dz.U. L 350 z 30.12.2008, s. 60.
2 Artykuł 30.
3 Motyw 5 dyrektywy 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, Dz.U. L 281 z 23.11.1995, s. 31.
4 Artykuł 1.
5 Artykuł 1 ust. 5.
6 Artykuł 1 ust. 2.

wykonywania sankcji karnych. Dane te są przekazywane lub udostępniane lub też zostały już przekazane lub udostępnione:

- między państwami członkowskimi,

- przez państwa członkowskie organom lub systemom informacyjnym utworzonym na podstawie tytułu VI Traktatu o Unii Europejskiej („Współpraca policyjna i wymiarów sprawiedliwości w sprawach karnych"); lub

- właściwym organom państw członkowskich przez organy lub systemy informacyjne utworzone na podstawie Traktatu o Unii Europejskiej lub Traktatu ustanawiającego Wspólnotę Europejską.

Dane osobowe, które zostały przekazane przez jedno państwo członkowskie do drugiego, mogą być przekazywane państwom trzecim lub instytucjom międzynarodowym, pod warunkiem spełnienia pewnych wymogów[7].

Decyzję ramową stosuje się w całości do Zjednoczonego Królestwa i Irlandii, ponieważ stanowi ona rozwinięcie dorobku prawnego Schengen. Zjednoczone Królestwo oraz Irlandia są stronami decyzji ramowej zgodnie z art. 5 Protokołu w sprawie dorobku Schengen włączonego w ramy Unii Europejskiej, załączonego do Traktatu o Unii Europejskiej i Traktatu ustanawiającego Wspólnotę Europejską, oraz decyzją Rady 2000/365/WE i 2002/192/WE.

W odniesieniu do Islandii, Norwegii, Szwajcarii i Liechtensteinu decyzja ramowa stanowi rozwinięcie dorobku prawnego Schengen w rozumieniu umowy i protokołów zawartych przez Radę Unii Europejskiej albo Unię Europejską z Islandią i Norwegią, Konfederacją Szwajcarską i Liechtensteinem, oraz decyzji Rady 1999/437/WE, 2008/149/WSiSW i 2008/262/WSiSW.

1.2. Treść decyzji ramowej 2008/977/WSiSW

Do **zakresu** decyzji ramowej nie włączono przetwarzania danych osobowych na poziomie krajowym przez właściwe organy sądowe i policyjne w państwach członkowskich (art. 1 ust. 2).

Co do zasady sektorowe instrumenty legislacyjne dotyczące współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych, które zawierają przepisy w sprawie ochrony danych osobowych i które zostały przyjęte **przed** wejściem w życie decyzji ramowej, mają pierwszeństwo przed jej przepisami (art. 28). Niniejsza decyzja ramowa nie narusza aktów uznanych za ustanawiające „wyczerpujący i spójny zbiór zasad" obejmujący ochronę danych (motyw 39). Inne przepisy właściwe dla danego sektora obejmujące zasady ochrony danych o bardziej ograniczonym zakresie mają pierwszeństwo przed przepisami decyzji ramowej wyłącznie, jeżeli zasady te są bardziej surowe niż przepisy decyzji ramowej. W odmiennych przypadkach stosuje się decyzję ramową (motyw 40).

Decyzja ramowa określa cele ochrony danych w ramach działalności policji i wymiarów sprawiedliwości. Ustanawia ona zasady przetwarzania danych osobowych zgodnie z prawem,

---

[7] Artykuł 13.

aby zagwarantować, że każda informacja, która może być przedmiotem wymiany, jest przetwarzana zgodnie z prawem i zgodnie z podstawowymi zasadami jakości danych.

Ponadto określa ona prawa podmiotów danych, aby zapewnić ochronę danych osobowych bez szkody dla dochodzeń w sprawach karnych. W tym celu podmioty danych muszą być poinformowane i muszą mieć zapewniony dostęp do swoich danych osobowych.

Krajowe organy nadzorcze, działające w pełni niezależnie podczas wykonywania zadań, które zostały im powierzone, są zobowiązane do doradzania i monitorowania stosowania środków przyjętych przez państwa członkowskie w celu transpozycji decyzji ramowej.

1.3. Zobowiązanie Komisji do przedstawiania sprawozdań z wdrażania

Zgodnie z art. 29 ust. 1 decyzji ramowej państwa członkowskie są zobowiązane do podjęcia środków celem dostosowania się do decyzji ramowej do dnia 27 listopada 2010 r.

Zgodnie z art. 29 ust. 2 państwa członkowskie są zobowiązane do przekazania Sekretariatowi Generalnemu Rady i Komisji tekstu przepisów przenoszących obowiązki nałożone na nie na mocy niniejszej decyzji ramowej do ich prawa krajowego, oraz informacji o organach nadzorczych, o których mowa w art. 25 decyzji ramowej.

Komisja jest zobowiązana do przygotowania sprawozdania na podstawie informacji przedłożonych przez państwa członkowskie. Rada musi przed dniem 27 listopada 2011 r. ocenić zakres, w jakim państwa członkowskie przestrzegają przepisów niniejszej decyzji ramowej

1.4. Źródła informacji wykorzystanych w sprawozdaniu

Do **9 listopada 2011 r.** 26 z 27 państw członkowskich, jak również Liechtenstein, Norwegia, Islandia i Szwajcaria, przekazały Komisji informacje na temat wdrażania decyzji ramowej.

Z tych **26** państw członkowskich **14** państw wskazało, że ich obowiązujące ustawodawstwo wdraża decyzję ramową (Austria, Belgia, Republika Czeska, Dania, Niemcy, Estonia, Irlandia, Litwa, Luksemburg, Łotwa, Słowacja, Szwecja, Węgry i Zjednoczone Królestwo). Niemcy, Irlandia, Estonia i Szwecja wskazały, że nadal badają potrzebę wprowadzenia dalszych środków wykonawczych.

W odniesieniu do **9** państw członkowskich można uznać, że decyzja ramowa została wdrożona częściowo, ponieważ poinformowały one, iż ustawodawstwo potrzebne do wdrożenia decyzji nadal pozostaje do przyjęcia.

Cztery państwa członkowskie albo nie odpowiedziały na wniosek Komisji o przesłanie informacji (Rumunia), albo wskazały, że decyzja ramowa nie została wdrożona (Grecja, Włochy[8], Cypr).

---

[8] **Włochy** poinformowały Komisję, że szczegółowe akty wykonawcze nie zostały jeszcze oficjalnie przyjęte. Dotyczy to włoskiego kodeksu ochrony danych osobowych, kodeksu postępowania karnego i innych aktów zawierających przepisy odnoszące się do przetwarzania w tych obszarach. Inne państwa członkowskie przyjęły inne podejście i wskazały, że przepisy dotyczące ochrony danych stosuje się również do przetwarzania danych osobowych przez policję i wymiar sprawiedliwości na poziomie krajowym, jak również do przetwarzania o charakterze transgranicznym przez policję i wymiar

Treść informacji przekazanych w kwestionariuszu, w szczególności ich poziom szczegółowości, różni się między państwami członkowskimi. Tabela 1 przedstawia odpowiedzi w ogólnym zarysie: odzwierciedla ocenę dokonaną przez państwa członkowskie dotyczącą etapu wdrażania decyzji ramowej.

2. TRANSPOZYCJA DECYZJI RAMOWEJ

2.1. Decyzja ramowa na podstawie dawnego art. 34 ust. 2 lit. b) Traktatu o Unii Europejskiej

Podstawą niniejszej decyzji ramowej jest Traktat o Unii Europejskiej (TUE), w szczególności jego art. 30 i art. 31 lit. e) oraz art. 34 ust. 2 lit. b).

Najbliższym odpowiednikiem decyzji ramowej jako instrumentu legislacyjnego jest dyrektywa, ponieważ oba instrumenty wiążą państwa członkowskie w odniesieniu do rezultatu, który ma być osiągnięty, ale pozostawiają organom krajowym swobodę wyboru formy i metody wykonania. Decyzje ramowe nie wywołują jednak skutku bezpośredniego[9].

Na podstawie art. 10 Protokołu w sprawie postanowień przejściowych dotyczących aktów przyjętych na podstawie Tytułu V i VI Traktatu o Unii Europejskiej przed wejściem w życie Traktatu z Lizbony (nr 36), załączonego do Traktatów, uprawnienia przyznane Komisji na mocy art. 258 TFUE nie mają zastosowania (a uprawnienia Trybunału Sprawiedliwości UE pozostają ograniczone) w odniesieniu do aktów objętych „dawnym trzecim filarem" w okresie przejściowym trwającym pięć lat od wejścia w życie Traktatu z Lizbony (tj. do dnia 1 grudnia 2014 r.).

Poniżej przedstawiono informacje szczegółowe dotyczące wdrażania czterech najważniejszych przepisów decyzji ramowej na podstawie odpowiedzi państw członkowskich udzielonych na wniosek Komisji z dnia 9 grudnia 2010 r.

2.1.1. Zakres krajowych środków wykonawczych

Decyzję ramową stosuje się wyłącznie do przetwarzana danych osobowych przekazanych lub udostępnionych między państwami członkowskimi (art. 1 ust. 2). Zakres decyzji ramowej nie obejmuje przetwarzania danych osobowych przez policję i wymiar sprawiedliwości w sprawach karnych.

Tabela 2 Załącznika przedstawia ogólny zarys środków wykonawczych w państwach członkowskich. Większość państw członkowskich odniosła się do ogólnego ustawodawstwa dotyczącego ochrony danych jako środków wykonawczych do decyzji ramowej oraz uzupełniła tę informację o odniesienia do sektorowego ustawodawstwa dotyczącego policji, wymiaru sprawiedliwości, organów celnych i podatkowych. Niektóre państwa członkowskie podjęły decyzję o nieprzyjmowaniu aktów ustawodawczych, a o wydaniu okólników administracyjnych (np. Niemcy i Zjednoczone Królestwo).

---

sprawiedliwości w sprawach karnych. Ponadto poinformowały one Komisję o dodatkowych środkach wykonawczych, które są obecnie przygotowywane.

9 Zobacz sprawa C-105/03, Pupino, wyrok z 16.5.2005 r., pkt 34, 43-45, 47, 61, w którym Trybunał Sprawiedliwości orzekł, że sądy krajowe, dokonując wykładni przepisów krajowych, zobowiązane są do stosowania spójnej wykładni, w tym w odniesieniu do decyzji ramowych.

Większość państw członkowskich wskazała, że **ogólne ustawodawstwo dotyczące ochrony danych ma zastosowanie do przetwarzania danych osobowych przez policję i wymiar sprawiedliwości tak na poziomie krajowym, jak i w kontekście transgranicznym[10], jednak często istnieje obok kodeksów postępowania karnego i aktów o danych policyjnych lub o policji[11].** Do kodeksów postępowania karnego lub podobnego ustawodawstwa odniosło się trzynaście państw członkowskich (Belgia, Republika Czeska, Niemcy, Estonia, Włochy, Luksemburg, Węgry, Malta, Niderlandy, Słowenia, Słowacja, Finlandia i Szwecja). Siedem państw członkowskich (Republika Czeska, Niemcy, Węgry, Niderlandy, Słowenia, Finlandia i Szwecja) poinformowało o obowiązywaniu szczególnych aktów o danych policyjnych lub aktów o policji[12]. Niektóre państwa członkowskie (np. Bułgaria, Portugalia, Litwa) dodały, że przyjęły przepisy szczególne, aby wdrożyć niektóre przepisy decyzji ramowej nieobjęte przepisami ogólnymi, które dotyczą wyłącznie przetwarzania danych osobowych w kontekście transgranicznym[13].

Trzy państwa członkowskie uznały ograniczony zakres decyzji ramowej za problematyczną kwestię. Włochy i Niderlandy poinformowały o trudnościach w wyodrębnieniu w praktyce przetwarzania danych w kontekście transgranicznym na podstawie decyzji ramowej 2008/977 od przetwarzania na poziomie krajowym. Związana z tym złożoność powoduje, że organy ścigania w państwach członkowskich muszą sobie radzić z różnymi zasadami przetwarzania tych samych danych osobowych. Polska wskazała ogólnie na braki decyzji ramowej. Ponadto podkreśliła zwłaszcza swoje poparcie dla celu Komisji, jakim jest ustanowienie kompleksowych ram oraz rozszerzenie przepisów dotyczących ochrony danych na dziedzinę współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych.[14]

2.1.2. Informowanie podmiotów danych (Artykuł 16, motywy 26–27)

Na podstawie decyzji ramowej państwo członkowskie musi dopilnować, żeby właściwe organy poinformowały podmioty danych o tym, że ich dane osobowe są przetwarzane lub przekazywane innemu państwu członkowskiemu w celu zapobiegania przestępstwom, prowadzenia dochodzeń, wykrywania przestępstw, ich ścigania lub wykonywania sankcji karnych. Prawo krajowe powinno określić formę, treść, metodę oraz odstępstwa (tj. nieudostępnianie lub ograniczone udostępnianie). Może przyjąć to ogólną formę poprzez przyjęcie aktu prawnego lub opublikowanie wykazu operacji związanych z przetwarzaniem. Jeżeli dane zostały przekazane innemu państwu członkowskiemu, każde państwo członkowskie może domagać się, aby inne państwo członkowskie nie informowało podmiotu danych.

Tabela 3 pokazuje, że **prawie wszystkie** państwa członkowskie wskazały, iż przekazują podmiotom danych **niektóre** informacje odnoszące się do przetwarzania ich danych osobowych. **Francja** zasygnalizowała, że nie podejmuje takich kroków. **Dania** również nie przyznała tego prawa, ale poinformowała, że administrator musi prowadzić rejestr i informować opinię publiczną.

---

10 Tak było również przed przyjęciem decyzji ramowej (zob. Dokument roboczy służb Komisji, Ocena skutków, SEC(2005) 1241 z 4.10.2005, pkt 5.1.2.).

11 Zobacz Tabela 2.

12 Zobacz Tabela 2.

13 Zobacz uwagi przesłane przez Niderlandy.

14 Zobacz również stanowisko Polski (Ministerstwo Spraw Wewnętrznych) w konsultacjach społecznych zainicjowanych przez Komisję pod koniec 2010 r. (o którym mowa w odpowiedzi na kwestionariusz): http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/pl_min_pl.pdf.

Prawo do informacji jest poddane **ograniczeniom w znaczącej większości państw członkowskich.** Ustawodawstwo krajowe ogranicza to prawo dla celów zapobiegania, dochodzenia, wykrywania lub ścigania przestępstw albo przewiduje, że do przetwarzania danych osobowych przez określonych administratorów (policję lub wymiar sprawiedliwości) to prawo nie ma zastosowania. W niektórych przypadkach ograniczenia/odstępstwa są określane bez wyszczególnienia poszczególnych działań, do których mają się stosować. Znacząca liczba państw członkowskich wskazała takie ograniczenia w przypadku policji, żandarmerii wojskowej, sądów, organów celnych i podatkowych.

Niderlandy wyraziły opinię, że ogólne zobowiązanie do informowania podmiotu danych nie jest w pełni spójne z charakterem pracy policji lub wymiaru sprawiedliwości, ale zostały wprowadzone pewne uregulowania, aby przekazać wystarczającą ilość informacji podmiotowi danych zgodnie z wymogami dotyczącymi przetwarzania danych przez policję lub organy wymiaru sprawiedliwości (tj. w ustawach zawarto informacje na temat przypadków oraz warunków przetwarzania danych; prokurator informuje podmiot danych o wykonywaniu szczególnych uprawnień związanych z dochodzeniem, jeżeli na przeszkodzie nie stoi interes dochodzenia). Niderlandy są również zdania, iż nie ma potrzeby wdrażania niniejszego przepisu, ponieważ art. 16 ust. 1 odsyła wprost do krajowego ustawodawstwa państw członkowskich.

Decyzja ramowa ustanawia prawo do uzyskania informacji przez podmioty danych, ale nie zawiera żadnych szczegółowych elementów dotyczących metod lub możliwych odstępstw. Nawet jeżeli, według państw członkowskich, prawo do informacji zostało ogólnie przyznane, jego realizacja znacznie się różni.

2.1.3. Prawo dostępu podmiotów danych (art. 17)

Decyzja ramowa przewiduje, że podmiot danych ma prawo do uzyskania, bez ograniczeń, bez zbędnej zwłoki lub nadmiernych kosztów:

a) przynajmniej potwierdzenia ze strony administratora lub krajowego organu nadzorczego, czy odnoszące się do niego dane zostały przekazane lub udostępnione, oraz informacji o odbiorcy lub kategoriach odbiorców, którym dane zostały ujawnione, a także powiadomienia o tym, jakie dane są przetwarzane, lub

b) przynajmniej potwierdzenia ze strony krajowego organu nadzorczego, że dokonano wszystkich koniecznych weryfikacji.

Państwa członkowskie mogą ustanowić ograniczenia dotyczące prawa dostępu, aby uniknąć przeszkód w urzędowych lub prawnych śledztwach, dochodzeniach lub postępowaniach; i niekorzystnego wpływu na zapobieganie przestępstwom, ich ściganie, wykrywanie lub karanie lub na wykonywanie sankcji karnych; aby chronić bezpieczeństwo publiczne; bezpieczeństwo narodowe oraz podmioty danych lub prawa i wolności innych osób (art. 17 ust. 2). Każda odmowa administratora musi zostać sporządzona na piśmie (art. 17 ust. 3).

Informacje udostępnione przez państwa członkowskie i zebrane w tabeli 4 na temat prawa dostępu odzwierciedlają sytuację dotyczącą udzielania informacji podmiotowi danych. Można wnioskować, że wszystkie **państwa członkowskie**[15] **przyznały pewną formę prawa**

[15] Można wysunąć taki wniosek, chociaż niektóre państwa członkowskie nie przedstawiły szczegółowego zakresu (zob. dane szczegółowe w tabeli 3).

dostępu podmiotom danych. Prawo to co do zasady jest wpisane do krajowych przepisów ogólnych dotyczących ochrony danych. W wielu państwach członkowskich zostały również wprowadzone regulacje dotyczące szczegółowego zakresu prawa dostępu w ustawodawstwie sektorowym (takim jak akty o policji).

Jednocześnie wszystkie państwa członkowskie przewidują **odstępstwa od prawa do dostępu**. Najczęściej wymieniane przesłanki nieprzyznawania prawa dostępu to:

– zapobieganie przestępstwom, prowadzenie dochodzeń w sprawie przestępstw, ich wykrywanie i ściganie;

– bezpieczeństwo narodowe, obronność i bezpieczeństwo publiczne;

– ochrona interesów gospodarczych i finansowych państwa członkowskiego i UE (w tym w kwestiach walutowych, budżetowych i podatkowych)[16];

– ochrona praw i wolności podmiotu danych oraz praw i wolności innych osób.

W odniesieniu do sposobu, w jaki **przyznaje się prawo dostępu**, niektóre państwa członkowskie ustosunkowały się do tej kwestii wyraźnie, inne – nie. Niektóre państwa członkowskie wskazały, że przyznają podmiotom danych prawo do wysłania wniosku o dostęp do ich danych bezpośrednio do właściwego organu (tj. Austria, Niemcy, Bułgaria, Finlandia, Irlandia, Łotwa, Malta, Niderlandy, Polska, Słowacja, Szwecja, Zjednoczone Królestwo), podczas gdy inne zezwalają jedynie na „pośredni" dostęp (Belgia, Francja). W tym ostatnim przypadku dostęp do wszystkich danych osobowych związanych z podmiotem danych ma krajowy organ nadzorczy, a nie podmiot danych. W Finlandii i na Litwie podmiot danych ma wybór. W Portugalii co do zasady zapewnia się dostęp bezpośredni, ale w przypadkach, w których przetwarzanie danych ma związek z bezpieczeństwem państwa lub zapobieganiem przestępstwom lub prowadzeniem dochodzeń w sprawie przestępstw, umożliwia się dostęp pośredni. Podobna sytuacja panuje w Luksemburgu, w którym co do zasady przyznaje się dostęp bezpośrednio, ale gdy zastosowanie ma odstępstwo, wniosek o dostęp należy skierować do organu nadzorczego ds. ochrony danych.

Decyzja ramowa zawiera ogólne przepisy zapewniające podmiotom danych prawo dostępu do ich danych. Nie zawiera szczegółowych informacji, jakie dane muszą być udostępnione podmiotowi danych. Pozostawia również państwom członkowskim decyzję, czy podmioty danych mogą wykonywać swoje prawo bezpośrednio czy muszą skorzystać z pośrednictwa.

2.1.4. Krajowe organy nadzorcze (art. 25)

W decyzji ramowej 2008/977 uznano, że ustanowienie przez państwa członkowskie organów nadzorczych, pełniących swoje funkcje w sposób całkowicie niezależny, jest zasadniczym elementem ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i wymiarów sprawiedliwości między państwami członkowskimi (motyw 33). Stanowi ona ponadto, że "należy również" przyznać taki zakres odpowiedzialności organom nadzorczym ustanowionym uprzednio w państwach członkowskich na podstawie dyrektywy (motyw 34). Artykuł 25 decyzji ramowej 2008/977 odzwierciedla istotną część przepisu art. 28 (ust. 1-4, ust. 7) dyrektywy 95/46/WE dotyczącego organów nadzorczych w odniesieniu do uprawnień

[16] W art. 17 decyzji ramowej 2008/977 nie wymienia się wyraźnie odstępstwa. Artykuł odzwierciedla jednak odstępstwo wymienione w art. 13 ust. 1 dyrektywy 95/46/WE.

organu, obowiązku działania w pełnej niezależności oraz obowiązku zachowania tajemnicy służbowej. Każdy organ musi być wyposażony w pewne uprawnienia, obejmujące uprawnienia dochodzeniowe (w tym dostęp do danych oraz prawo do zbierania wszelkich niezbędnych informacji), skuteczne uprawnienia interwencyjne (takie jak wydawanie opinii i ich publikacja przed przeprowadzeniem operacji przetwarzania danych; nakazywanie tymczasowej lub ostatecznej blokady dostępu do danych, ich usunięcia lub zniszczenia; nakładanie czasowego lub ostatecznego zakazu przetwarzania danych; wydawanie administratorowi danych ostrzeżeń lub upomnień; przekazywanie sprawy parlamentowi państwa członkowskiego lub innym instytucjom politycznym) oraz uprawnienie do podejmowania postępowań prawnych.

Tabela 5 pokazuje, że w większości przypadków krajowe organy nadzorcze odpowiedzialne za monitorowanie wdrażania i stosowania przepisów ogólnych dotyczących ochrony danych są odpowiedzialne za nadzór nad wdrażaniem i stosowaniem decyzji ramowej 2008/977.

Szwecja wskazała, że nadal nie wyznaczono Urzędu nadzoru danych jako właściwego organu nadzorczego na podstawie art. 25 decyzji ramowej.

Niektóre państwa członkowskie wyraźnie podniosły kwestię nadzoru nad danymi przetwarzanymi przez wymiar sprawiedliwości[17]. Dania wskazała, że odpowiedzialny za nadzór nad przetwarzaniem danych jest sąd administracyjny, a Austria zauważyła, że organ nadzorczy ds. ochrony danych nie jest właściwy do podejmowania decyzji dotyczących skarg na temat naruszenia przepisów ochrony danych przez sądownictwo. W Luksemburgu nadzór nad przetwarzaniem jest objęty właściwością Komisji ds. ochrony danych. Działania związane z przetwarzaniem, wykonywane w ramach krajowych przepisów wdrażających międzynarodową konwencję, są nadzorowane przez organ składający się z *Procureur Général d'Etat* lub osoby przez niego upoważnionej oraz dwóch członków Komisji ds. ochrony danych, których kandydatury zostały przez niego wniesione, i powołanych przez ministra.

2.1.5. Inne kwestie zasygnalizowane przez państwa członkowskie

Z 26 państw członkowskich, 20 – z których 8 w ogóle nie odpowiedziało na to pytanie (Belgia, Dania, Estonia, Grecja, Węgry, Luksemburg, Cypr i Austria) – nie wskazało na żadne szczególne problemy dotyczące decyzji ramowej. Sześć państw członkowskich przedstawiło komentarze na temat kwestii uznanych przez nie za problemowe, co zostało zaprezentowane w tabeli 6. Obejmują one poniższe kwestie.

- Polska uznała, że decyzja ramowa jest obarczona licznymi błędami, które należy naprawić i wyraziła poparcie dla reformy w celu ustanowienia kompleksowego i spójnego systemu ochrony danych osobowych na poziomie UE;

- Włochy i Niderlandy poinformowały o trudnościach w wyodrębnieniu w praktyce przetwarzania danych w kontekście transgranicznym na podstawie decyzji ramowej 2008/977 od przetwarzania na poziomie krajowym i o związanych z tym trudnościach dla organów ścigania w państwach członkowskich, które muszą radzić sobie z różnymi zasadami przetwarzania tych samych danych osobowych.

---

[17] Zobacz motyw 35, ostatnie zdanie, decyzji ramowej, wskazujący, że uprawnienia organów nadzorczych „nie powinny kolidować ze szczególnymi zasadami określonymi w odniesieniu do postępowań karnych ani z niezawisłością wymiaru sprawiedliwości".

- Włochy, Republika Czeska i Niderlandy zaprezentowały krytyczne stanowisko wobec zasad dotyczących międzynarodowego przekazywania włączonych do decyzji ramowej. Włochy wskazały w szczególności na potrzebę zapewnienia odpowiedniego i bardziej jednolitego poziomu ochrony danych w przypadku przekazywania ich do państw trzecich. Niderlandy uznały za kwestię problemową niewłączenie do decyzji ramowej kryteriów pozwalających na określenie odpowiedniego poziomu ochrony w państwie trzecim, co prowadzi do jej niejednolitego wdrażania przez państwa członkowskie. Republika Czeska uznała ostatecznie zasady dotyczące międzynarodowego przekazywania w decyzji ramowej za „nierealistyczne";

- Francja odniosła się do konkretnego problemu na poziomie krajowym dotyczącego przechowywania danych przekazanych z i do państwa trzeciego mającego inne wymogi w tym zakresie; - Słowacja stwierdziła, że niezbędne jest bardziej szczegółowe wyodrębnienie przetwarzania danych przez policję od przetwarzania przez wymiar sprawiedliwości (postępowanie sądowe);

- Zarówno Republika Czeska, jak i Niderlandy, wskazały, że konieczność uwzględniania licznych przepisów dotyczących ochrony danych na poziomie międzynarodowym (takim jak Rada Europy), unijnym i krajowym dezorientuje organy ścigania.

3. ZADANIA DO WYKONANIA

Niniejsze sprawozdanie podsumowuje wdrażanie i funkcjonowanie decyzji ramowej w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych.

Trudności praktyczne, których doświadczyła pewna liczba państw członkowskich przy wyodrębnianiu przetwarzania na poziomie krajowym od przetwarzania w kontekście transgranicznym, mogą być rozwiązane poprzez przyjęcie jednolitego zbioru przepisów obejmujących przetwarzanie danych zarówno na poziomie krajowymi, jak i w kontekście transgranicznym. Kwestia zakresu oraz ewentualnych odstępstw na poziomie UE w odniesieniu do prawa podmiotów danych do informacji wymaga dalszego wyjaśnienia. Minimalne zharmonizowane kryteria dotyczące prawa dostępu podmiotów danych mogłyby wzmocnić prawa podmiotów danych, przy jednoczesnym zapewnieniu odstępstw, aby umożliwić policji i wymiarowi sprawiedliwości właściwe wykonywanie ich zadań.

Na podstawie art. 16 Traktatu o funkcjonowaniu Unii Europejskiej, do którego wpisano prawo do ochrony danych osobowych, istnieje obecnie możliwość ustanowienia kompleksowych ram ochrony danych, zapewniających zarówno wysoki poziom ochrony danych osób fizycznych w dziedzinie współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych, jak i łatwiejszą wymianę danych osobowych między organami policji i wymiaru sprawiedliwości państw członkowskich, przy pełnym poszanowaniu zasady pomocniczości.