KOMISJA WSPÓLNOT EUROPEJSKICH

Bruksela, dnia 4.10.2005
COM(2005) 475 końcowy

2005/0202 (CNS)

Wniosek

DECYZJA RAMOWA RADY

w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych

{SEC(2005) 1241}

(przedstawiona przez Komisję)

UZASADNIENIE

1) KONTEKST WNIOSKU

- **Podstawa i cele wniosku**

Dnia 4 listopada 2004 r. Rada Europejska przyjęła Program Haski mający na celu wzmacnianie wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej[1]. W programie tym Komisję wezwano do przedstawienia najpóźniej do końca roku 2005 wniosków w sprawie wprowadzania w życie zasady udostępniania informacji w celu usprawnienia transgranicznej wymiany między Państwami Członkowskimi informacji istotnych dla ochrony porządku publicznego. W Programie Haskim podkreślono fakt, że we wnioskach tych należy ściśle przestrzegać kluczowych warunków w zakresie ochrony danych.

W czerwcu 2005 r. Rada i Komisja przyjęły plan działania służący realizacji Programu Haskiego[2]. Plan ten został opracowany w oparciu o komunikat Komisji do Rady i Parlamentu Europejskiego – Program Haski: Dziesięć priorytetów na najbliższe pięć lat. Partnerstwo na rzecz odnowy europejskiej w dziedzinie wolności, bezpieczeństwa i sprawiedliwości[3]. Zgodnie z wyżej wymienionym planem działania Komisja przedstawia *w 2005 r. wnioski 1) w sprawie ustanowienia zasady udostępniania informacji istotnych dla ochrony porządku publicznego oraz 2) w sprawie odpowiedniej ochrony praw i skutecznych środków prawnych w kontekście przekazywania danych osobowych dla celów współpracy policyjnej i sądowej w sprawach karnych.* Dnia 13 lipca 2005 r. Rada (Wymiar Sprawiedliwości i Sprawy Wewnętrzne) w swoim oświadczeniu w sprawie odpowiedzi UE na zamachy terrorystyczne w Londynie[4] wezwała Komisję do przedstawienia tych wniosków do października 2005 r.

Niniejsza decyzja ramowa zapewnia ochronę danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych między Państwami Członkowskimi Unii Europejskiej (Traktat UE, tytuł VI). Ma ona na celu usprawnienie tej współpracy, w szczególności w odniesieniu do zapobiegania terroryzmowi i jego zwalczania, przy ścisłym przestrzeganiu kluczowych warunków w zakresie ochrony danych. Decyzja ta zapewnia przestrzeganie praw podstawowych, poświęcając szczególną uwagę prawu do prywatności i do ochrony danych osobowych, na całym obszarze Unii Europejskiej, w szczególności w celu wprowadzenia w życie zasady udostępniania informacji. Celem jej jest również zagwarantowanie, że różnice w poziomie ochrony danych w poszczególnych Państwach Członkowskich nie będą utrudniać wymiany istotnych informacji między Państwami Członkowskimi.

- **Kontekst ogólny**

Z inicjatywy Włoch[5] ochrona danych osobowych w ramach trzeciego filaru została poddana dyskusji już w roku 1998. W tamtym czasie Rada ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych przyjęła tak zwany wiedeński plan działania[6]. Przewidywał on, że – w związku z horyzontalnymi problemami w kontekście współpracy policyjnej i sądowej w sprawach karnych – możliwości zharmonizowania zasad w zakresie ochrony danych powinny zostać zbadane w ciągu dwóch lat od wejścia w życie Traktatu. Jednakże w 2001 r. projekt

---

1 Dz.U. C 53 z 3.3.2005, str. 1.
2 Dz.U. C 198 z 12.8.2005, str. 1.
3 COM(2005) 184 z 10.5.2005, Bruksela.
4 Dokument roboczy Rady 11158/1/05 REV 1 JAI 255.
5 Dokument roboczy Rady 8321/98JAI 15.
6 Dz.U. C 19 z 23.1.1999, str. 1.

rezolucji w sprawie ochrony danych osobowych w aktach prawnych dotyczących trzeciego filaru Unii Europejskiej nie został przyjęty[7]. W czerwcu 2003 r. sprawująca prezydencję Grecja zaproponowała wykaz ogólnych zasad w zakresie ochrony danych osobowych w trzecim filarze[8], opracowanych w nawiązaniu do dyrektywy o ochronie danych osobowych 95/46/WE oraz do Karty Praw Podstawowych Unii Europejskiej. W 2005 r. organy ds. ochrony danych Państw Członkowskich Unii Europejskiej, wraz z Europejskim Inspektorem Ochrony Danych (zwanym dalej EIOD), wyraziły silne poparcie dla nowego aktu prawnego w zakresie ochrony danych osobowych w trzecim filarze[9]. Parlament Europejski zalecił harmonizację istniejących zasad z zakresu ochrony danych osobowych w odniesieniu do aktów prawnych trzeciego filaru poprzez zebranie ich w jednym akcie prawnym, który zagwarantuje ten sam poziom ochrony danych, jaki został zapewniony w ramach pierwszego filaru[10].

Zgodnie z Programem Haskim wprowadzenie zasady udostępniania informacji jest zależne od kluczowych warunków w zakresie ochrony danych. Rada Europejska uznała w sposób oczywisty, że istniejące obecnie na poziomie europejskim przepisy z zakresu ochrony danych nie są wystarczające do celów wprowadzania w życie zasady udostępniania informacji, która może obejmować ustalenia takie jak wzajemny dostęp do krajowych baz danych i ich interoperacyjność czy dostęp bezpośredni (przez Internet).

Obawy co do wystarczającego poziomu ochrony danych znalazły również odzwierciedlenie w umowie o współpracy, która została podpisana przez siedem Państw Członkowskich (Niemcy, Austrię, Belgię, Niderlandy, Luksemburg, Francję i Hiszpanię) dnia 27 maja 2005 r. w Prüm i którą te państwa zalecają jako wzór ustaleń w zakresie wymiany informacji między Państwami Członkowskimi Unii jako całości. Umowa ta zapewnia, przy spełnieniu szczególnych warunków, organom porządku publicznego jednej z Umawiających się Stron bezpośredni zautomatyzowany dostęp do danych osobowych, jakimi dysponuje inna Umawiająca się Strona. Jednak tej formy współpracy nie stosuje się, zanim określone w umowie przepisy z zakresu ochrony danych nie zostaną przetransponowane do prawa krajowego Stron.

- **Obowiązujące przepisy w dziedzinie, której dotyczy wniosek**

Karta Praw Podstawowych Unii Europejskiej[11] wyraźnie potwierdza prawo do prywatności (art. 7) oraz prawo do ochrony danych osobowych (art. 8). Dane te muszą być przetwarzane rzetelnie, w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej prawem. Każda osoba ma prawo dostępu do zebranych danych, które jej dotyczą, i prawo do dokonania ich sprostowania. Przestrzeganie tych zasad podlega kontroli niezależnego organu.

Dyrektywa 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

---

7 Dokument Roboczy Rady 6316/2/01 REV 2 JAI 13.

8 2514. posiedzenie Rady, Wymiar Sprawiedliwości i Sprawy Wewnętrzne, Luksemburg, 5-6 czerwca 2003 r., dokument Rady 9845/03 (Presse 150), str. 32.

9 Dokument będący deklaracją i przedstawiający stanowisko w sprawie egzekwowania prawa i wymiany informacji w UE, przyjęty na wiosennej konferencji europejskich organów ds. ochrony danych w Krakowie w dniach 25-26 kwietnia 2005 r.

10 Nr 1 h zalecenia Parlamentu Europejskiego dla Rady Europejskiej i Rady w sprawie wymiany informacji i współpracy dotyczących przestępstw terrorystycznych (2005/2046(INI)), przyjętego dnia 7 czerwca 2005 r.

11 Dz.U. C 364 z 18.12.2000, str. 1, 10.

przepływu tych danych[12] zawiera podstawowe zasady dotyczące zgodnego z prawem przetwarzania danych osobowych jak również praw podmiotu danych. Dyrektywa ta zawiera przepisy dotyczące środków sądowych, odpowiedzialności i sankcji, transferu danych osobowych do krajów trzecich, kodeksów postępowania, poszczególnych organów nadzorczych i grupy roboczej oraz wspólnotowych środków wykonawczych. Jednakże wyżej wymienionej dyrektywy nie stosuje się w odniesieniu do działań, które nie są objęte prawem wspólnotowym, jak to ma miejsce w przypadku działań określonych w tytule VI Traktatu o Unii Europejskiej (Traktatu UE). Państwa Członkowskie mają zatem prawo do decydowania w swoim imieniu w sprawie właściwych standardów ochrony i przetwarzania danych. W kontekście tytułu VI Traktatu UE ochrona danych osobowych określona jest w ramach różnych, szczególnych aktów prawnych. W szczególności w ramach aktów prawnych, które ustanawiają wspólne systemy informacyjne na poziomie europejskim, takich jak: Konwencja Wykonawcza do Układu z Schengen z 1990 r., zawierająca przepisy szczególne z zakresu ochrony danych mające zastosowanie do Systemu Informacyjnego Schengen[13]; Konwencja o Europolu z 1995 r.[14] wraz z, między innymi, zasadami regulującymi przekazywanie danych osobowych przez Europol państwom trzecim i instytucjom trzecim[15]; decyzja ustanawiająca Eurojust z 2002 r.[16] wraz z przepisami regulaminu wewnętrznego Eurojustu dotyczącymi przetwarzania i ochrony danych osobowych[17]; Konwencja w sprawie wykorzystania technologii informatycznych do celów odpraw celnych z 1995 r., zawierająca przepisy z zakresu ochrony danych osobowych mające zastosowanie do Systemu Informacji Celnej[18]; oraz Konwencja o wzajemnej pomocy w sprawach karnych pomiędzy Państwami Członkowskimi Unii Europejskiej z 2000 r., w szczególności art. 23[19]. W odniesieniu do Systemu Informacyjnego Schengen należy zwrócić szczególną uwagę na ustanowienie, działanie i użycie Systemu Informacyjnego Schengen drugiej generacji (SIS II), na temat którego Komisja już przedstawiła wnioski w sprawie decyzji Rady[20] i dwóch rozporządzeń[21].

Ponadto należy zwrócić szczególną uwagę na art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności oraz na Konwencję Rady Europy nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z 1981 r., na jej protokół dodatkowy z 2001 r. odnoszący się do organów nadzoru i transgranicznego przepływu danych oraz na zalecenie nr R (87) 15 z 1987 r. regulujące wykorzystanie danych osobowych w sektorze policji. Wszystkie Państwa Członkowskie są stronami Konwencji, ale nie wszystkie są stronami protokołu dodatkowego.

---

12 Dz.U. L 281 z 23.11.1995, str. 31.
13 Dz.U. L 239 z 22.9.2000, str. 19.
14 Dz.U. C 316 z 27.11.1995, str. 2.
15 Dz.U. C 88 z 30.3.1999, str. 1.
16 Dz.U. L 63 z 6.3.2002, str. 1.
17 Dz.U. C 68 z 19.3.2005, str. 1.
18 Dz.U. C 316 z 27.11.1995, str. 34.
19 Dz.U. C 197 z 12.7.2000, str. 1, 15.
20 COM(2005) 230.
21 COM(2005) 236, COM(2005) 237.

- **Spójność z innymi politykami i celami Unii**

Należy zdać sobie sprawę ze specyfiki przetwarzania danych i ochrony danych w ramach stosowania przepisów tytułu VI Traktu o Unii Europejskiej. Z jednej strony, działania te nie powinny podważać spójności z polityką ogólną Unii w kwestii prywatności i ochrony danych zgodnie z Kartą Praw Podstawowych UE i dyrektywą 95/46/WE. Podstawowe zasady ochrony danych mają zastosowanie do przetwarzania danych w pierwszym i trzecim filarze. Ponadto należy zapewnić spójność z innymi aktami prawnymi, określając szczególne zobowiązania związane z informacjami, co do których istnieje prawdopodobieństwo, że okażą się istotne dla celów zapobiegania i zwalczania przestępczości. Należy śledzić rozwój sytuacji w odniesieniu do zachowywania przetwarzanych i przechowywanych danych w związku ze świadczeniem publicznie dostępnych usług łączności elektronicznej lub dostarczaniem danych na temat publicznych sieci łączności do celów zapobiegania przestępstwom, ich ścigania, wykrywania i karania, w tym również terroryzmu. Należy uwzględnić w szczególności bliski związek między niniejszym wnioskiem w sprawie decyzji ramowej a wnioskiem Komisji w sprawie dyrektywy Parlamentu Europejskiego i Rady dotyczącej przechowywania przetwarzanych danych w związku ze świadczeniem publicznie dostępnych usług łączności elektronicznej, zmieniającej dyrektywę 2002/58/WE[22].

2) KONSULTACJE Z ZAINTERESOWANYMI STRONAMI ORAZ OCENA SKUTKÓW

- **Konsultacje z zainteresowanymi stronami**

Metody konsultacji, główne sektory objęte konsultacjami i ogólny profil respondentów

Dnia 22 listopada 2004 r. i 21 czerwca 2005 r. Komisja zaprosiła ekspertów rządowych z Państw Członkowskich, Islandii, Norwegii i Szwajcarii i przeprowadziła z nimi konsultacje, zaś dnia 11 stycznia 2005 r. zasięgnęła opinii organów ds. ochrony danych tych państw. Obecni byli również przedstawiciele EIOD, Europolu, Eurojustu oraz sekretariatu wspólnych organów nadzoru. Główny cel konsultacji stanowiło znalezienie odpowiedzi na pytanie, czy istnieje potrzeba ustanowienia aktu prawnego w zakresie przetwarzania i ochrony danych osobowych w trzecim filarze oraz, w przypadku odpowiedzi twierdzącej, jaka powinna być istota tego typu aktu. Komisja zasięgnęła opinii stron, z którymi przeprowadzała konsultacje, posługując się między innymi kwestionariuszem i dokumentem do dyskusji, w kwestii ich stanowiska w sprawie ogólnej zawartości nowego aktu prawnego i jego związku z istniejącymi aktami prawnymi, podstawy prawnej, możliwego zakresu, zasad odnoszących się do jakości danych, kryteriów zgodności z prawem przetwarzania danych przez organy policyjne lub sądowe, danych osobowych osób niebędących podejrzanymi, wymogów odnośnie przekazywania danych osobowych właściwym organom w innych Państwach Członkowskich i w krajach trzecich, praw podmiotu danych, organów nadzoru i ewentualnego organu doradczego w zakresie ochrony danych w trzecim filarze.

Grupa robocza utworzona zgodnie z art. 29 dyrektywy 95/46/WE była regularnie informowana o podejmowanych krokach. Dnia 12 kwietnia i 21 czerwca 2005 r. Komisja wzięła udział w spotkaniach policyjnej grupy roboczej na konferencji europejskich organów ds. ochrony danych. Dnia 31 stycznia 2005 r. Komisja uczestniczyła w „Publicznym Seminarium: ochrona danych a bezpieczeństwo obywateli: jakie zasady dla Unii Europejskiej?" zorganizowanym przez Komitet ds. swobód obywatelskich, sprawiedliwości i spraw wewnętrznych. Komisja wzięła po uwagę wyniki wiosennej konferencji europejskich organów ds. ochrony danych, mającej miejsce w Krakowie w dniach 25-26 kwietnia 2005 r.,

[22] COM(2005) 438 z 21.9.2005.

oraz stanowisko Parlamentu Europejskiego określone między innymi w zaleceniu Parlamentu Europejskiego dla Rady Europejskiej i Rady w sprawie wymiany informacji i współpracy dotyczących przestępstw terrorystycznych (2005/2046(INI)) przyjętym dnia 7 czerwca 2005 r.

Streszczenie odpowiedzi oraz sposób ich uwzględnienia

Zarówno Parlament Europejski jak i organy ds. ochrony danych w Unii Europejskiej udzielają silnego poparcia idei ustanowienia aktu prawnego dotyczącego ochrony danych osobowych w trzecim filarze. Przedstawiciele rządów Państw Członkowskich oraz Islandii, Norwegii i Szwajcarii, a także Europolu i Eurojustu nie wyrazili wspólnego stanowiska w tym względzie. Jednakże Komisja może wnosić, że nie wyrażono żadnego istotnego sprzeciwu wobec idei ustanowienia takiego aktu. Wydaje się, że panowała zgodność co do tego, że wprowadzeniu w życie zasady udostępniania informacji muszą dla równowagi towarzyszyć właściwe zasady w zakresie ochrony danych. Niektóre Państwa Członkowskie uznały, że najpierw należy określić stosowany w przyszłości sposób wymiany informacji, a dopiero potem ustalić zasady dotyczące ochrony danych osobowych. Inne wolały włączyć wykaz przepisów szczególnych do aktu w sprawie zasady udostępniania informacji.

Rozważywszy różne opinie, Komisja staje na stanowisku, że wprowadzenie w życie zasady udostępniania informacji doprowadzi do dalszego rozwoju i zasadniczej zmiany jakości i intensywności wymiany informacji między Państwami Członkowskimi. Rozwój taki będzie miał znaczący wpływ na dane osobowe i prawo do ochrony danych. Należy zatem zapewnić mu odpowiednią przeciwwagę. Niedawne inicjatywy w kwestii zapewnienia bezpośredniego, zautomatyzowanego dostępu – przynajmniej na zasadzie wynik/brak wyników – prawdopodobnie prowadziłyby do zwiększenia ryzyka wymiany bezprawnie przechowywanych, nieścisłych czy nieaktualnych danych, co musi zostać wzięte pod uwagę. Inicjatywy te wiążą się z tym, że kontroler danych nie będzie już w stanie sprawdzać *w każdym, osobnym przypadku* zgodności z prawem przekazania danych oraz ich ścisłości. W konsekwencji należy jednocześnie wprowadzić ścisłe zobowiązania do ciągłego utrzymywania i sprawdzania jakości danych, do których przyznano bezpośredni, zautomatyzowany dostęp.

Wziąwszy pod uwagę w szczególności skutki wprowadzenia w życie zasady udostępniania informacji, przepisy uwzględniające wyłącznie poszczególne aspekty ochrony danych są niewystarczające. Akt prawny w sprawie ochrony danych osobowych w trzecim filarze może przyczynić się zasadniczo do umacniania współpracy policyjnej i sądowej w sprawach karnych, jeśli skuteczność zostanie uwzględniona w równym stopniu, co zgodność z prawem i z prawami podstawowymi, a w szczególności z prawem do ochrony danych osobowych.

W szczególności pod względem wprowadzania w życie zasady udostępniania informacji taki akt prawny jest szczególnie konieczny i musi zostać opracowany równolegle z wprowadzeniem w życie tej zasady. Niniejsza decyzja ramowa powinna nawiązywać w formie i treści do dyrektywy 95/46/WE na ile tylko to możliwe, przy jednoczesnym uwzględnieniu szczególnych potrzeb w zakresie współpracy policyjnej i sądowej w sprawach karnych oraz w świetle zasady proporcjonalności. Zalecenie Rady Europy nr R(87)15 regulujące wykorzystanie danych osobowych w sektorze policji z 1987 r. zostało wzięte pod uwagę w celu transponowania jego głównych zasad do wiążących prawnie przepisów na poziomie UE. Należy ustanowić jasne zasady w zakresie ochrony danych osobowych, które zostaną lub zostały udostępnione właściwym organom innych Państw Członkowskich. Wiąże się to z ustanowieniem systemu zapewniającego jakość przetwarzania określonych danych. System taki musi obejmować przepisy określające właściwe prawa podmiotu danych oraz

uprawnienia organów nadzoru, gdyż istnieje prawdopodobieństwo, że korzystanie z tych praw i uprawnień przyczyni się do jakości danych, których dotyczy.

- **Ocena skutków**

Wzięto pod uwagę następujące opcje: stosowanie dyrektywy 95/46/WE; brak wniosku lub późniejszy wniosek w sprawie ochrony danych osobowych w trzecim filarze; ograniczony zestaw przepisów szczególnych w akcie prawnym dotyczącym wymiany informacji zgodnie z zasadą udostępniania informacji; decyzja ramowa w sprawie ochrony danych osobowych w trzecim filarze. Przy uwzględnieniu ostatniej opcji zbadano, czy tego typu akt prawny powinien również mieć zastosowanie do wymiany informacji za pośrednictwem systemów informatycznych i organów ustanowionych na poziomie UE.

Podstawowe i wyczerpujące przepisy dyrektywy 95/46/WE nie mają zastosowania w trzecim filarze, zgodnie z tym, co zostało określone w art. 3 ust. 2. Nawet skreślenie tego artykułu nie mogłoby automatycznie skutkować możliwością zastosowania dyrektywy do współpracy policyjnej i sądowej w sprawach karnych. Po pierwsze, w dyrektywie tej nie zostały w pełni wzięte pod uwagę szczególne aspekty tej współpracy; aspekty te wymagałyby większej dokładności. Po drugie, należy przestrzegać wymagań co do legislacji, objętych przepisami tytułu VI Traktatu o Unii Europejskiej, które mają na celu umocnienie współpracy policyjnej i sądowej w sprawach karnych. Opcję braku wniosku lub późniejszego wniosku w sprawie ochrony danych osobowych w trzecim filarze należy wykluczyć. Istnieje prawdopodobieństwo, że opcja ta wiązałaby się z wprowadzeniem nowych form wymiany informacji wraz z wprowadzeniem w życie zasady udostępniania informacji, z pominięciem zapewnienia ścisłego przestrzegania kluczowych warunków w zakresie ochrony danych. Ograniczony zestaw przepisów szczególnych w akcie prawnym dotyczącym wymiany informacji w ramach zasady udostępniania informacji jest niewystarczający, wziąwszy pod uwagę prawdopodobny wpływ tej ostatniej. Decyzja ramowa w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych jest jedyną w pełni zadowalającą opcją. Opcja ta prawdopodobnie nie będzie źródłem znaczących, jeśli w ogóle jakichkolwiek, kosztów administracyjnych dla Państw Członkowskich.

Komisja dokonała oceny skutków; ocena ta figuruje w programie pracy, a sprawozdanie na temat oceny skutków dostępne jest na stronie http://europa.eu.int/comm/dgs/justice_home/evaluation/dg_coordination_evaluation_annexe_en.htm.

3) ASPEKTY PRAWNE WNIOSKU

- **Streszczenie proponowanych działań**

Proponowana decyzja ramowa obejmuje ogólne zasady dotyczące zgodnego z prawem przetwarzania danych osobowych, przepisy dotyczące szczególnych form przetwarzania (przekazywanie i udostępnianie danych osobowych właściwym organom innych Państw Członkowskich, dalsze przetwarzanie, a w szczególności dalsze przekazywanie danych otrzymanych od właściwych organów innych Państw Członkowskich lub udostępnionych przez te ostatnie), praw podmiotu danych, poufności i bezpieczeństwa w odniesieniu do przetwarzania, środków sądowych, odpowiedzialności, sankcji, organów nadzorczych i grupy roboczej ds. ochrony osób w zakresie przetwarzania danych osobowych do celów zapobiegania przestępstwom, ich ścigania, wykrywania i karania. Należy zwrócić szczególną uwagę na zasadę, zgodnie z którą transfer danych osobowych jest dokonywany wyłącznie do tych krajów trzecich i organów międzynarodowych, które zapewniają odpowiedni poziom

ochrony. Decyzja ramowa przewiduje określony mechanizm, którego celem jest zapewnienie przestrzegania tej zasady w całej UE.

- **Podstawa prawna**

Niniejsza decyzja ramowa oparta jest na art. 30, art. 31 oraz art. 34 ust. 2, lit. b) Traktatu o Unii Europejskiej. W szczególności w świetle wprowadzenia zasady udostępniania informacji, właściwe przepisy dotyczące przetwarzania i ochrony danych osobowych, włącznie ze wspólnymi normami przekazywania danych osobowych krajom trzecim i organom międzynarodowym, mają zasadnicze znaczenie dla usprawnienia współpracy policyjnej i sądowej w sprawach karnych, w szczególności w walce przeciw terroryzmowi i poważnym przestępstwom. Ponadto Państwa Członkowskie w pełni zaufają sobie nawzajem jedynie, jeśli będą istnieć jasne, wspólne zasady w zakresie ewentualnego dalszego przekazywania podlegających wymianie danych innym stronom, w szczególności krajom trzecim. Proponowane przepisy gwarantują, że różnice w poziomie ochrony w poszczególnych Państwach Członkowskich nie będą stawać na przeszkodzie wymianie informacji między właściwymi organami.

- **Zasady pomocniczości i proporcjonalności**

Niniejsza decyzja ramowa dotyczy sytuacji, które są szczególnie istotne dla współpracy policyjnej i sądowej w sprawach karnych między Państwami Członkowskimi, w szczególności w odniesieniu do wymiany informacji mającej na celu zapewnienie i promowanie skutecznych i zgodnych z prawem środków w zakresie zapobiegania i zwalczania przestępczości, w szczególności w odniesieniu do poważnych przestępstw i terroryzmu, we *wszystkich* Państwach Członkowskich. Rozwiązania na poziomie krajowym, dwustronnym czy wielostronnym mogą okazać się pomocne w przypadku poszczególnych Państw Członkowskich, ale nie uwzględniają konieczności zapewnienia bezpieczeństwa wewnętrznego na terenie całej Unii. Zapotrzebowanie na informacje ze strony organów porządku publicznego zależy w dużym stopniu od poziomu integracji między państwami. Przewiduje się nasilenie wymiany informacji między Państwami Członkowskimi do celów egzekwowania prawa i z tego względu należy ją uzupełnić o spójne zasady przetwarzania danych i ochrony danych. Niniejsza decyzja ramowa w pełni przestrzega zasady pomocniczości, określonej w art. 2 Traktatu o Unii Europejskiej oraz art. 5 Traktatu ustanawiającego Wspólnotę Europejską, gdyż celem jej jest zbliżenie przepisów ustawowych i wykonawczych Państw Członkowskich, czego nie mogą osiągnąć w sposób wystarczający Państwa Członkowskie działające jednostronnie i co wymaga wspólnych działań na poziomie Unii Europejskiej. Zgodnie z zasadą proporcjonalności, określoną w ostatnim z wymienionych artykułów, niniejsza decyzja nie wykracza poza to, co jest konieczne do osiągnięcia zamierzonego celu. W szczególności niniejsza decyzja dotyczy przetwarzania danych osobowych tylko w przypadku, gdy są one istotne dla celów współpracy policyjnej i sądowej w sprawach karnych.

- **Wybór instrumentów prawnych**

Proponowany instrument: decyzja ramowa. Niniejszy akt prawny ma na celu zbliżenie przepisów ustawowych i wykonawczych Państw Członkowskich w odniesieniu do ochrony danych osobowych przetwarzanych w celu zapobiegania i zwalczania przestępczości.

4) NASTĘPSTWA BUDŻETOWE

Wprowadzenie w życie proponowanej decyzji ramowej wiąże się jedynie z niskimi dodatkowymi wydatkami administracyjnymi, które zostaną pokryte z budżetu Wspólnot Europejskich, przeznaczonymi na spotkania i obsługę sekretariatu komitetu i organu doradczego, które mają zostać ustanowione zgodnie z art. 16 i 31.

2005/0202 (CNS)

Wniosek

DECYZJA RAMOWA RADY

w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych

KOMISJA WSPÓLNOT EUROPEJSKICH,

uwzględniając Traktat ustanawiający Unię Europejską, w szczególności jego art. 30, art. 31 i art. 34 ust. 2 lit. b),

uwzględniając wniosek Komisji[23],

uwzględniając opinię Parlamentu Europejskiego[24],

a także mając na uwadze, co następuje:

(1) Unia Europejska postawiła sobie za cel utrzymanie i rozwój Unii jako obszaru wolności, bezpieczeństwa i sprawiedliwości; wysoki poziom bezpieczeństwa zostanie zapewniony poprzez wspólne działanie Państw Członkowskich w zakresie współpracy policyjnej i sądowej w sprawach karnych.

(2) Wspólne działania w zakresie współpracy policyjnej zgodnie z art. 30 ust. 1 lit. b) Traktatu o Unii Europejskiej oraz wspólne działania w zakresie współpracy sądowej w sprawach karnych zgodnie z art. 31 ust. 1 lit. a) Traktatu o Unii Europejskiej pociągają za sobą konieczność przetwarzania istotnych informacji; przetwarzanie to powinno podlegać właściwym przepisom dotyczącym ochrony danych osobowych.

(3) Legislacja objęta zakresem stosowania przepisów tytułu VI Traktatu o Unii Europejskiej powinna umacniać współpracę policyjną i sądową w sprawach karnych, przy uwzględnieniu jej skuteczności jak również zgodności z prawem i z prawami podstawowymi, w szczególności z prawem do prywatności i do ochrony danych osobowych. Do osiągnięcia obu tych celów mogą się przyczynić wspólne normy dotyczące przetwarzania i ochrony danych osobowych przetwarzanych dla celów zapobiegania i zwalczania przestępczości.

(4) W Programie Haskim mającym na celu wzmacnianie wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej, przyjętym przez Radę Europejską dnia 4 listopada 2004 r., podkreślono potrzebę innowacyjnego stanowiska w sprawie transgranicznej wymiany informacji istotnych dla ochrony porządku publicznego przy ścisłym przestrzeganiu kluczowych warunków w zakresie ochrony danych oraz wezwano Komisję do przedstawienia najpóźniej do końca roku 2005 wniosków w tej sprawie. Znalazło to odzwierciedlenie w *planie działania Rady i Komisji służącym realizacji Programu Haskiego mającego na celu wzmacnianie wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej*[25].

---

23 …

24 …

25 Dz.U. C 198 z 12.8.2005, str. 1.

(5) Wymianę danych osobowych w ramach współpracy policyjnej i sądowej w sprawach karnych, zwłaszcza zgodnie z zasadą udostępniania informacji określoną w Programie Haskim, powinny wspierać jasne, wiążące przepisy umacniające wzajemne zaufanie właściwych organów oraz gwarantujące, że istotne informacje są chronione w sposób wykluczający jakiekolwiek czynniki stojące na przeszkodzie tej współpracy między Państwami Członkowskimi przy jednoczesnym pełnym przestrzeganiu praw podstawowych osób fizycznych. Obowiązujące akty prawne na poziomie europejskim nie wystarczają. Przepisy 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[26] nie mają zastosowania w odniesieniu do przetwarzania danych osobowych w trakcie prowadzenia działań, które nie są objęte zakresem stosowania prawa wspólnotowego, takich jak działania określone w tytule VI Traktatu o Unii Europejskiej, ani w żadnym przypadku do operacji przetwarzania dotyczących bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa i działań państwa w zakresie prawa karnego.

(6) Akt prawny dotyczący wspólnych norm w odniesieniu do ochrony danych osobowych przetwarzanych dla celów zapobiegania i zwalczania przestępczości powinien zachować spójność z ogólną polityką Unii Europejskiej w kwestii prywatności i ochrony danych. W miarę możliwości, uwzględniając konieczność polepszenia skuteczności zgodnych z prawem działań organów policyjnych, celnych i innych właściwych organów, akt ten powinien opierać się na istniejących i sprawdzonych zasadach i definicjach, w szczególności tych określonych w dyrektywie 95/46/WE Parlamentu Europejskiego i Rady lub odnoszących się do wymiany informacji przez Europol, Eurojust lub przetwarzania ich za pomocą Systemu Informacji Celnej czy innych porównywalnych instrumentów.

(7) Zbliżenie przepisów prawnych Państw Członkowskich nie powinno skutkować w żaden sposób osłabieniem zapewnianej przez nie ochrony danych, a wręcz przeciwnie – powinno mieć na celu zapewnienie wysokiego poziomu ochrony w obrębie Unii.

(8) Należy wyszczególnić cele ochrony danych w ramach działań policyjnych i sądowych oraz określić zasady dotyczące zgodności z prawem przetwarzania danych osobowych w celu zagwarantowania, że wszelkie informacje, które mogą podlegać wymianie, zostały przetworzone zgodnie z prawem i z podstawowymi zasadami odnoszącymi się do jakości danych. Jednocześnie nie powinno się w żaden sposób narażać zgodnych z prawem działań organów policyjnych, celnych, sądowych ani innych właściwych organów.

(9) Zapewnienie wysokiego poziomu ochrony danych osobowych obywateli Europy wymaga wspólnych przepisów w celu określenia zgodności z prawem i jakości danych przetwarzanych przez właściwe organy w innych Państwach Członkowskich.

(10) Wskazane jest określenie na szczeblu europejskim warunków, których muszą przestrzegać właściwe organy Państw Członkowskich, aby uzyskać zezwolenie na przekazywanie i udostępnianie danych osobowych organom i stronom prywatnym w innych Państwach Członkowskich.

(11) Dalsze przetwarzanie danych osobowych uzyskanych od właściwego organu innego Państwa Członkowskiego lub udostępnionych przez ten organ, w szczególności dalsze

---

[26] Dz.U. L 281 z 23.11.1995, str. 31.

przekazywanie lub udostępnianie tego typu danych, powinno podlegać wspólnym zasadom na szczeblu europejskim.

(12) W przypadku gdy Państwo Członkowskie Unii Europejskiej dokonuje transferu danych osobowych do krajów trzecich lub organów międzynarodowych, dane te powinny z zasady korzystać z odpowiedniego poziomu ochrony.

(13) Niniejsza decyzja ramowa powinna określać procedurę przyjmowania środków niezbędnych do dokonania oceny poziomu ochrony danych w danym kraju trzecim lub organie międzynarodowym.

(14) W celu zapewnienia takiej ochrony danych osobowych, która by nie zagrażała celom dochodzeń w sprawach karnych, konieczne jest określenie praw podmiotu danych.

(15) Wskazane jest ustanowienie wspólnych zasad w zakresie poufności i bezpieczeństwa w odniesieniu do przetwarzania, odpowiedzialności i sankcji w przypadku niezgodnego z prawem wykorzystania danych przez właściwe organy jak również środków sądowych udostępnionych podmiotowi danych. Ponadto konieczne jest, aby Państwa Członkowskie zapewniły sankcje karne w odniesieniu do szczególnie poważnych, umyślnie popełnionych naruszeń przepisów w zakresie ochrony danych.

(16) Ustanowienie przez Państwa Członkowskie organów nadzoru, pełniących swoje funkcje w sposób całkowicie niezależny, jest zasadniczym elementem ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej między Państwami Członkowskimi.

(17) Organy takie powinny dysponować niezbędnymi do wykonywania nałożonych na nie obowiązków środkami, obejmującymi kompetencje w zakresie przeprowadzania dochodzenia i podejmowania działań interwencyjnych, szczególnie w przypadku skarg ze strony osób fizycznych, oraz uprawnienia w zakresie występowania przed sądem. Organy te powinny pomagać w zapewnianiu przejrzystości przetwarzania danych w Państwach Członkowskich, których jurysdykcji podlegają. Jednakże kompetencje tych organów nie powinny kolidować ze szczególnymi zasadami określonymi w odniesieniu do postępowań karnych ani z niezawisłością wymiaru sprawiedliwości.

(18) Należy ustanowić grupę roboczą do spraw ochrony osób w zakresie przetwarzania danych osobowych do celów zapobiegania przestępstwom, ich ścigania, wykrywania i karania, która przy wypełnianiu swoich funkcji powinna zachować pełną niezależność. Powinna ona doradzać Komisji i Państwom Członkowskim oraz, w szczególności, przyczyniać się do jednolitego stosowania przepisów krajowych przyjętych zgodnie z niniejszą decyzją ramową.

(19) Artykuł 47 Traktatu o Unii Europejskiej stanowi, że żaden z tych przepisów nie narusza przepisów Traktatów ustanawiających Wspólnoty Europejskie ani kolejnych Traktatów lub aktów prawnych, które je zmieniają lub uzupełniają. Niniejsza decyzja ramowa nie wpływa również na ochronę danych osobowych na mocy prawa wspólnotowego, w szczególności nie narusza przepisów dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, rozporządzenia (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[27] ani dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych

[27] Dz.U. L 8 z 12.1.2001, str. 1.

osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[28].

(20) Niniejsza decyzja ramowa pozostaje bez uszczerbku dla przepisów szczególnych dotyczących ochrony danych określonych w odpowiednich aktach prawnych odnoszących się do przetwarzania i ochrony danych osobowych przez Europol, Eurojust i System Informacji Celnej.

(21) Przepisy odnoszące się do ochrony danych osobowych, określone w tytule IV Konwencji wykonawczej z roku 1990 do Układu z Schengen z dnia 14 czerwca 1985 r. w sprawie stopniowego znoszenia kontroli na wspólnych granicach (zwanej dalej „Konwencją z Schengen")[29], włączonej w ramy Unii Europejskiej na mocy Protokołu dołączonego do Traktatu o Unii Europejskiej oraz Traktatu ustanawiającego Wspólnotę Europejską, dla celów objętych zakresem stosowania Traktatu WE powinny zostać zastąpione przepisami niniejszej decyzji ramowej.

(22) Niniejsza decyzja ramowa powinna mieć zastosowanie do danych osobowych, które są przetwarzane w ramach Systemu Informacyjnego Schengen drugiej generacji, oraz związanej z nimi wymiany dodatkowych informacji zgodnie z decyzją JHA/2006/ … w sprawie utworzenia, działania i wykorzystania Systemu Informacyjnego Schengen drugiej generacji.

(23) Niniejsza decyzja ramowa pozostaje bez uszczerbku dla zasad odnoszących się do bezprawnego dostępu do danych, zgodnie z tym, co zostało przewidziane w decyzji ramowej Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[30].

(24) Należy zastąpić art. 23 Konwencji o wzajemnej pomocy w sprawach karnych pomiędzy Państwami Członkowskimi Unii Europejskiej[31].

(25) Wszelkie odniesienia do Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z dnia 28 stycznia 1981 r. powinny być rozumiane jako odniesienia do niniejszej decyzji ramowej.

(26) Z uwagi na fakt, że cele proponowanych działań, a mianowicie określenie wspólnych zasad w odniesieniu do ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, nie mogą być osiągnięte w sposób wystarczający przez Państwa Członkowskie działające osobno, natomiast mogą, z uwagi na zakres i skutki tych działań, zostać lepiej zrealizowane na poziomie Unii Europejskiej, Rada może przyjąć środki zgodnie z zasadą pomocniczości, która została określona w art. 5 Traktatu WE i o której mowa w art. 2 Traktatu UE. Zgodnie z zasadą proporcjonalności określoną w art. 5 Traktatu WE niniejsza decyzja ramowa nie wykracza poza to, co jest konieczne do osiągnięcia zamierzonych celów.

(27) Niniejsza decyzja ramowa ma zastosowanie do Zjednoczonego Królestwa zgodnie z art. 5 Protokołu włączającego dorobek Schengen w ramy Unii Europejskiej, załączonego do Traktatu UE i Traktatu WE, oraz art. 8 ust. 2 decyzji Rady 2000/365/WE z dnia 29 maja 2000 r. dotyczącej wniosku Zjednoczonego Królestwa

---

28 Dz.U. L 201 z 31.7.2001, str. 37.
29 Dz.U. L 239 z 22.9.2000, str. 19.
30 Dz.U. L 69 z 16.3.2005, str. 67.
31 Dz.U. C 197 z 12.7.2000, str. 3.

Wielkiej Brytanii i Irlandii Północnej o zastosowanie wobec nich niektórych przepisów dorobku Schengen[32].

(28) Niniejsza decyzja ramowa ma zastosowanie do Irlandii zgodnie z art. 5 Protokołu włączającego dorobek Schengen w ramy Unii Europejskiej załączonego do Traktatu o UE i Traktatu WE oraz art. 6 ust. 2 decyzji Rady 2002/192/WE z dnia 28 lutego 2002 r. dotyczącej wniosku Irlandii o zastosowanie wobec niej niektórych przepisów dorobku Schengen.

(29) W odniesieniu do Islandii i Norwegii niniejsza decyzja ramowa stanowi rozwinięcie przepisów dorobku Schengen, w rozumieniu Układu zawartego przez Radę Unii Europejskiej i Republikę Islandii oraz Królestwo Norwegii dotyczącego włączenia tych dwóch państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen, które mieszczą się w obszarze określonym w art. 1 pkt H decyzji Rady 1999/437/WE z dnia 17 maja 1999 r. w sprawie niektórych warunków stosowania tego Układu[33].

(30) W odniesieniu do Szwajcarii niniejsza decyzja stanowi rozszerzenie przepisów dorobku Schengen w rozumieniu umowy podpisanej przez Unię Europejską, Wspólnotę Europejską i Konfederację Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen, które mieszczą się w obszarze określonym w art. 1 pkt H decyzji Rady 1999/437/WE z dnia 17 maja 1999 r. rozumianym w powiązaniu z art. 4 ust. 1 decyzji Rady 2004/849/WE w sprawie podpisania w imieniu Unii Europejskiej oraz tymczasowego stosowania niektórych postanowień tej umowy[34].

(31) Niniejsza decyzja ramowa stanowi akt bazujący na dorobku Schengen lub jest z nim w inny sposób powiązana w rozumieniu art. 3 ust. 1 Aktu Przystąpienia z 2003 r.

(32) Niniejsza decyzja ramowa respektuje prawa podstawowe i przestrzega zasad uznanych w szczególności w Karcie Praw Podstawowych Unii Europejskiej. Niniejsza decyzja ramowa ma na celu zapewnienie pełnego poszanowania praw do prywatności i do ochrony danych osobowych określonych w art. 7 i 8 Karty Praw Podstawowych Unii Europejskiej,

PRZYJMUJE NINIEJSZĄ DECYZJĘ RAMOWĄ:

ROZDZIAŁ I
CEL, DEFINICJE I ZAKRES

Artykuł 1
Cel

1. Niniejsza decyzja ramowa określa wspólne normy w celu zapewnienia ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w ramach współpracy policyjnej i sądowej w sprawach karnych, określonej w tytule VI Traktatu o Unii Europejskiej.

2. Państwa Członkowskie gwarantują, że ujawnienie danych osobowych właściwym organom innych Państw Członkowskich nie podlega ograniczeniom ani nie jest

---

32 Dz.U. L 131 z 1.6.2000, str. 43.
33 Dz.U. L 176 z 10.7.1999, str. 31.
34 Dz.U. L 368 z 15.12.2004, str. 26.

zabronione ze względów związanych z ochroną danych osobowych, zgodnie z tym, co zostało określone w niniejszej decyzji ramowej.

Artykuł 2
Definicje

Do celów niniejszej decyzji ramowej pojęcie:

a) „dane osobowe" oznacza wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („podmiotu danych"); osoba możliwa do zidentyfikowania to taka osoba, która może być zidentyfikowana bezpośrednio lub pośrednio, w szczególności poprzez odniesienie do numerów identyfikacyjnych lub do jednego czy więcej znaków szczególnych związanych z jej tożsamością fizyczną, psychologiczną, psychiczną, ekonomiczną, kulturową czy społeczną;

b) „przetwarzanie danych osobowych" („przetwarzanie") oznacza każdą operację lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, takich jak gromadzenie, zapis, porządkowanie, przechowywanie, zmienianie lub przekształcanie, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie przez przekazanie, rozpowszechnianie lub udostępnianie w inny sposób, zestawianie lub kompilowanie, blokowanie, usuwanie lub niszczenie;

c) „zbiór danych osobowych" („zbiór") oznacza każdy uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów scentralizowanych, zdecentralizowanych, czy rozproszonych funkcjonalnie lub geograficznie;

d) „kontroler danych" oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, który samodzielnie lub wspólnie z innymi określa cele i sposoby przetwarzania danych osobowych; w przypadku gdy cele przetwarzania i stosowane środki określa prawo krajowe lub przepisy przyjęte zgodnie z tytułem VI Traktatu o Unii Europejskiej, kontroler danych lub szczegółowe kryteria potrzebne do jego wyznaczenia mogą zostać wyznaczone przepisami prawa krajowego lub przepisami na mocy tytułu VI Traktatu o Unii Europejskiej;

e) „przetwarzający dane" oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ przetwarzający dane osobowe w imieniu kontrolera danych;

f) „strona trzecia" oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ niebędący podmiotem danych, ani kontrolerem danych, ani przetwarzającym lub jedną z osób, które pod bezpośrednim zwierzchnictwem kontrolera danych lub przetwarzającego dane są upoważnione do przetwarzania danych;

g) „odbiorca" oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, któremu ujawniane są dane, bez względu na to, czy jest osobą trzecią czy nie;

h) „zgoda podmiotu danych" oznacza konkretne i świadome, dobrowolne wyrażenie przez podmiot danych przyzwolenia na przetwarzanie odnoszących się do niego danych osobowych;

i) „organy międzynarodowe" oznacza organy lub organizacje ustanowione na mocy międzynarodowych porozumień;

j) „właściwe organy" oznacza organy policyjne, celne, sądowe i inne właściwe organy Państw Członkowskich w rozumieniu art. 29 Traktatu o Unii Europejskiej.

Artykuł 3
Zakres stosowania

1. Niniejsza decyzja ramowa ma zastosowanie do przetwarzania danych osobowych w całości lub w części w sposób zautomatyzowany oraz innego przetwarzania danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych przez właściwe organy dla celów zapobiegania przestępstwom, ich ścigania, wykrywania i karania.

2. Przepisów niniejszej decyzji ramowej nie stosuje się w odniesieniu do przetwarzania danych osobowych przez

   – Europejski Urząd Policji (Europol),

   – Europejską Jednostkę Współpracy Sądowej (Eurojust),

   – System Informacji Celnej ustanowiony zgodnie z Konwencją sporządzoną na podstawie art. K.3 Traktatu o Unii Europejskiej w sprawie wykorzystania technologii informatycznych do celów odpraw celnych oraz zgodnie ze wszelkimi wniesionymi do niej zmianami.

ROZDZIAŁ II
OGÓLNE ZASADY ZGODNOŚCI Z PRAWEM PRZETWARZANIA DANYCH OSOBOWYCH

Artykuł 4
Zasady dotyczące jakości danych

1. Państwa Członkowskie stanowią, że dane osobowe muszą być:

   a) przetwarzane w sposób rzetelny i zgodny z prawem;

   b) gromadzone do konkretnych, jednoznacznych i zgodnych z prawem celów i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Dalsze przetwarzanie danych do celów historycznych, statystycznych lub naukowych nie jest uznane za niezgodne z tymi celami pod warunkiem, że Państwa Członkowskie zapewniają właściwe środki bezpieczeństwa;

   c) odpowiednie, istotne oraz nienadmierne w stosunku do celów, dla których są gromadzone lub przetwarzane dalej;

   d) ścisłe oraz, w miarę konieczności, aktualizowane. Należy podjąć wszelkie uzasadnione działania, aby zapewnić usunięcie lub poprawienie nieścisłych lub niekompletnych danych, biorąc pod uwagę cele, dla których zostały zgromadzone lub dla których są dalej przetwarzane, usuwane lub poprawiane. Państwa Członkowskie mogą rozróżniać przetwarzanie danych w zależności od różnych stopni ścisłości i wiarygodności – w takim przypadku muszą zapewnić wprowadzenie rozróżnienia danych zgodnie z charakteryzującym je stopniem ścisłości i wiarygodności, w szczególności oddzielenia danych opartych na faktach od danych opartych na opinii i prywatnych ocenach;

   e) przetrzymywane w formie, która pozwala na zidentyfikowanie podmiotów danych przez czas nie dłuższy, niż jest to konieczne do celów, dla których dane były gromadzone lub dla których są przetwarzane dalej. Państwa Członkowskie określają odpowiednie środki bezpieczeństwa w odniesieniu do

danych osobowych przechowywanych przez dłuższy czas do użytku historycznego, statystycznego lub naukowego.

2. Na kontrolerze danych spoczywa obowiązek zapewnienia przestrzegania przepisów ust. 1.

3. Państwa Członkowskie zapewniają wprowadzenie wyraźnego rozróżnienia między danymi osobowymi

   – osoby, która jest podejrzana o popełnienie przestępstwa lub udział w nim,

   – osoby, która została skazana za przestępstwo,

   – osoby, co do której istnieją poważne podstawy by sądzić, że popełni ona przestępstwo,

   – osoby, która może zostać wezwana na świadka podczas dochodzeń w związku z przestępstwami lub związanym z nimi postępowaniem karnym,

   – osoby, która była ofiarą przestępstwa lub której dotyczą pewne fakty pozwalające sądzić, że może ona stać się ofiarą przestępstwa,

   – osoby, która może dostarczyć informacji dotyczących przestępstwa,

   – osoby, która zapewnia kontakt z jedną z osób wymienionych powyżej lub jest jej wspólnikiem, oraz

   – osoby, która nie należy do żadnej z wyżej określonych kategorii.

4. Państwa Członkowskie stanowią, że przetwarzanie danych osobowych jest konieczne wyłącznie, jeśli:

   – istnieją oparte na ustalonych faktach, poważne podstawy by sądzić, że dane osobowe, których to dotyczy, umożliwiłyby, ułatwiłyby lub przyspieszyłyby zapobieganie przestępstwom, ich ściganie, wykrywanie lub karanie, oraz

   – nie istnieją żadne inne środki, które by wywierały mniejszy wpływ na podmiot danych oraz

   – przetwarzanie danych nie jest nadmierne w stosunku do przestępstwa, którego dotyczy.

Artykuł 5
Kryteria zapewniające zgodność przetwarzania danych z prawem

Państwa Członkowskie stanowią, że dane osobowe mogą być przetwarzane przez właściwe organy wyłącznie, jeśli jest to przewidziane przepisami stanowiącymi, że przetwarzanie jest konieczne do celów wypełniania zgodnych z prawem zadań danego organu oraz do celów zapobiegania przestępstwom, ich ścigania, wykrywania lub karania.

Artykuł 6
Przetwarzanie szczególnych kategorii danych

1. Państwa Członkowskie zabraniają przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych i danych dotyczących zdrowia lub życia seksualnego.

2. Ustęp 1 nie ma zastosowania, w przypadku gdy:

– przetwarzanie jest przewidziane prawem i bezwzględnie konieczne do wypełniania zgodnych z prawem zadań danego organu w celu zapobiegania przestępstwom, ich ścigania, wykrywania lub karania lub gdy podmiot danych udzielił wyraźnej zgody na przetwarzanie związanych z nim danych, oraz

– Państwa Członkowskie przewidują odpowiednie szczególne środki bezpieczeństwa, na przykład zapewnienie dostępu do określonych danych wyłącznie pracownikom, którzy są odpowiedzialni za wypełnianie zgodnych z prawem zadań, stanowiące uzasadnienie dla przetwarzania danych.

Artykuł 7
Terminy przechowywania danych osobowych

1. Państwa Członkowskie stanowią, że dane osobowe nie są przechowywane przez okres dłuższy, niż jest to konieczne do celów, dla których dane zostały zgromadzone, chyba że prawo krajowe stanowi inaczej. Dane osób, o których mowa w art. 4 ust. 3 tiret ostatnie, są przechowywane jedynie tak długo, jak jest to bezwarunkowo konieczne dla celów, dla których zostały zgromadzone.

2. Państwa Członkowskie przewidują odpowiednie środki proceduralne i techniczne, aby zapewnić przestrzeganie terminów przechowywania danych osobowych. Przestrzeganie tych terminów jest poddawane regularnym przeglądom.

ROZDZIAŁ III – Szczególne formy przetwarzania

SEKCJA I – PRZEKAZYWANIE I UDOSTĘPNIANIE DANYCH OSOBOWYCH WŁAŚCIWYM ORGANOM INNYCH PAŃSTW CZŁONKOWSKICH

Artykuł 8
Przekazywanie i udostępnianie danych osobowych właściwym organom innych Państw Członkowskich

Państwa Członkowskie stanowią, że dane osobowe mogą być przekazywane lub udostępniane właściwym organom innych Państw Członkowskich wyłącznie, jeśli jest to konieczne do wypełnienia zgodnych z prawem zadań danego organu przekazującego lub otrzymującego dane oraz do celów zapobiegania przestępstwom, ich ścigania, wykrywania lub karania.

Artykuł 9
Weryfikacja jakości przekazywanych lub udostępnianych danych

1. Państwa Członkowskie stanowią, że jakość danych osobowych jest poddawana weryfikacji najpóźniej przed ich przekazaniem lub udostępnieniem. W najszerszym możliwym zakresie, przy każdorazowym przekazaniu danych powinny być wskazane orzeczenia sądowe oraz decyzje niewyegzekwowane drogą sądową, a dane oparte na opiniach lub prywatnych ocenach powinny być sprawdzone u źródła przed przekazaniem informacji wraz ze wskazaniem stopnia ich ścisłości lub wiarygodności.

2. Państwa Członkowskie stanowią, że jakość danych osobowych, które są udostępniane w sposób bezpośredni i zautomatyzowany właściwym organom innych Państw Członkowskich, jest poddawana regularnym przeglądom w celu zagwarantowania tego, że udostępniane dane są ścisłe i zaktualizowane.

3. Państwa Członkowskie stanowią, że dane osobowe, które nie są już ścisłe lub aktualne, nie są przekazywane ani udostępniane.

4. Państwa Członkowskie stanowią, że właściwy organ, który przekazał lub udostępnił dane osobowe właściwemu organowi innego Państwa Członkowskiego, bezzwłocznie informuje ten ostatni w przypadku, gdy stwierdzi, albo z własnej inicjatywy, albo w następstwie otrzymania wniosku od podmiotu danych, że danych, których to dotyczy, nie należało przekazywać czy udostępniać lub że zostały przekazane czy udostępnione dane niedokładne lub nieaktualne.

5. Państwa Członkowskie stanowią, że właściwy organ, który został poinformowany zgodnie z ust. 4, usuwa lub dokonuje sprostowania danych, których to dotyczy. Ponadto organ ten dokonuje sprostowania danych, jeśli wykryje, że dane te są nieścisłe. Jeżeli zdaniem tego organu istnieją poważne podstawy by sądzić, że otrzymane dane osobowe są nieścisłe lub że należy je usunąć, bezzwłocznie powiadamia o tym właściwy organ, który przekazał lub udostępnił dane, których to dotyczy.

6. Państwa Członkowskie stanowią, bez uszczerbku dla krajowej procedury karnej, że dane osobowe oznacza się na wniosek podmiotu danych w przypadku, gdy podmiot danych kwestionuje ich ścisłość oraz gdy nie można mieć pewności co do ich ścisłości lub nieścisłości. Oznaczenie takie może zostać usunięte wyłącznie za zgodą podmiotu danych lub na podstawie orzeczenia właściwego sądu lub decyzji właściwego organu nadzoru.

7. Państwa Członkowskie stanowią, że dane osobowe otrzymane od organu innego Państwa Członkowskiego są usuwane w przypadku gdy:

   – danych tych nie należało przekazać, udostępnić lub otrzymać,

   – po upływie terminu określonego przepisami prawa innego Państwa Członkowskiego organ, który przekazał lub udostępnił dane, powiadomi organ otrzymujący te dane o istnieniu takiego terminu w momencie przekazywania lub udostępniania tych danych, chyba że dane osobowe są w dalszym stopniu potrzebne do celów postępowania sądowego,

   – dane te nie są lub przestały być konieczne do celów, dla których zostały przekazane lub udostępnione.

8. Jeżeli dane osobowe nie zostały przekazane na wniosek, organ otrzymujący te dane sprawdza bezzwłocznie, czy dane te są konieczne do celów, dla których zostały one przekazane.

9. Dane osobowe nie są usuwane, tylko podlegają zablokowaniu zgodnie z prawem krajowym, jeśli istnieją poważne podstawy by sądzić, że ich usunięcie mogłoby zaszkodzić interesom zasługującego na ochronę podmiotu danych. Z zablokowanych danych korzysta się lub przekazuje się je wyłącznie do celów innych niż te, dla których zostały one usunięte.

Artykuł 10
Odnotowywanie i dokumentacja

1. Państwa Członkowskie stanowią, że każdorazowe zautomatyzowane przekazanie i otrzymanie danych osobowych, w szczególności poprzez przyznanie bezpośredniego, zautomatyzowanego dostępu, jest odnotowywane w celu umożliwienia późniejszej weryfikacji przyczyn przekazania, przekazanych danych, daty przekazania, organów biorących w nim udział oraz, w odniesieniu do organu otrzymującego dane, osób, które otrzymały dane i które doprowadziły do ich otrzymania.

2. Państwa Członkowskie stanowią, że każdorazowe niezautomatyzowane przekazanie i otrzymanie danych osobowych zostaje udokumentowane w celu zapewnienia późniejszej weryfikacji w kwestii przyczyn przekazania, przekazanych danych, daty przekazania, organów biorących w nim udział oraz, w odniesieniu do organu otrzymującego dane, osób, które otrzymały dane i które doprowadziły do ich otrzymania.

3. Organ, który odnotował lub udokumentował tego typu informacje, bezzwłocznie je przekazuje właściwemu organowi nadzoru na wniosek tego ostatniego. Z informacji tych korzysta się wyłącznie w celu kontroli ochrony danych oraz w celu zapewnienia właściwego przetwarzania danych jak również integralności danych i ich zabezpieczenia.

SEKCJA II – DALSZE PRZETWARZANIE, W SZCZEGÓLNOŚCI DALSZE PRZEKAZYWANIE I TRANSFER DANYCH OTRZYMANYCH OD WŁAŚCIWYCH ORGANÓW INNYCH PAŃSTW CZŁONKOWSKICH LUB UDOSTĘPNIONYCH PRZEZ TE ORGANY

Artykuł 11
Dalsze przetwarzanie danych osobowych otrzymanych od właściwego organu innego Państwa Członkowskiego lub udostępnionych przez ten organ

1. Państwa Członkowskie stanowią, że dane osobowe otrzymane od właściwego organu innego Państwa Członkowskiego lub udostępnione przez ten organ są poddawane dalszemu przetwarzaniu wyłącznie zgodnie z niniejszą decyzją ramową, w szczególności jej art. 4, 5 i 6,

   a) w określonym celu, dla którego zostały przekazane lub udostępnione, lub

   b) jeśli zachodzi taka konieczność, do celów zapobiegania przestępstwom, ich ścigania, wykrywania i karania lub do celów zapobiegania zagrożeniom dla bezpieczeństwa publicznego lub dla bezpieczeństwa danej osoby, za wyjątkiem przypadku, gdy nad tego typu względami przeważa konieczność ochrony interesów lub praw podstawowych podmiotu danych.

2. Dane osobowe, których to dotyczy, przetwarzane są dalej dla celów, o których mowa w ust. 1 lit. b) niniejszego artykułu, wyłącznie za uprzednią zgodą organu, który przekazał lub udostępnił te dane osobowe.

3. Ustęp 1 lit. b) nie ma zastosowania w przypadku, gdy szczególne akty prawne na mocy tytułu VI Traktatu o Unii Europejskiej wyraźnie określają, że dane osobowe

otrzymane od właściwego organu innego Państwa Członkowskiego lub udostępnione przez ten organ są przetwarzane wyłącznie do celów, dla których zostały przekazane lub udostępnione.

Artykuł 12
Przekazywanie danych innym właściwym organom

Państwa Członkowskie stanowią, że dane osobowe otrzymane od właściwego organu innego Państwa Członkowskiego lub udostępnione przez ten organ są przekazywane dalej lub udostępniane innym właściwym organom danego Państwa Członkowskiego jedynie, jeśli spełnione są łącznie następujące wymogi:

a) przekazanie lub udostępnienie jest określone przepisami prawnymi, które w sposób jasny do niego zobowiązują lub na nie zezwalają.

b) przekazanie lub udostępnienie danych jest konieczne do celów wypełnienia zgodnych z prawem zadań organu, który otrzymał te dane, lub organu, któremu zostaną one dalej przekazane.

c) przekazanie lub udostępnienie danych jest konieczne do szczególnych celów, dla jakich zostały przekazane lub udostępnione, lub do celów zapobiegania przestępstwom, ich ścigania, wykrywania i karania, lub do celów zapobiegania zagrożeniom dla bezpieczeństwa publicznego lub dla bezpieczeństwa danej osoby, za wyjątkiem przypadku, gdy nad tego typu względami przeważa konieczność ochrony interesów lub praw podstawowych podmiotu danych.

d) właściwy organ danego Państwa Członkowskiego, który przekazał lub udostępnił dane właściwemu organowi, który zamierza przesłać dalej te dane lub je udostępnić, wyraził uprzednio zgodę na ich dalsze przekazanie lub udostępnienie.

Artykuł 13
Przekazywanie danych organom innym niż właściwe organy

Państwa Członkowskie stanowią, że dane osobowe otrzymane od właściwego organu innego Państwa Członkowskiego lub udostępnione przez ten organ są przekazywane dalej organom, innym niż właściwe organy, danego Państwa Członkowskiego jedynie w szczególnych przypadkach oraz jeśli spełnione są łącznie następujące wymogi:

a) przekazanie danych jest określone przepisami prawnymi, które w sposób jasny do niego zobowiązują lub na nie zezwalają, oraz

b) przekazanie danych jest

konieczne do szczególnych celów, dla jakich dane te zostały przekazane lub udostępnione, lub dla celów zapobiegania przestępstwom, ich ścigania, wykrywania czy karania, lub do celów zapobiegania zagrożeniom dla bezpieczeństwa publicznego lub dla bezpieczeństwa danej osoby, za wyjątkiem przypadku, gdy nad tego typu względami przeważa konieczność ochrony interesów lub praw podstawowych podmiotu danych,

lub

konieczne ponieważ dane, których to dotyczy, są niezbędne organowi, któremu dane te zostaną dalej przekazane, aby mógł on wypełnić swoje zgodne z prawem zadania oraz pod warunkiem, że cel gromadzenia lub przetwarzania, do jakiego ma przystąpić ten organ, nie jest niezgodny z pierwotnym przetwarzaniem oraz że

zobowiązania prawne właściwego organu, który zamierza przekazać te dane, nie są z nim sprzeczne,

lub

bez wątpienia w interesie podmiotu danych, a podmiot ten wyraził zgodę albo też okoliczności stwarzają wyraźne domniemanie takiej zgody;

c) Właściwy organ danego Państwa Członkowskiego, który przekazał lub udostępnił dane właściwemu organowi, który zamierza przesłać dalej te dane, wyraził uprzednio zgodę na ich dalsze przekazanie.

Artykuł 14
Przekazanie danych podmiotom prywatnym

Państwa Członkowskie stanowią, bez uszczerbku dla zasad krajowej procedury karnej, że dane osobowe otrzymane od właściwego organu innego Państwa Członkowskiego lub udostępnione przez ten organ są przekazywane dalej podmiotom prywatnym w danym Państwie Członkowskim jedynie w szczególnych przypadkach oraz jeśli spełnione są łącznie następujące wymogi:

a) przekazanie danych jest określone przepisami prawnymi, które w sposób jasny do niego zobowiązują lub na nie zezwalają, oraz

b) przekazanie danych jest konieczne do celów, dla jakich dane te zostały przekazane czy udostępnione, lub do celów zapobiegania przestępstwom, ich ścigania, wykrywania czy karania, lub do celów zapobiegania zagrożeniom dla bezpieczeństwa publicznego lub dla bezpieczeństwa danej osoby, za wyjątkiem przypadku, gdy nad tego typu względami przeważa konieczność ochrony interesów lub praw podstawowych podmiotu danych, oraz

c) właściwy organ danego Państwa Członkowskiego, który przekazał lub udostępnił dane właściwemu organowi, który zamierza przesłać dalej te dane, wyraził uprzednio zgodę na ich dalsze przekazanie podmiotom prywatnym.

Artykuł 15
Transfer danych do właściwych organów w krajach trzecich lub organów międzynarodowych

1. Państwa Członkowskie stanowią, że dane osobowe otrzymane od właściwego organu innego Państwa Członkowskiego lub udostępnione przez ten organ nie podlegają dalszemu transferowi do właściwych organów krajów trzecich lub organów międzynarodowych, za wyjątkiem przypadku, gdy tego typu transfer jest zgodny z niniejszą decyzją ramową oraz, w szczególności, spełnione są łącznie następujące wymogi:

   a) Transfer jest określony przepisami prawnymi, które w sposób jasny do niego zobowiązują lub na niego zezwalają.

   b) Transfer danych jest konieczny do celów, dla jakich dane te zostały przekazane czy udostępnione, lub do celów zapobiegania przestępstwom, ich ścigania, wykrywania czy karania, lub do celów zapobiegania zagrożeniom dla bezpieczeństwa publicznego lub dla bezpieczeństwa danej osoby, za wyjątkiem przypadku, gdy nad tego typu względami przeważa konieczność ochrony interesów lub praw podstawowych podmiotu danych.

c) Właściwy organ innego Państwa Członkowskiego, który przekazał lub udostępnił dane właściwemu organowi, który zamierza dokonać ich dalszego transferu, wyraził uprzednio zgodę na dokonanie dalszego ich transferu.

d) Kraj trzeci lub organ międzynarodowy, do którego dokonuje się transferu danych, zapewnia odpowiedni poziom ochrony danych osobowych.

2. Państwa Członkowskie gwarantują, że oceny w kwestii tego, czy poziom ochrony danych zapewniony przez kraj trzeci lub organ międzynarodowy jest odpowiedni, dokonuje się w świetle wszystkich okoliczności dotyczących każdorazowego transferu danych lub danej kategorii transferów. Ocena ta wynika w szczególności ze zbadania następujących elementów: typu danych, celów transferu danych i czasu trwania przetwarzania, kraju pochodzenia i kraju przeznaczenia, ogólnych i sektorowych przepisów prawa mających zastosowanie w danym kraju trzecim lub, w przypadku organu, o którym mowa, mających zastosowanie zasad wykonywania zawodu i zasad bezpieczeństwa, jak również istnienia wystarczających środków bezpieczeństwa wprowadzonych przez adresata transferu.

3. Państwa Członkowskie i Komisja informują się nawzajem o przypadkach, w których ich zdaniem dany kraj trzeci lub organ międzynarodowy nie zapewnia odpowiedniego poziomu ochrony danych w rozumieniu ust. 2.

4. W przypadku gdy, zgodnie z procedurą określoną w art. 16, zostaje ustalone, że dany kraj trzeci lub organ międzynarodowy nie zapewnia odpowiedniego poziomu ochrony danych w rozumieniu ust. 2, Państwa Członkowskie podejmują konieczne środki, aby zapobiec transferom danych osobowych do tego kraju trzeciego lub organu międzynarodowego.

5. Zgodnie z procedurą określoną w art. 16 możliwe jest ustalenie, że dany kraj trzeci lub organ międzynarodowy zapewnia odpowiedni poziom ochrony danych w rozumieniu ust. 2 poprzez odpowiednie przepisy prawa krajowego lub przystąpienie do międzynarodowych porozumień, w celu ochrony życia osobistego i podstawowych swobód i praw osób fizycznych.

6. Dane osobowe otrzymane od właściwego organu innego Państwa Członkowskiego mogą wyjątkowo podlegać dalszemu transferowi do właściwych organów krajów trzecich lub organów międzynarodowych, w których nie zapewnia się lub które nie zapewniają odpowiedniego poziomu ochrony danych, jeśli jest to bezwzględnie konieczne w celu ochrony istotnych interesów Państwa Członkowskiego lub aby zapobiec poważnemu bezpośredniemu zagrożeniu dla bezpieczeństwa publicznego lub bezpieczeństwa danej osoby lub osób.

Artykuł 16

Komitet

1. W przypadku odniesień do niniejszego artykułu Komisję wspiera komitet złożony z przedstawicieli Państw Członkowskich pod przewodnictwem przedstawiciela Komisji.

2. Na wniosek przewodniczącego komitet uchwala swój regulamin wewnętrzny sporządzony na podstawie wzoru regulaminu opublikowanego w *Dzienniku Urzędowym Unii Europejskiej*.

3. Przedstawiciel Komisji przedkłada komitetowi projekt środków, jakie mają być podjęte. Komitet wydaje opinię dotyczącą tego projektu w terminie wyznaczonym

przez przewodniczącego z uwzględnieniem pilności sprawy. W przypadku decyzji, które muszą być przyjęte przez Radę na wniosek Komisji, opinia zostaje wydana większością głosów określoną w art. 205 ust. 2 Traktatu ustanawiającego Wspólnotę Europejską. Głosy przedstawicieli Państw Członkowskich w ramach Komitetu są ważone w sposób określony w wyżej wymienionym artykule. Przewodniczący nie posiada prawa głosu.

4. Komisja przyjmuje zamierzone środki, jeżeli są one zgodne z opinią komitetu. Jeżeli zamierzone środki nie są zgodne z opinią komitetu lub opinia nie zostanie wydana, Komisja bezzwłocznie przedstawia Radzie wniosek w sprawie środków, które mają zostać podjęte, informując o tym Parlament Europejski.

5. Rada może stanowić większością kwalifikowaną w sprawie wniosku, w terminie dwóch miesięcy od daty jego przedstawienia Radzie.

   Jeżeli w tym terminie Rada większością kwalifikowaną wyrazi sprzeciw wobec wniosku, Komisja ponownie go bada. Może ona przedłożyć Radzie zmieniony wniosek, ponownie przedłożyć ten sam wniosek lub przedstawić projekt aktu prawnego. Jeżeli po upływie wskazanego terminu Rada ani nie przyjęła proponowanego aktu wykonawczego, ani nie wyraziła swojego sprzeciwu wobec wniosku dotyczącego środków wykonawczych, proponowany akt wykonawczy jest przyjmowany przez Komisję.

Artykuł 17
Odstępstwa od przepisów art. 12, 13, 14 i 15

Przepisów art. 12, 13, 14 i 15 nie stosuje się w przypadku, gdy szczególne akty prawne na mocy tytułu VI Traktatu o Unii Europejskiej wyraźnie określają, że dane osobowe otrzymane od właściwego organu innego Państwa Członkowskiego lub udostępnione przez ten organ nie są przekazywane dalej lub są przekazywane dalej wyłącznie zgodnie z bardziej szczegółowymi warunkami.

Artykuł 18
Informacje udzielane na wniosek właściwego organu

Państwa Członkowskie stanowią, że właściwy organ, od którego dane osobowe zostały otrzymane lub przez który zostały udostępnione, zostanie poinformowany w odpowiedzi na swój wniosek w kwestii ich dalszego przetwarzania i osiągniętych wyników.

ROZDZIAŁ IV
PRAWA PODMIOTU DANYCH

Artykuł 19
Prawo do informacji w przypadkach pozyskiwania danych od podmiotu danych za jego wiedzą

1. Państwa Członkowskie stanowią, że kontroler danych lub jego przedstawiciel musi dostarczyć podmiotowi danych, od którego pozyskiwane są za jego wiedzą dane odnoszące się do niego, przynajmniej następujące bezpłatne informacje chyba, że podmiot danych już je posiada:

   a) tożsamość kontrolera danych i jego ewentualnego przedstawiciela;

   b) cele przetwarzania, do których przeznaczone są dane;

c) wszelkie dalsze informacje, takie jak

– podstawa prawna przetwarzania,

– odbiorcy lub kategorie odbiorców danych,

– czy odpowiedzi na pytania lub inne formy współpracy są obowiązkowe czy dobrowolne, jak również jakie są ewentualne konsekwencje nieudzielenia odpowiedzi lub braku współpracy,

– istnienie prawa dostępu do danych dotyczących tej osoby oraz do ich sprostowania

o ile takie dalsze informacje są konieczne, biorąc od uwagę szczególne okoliczności, w których dane są gromadzone, w celu zagwarantowania rzetelnego w odniesieniu do podmiotu danych przetwarzania danych.

2. Dostarczenia informacji określonych w ust. 1 odmawia się lub dostarcza się je w stopniu ograniczonym jedynie, jeśli jest to konieczne,

a) aby kontroler mógł w sposób właściwy wypełnić swoje zgodne z prawem obowiązki,

b) aby uniknąć negatywnego wpływu na toczące się dochodzenie lub postępowanie lub na wypełnianie zgodnych z prawem obowiązków właściwych organów,

c) w celu ochrony bezpieczeństwa publicznego i porządku publicznego w Państwie Członkowskim,

d) w celu ochrony praw i swobód stron trzecich,

za wyjątkiem przypadku, gdy nad tego typu względami przeważa konieczność ochrony interesów lub praw podstawowych podmiotu danych.

3. W przypadku gdy odmawia się udzielenia informacji, o których mowa w ust. 1, lub jeśli dostęp do nich jest ograniczony, kontroler danych informuje podmiot danych o tym, że może on odwołać się do właściwego organu nadzoru, bez uszczerbku dla jakiegokolwiek środka sądowego oraz bez uszczerbku dla krajowej procedury karnej.

4. Przyczyny odmowy lub ograniczenia przewidzianych w ust. 2 nie zostają podane, jeśli poinformowanie o nich może negatywnie wpłynąć na cel odmowy. W takim przypadku kontroler danych informuje podmiot danych o tym, że może on odwołać się do właściwego organu nadzoru, bez uszczerbku dla jakiegokolwiek środka sądowego oraz bez uszczerbku dla krajowej procedury karnej. Jeśli podmiot danych występuje z odwołaniem do organu nadzoru, ten ostatni rozpatruje odwołanie. Organ nadzoru, rozpatrując odwołanie, informuje podmiot danych wyłącznie o tym, czy dane zostały przetworzone w sposób prawidłowy oraz, jeśli nie, czy dokonano wszelkich niezbędnych korekt.

Artykuł 20

Prawo do informacji w przypadku, gdy danych nie uzyskano od podmiotu danych lub uzyskano je od niego bez jego wiedzy

1. Gdy dane nie zostały uzyskane od podmiotu danych lub uzyskano je od niego bez jego wiedzy lub gdy podmiot danych nie był świadomy, że gromadzone są dotyczące go dane, Państwa Członkowskie stanowią, że kontroler danych lub jego przedstawiciel musi w chwili rozpoczęcia rejestrowania danych osobowych lub, jeśli

przewidywane jest ich ujawnienie stronie trzeciej, w rozsądnym czasie od momentu ujawnienia danych po raz pierwszy, bezpłatnie udzielić podmiotowi danych przynajmniej następujących informacji chyba, że podmiot danych już je ma lub udzielenie informacji okazuje się niemożliwe lub wymagałoby nieproporcjonalnego wysiłku:

a) tożsamość kontrolera danych i jego ewentualnego przedstawiciela;

b) cele przetwarzania danych;

c) wszelkie dalsze informacje, takie jak

– podstawa prawna przetwarzania,

– kategorie tych danych;

– odbiorcy lub kategorie odbiorców danych,

– istnienie prawa dostępu do danych dotyczących tej osoby oraz do ich sprostowania

o ile takie dalsze informacje są konieczne, biorąc od uwagę szczególne okoliczności, w których dane są przetwarzane, w celu zagwarantowania rzetelnego w odniesieniu do podmiotu danych przetwarzania danych.

2. Informacje określone w ust. 1 nie zostają dostarczone, jeśli jest to konieczne

a) aby kontroler danych mógł w sposób właściwy wypełnić swoje zgodne z prawem obowiązki,

b) aby uniknąć negatywnego wpływu na toczące się dochodzenie lub postępowanie lub na wypełnianie zgodnych z prawem obowiązków właściwych organów,

c) w celu ochrony bezpieczeństwa publicznego i porządku publicznego w Państwie Członkowskim,

d) w celu ochrony praw i swobód stron trzecich,

za wyjątkiem przypadku, gdy nad tego typu względami przeważa konieczność ochrony interesów lub praw podstawowych podmiotu danych.

Artykuł 21

Prawo dostępu do danych oraz do ich sprostowania, usunięcia lub zablokowania

1. Państwa Członkowskie gwarantują każdemu podmiotowi danych prawo do uzyskania od kontrolera danych:

a) bez ograniczeń, w rozsądnych odstępach czasowych oraz bez zbędnej zwłoki i bez opłat:

– potwierdzenia co do tego, czy odnoszące się do niego dane są w tym momencie przetwarzane oraz informacji co najmniej o celu przetwarzania odnośnych danych, kategorii tych danych, podstawy prawnej dla przetwarzania oraz odbiorców lub kategorii odbiorców, którym dane zostały ujawnione;

– przekazania mu w zrozumiałej formie danych podlegających przetwarzaniu i wszelkich dostępnych informacji o ich źródle;

b) w stosownych przypadkach sprostowania, usunięcia lub zablokowania danych, których przetwarzanie jest niezgodne z przepisami niniejszej decyzji ramowej, w szczególności z powodu niepełnego lub nieścisłego charakteru tych danych;

c) powiadomienia stron trzecich, którym dane zostały ujawnione, o wszelkich sprostowaniach, o usunięciu lub zablokowaniu dokonanych zgodnie z lit. b), o ile nie jest to niemożliwe lub nie wymaga nieproporcjonalnego wysiłku.

2. Każde działanie, do którego podmiot danych jest uprawniony zgodnie z ust. 1, spotka się z odmową, jeśli jest to konieczne

a) aby kontroler danych mógł w sposób właściwy wypełnić swoje zgodne z prawem obowiązki,

b) aby uniknąć negatywnego wpływu na toczące się dochodzenie lub postępowanie lub na wypełnianie zgodnych z prawem obowiązków właściwych organów,

c) w celu ochrony bezpieczeństwa publicznego i porządku publicznego w Państwie Członkowskim,

d) w celu ochrony praw i swobód stron trzecich,

za wyjątkiem przypadku, gdy nad tego typu względami przeważa konieczność ochrony interesów lub praw podstawowych podmiotu danych.

3. Odmowa w odniesieniu do praw określonych w ust. 1 lub ich ograniczenie są formułowane na piśmie. W przypadku gdy odmawia się skorzystania z prawa, o którym mowa w ust. 1, lub ogranicza się korzystanie z niego, kontroler danych informuje podmiot danych o tym, że może on odwołać się do właściwego organu nadzoru, bez uszczerbku dla jakiegokolwiek środka sądowego oraz bez uszczerbku dla krajowej procedury karnej.

4. Przyczyny odmowy przewidzianej w ust. 2 nie zostają podane podmiotowi danych, jeśli poinformowanie o nich może negatywnie wpłynąć na cel odmowy. W takim przypadku kontroler danych informuje podmiot danych o tym, że może on odwołać się do właściwego organu nadzoru, bez uszczerbku dla jakiegokolwiek środka sądowego oraz bez uszczerbku dla krajowej procedury karnej. Jeśli podmiot danych występuje z odwołaniem do organu nadzoru, ten ostatni rozpatruje odwołanie. Organ nadzoru, rozpatrując odwołanie, informuje podmiot danych wyłącznie o tym, czy dane zostały przetworzone w sposób prawidłowy oraz, jeśli nie, czy dokonano wszelkich niezbędnych korekt.

Artykuł 22

Informacje udzielane stronom trzecim w następstwie sprostowania, zablokowania lub usunięcia danych

Państwa Członkowskie stanowią, że zostają przedsięwzięte odpowiednie środki techniczne w celu zagwarantowania, że w przypadkach, w których kontroler danych dokonuje sprostowania, zablokowania lub usunięcia danych osobowych w odpowiedzi na wniosek, automatycznie sporządzany jest wykaz dostawców i adresatów tych danych. Kontroler danych pilnuje, aby strony figurujące w wykazie zostały poinformowane o zmianach dokonanych na danych osobowych.

ROZDZIAŁ V
Poufność i bezpieczeństwo przetwarzania danych

Artykuł 23
Poufność

Żadnej osobie działającej z upoważnienia kontrolera danych lub przetwarzającego dane, włącznie z samym przetwarzającym dane, która posiada dostęp do danych osobowych, nie wolno przetwarzać ich bez instrukcji pochodzących od kontrolera danych, o ile nie wymaga tego prawo. Wszystkie osoby powołane do współpracy z właściwym organem Państwa Członkowskiego lub pracujące dla niego muszą przestrzegać ścisłych zasad poufności.

Artykuł 24
Bezpieczeństwo

1. Państwa Członkowskie stanowią, że kontroler danych musi wdrożyć odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkową lub niezgodną z prawem utratą, przekształceniem, nieuprawnionym ujawnieniem lub udostępnieniem, w szczególności w przypadku, gdy przetwarzanie wiąże się z przekazaniem za pomocą sieci informatycznej lub udostępnieniem poprzez udzielenie bezpośredniego, zautomatyzowanego dostępu, oraz przed wszelką inną sprzeczną z prawem formą przetwarzania, biorąc pod uwagę w szczególności ryzyko, jakie wiąże się z przetwarzaniem, oraz charakter chronionych danych.

   Przy uwzględnieniu stanu wiedzy w tej dziedzinie oraz kosztu wdrożenia, środki takie zapewniają poziom bezpieczeństwa stosowny do ryzyka, z jakim wiąże się przetwarzanie, i charakteru chronionych danych. Środki są uważane za konieczne, gdy wysiłek, jakiego wymagają, nie jest nieproporcjonalny do celu, jaki miał zostać osiągnięty w odniesieniu do ochrony danych.

2. W odniesieniu do zautomatyzowanego przetwarzania danych każde Państwo Członkowskie wdraża środki służące do:

   a) odmówienia nieupoważnionym osobom dostępu do sprzętu używanego do przetwarzania danych osobowych (kontrola dostępu do sprzętu);

   b) zapobiegania nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usunięciu nośników danych (kontrola nośników danych);

   c) zapobiegania nieuprawnionemu wprowadzaniu danych i nieuprawnionej inspekcji, zmienianiu i usuwaniu przechowywanych danych osobowych (kontrola przechowywania);

   d) zapobiegania używaniu systemów zautomatyzowanego przetwarzania danych przez osoby nieuprawnione, korzystające ze sprzętu do przekazywania danych (kontrola użytkowników);

   e) zagwarantowania, że osoby upoważnione do korzystania ze zautomatyzowanego systemu przetwarzania danych mają dostęp wyłącznie do tych danych, do których wglądu są upoważnione (kontrola dostępu danych);

   f) umożliwienia weryfikacji i ustalenia, którym organom dane osobowe zostały przekazane lub mogą zostać przekazane lub udostępnione przy użyciu sprzętu do przekazywania danych (kontrola przekazywania);

g) umożliwienia późniejszej weryfikacji i ustalenia, które dane osobowe zostały wprowadzone do zautomatyzowanych systemów przetwarzania danych oraz kiedy i przez kogo zostały one wprowadzone (kontrola wprowadzania danych);

h) zapobiegania nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas transferów danych osobowych lub podczas przewożenia nośników danych (kontrola transportu);

i) zapewnienia natychmiastowej naprawy zainstalowanych systemów w przypadku zakłóceń (przywrócenie poprzedniego stanu);

j) zagwarantowania, że funkcje systemu działają bez usterek, że pojawienie się usterek w ich działaniu jest natychmiast zgłaszane (wiarygodność) oraz że przechowywane dane nie mogą zostać uszkodzone poprzez nieprawidłowe działanie systemu (integralność).

3. Państwa Członkowskie stanowią, że kontroler danych musi, w przypadku gdy przetwarzania dokonuje się w jego imieniu, wybrać przetwarzającego dane, który przedsięweźmie podczas przetwarzania danych wystarczające kroki w odniesieniu do technicznych środków bezpieczeństwa i środków organizacyjnych, oraz musi zapewnić zgodność z tymi środkami.

4. Przeprowadzanie przetwarzania za pośrednictwem przetwarzającego dane musi być regulowane umową lub aktem prawnym, na mocy których przetwarzający podlega kontrolerowi danych i które w szczególności określają, że:

– przetwarzający dane działa wyłącznie na podstawie instrukcji pochodzących od kontrolera danych,

– zobowiązania przewidziane w ust. 1 i 2, określone przepisami prawa Państwa Członkowskiego, w którym przetwarzający dane ma siedzibę, spoczywają również na przetwarzającym dane.

5. Do celów dowodowych części umowy lub aktu prawnego odnoszące się do ochrony danych i wymagania dotyczące środków, do których odnosi się ust. 1, są sporządzane na piśmie lub w innej równorzędnej formie.

Artykuł 25
Rejestr

1. Państwa Członkowskie stanowią, że każdy kontroler danych prowadzi rejestr obejmujący wszelkie operacje przetwarzania lub zestawy takich operacji, które mają służyć jednemu celowi lub kilku powiązanym ze sobą celom. Rejestr ten obejmuje informacje, które zawierają

a) nazwisko i adres kontrolera danych i jego ewentualnego przedstawiciela;

b) cel lub cele przetwarzania danych;

c) opis jednej lub wielu kategorii podmiotów danych i odnoszących się do nich danych lub kategorii danych;

d) podstawę prawną operacji przetwarzania, dla której przeznaczone są dane;

e) odbiorcę lub kategorie odbiorców, którym dane mogą być ujawnione;

f) proponowane transfery danych do krajów trzecich;

g) ogólny opis pozwalający na wstępną ocenę, czy środki podjęte zgodnie z art. 24 w celu zapewnienia bezpieczeństwa przetwarzania są odpowiednie.

2. Państwa Członkowskie precyzują warunki i procedury dotyczące zgłaszania organowi nadzoru informacji określonych w ust. 1.

Artykuł 26
Kontrola wstępna

1. Państwa Członkowskie ustalają, które operacje przetwarzania mogą powodować szczególne zagrożenia w odniesieniu do praw i swobód podmiotów danych oraz dbają, aby te operacje przetwarzania były kontrolowane jeszcze przed ich przeprowadzeniem.

2. Taka kontrola wstępna jest prowadzona przez organ nadzoru po otrzymaniu powiadomienia od kontrolera danych lub przez urzędnika do spraw ochrony danych osobowych, który w przypadku wątpliwości musi skonsultować się z organem nadzoru.

3. Państwa Członkowskie mogą również prowadzić takie kontrole w kontekście opracowywania danego środka przez parlament krajowy lub też w oparciu o środek legislacyjny określający charakter przetwarzania oraz właściwe środki bezpieczeństwa.

ROZDZIAŁ VI
ŚRODKI SĄDOWE ORAZ ODPOWIEDZIALNOŚĆ

Artykuł 27
Środki odwoławcze

Bez uszczerbku dla jakiegokolwiek administracyjnego środka odwoławczego, który może zostać przewidziany, między innymi w postaci odniesienia się do organu nadzoru określonego w art. 30, jako poprzedzający skierowanie sprawy do organu sądowego, Państwa Członkowskie określają prawo każdej osoby do środka sądowego w przypadku wszelkiego naruszenia praw przysługujących jej na mocy mającego zastosowanie do przedmiotowego przetwarzania prawa krajowego zgodnie z niniejszą decyzją ramową.

Artykuł 28
Odpowiedzialność prawna

1. Państwa Członkowskie stanowią, że każda osoba, która poniosła szkody w wyniku niezgodnej z prawem operacji przetwarzania danych lub czynu niezgodnego z przepisami prawa krajowego przyjętego na mocy niniejszej decyzji ramowej, ma prawo do rekompensaty ze strony kontrolera danych za poniesioną szkodę. Kontroler danych może zostać całkowicie lub częściowo zwolniony z odpowiedzialności, jeśli udowodni, że nie jest odpowiedzialny za zdarzenie stanowiące podstawę szkody.

2. Jednakże właściwy organ, który otrzymał dane osobowe od właściwego organu innego Państwa Członkowskiego, ponosi odpowiedzialność względem poszkodowanej strony za szkody wywołane z powodu posługiwania się nieścisłymi lub nieaktualnymi danymi. Nie może zaprzeczyć swojej odpowiedzialności na tej podstawie, że otrzymał nieścisłe lub nieaktualne dane od innego organu. Jeżeli organ otrzymujący dane wypłaci odszkodowanie z powodu posługiwania się nieścisłymi

danymi przekazanymi lub udostępnionymi przez właściwy organ innego Państwa Członkowskiego, ten ostatni zwróci organowi otrzymującemu dane pełną kwotę wypłaconego odszkodowania.

Artykuł 29
Sankcje

1. Państwa Członkowskie przyjmują odpowiednie środki w celu zapewnienia pełnego wdrożenia przepisów niniejszej decyzji ramowej oraz w szczególności określają nałożenie skutecznych, proporcjonalnych i odstraszających sankcji w przypadku naruszenia przepisów przyjętych zgodnie z niniejszą decyzją ramową.

2. Państwa Członkowskie przewidują skuteczne, proporcjonalne i odstraszające sankcje karne w przypadku umyślnie popełnionych przestępstw wiążących się z poważnymi naruszeniami przepisów przyjętych zgodnie z niniejszą decyzją ramową, w szczególności przepisów, których celem jest zapewnienie poufności i bezpieczeństwa w odniesieniu do przetwarzania danych.

ROZDZIAŁ VII
ORGAN NADZORU I GRUPA ROBOCZA DS. OCHRONY OSÓB W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

Artykuł 30
Organ nadzoru

1. Każde Państwo Członkowskie wyznacza jeden lub więcej organów publicznych odpowiedzialnych za monitorowanie stosowania w obrębie jego terytorium przepisów przyjętych przez Państwa Członkowskie zgodnie z niniejszą decyzją ramową. Organy te wypełniają funkcje, które im powierzono, w sposób całkowicie niezależny.

2. Każde Państwo Członkowskie zapewnia uwzględnienie opinii organów nadzoru podczas opracowywania środków administracyjnych lub regulacji prawnych odnoszących się do ochrony praw i swobód osób fizycznych w odniesieniu do przetwarzania danych osobowych do celów zapobiegania przestępstwom, ich ścigania, wykrywania i karania.

3. Każdemu organowi zostają zapewnione w szczególności:

   – uprawnienia w zakresie prowadzenia dochodzeń, takie jak uprawnienia dotyczące dostępu do danych stanowiących przedmiot operacji przetwarzania i uprawnienia dotyczące gromadzenia wszelkich informacji niezbędnych do wykonywania jego obowiązków w zakresie nadzoru,

   – skuteczne uprawnienia w zakresie interweniowania, takie jak na przykład dotyczące przedstawiania opinii jeszcze przed operacjami przetwarzania zgodnymi z art. 26, oraz właściwego publikowania takich opinii, dotyczące polecenia zablokowania, usunięcia lub zniszczenia danych, wprowadzenia czasowego lub ostatecznego zakazu przetwarzania, ostrzeżenia lub upomnienia kontrolera danych czy skierowania sprawy do parlamentów krajowych lub innych instytucji politycznych,

– uprawnienia w zakresie wszczynania postępowania sądowego w przypadku, gdy przepisy krajowe przyjęte zgodnie z niniejszą decyzją ramową zostały naruszone lub w celu zwrócenia uwagi organów sądowych na te naruszenia.

Od decyzji organów nadzoru, które są powodem skarg, można się odwoływać za pośrednictwem sądów.

4. Każdy organ nadzoru rozpatruje roszczenia zgłoszone przez jakąkolwiek osobę, odnoszące się do ochrony praw i swobód tej osoby w odniesieniu do przetwarzania danych osobowych. Osoba ta jest informowana o rezultacie zgłoszenia roszczeń.

5. Każdy organ nadzoru regularnie sporządza sprawozdanie na temat swojej działalności. Sprawozdanie to zostaje podane do publicznej wiadomości.

6. Bez względu na prawo krajowe mające zastosowanie do przedmiotowego przetwarzania, każdy organ nadzoru posiada kompetencje w zakresie wykonywania na terytorium swojego Państwa Członkowskiego uprawnień powierzonych mu zgodnie z ust. 3. Każdy organ nadzoru może zostać wezwany do wykonania swoich uprawnień przez organ innego Państwa Członkowskiego.

7. Organy nadzoru współpracują ze sobą jak również z organami nadzoru określonymi na mocy tytułu VI Traktatu o Unii Europejskiej oraz z europejskim inspektorem ochrony danych w zakresie, w jakim jest to konieczne do wykonywania ich obowiązków, w szczególności poprzez wymianę wszystkich użytecznych informacji.

8. Państwa Członkowskie stanowią, że członkowie i pracownicy organu nadzoru, nawet po upływie ich okresu zatrudnienia, podlegają obowiązkowi zachowania tajemnicy zawodowej w odniesieniu do informacji poufnych, do których mają dostęp.

9. Uprawnienia organu nadzoru w żaden sposób nie umniejszają niezawisłości wymiaru sprawiedliwości, a decyzje wydawane przez ten organ pozostają bez uszczerbku dla wykonywania zgodnych z prawem zadań wymiaru sprawiedliwości podczas postępowań karnych.

Artykuł 31

Grupa robocza ds. ochrony osób w zakresie przetwarzania danych osobowych do celów zapobiegania przestępstwom, ich ścigania, wykrywania i karania

1. Niniejszym zostaje ustanowiona grupa robocza ds. ochrony osób w zakresie przetwarzania danych osobowych do celów zapobiegania przestępstwom, ich ścigania, wykrywania i karania, zwana dalej „grupą roboczą”. Grupa ta ma charakter doradczy i działa w sposób niezależny.

2. Grupa robocza składa się z przedstawiciela organu lub organów nadzoru wyznaczonych przez każde Państwo Członkowskie, z przedstawiciela europejskiego inspektora ochrony danych oraz z przedstawiciela Komisji.

Każdego członka grupy roboczej wyznacza instytucja, organ lub organy, które reprezentuje. Jeżeli dane Państwo Członkowskie wyznaczyło więcej niż jeden organ nadzoru, organy te mianują wspólnego przedstawiciela.

Osoby pełniące funkcję przewodniczących wspólnych organów nadzoru ustanowionych na mocy tytułu VI Traktatu o Unii Europejskiej są uprawnione do uczestniczenia w spotkaniach grupy roboczej lub do wyznaczenia osoby reprezentującej je podczas tych spotkań. Organ lub organy nadzoru wyznaczone przez Islandię, Norwegię i Szwajcarię są uprawnione do wyznaczania

reprezentantów do udziału w spotkaniach grupy roboczej, o ile poruszane są na nich kwestie związane z dorobkiem Schengen.

3. Grupa robocza wydaje decyzje zwykłą większością głosów przedstawicieli organów nadzoru Państw Członkowskich.

4. Grupa robocza wybiera przewodniczacego. Kadencja przewodniczącego trwa dwa lata i jest odnawialna.

5. Komisja zapewnia obsługę sekretariatu grupy roboczej.

6. Grupa robocza przyjmuje swój regulamin wewnętrzny.

7. Grupa robocza rozpatruje tematy wpisane do porządku obrad przez przewodniczącego z jego inicjatywy lub na wniosek przedstawiciela organów nadzoru, Komisji, europejskiego inspektora ochrony danych lub przewodniczących wspólnych organów nadzoru.

Artykuł 32

Zadania

1. Grupa robocza

   a) bada każdą kwestię dotyczącą stosowania środków krajowych przyjętych zgodnie z niniejszą decyzją ramową w celu przyczynienia się do jednolitego stosowania tego typu środków,

   b) wydaje opinie w sprawie poziomu ochrony danych w Państwach Członkowskich i w krajach trzecich i organach międzynarodowych, w szczególności w celu zagwarantowania, że transfer danych osobowych do krajów trzecich lub organów międzynarodowych, które zapewniają odpowiedni poziom ochrony danych, jest dokonywany zgodnie z art. 15 niniejszej decyzji ramowej,

   c) doradza Komisji i Państwom Członkowskim w sprawie wszelkich proponowanych zmian dotyczących niniejszej decyzji ramowej, w sprawie wszelkich dodatkowych lub szczególnych środków mających na celu ochronę praw i swobód osób fizycznych w odniesieniu do przetwarzania danych osobowych do celów zapobiegania przestępstwom, ich ścigania, wykrywania i karania oraz w sprawie wszelkich innych proponowanych środków wpływających na tego typu prawa i swobody.

2. Jeśli grupa robocza uzna, że między przepisami prawa i praktykami stosowanymi przez Państwa Członkowskie pojawiają się rozbieżności, które mogą mieć negatywny wpływ na równoważność ochrony osób w odniesieniu do przetwarzania danych osobowych w Unii Europejskiej, powiadamia o tym Radę i Komisję.

3. Grupa robocza może, z własnej inicjatywy lub z inicjatywy Komisji lub Rady, opracować zalecenia w sprawie wszystkich kwestii odnoszących się do ochrony osób w odniesieniu do przetwarzania danych osobowych w Unii Europejskiej do celów zapobiegania przestępstwom, ich ścigania, wykrywania i karania.

4. Opinie i zalecenia grupy roboczej są przekazywane Radzie, Komisji i Parlamentowi Europejskiemu oraz komitetowi określonemu w art. 16.

5. Komisja, w oparciu o informacje dostarczone przez Państwa Członkowskie, informuje grupę roboczą o działaniach podjętych w odpowiedzi na jej opinie i

zalecenia. Informuje również o nich w sprawozdaniu, które także jest przesyłane Parlamentowi Europejskiemu i Radzie. Sprawozdanie to zostaje podane do publicznej wiadomości. Państwa Członkowskie informują grupę roboczą o wszelkich podjętych przez nie zgodnie z ust. 1 działaniach.

6. Grupa robocza sporządza roczne sprawozdanie na temat stanu ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych do celów zapobiegania, wykrywania i karania przestępstw w Unii Europejskiej i w krajach trzecich, które przekazuje Komisji, Parlamentowi Europejskiemu i Radzie. Sprawozdanie to zostaje podane do publicznej wiadomości.

ROZDZIAŁ VIII
Przepisy końcowe

Artykuł 33
Zmiany w Konwencji z Schengen

Do celów kwestii objętych zakresem stosowania Traktatu UE, niniejsza decyzja ramowa zastępuje art. 126-130 Konwencji z Schengen.

Artykuł 34
Związek z innymi aktami prawnymi dotyczącymi przetwarzania i ochrony danych osobowych

1. Niniejsza decyzja ramowa zastępuje art. 23 Konwencji o wzajemnej pomocy w sprawach karnych pomiędzy Państwami Członkowskimi Unii Europejskiej.

2. Wszelkie odniesienia do Konwencji Rady Europy nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z dnia 28 stycznia 1981 r. należy rozumieć jako odniesienia do niniejszej decyzji ramowej.

Artykuł 35
Wykonanie

1. Państwa Członkowskie podejmują niezbędne środki w celu zastosowania się do niniejszej decyzji ramowej w terminie do dnia 31 grudnia 2006 r.

2. W tym samym terminie Państwa Członkowskie przekazują do Sekretariatu Generalnego Rady i do Komisji treść przepisów transponujących do ich prawa krajowego zobowiązania nałożone na nie na mocy niniejszej decyzji ramowej jak również informacje w sprawie wyznaczenia organu lub organów nadzoru określonych w art. 29. Na podstawie tych informacji oraz pisemnego sprawozdania Komisji Rada dokona przed dniem 31 grudnia 2007 r. oceny zakresu, w jakim Państwa Członkowskie przedsięwzięły niezbędne środki w celu zastosowania się do niniejszej decyzji ramowej.

Artykuł 36
Wejście w życie

Niniejsza decyzja ramowa wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Brukseli, dnia […] r.

W imieniu Rady
Przewodniczący

ZAŁĄCZNIK

LEGISLACYJNE ZESTAWIENIE FINANSOWE

Dziedzina polityki: Wymiar Sprawiedliwości i Sprawy Wewnętrzne

Rodzaje działalności: 1806 – Ustanowienie prawdziwego obszaru wolności, bezpieczeństwa i sprawiedliwości w sprawach karnych i cywilnych

TYTUŁ DZIAŁANIA: WNIOSEK DOTYCZĄCY DECYZJI RAMOWEJ RADY W SPRAWIE OCHRONY DANYCH OSOBOWYCH PRZETWARZANYCH W RAMACH WSPÓŁPRACY POLICYJNEJ I SĄDOWEJ

1. POZYCJE I NAGŁÓWKI W BUDŻECIE

nie dotyczy

2. DANE OGÓLNE

2.1. Przydział całkowity na działanie (Część B): mln EUR na zobowiązanie

nie dotyczy

2.2. Okres stosowania:

początek w 2006 r.

2.3. Całkowity wieloletni preliminarz wydatków:

a) Harmonogram przydziału środków na zobowiązania / środków na płatności (interwencja finansowa) (*patrz punkt 6.1.1*)

mln EUR *(do trzech miejsc po przecinku)*

	[2006]	[2007]	[2008]	[2009]	[2010]	[2011]	Ogółem
Zobowiązania							
Płatności							

b) Pomoc techniczna i administracyjna oraz wydatki wspierające *(patrz punkt 6.1.2)*

Zobowiązania							
Płatności							

Suma częściowa a+b							
Zobowiązania							
Płatności							

c) Całkowity wpływ finansowy zasobów ludzkich i pozostałych wydatków administracyjnych*(patrz punkty 7.2 i 7.3)*

Zobowiązania/płatności	0.389	0.389	0.389	0.389	0.389	0.389	2,334

OGÓŁEM a+b+c							
Zobowiązania							
Płatności							

2.4. Zgodność z programowaniem finansowym i perspektywą finansową

nie dotyczy

2.5. Wpływ finansowy na dochody:

Wniosek nie ma skutków finansowych

3. CECHY BUDŻETU

Rodzaj wydatków		**Nowe**	**Wkład EFTA**	**Wkład krajów wnioskujących**	**Dział w perspektywie finansowej**
Nieobligatoryjne	Niezróżnicowane	nie dotyczy	nie dotyczy	nie dotyczy	**Brak** Nie dotyczy

4. PODSTAWA PRAWNA

Artykuł 30, 31 i 34 ust. 2 lit. b) Traktatu UE

5. OPIS I UZASADNIENIE

5.1. Potrzeba udziału Wspólnoty

5.1.1. Cele

Proponowana decyzja ramowa określa wspólne normy odnoszące się do ochrony danych osobowych przetwarzanych przez właściwe organy w kontekście działań określonych w tytule VI Traktatu o Unii Europejskiej (współpraca policyjna i sądowa w sprawach karnych). Niezależne publiczne organy nadzoru kontrolują stosowanie przepisów krajowych zgodnych z niniejszą decyzją ramową w Państwach Członkowskich. Niniejszym na szczeblu Unii Europejskiej zostaje ustanowiona grupa robocza do spraw ochrony osób w zakresie przetwarzania danych osobowych do celów zapobiegania przestępstwom, ich ścigania, wykrywania i karania, zwana dalej „grupą roboczą". Grupa robocza składa się z przedstawiciela organu lub organów nadzoru wyznaczonych przez każde Państwo Członkowskie, z przedstawiciela europejskiego inspektora ochrony danych oraz z przedstawiciela Komisji. Grupa robocza bada każdą kwestię dotyczącą stosowania środków krajowych przyjętych zgodnie z niniejszą decyzją ramową w celu przyczynienia się do jednolitego stosowania tego typu środków. Wydaje opinie w sprawie poziomu ochrony danych w Państwach Członkowskich i w krajach trzecich oraz doradza Komisji i Państwom Członkowskim w sprawie wszelkich proponowanych zmian dotyczących niniejszej decyzji ramowej jak również w sprawie wszelkich

dodatkowych lub szczególnych środków mających na celu ochronę praw podstawowych.

Ponadto zgodnie z art. 16 niniejszej decyzji ramowej komitet złożony z przedstawicieli Państw Członkowskich pod przewodnictwem przedstawiciela Komisji wspomaga Komisję w celu dokonania oceny, w miarę konieczności, poziomu ochrony danych w kraju trzecim.

5.1.2. Środki podjęte w związku z oceną ex ante

Przeprowadzono konsultacje z przedstawicielami rządów i niezależnych organów nadzoru Państw Członkowskich jak również Islandii, Norwegii i Szwajcarii, europejskiego inspektora ochrony danych, Europolu i Eurojustu. Komisja, biorąc pod uwagę różne opinie, proponuje w szczególności ustanowić grupę roboczą opisaną powyżej. W celu oszacowania możliwych kosztów związanych z tym środkiem Komisja sprawdziła, ile wynoszą koszty (koszty podróży, pomocy sekretariatu przy przygotowywaniu i organizowaniu spotkań) ponoszone obecnie przez grupę roboczą ustanowioną zgodnie z art. 29 dyrektywy 95/46/WE.

5.2. Planowane działanie i uzgodnienia dotyczące interwencji budżetu

Spotkania wyżej wymienionej grupy roboczej będą się odbywać regularnie, według przewidywań pięć razy w roku. Spotkania komitetu określonego w art. 16 będą mieć miejsce w razie wystąpienia takiej konieczności i tak często, jak będzie to konieczne, prawdopodobnie również pięć razy w roku. Należy zwrócić poniesione koszty jednemu uczestnikowi z każdego Państwa Członkowskiego i państwa obszaru Schengen (Islandii, Norwegii). Przykład grup ustanowionych zgodnie z art. 29 i 31 dyrektywy 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 może pomóc w określeniu kosztów.

5.3. Metody wdrażania

Komisja powinna być organizatorem i gospodarzem wszystkich tych spotkań. Komisja będzie musiała zapewnić obsługę sekretariatu dla wyżej wymienionej grupy roboczej i komitetu oraz przygotowywać/organizować ich spotkania.

6. WPŁYW FINANSOWY

6.1. Całkowity wpływ finansowy na Część B - (podczas całego planowanego okresu)

6.1.1. Interwencja finansowa

nie dotyczy

6.1.2. Pomoc techniczna i administracyjna, wydatki pomocnicze i wydatki IT (przydział środków na zobowiązania)

nie dotyczy

6.2. Kalkulacja kosztów na działanie przewidziane w Części B (w czasie całego planowanego okresu)

nie dotyczy

7. WPŁYW NA WYDATKI ZWIĄZANE Z PERSONELEM I ADMINISTRACYJNE

Kwota wpływu na wydatki związane z personelem i administracyjne zostanie pokryta w kontekście przydziału zasobów z zarządzającej DG w ramach corocznej procedury przydziału środków.

Przydział stanowisk zależy również od przyznania funkcji i zasobów w kontekście perspektyw finansowych na lata 2007-2013.

7.1. Wpływ na zasoby ludzkie

Rodzaj stanowiska		Personel oddelegowany do zarządzania działaniem przy użyciu istniejących lub dodatkowych zasobów		Ogółem	Opis zadań wynikających z działania
		Liczba stanowisk stałych	Liczba stanowisk czasowych		
Urzędnicy lub personel tymczasowy	A. B C	0,25 A 0,50 B 1,00 C		0,25A 0,50B 1,00C	Zapewnianie pomocy sekretariatu, przygotowywanie spotkań grupy roboczej i komitetu
Pozostałe zasoby ludzkie					
Ogółem					

7.2. Całkowity wpływ finansowy na zasoby ludzkie

Rodzaj zasobów ludzkich	Suma (EUR)	Metoda obliczeniowa *
Urzędnicy Pracownicy czasowi	1. rok189 000	1 X 108 000 0.5 X 108 000 0,25 X 108 000 = 189 000
Pozostałe zasoby ludzkie (określić linię budżetową)		
Ogółem	189 000	

Podane wysokości odpowiadają wydatkom całkowitym na okres 12 miesięcy.

7.3. Inne wydatki administracyjne wynikające z działania

Linia budżetowa (numer i treść)	Suma (EUR)	Metoda obliczeniowa
Przydział całkowity (Tytuł A7) A0701 – Podróże służbowe A07030 – Spotkania A07031 – Komitety obowiązkowe A07032 – Komitety nieobowiązkowe A07040 – Konferencje A0705 – Badania i konsultacje Inne wydatki (określić)	200 000	10 spotkań* 27 * 740 EUR
Systemy informatyczne (A-5001/A-4300)		
Inne wydatki – Część A (określić)		
Ogółem	200 000	

Podane wysokości odpowiadają wydatkom całkowitym na okres 12 miesięcy.

Należy określić rodzaj komitetu i grupę, do której należy.

I.	Całkowita suma roczna (7.2 + 7.3)	389 000 EUR
II.	Czas trwania działania	
III.	Koszt całkowity działania (I x II)	

8. KONTYNUACJA I OCENA

8.1. Uzgodnienia związane z kontynuacją

Grupa robocza i komitet określą swój regulamin wewnętrzny, obejmujący zasady w zakresie poufności. Parlament Europejski będzie informowany w sposób analogiczny do określonego w art. 7 decyzji Rady 99/468/WE z dnia 28 czerwca 1999 r.

ustanawiającej warunki wykonywania uprawnień wykonawczych przyznanych Komisji (Dz.U. L 184 z 17.7.1999, str. 23).

8.2. Uzgodnienia dotyczące planowanej oceny i jej harmonogram

nie dotyczy

9. ŚRODKI PRZECIWDZIAŁANIA NADUŻYCIOM

nie dotyczy

XXX