III

(Akty przyjęte na mocy Traktatu UE)

AKTY PRZYJĘTE NA MOCY TYTUŁU VI TRAKTATU UE

DECYZJA RAMOWA RADY 2008/977/WSiSW

z dnia 27 listopada 2008 r.

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

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o Unii Europejskiej, w szczególności jego art. 30 i 31 oraz art. 34 ust. 2 lit. b),

uwzględniając wniosek Komisji,

uwzględniając opinię Parlamentu Europejskiego [1],

a także mając na uwadze, co następuje:

(1) Unia Europejska postawiła sobie za cel utrzymanie i rozwój Unii jako obszaru wolności, bezpieczeństwa i sprawiedliwości, na którym wysoki poziom bezpieczeństwa ma zostać zapewniony przez wspólne działanie państw członkowskich w zakresie współpracy policyjnej i sądowej w sprawach karnych.

(2) Wspólne działanie w zakresie współpracy policyjnej zgodnie z art. 30 ust. 1 lit. b) Traktatu o Unii Europejskiej oraz wspólne działanie w zakresie współpracy sądowej w sprawach karnych zgodnie z art. 31 ust. 1 lit. a) Traktatu o Unii Europejskiej pociągają za sobą potrzebę przetwarzania istotnych informacji, które powinno podlegać właściwym przepisom o ochronie danych osobowych.

(3) Akty prawne objęte zakresem zastosowania tytułu VI Traktatu o Unii Europejskiej powinny poprawiać współpracę policyjną i sądową w sprawach karnych pod względem jej skuteczności i legalności oraz zgodności z prawami podstawowymi, w szczególności z prawem do prywatności i do ochrony danych osobowych. W osiąganiu obu tych celów mogą pomóc wspólne normy przetwarzania i ochrony danych osobowych, które przetwarza się w celu zapobiegania przestępczości i jej zwalczania.

(4) W programie haskim, mającym na celu wzmacnianie wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej, przyjętym przez Radę Europejską w dniu 4 listopada 2004 r., podkreślono potrzebę wypracowania 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 [2].

(5) Wymianę danych osobowych w ramach współpracy policyjnej i sądowej w sprawach karnych — zwłaszcza z uwagi na zasadę udostępniania informacji określoną w programie haskim — powinny wspierać jasne przepisy umacniające wzajemne zaufanie właściwych organów oraz zapewniające ochronę odnośnych informacji w sposób wyłączający wszelką dyskryminację w odniesieniu do takiej współpracy między państwami członkowskimi, przy równoczesnym pełnym poszanowaniu praw podstawowych osób fizycznych. Akty prawne obowiązujące na poziomie europejskim nie wystarczają; 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 przepływu tych danych [3] nie ma zastosowania do przetwarzania danych osobowych podczas 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.

[1] Dz.U. C 125 E z 22.5.2008, s. 154.

[2] Dz.U. C 198 z 12.8.2005, s. 1.

[3] Dz.U. L 281 z 23.11.1995, s. 31.

(6) Niniejszą decyzję ramową stosuje się wyłącznie do danych gromadzonych lub przetwarzanych przez właściwe organy w celu zapobiegania przestępstwom, ich ścigania, wykrywania lub karania lub w celu wykonywania sankcji karnych. Niniejsza decyzja ramowa powinna pozostawić w gestii państw członkowskich bardziej szczegółowe określenie na poziomie krajowym, jakie inne cele należy uważać za niezgodne z celem, do którego dane osobowe były pierwotnie gromadzone. Dalsze przetwarzanie danych osobowych do celów historycznych, statystycznych lub naukowych nie powinno na ogół być uważane za niezgodne z pierwotnym celem przetwarzania.

(7) Zakres zastosowania niniejszej decyzji ramowej jest ograniczony do przetwarzania danych osobowych przekazywanych lub udostępnianych pomiędzy państwami członkowskimi. Ograniczenie to nie powinno wywierać żadnych skutków dla kompetencji Unii do przyjmowania aktów odnoszących się do gromadzenia i przetwarzania danych osobowych na poziomie krajowym lub praktycznych uzgodnień dotyczących przyjmowania ich przez Unię w przyszłości.

(8) W celu ułatwienia wymiany danych w Unii państwa członkowskie zamierzają zapewnić, aby poziom ochrony danych osiągnięty podczas krajowego przetwarzania danych odpowiadał poziomem ochronie określonej w niniejszej decyzji ramowej. W odniesieniu do przetwarzania danych na poziomie krajowym niniejsza decyzja ramowa nie wyklucza tego, by dla ochrony danych osobowych państwa członkowskie wprowadzały gwarancje bardziej rygorystyczne niż gwarancje ustanowione na mocy niniejszej decyzji ramowej.

(9) Niniejsza decyzja ramowa nie powinna mieć zastosowania do danych osobowych, które państwo członkowskie uzyskało w ramach zakresu zastosowania niniejszej decyzji ramowej i które z tego państwa pochodzą.

(10) Zbliżenie przepisów państw członkowskich nie powinno w żadnym razie skutkować osłabieniem zapewnianej przez nie ochrony danych, a wręcz przeciwnie – powinno mieć na celu zapewnienie wysokiego poziomu ochrony w obrębie Unii.

(11) Należy wyszczególnić cele ochrony danych w ramach działań policyjnych i sądowych oraz ustanowić zasady określające, czy przetwarzanie danych osobowych jest zgodne z prawem, by dzięki temu wszelkie informacje, które mogą podlegać wymianie, były przetwarzane legalnie i zgodnie z podstawowymi zasadami odnoszącymi się do jakości danych. Jednocześnie nie powinno to w żaden sposób zagrażać legalnym działaniom organów policyjnych, celnych, sądowych ani innych właściwych organów.

(12) Zasadę ścisłości danych należy stosować, uwzględniając charakter i cel danego procesu przetwarzania. Na przykład dane uzyskiwane szczególnie w postępowaniu sądowym oparte są na indywidualnej, subiektywnej ocenie i w niektórych przypadkach są całkowicie niewerifikowalne. Zatem wymóg ścisłości danych nie może odnosić się do ścisłości oświadczenia, lecz jedynie do faktu, że dane oświadczenie zostało złożone.

(13) Archiwizowanie danych w postaci osobnego zestawu danych powinno być dopuszczalne tylko wtedy, gdy dane te nie są już wymagane ani wykorzystywane w celu zapobiegania przestępstwom, ich ścigania, wykrywania i karania oraz wykonywania sankcji karnych. Archiwizowanie danych w postaci osobnego zestawu powinno być dopuszczalne także wtedy, gdy archiwizowane dane są przechowywane w bazie danych wraz z innymi danymi w taki sposób, że nie można ich już wykorzystywać w celu zapobiegania przestępstwom, ich ścigania, wykrywania i karania oraz wykonywania sankcji karnych. Okres przechowywania danych w archiwum powinien zależeć od celu ich zarchiwizowania oraz od tego, czy leży to w uzasadnionym interesie osób, których dotyczą dane. W przypadku archiwizacji badań historycznych można także przewidzieć bardzo długi okres przechowywania.

(14) Dane mogą być usuwane również poprzez zniszczenie ich nośnika.

(15) W odniesieniu do nieścisłych, niekompletnych lub nieaktualnych danych przekazanych lub udostępnionych innym państwom członkowskim i przetwarzanych dalej przez organy quasi-sądowe, to jest organy uprawnione do podejmowania wiążących prawnie decyzji, korektę lub usuwanie danych, lub blokowanie do nich dostępu powinno być prowadzone zgodnie z prawem krajowym.

(16) Zapewnienie osobom fizycznym wysokiego poziomu ochrony danych osobowych wymaga wspólnych przepisów, które określą zgodność z prawem i jakość danych przetwarzanych przez właściwe organy w innych państwach członkowskich.

(17) Celowe jest, aby na szczeblu europejskim określić, pod jakimi warunkami właściwe organy państw członkowskich mogą przekazywać i udostępniać dane osobowe otrzymane od innych państw członkowskich organom publicznym i podmiotom prywatnym w państwach członkowskich. W wielu przypadkach przekazywanie danych osobowych przez organy sądowe, policyjne lub celne podmiotom prywatnym jest konieczne, by można było karać przestępstwa lub zapobiegać bezpośrednim i poważnym zagrożeniom bezpieczeństwa publicznego lub zapobiegać poważnym naruszeniom praw osób fizycznych, na przykład poprzez powiadamianie banków i instytucji kredytowych o fałszerstwach papierów wartościowych lub – w związku z przestępstwami związanymi z pojazdami – poprzez przekazywanie firmom ubezpieczeniowym danych osobowych, by zapobiegać nielegalnemu handlowi skradzionymi pojazdami silnikowymi lub by usprawnić odzyskiwanie skradzionych samochodów z zagranicy. Niniejszy przepis nie dotyczy przekazywania zadań policyjnych lub sądowych podmiotom prywatnym.

(18) Zawarte w niniejszej decyzji ramowej zasady dotyczące przekazywania danych osobowych przez organy sądowe, policyjne lub celne podmiotom prywatnym nie dotyczą ujawniania danych podmiotom prywatnym (takim jak adwokaci i ofiary przestępstwa) w kontekście postępowania karnego.

(19) Dalsze przetwarzanie danych osobowych uzyskanych od właściwego organu innego państwa członkowskiego lub udostępnionych przez ten organ, a zwłaszcza dalsze przekazywanie lub udostępnianie takich danych, powinno podlegać wspólnym zasadom na szczeblu europejskim.

(20) Jeżeli dane osobowe mogą być dalej przetwarzane za zgodą państwa członkowskiego, od którego te dane uzyskano, to każde państwo członkowskie powinno mieć możliwość określenia warunków takiej zgody, w tym na przykład poprzez udzielenie ogólnej zgody co do określonych kategorii informacji lub określonych kategorii dalszego przetwarzania.

(21) Jeżeli dane osobowe mogą być dalej przetwarzane w postępowaniach administracyjnych, to postępowania te obejmują też czynności prowadzone przez organy regulacyjne i nadzorcze.

(22) Legalne działania organów policyjnych, celnych, sądowych i innych właściwych organów mogą wymagać przesyłania danych organom państw trzecich lub organizacjom międzynarodowym, które zobowiązane są do zapobiegania przestępstwom, ich ścigania, wykrywania lub karania lub do wykonywania sankcji karnych.

(23) Jeżeli państwo członkowskie przekazuje dane osobowe państwom trzecim lub podmiotom międzynarodowym, dane te powinny z zasady być odpowiednio chronione.

(24) Przekazywanie danych osobowych z któregokolwiek państwa członkowskiego do państw trzecich lub podmiotów międzynarodowych powinno zasadniczo mieć miejsce wyłącznie za zgodą na ich przekazanie wydaną przez państwo członkowskie, od którego uzyskano te dane. Każde państwo członkowskie powinno mieć możliwość określenia warunków takiej zgody, w tym na przykład poprzez udzielenie ogólnej zgody co do określonych kategorii informacji lub określonych państw.

(25) Dla dobra sprawnej ochrony porządku publicznego konieczne jest, by – gdy charakter zagrożenia bezpieczeństwa publicznego w państwie członkowskim lub państwie trzecim jest tak bezpośredni, że uniemożliwia uzyskanie uprzedniej zgody na czas – właściwy organ mógł przekazać stosowne dane osobowe zainteresowanemu państwu trzeciemu bez takiej uprzedniej zgody. Ta sama zasada mogłaby mieć zastosowanie, gdy wchodzą w grę inne podstawowe i równie istotne interesy państwa członkowskiego, np. gdy mogłaby być bezpośrednio i poważnie zagrożona infrastruktura krytyczna państwa członkowskiego lub gdy system finansowy państwa członkowskiego mógłby zostać poważnie naruszony.

(26) Może być konieczne, aby informować osoby, których dotyczą dane, o przetwarzaniu ich danych — zwłaszcza gdy tajne czynności pobierania danych spowodowały poważną ingerencję w ich prawa — i w ten sposób zapewnić im możliwość skorzystania ze skutecznej ochrony prawnej.

(27) Państwo członkowskie powinno zapewnić poinformowanie osoby, której dotyczą dane, o tym, że jej dane osobowe mogą być lub są gromadzone, przetwarzane lub przekazywane innemu państwu członkowskiemu do zapobiegania przestępstwom, prowadzenia dochodzeń, wykrywania przestępstw, ich ścigania lub do wykonywania sankcji karnych. Warunki realizacji prawa osoby, której dotyczą dane, do otrzymywania informacji, oraz odnośne wyjątki powinny być określone w prawie krajowym. Może przybrać to formę ogólną, na przykład przez uchwalenie przepisów lub opublikowanie wykazu operacji przetwarzania.

(28) Aby zapewnić ochronę danych osobowych, a równocześnie nie udaremniać celu dochodzenia w sprawach karnych, należy określić prawa osoby, której dotyczą dane.

(29) Niektóre państwa członkowskie zapewniły osobie, której dotyczą dane wykorzystywane w postępowaniu karnym, prawo do dostępu do tych danych przez system, w którym krajowy organ nadzoru ma w zastępstwie tej osoby nieograniczony dostęp do wszystkich danych osobowych z nią związanych oraz może korygować, usuwać lub aktualizować nieścisłe dane. Jeżeli chodzi o taki pośredni dostęp, prawo krajowe tych państw członkowskich może stanowić, że krajowy organ nadzoru będzie informował osobę, której dotyczą dane, wyłącznie o tym, że dokonano wszystkich niezbędnych weryfikacji. Jednakże w konkretnych sprawach, takich jak dostęp do rejestrów sądowych w celu otrzymania wypisu ze swojej kartoteki w rejestrze karnym lub dokumentów dotyczących przesłuchania przez służby policyjne, odnośne państwa członkowskie stwarzają osobie, której dotyczą dane, także możliwość bezpośredniego dostępu do tych danych.

(30) Celowe jest, aby ustanowić wspólne zasady poufności i bezpieczeństwa w przetwarzaniu danych, zasady odpowiedzialności prawnej i sankcje za niezgodne z prawem wykorzystanie danych przez właściwe organy, jak również środki odwoławcze dla osób, których dotyczą dane. Jednak każde państwo członkowskie już we własnym zakresie decyduje, jakie przepisy stosuje w dziedzinie odszkodowań i jakie sankcje za naruszenie krajowych przepisów o ochronie danych.

(31) Niniejsza decyzja ramowa pozwala, by podczas realizacji ustanowionych w niej zasad uwzględnić zasadę publicznego dostępu do dokumentów urzędowych.

(32) Gdy konieczna jest ochrona danych osobowych w związku z przetwarzaniem, które ze względu na swoją skalę lub rodzaj stanowi określone zagrożenie dla podstawowych praw i wolności, na przykład przetwarzaniem z wykorzystaniem nowych technologii, mechanizmów lub procedur, należy zapewnić konsultacje z właściwymi krajowymi organami nadzoru przed utworzeniem zbiorów danych przeznaczonych do przetwarzania tych danych.

(33) 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.

(34) Organy nadzorcze ustanowione już w państwach członkowskich na mocy dyrektywy 95/46/WE powinny mieć także możliwość podejmowania zadań, które mają zostać powierzone krajowym organom nadzoru ustanowionym na mocy niniejszej decyzji ramowej.

(35) Te organy nadzorcze powinny dysponować środkami niezbędnymi do wykonywania swoich zadań, w tym uprawnieniami dochodzeniowymi i interwencyjnymi, szczególnie na wypadek skarg osób fizycznych, lub uprawnieniami do tego, by wnosić sprawę do sądu. Te organy nadzorcze powinny pomagać w zapewnianiu przejrzystości przetwarzania danych w państwach członkowskich, których jurysdykcji podlegają. Jednakże uprawnienia tych organów nie powinny kolidować ze szczególnymi zasadami określonymi w odniesieniu do postępowań karnych ani z niezawisłością wymiaru sprawiedliwości.

(36) Artykuł 47 Traktatu o Unii Europejskiej stanowi, że żadne postanowienie tego Traktatu nie może naruszać traktatów ustanawiających Wspólnoty Europejskie ani późniejszych traktatów lub aktów prawnych zmieniających lub uzupełniających te traktaty. Zatem niniejsza decyzja ramowa nie wpływa również na ochronę danych osobowych na mocy prawa wspólnotowego, a w szczególności nie narusza przepisów dyrektywy 95/46/WE, 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 ([1]) ani dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) ([2]).

(37) Niniejsza decyzja ramowa nie narusza przepisów, które dotyczą bezprawnego dostępu do danych i są określone w decyzji ramowej Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne ([3]).

(38) Niniejsza decyzja ramowa nie narusza istniejących obowiązków i zobowiązań państw członkowskich lub Unii wynikających z dwustronnych lub wielostronnych umów z państwami trzecimi. Umowy, które zostaną zawarte w przyszłości, powinny być zgodne z przepisami o wymianie danych z państwami trzecimi.

(39) Kilka aktów przyjętych na podstawie tytułu VI Traktatu o Unii Europejskiej zawiera szczegółowe przepisy o ochronie danych osobowych wymienianych lub inaczej przetwarzanych zgodnie z tymi aktami. W niektórych przypadkach przepisy te stanowią wyczerpujący i spójny zbiór zasad obejmujących wszystkie istotne aspekty ochrony danych (zasady jakości danych, ich bezpieczeństwa, uregulowania co do praw i gwarancji przysługujących osobom, których dotyczą dane, regulacje co do organizacji nadzoru oraz odpowiedzialności prawnej) oraz regulują te kwestie bardziej szczegółowo niż niniejsza decyzja ramowa. Odnośne przepisy o ochronie danych określone w tych aktach, zwłaszcza w aktach regulujących działanie Europolu, Eurojustu, Systemu Informacji Schengen (SIS) i Systemu Informacji Celnej (CIS) oraz aktach dających organom państw członkowskich bezpośredni dostęp do niektórych systemów danych innych państw członkowskich, nie powinny zostać naruszone przez niniejszą decyzję ramową. To samo ma zastosowanie do przepisów o ochronie danych regulujące zautomatyzowane przekazywanie profili DNA, danych daktyloskopijnych i krajowych danych o rejestracji pojazdów między państwami członkowskimi na podstawie decyzji Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej ([4]).

(40) W innych przypadkach przepisy o ochronie danych zawarte w aktach, które przyjęto na podstawie tytułu VI Traktatu o Unii Europejskiej, mają węższy zakres zastosowania. Przepisy te narzucają często państwu członkowskiemu, które od innych państw członkowskich otrzymuje informacje z danymi osobowymi, określone warunki co do celów, do jakich może ono wykorzystywać te dane, ale w innych kwestiach ochrony danych odsyłają do konwencji Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, lub do prawa krajowego. Jeżeli przepisy tych aktów, które otrzymującemu państwu członkowskiemu narzucają warunki wykorzystywania lub dalszego przekazywania danych osobowych, są bardziej rygorystyczne niż przepisy zawarte w odnośnych częściach niniejszej decyzji ramowej, to te pierwsze przepisy powinny zachować niezmienioną moc. Jednakże pod wszystkimi innymi względami należy stosować przepisy określone w niniejszej decyzji ramowej.

(41) Niniejsza decyzja ramowa nie narusza konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych ani protokołu dodatkowego do tej konwencji z dnia 8 listopada 2001 r., ani też konwencji Rady Europy o współpracy sądowej w sprawach karnych.

([1]) Dz.U. L 8 z 12.1.2001, s. 1.
([2]) Dz.U. L 201 z 31.7.2002, s. 37.
([3]) Dz.U. L 69 z 16.3.2005, s. 67.
([4]) Dz.U. L 210 z 6.8.2008, s. 1.

(42) W związku z tym, że cel niniejszej decyzji ramowej, mianowicie określenie wspólnych zasad ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, nie mogą być w stopniu wystarczającym osiągnięte przez państwa członkowskie, natomiast z uwagi na skalę i skutki działania mogą zostać osiągnięte z większym powodzeniem na poziomie Unii, Unia może podjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu ustanawiającego Wspólnotę Europejską i o której mowa w art. 2 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w art. 5 Traktatu ustanawiającego Wspólnotę Europejską niniejsza decyzja ramowa nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.

(43) Zjednoczone Królestwo uczestniczy w niniejszej decyzji ramowej zgodnie z art. 5 Protokołu włączającego dorobek Schengen w ramy Unii Europejskiej, dołączonego do Traktatu o Unii Europejskiej i Traktatu ustanawiającego Wspólnotę Europejską, oraz art. 8 ust. 2 decyzji Rady 2000/365/WE z dnia 29 maja 2000 r. dotyczącej wniosku Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej o zastosowanie wobec niego niektórych przepisów dorobku Schengen ([1]).

(44) Irlandia uczestniczy w niniejszej decyzji ramowej zgodnie z art. 5 Protokołu włączającego dorobek Schengen w ramy Unii Europejskiej, załączonego do Traktatu o Unii Europejskiej i Traktatu ustanawiającego Wspólnotę Europejską, 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 ([2]).

(45) 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 ([3]), które wchodzą w zakres obszarów, o których mowa w art. 1 pkt H oraz I decyzji Rady 1999/437/WE ([4]) w sprawie niektórych warunków stosowania tego układu.

(46) W odniesieniu do Szwajcarii niniejsza decyzja ramowa stanowi rozwinięcie tych przepisów dorobku Schengen — w rozumieniu Umowy zawartej między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen ([5]) — które wchodzą w zakres obszarów, o których mowa w art. 1 pkt H oraz I decyzji 1999/437/WE w związku z art. 3 decyzji Rady 2008/149/WSiSW ([6]) w sprawie podpisania tej umowy w imieniu Unii Europejskiej.

(47) W odniesieniu do Liechtensteinu niniejsza decyzja ramowa stanowi rozwinięcie tych przepisów dorobku Schengen — w rozumieniu Protokołu między Unią Europejską, Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu o przystąpieniu Księstwa Liechtensteinu do Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen — które wchodzą w zakres obszarów, o których mowa w art. 1 pkt H oraz I decyzji Rady 1999/437/WE w związku z art. 3 decyzji Rady 2008/262/WSiSW ([7]) w sprawie podpisania tego protokołu w imieniu Unii Europejskiej.

(48) Niniejsza decyzja ramowa nie narusza praw podstawowych i jest zgodna z zasadami uznanymi w szczególności w Karcie praw podstawowych Unii Europejskiej ([8]). Niniejsza decyzja ramowa ma zapewnić pełne poszanowanie prawa do prywatności i do uzyskania ochrony danych osobowych, które to prawa odzwierciedlone są w art. 7 i 8 Karty,

PRZYJMUJE NINIEJSZĄ DECYZJĘ RAMOWĄ:

Artykuł 1

Cel i zakres zastosowania

1. Celem niniejszej decyzji ramowej jest zapewnienie wysokiego poziomu ochrony praw podstawowych i wolności osób fizycznych, a zwłaszcza ich prawa do prywatności, podczas przetwarzania danych osobowych w ramach współpracy policyjnej i sądowej w sprawach karnych, o której mowa w tytule VI Traktatu o Unii Europejskiej, przy równoczesnym zagwarantowaniu wysokiego poziomu bezpieczeństwa publicznego.

2. Zgodnie z niniejszą decyzją ramową państwa członkowskie chronią prawa podstawowe i wolności osób fizycznych, a zwłaszcza ich prawo do prywatności, gdy w celu zapobiegania przestępstwom, wykrywania przestępstw, ich ścigania lub karania lub wykonywania sankcji karnych dane osobowe:

a) są przekazywane lub udostępniane między państwami członkowskimi lub też zostały już przez nie sobie nawzajem przekazane lub udostępnione;

([1]) Dz.U. L 131 z 1.6.2000, s. 43.
([2]) Dz.U. L 64 z 7.3.2002, s. 20.
([3]) Dz.U. L 176 z 10.7.1999, s. 36.
([4]) Dz.U. L 176 z 10.7.1999, s. 31.
([5]) Dz.U. L 53 z 27.2.2008, s. 52.
([6]) Dz.U. L 53 z 27.2.2008, s. 50.
([7]) Dz.U. L 83 z 26.3.2008, s. 5.
([8]) Dz.U. C 303 z 14.12.2007, s. 1.

b) są przekazywane lub udostępniane przez państwa członkowskie organom lub systemom informacyjnym utworzonym na podstawie tytułu VI Traktatu o Unii Europejskiej lub też zostały już im przekazane lub udostępnione; lub

c) są przekazywane lub udostępniane właściwym organom państw członkowskich przez organy lub systemy informacyjne utworzone na podstawie Traktatu o Unii Europejskiej lub Traktatu ustanawiającego Wspólnotę Europejską lub też zostały już przez nie przekazane lub udostępnione.

3. Niniejszą decyzję ramową stosuje się do przetwarzania całkowicie lub częściowo w sposób zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych, które stanowią lub mają stanowić część zbioru danych.

4. Niniejsza decyzja ramowa nie narusza podstawowych interesów bezpieczeństwa narodowego i określonych działań wywiadowczych w zakresie bezpieczeństwa narodowego.

5. Niniejsza decyzja ramowa nie stanowi dla państw członkowskich przeszkody w ustanawianiu wyższych gwarancji ochrony bezpieczeństwa danych osobowych gromadzonych lub przetwarzanych na szczeblu krajowym niż gwarancje ustanowione na mocy niniejszej decyzji ramowej.

Artykuł 2

Definicje

Do celów niniejszej decyzji ramowej:

a) „dane osobowe" oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dotyczą dane"); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny lub jeden lub więcej szczególnych czynników określających jej tożsamością fizyczną, fizjologiczną, psychiczną, ekonomiczną, kulturową czy społeczną;

b) „przetwarzanie danych osobowych" oraz „przetwarzanie" oznacza każdą operację lub zestaw operacji dokonywanych na danych osobowych w sposób zautomatyzowany lub inny, takich jak gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez przekazanie, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie;

c) „blokowanie" oznacza znakowanie przechowywanych danych osobowych w celu ograniczenia ich przetwarzania w przyszłości;

d) „zbiór danych osobowych" oraz „zbiór" oznacza każdy uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, scentralizowany, zdecentralizowany lub rozproszony funkcjonalnie lub geograficznie;

e) „przetwarzający dane" oznacza każdy organ, który dane osobowe przetwarza w imieniu administratora danych;

f) „odbiorca" oznacza każdy organ, któremu dane są ujawniane;

g) „zgoda osoby, której dotyczą dane" oznacza dobrowolne konkretne i świadome oświadczenie woli, przez które osoba, której dotyczą dane, wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych;

h) „właściwe organy" oznaczają agencje lub organy utworzone na mocy aktów przyjętych przez Radę na podstawie tytułu VI Traktatu o Unii Europejskiej, oraz organy policyjne, celne, sądowe i inne właściwe organy państw członkowskich, które to organy na mocy prawa krajowego upoważnione są do przetwarzania danych osobowych w zakresie stosowania niniejszej decyzji ramowej;

i) „administrator danych" oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny organ, który samodzielnie lub wspólnie z innymi określa cele i sposoby przetwarzania danych osobowych;

j) „wstawianie odnośników" oznacza znakowanie przechowywanych danych osobowych, którego celem nie jest ograniczenie ich przetwarzania w przyszłości;

k) „anonimizacja danych" oznacza takie przekształcenie danych osobowych, po którym nie można już przyporządkować poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo można tego dokonać jedynie niewspółmiernie dużym nakładem czasu, kosztów i sił.

Artykuł 3

Zasady legalności, proporcjonalności i celowości

1. Właściwe organy mogą gromadzić dane osobowe tylko do określonych, jednoznacznych i legalnych celów w ramach swoich zadań oraz przetwarzać je tylko do celów, w jakich zostały zgromadzone. Dane są przetwarzane zgodnie z prawem, adekwatnie do celu, w jakim są gromadzone, w związku z tym celem i w sposób niewykraczający poza ten cel.

2. Dane wolno przetwarzać dalej w innym celu, o ile:

a) nie jest to sprzeczne z celami, w jakich zostały zgromadzone;

b) właściwe organy są upoważnione do tego, by przetwarzać takie dane w takim innym celu zgodnie z obowiązującymi przepisami prawa; oraz

c) przetwarzanie jest konieczne i proporcjonalne względem tego innego celu.

Ponadto właściwe organy mogą otrzymane dane przetwarzać dalej w celach historycznych, statystycznych lub naukowych, o ile państwa członkowskie zapewniają odpowiednie gwarancje, takie jak anonimizacja danych.

Artykuł 4

Korekta i usuwanie danych oraz blokowanie dostępu do nich

1. Dane osobowe są korygowane, jeżeli są nieścisłe, oraz w miarę możliwości i potrzeb uzupełniane i aktualizowane.

2. Dane osobowe zostają usunięte lub zanonimizowane, jeżeli nie są już potrzebne w celach, do których zostały legalnie zgromadzone lub w których są legalnie dalej przetwarzane. Niniejszy przepis nie wpływa na archiwizację tych danych w osobnym zbiorze przez odpowiedni okres zgodnie z prawem krajowym.

3. Dane osobowe blokuje się zamiast ich usunięcia, jeżeli istnieją uzasadnione podstawy, by sądzić, że usunięcie danych godziłoby w słuszne interesy osoby, której dotyczą dane. Dane, do których dostęp został zablokowany, mogą być przetwarzane jedynie w celu, z uwagi na który ich usunięcie nie było możliwe.

4. Jeżeli dane osobowe są zawarte w orzeczeniu sądowym lub zapisie związanym z wydaniem orzeczenia sądowego, korektę, usunięcie lub zablokowanie dostępu przeprowadza się zgodnie z krajowymi przepisami dotyczącymi postępowania sądowego.

Artykuł 5

Ustalenie terminów usunięcia danych i przeglądu

Ustala się odpowiednie terminy usunięcia danych osobowych lub okresowego przeglądu, mającego na celu ustalenie potrzeby dalszego przechowywania danych. Przestrzeganie tych terminów zapewniają odpowiednie rozwiązania proceduralne.

Artykuł 6

Przetwarzanie szczególnych kategorii danych

Dane osobowe, które ujawniają pochodzenie rasowe i etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe albo przynależność do związków zawodowych, oraz dane osobowe dotyczące stanu zdrowia i seksualności wolno przetwarzać tylko wtedy, gdy jest to bezwzględnie konieczne i gdy prawo krajowe przewiduje stosowne gwarancje.

Artykuł 7

Zautomatyzowane decyzje w indywidualnych sprawach

Decyzja wywołująca niekorzystne skutki prawne dla osoby, której dotyczą dane, lub mająca na tę osobę istotny wpływ i oparta wyłącznie na zautomatyzowanym przetwarzaniu danych mającym służyć ocenie niektórych aspektów o charakterze osobistym dotyczących osoby, której dotyczą dane, jest dopuszczalna tylko w przypadkach dozwolonych prawem, które przewiduje również środki ochrony uzasadnionych interesów osoby, której dotyczą dane.

Artykuł 8

Weryfikacja jakości przekazywanych lub udostępnianych danych

1. Właściwe organy podejmują wszelkie uzasadnione działania, aby nieścisłe, niepełne lub nieaktualne już dane osobowe nie były przekazywane ani udostępniane. W tym celu właściwe organy w miarę możliwości weryfikują jakość danych osobowych przed ich przekazaniem lub udostępnieniem. Ilekroć przekazuje się dane, dołącza się do nich w miarę możliwości informacje, dzięki którym odbierające je państwo członkowskie może ocenić stopień ścisłości, kompletności, aktualności i rzetelności tych danych. Jeżeli dane osobowe zostały przekazane w braku wniosku, odbierający je organ bezzwłocznie sprawdza, czy dane te są potrzebne w celach, w których zostały przekazane.

2. Jeżeli stwierdzono, że przekazano dane nieprawidłowe lub że dane przekazano nielegalnie, należy o tym bezzwłocznie poinformować odbiorcę. Takie dane muszą zostać bezzwłocznie skorygowane, usunięte lub zablokowane zgodnie z art. 4.

Artykuł 9

Terminy

1. W momencie przekazania lub udostępniania danych organ przekazujący może, zgodnie z prawem krajowym i zgodnie z art. 4 i 5, wskazać terminy przechowywania danych, po których upływie odbiorca musi te dane usunąć lub zablokować, lub dokonać przeglądu, mającego na celu ustalenie ich dalszej przydatności. Obowiązek ten nie ma zastosowania, jeżeli – w chwili upłynięcia tych terminów – dane są wymagane na potrzeby bieżącego ścigania lub karania przestępstw lub wykonywania sankcji karnych.

2. Jeżeli organ przekazujący dane nie wskazał terminu zgodnie z ust. 1, stosuje się terminy przechowywania danych określone prawem krajowym odbierającego je państwa członkowskiego, o których mowa w art. 4 i 5.

Artykuł 10

Odnotowywanie i dokumentacja

1. Każdy przypadek przekazania danych osobowych należy odnotować lub udokumentować w celach weryfikacji legalności przetwarzania danych i samokontroli oraz zapewnienia odpowiedniej integralności i bezpieczeństwa danych.

2. Wpisy lub dokumentacja sporządzone na mocy ust. 1 udostępniane są właściwemu organowi nadzoru, na jego żądanie, w celu kontroli ochrony danych. Właściwy organ nadzoru wykorzystuje te informacje wyłącznie w celu kontroli ochrony danych oraz zapewnienia odpowiedniego przetwarzania danych, jak również integralności i bezpieczeństwa danych.

Artykuł 11

Przetwarzanie danych osobowych otrzymanych lub udostępnionych przez inne państwo członkowskie

Dane osobowe otrzymane lub udostępnione przez właściwy organ innego państwa członkowskiego mogą być dalej przetwarzane zgodnie z wymogami określonymi w art. 3 ust. 2 wyłącznie w następujących celach, innych niż te, do których zostały przekazane lub udostępnione:

a) zapobieganie przestępstwom, ich ściganie, wykrywanie lub karanie lub wykonywanie sankcji karnych – w odniesieniu do przestępstw i sankcji karnych innych niż te, w stosunku do których przekazano lub udostępniono przedmiotowe dane;

b) inne postępowania sądowe i administracyjne bezpośrednio związane z zapobieganiem przestępstwom, ich ściganiem, wykrywaniem lub karaniem lub z wykonywaniem sankcji karnych;

c) zażegnania bezpośredniego i poważnego zagrożenia bezpieczeństwa publicznego; lub

d) w innym celu — wyłącznie za uprzednią zgodą państwa członkowskiego przekazującego dane lub za zgodą osoby, której dotyczą dane, udzieloną zgodnie z prawem krajowym.

Ponadto właściwe organy mogą otrzymane dane przetwarzać dalej w celach historycznych, statystycznych lub naukowych, o ile państwa członkowskie zapewniają odpowiednie gwarancje, takie jak anonimizacja danych.

Artykuł 12

Przestrzeganie krajowych ograniczeń w przetwarzaniu danych

1. Jeżeli, zgodnie z prawem przekazującego państwa członkowskiego, w określonych przypadkach do wymiany danych między właściwymi organami w tym państwie członkowskim mają zastosowanie szczególne ograniczenia w przetwarzaniu danych, organ przekazujący informuje odbiorcę o takich ograniczeniach. Odbiorca zapewnia, aby te ograniczenia w przetwarzaniu były przestrzegane.

2. W ramach stosowania ust. 1 państwa członkowskie nie stosują ograniczeń dotyczących przekazywania danych innym państwom członkowskim lub agencjom lub organom utworzonym na mocy tytułu VI Traktatu o Unii Europejskiej innych niż ograniczenia stosowane w analogicznych przypadkach przekazywania danych w kraju.

Artykuł 13

Przekazywanie danych właściwym organom w państwach trzecich lub instytucjom międzynarodowym

1. Państwa członkowskie określają, że dane osobowe przekazane lub udostępnione przez właściwy organ innego państwa członkowskiego mogą być przekazywane państwom trzecim lub instytucjom międzynarodowym tylko wtedy, gdy:

a) jest to konieczne do zapobiegania przestępstwom, ich ścigania, wykrywania lub karania lub do wykonywania sankcji karnych;

b) otrzymujący organ w państwie trzecim lub otrzymująca instytucja międzynarodowa odpowiadają za zapobieganie przestępstwom, ich ściganie, wykrywanie lub karanie lub za wykonywanie sankcji karnych;

c) państwo członkowskie, od którego uzyskano dane, wyraziło zgodę na ich przekazanie zgodnie ze swoim prawem krajowym; oraz

d) dane państwo trzecie lub dana instytucja międzynarodowa zapewniają odpowiedni stopień ochrony dla mającego nastąpić przetwarzania danych.

2. Przekazywanie danych bez uprzedniej zgody, o której mowa w ust. 1 lit. c), dopuszczalne jest jedynie wtedy, gdy przekazanie jest niezbędne dla zażegnania bezpośredniego i poważnego zagrożenia bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego lub podstawowych interesów państwa członkowskiego, a uprzedniej zgody nie można uzyskać na czas. Niezwłocznie informuje się o tym organ odpowiedzialny za wydanie zgody.

3. Na zasadzie odstępstwa od ust. 1 lit. d) dane osobowe można przekazać, gdy:

a) prawo krajowe państwa członkowskiego przekazującego na to zezwala ze względu na:

   (i) określony uzasadniony interes osoby, której dotyczą dane; lub

   (ii) uzasadniony interes ogólny, zwłaszcza z uwagi na ważny interes publiczny; lub

b) państwo trzecie lub otrzymująca instytucja międzynarodowa przewidują gwarancje, które dane państwo członkowskie uważa za odpowiednie zgodnie ze swoim prawem krajowym.

4. Odpowiedniość stopnia ochrony, o którym mowa w ust. 1 lit. d), jest oceniana w świetle wszystkich okoliczności towarzyszących operacji przekazania danych lub zestawu takich operacji. Szczególną uwagę zwraca się na charakter danych, cel i czas trwania proponowanej operacji lub proponowanych operacji przetwarzania, państwo pochodzenia danych oraz państwo lub instytucję międzynarodową ostatecznego przeznaczenia danych, przepisy prawa — zarówno ogólne, jak i branżowe — obowiązujące w danym państwie trzecim lub w danej instytucji międzynarodowej oraz stosowane zasady zawodowe i środki zabezpieczenia.

Artykuł 14

Przekazywanie danych podmiotom prywatnym w państwach członkowskich

1. Państwa członkowskie określają, że dane osobowe przekazane lub udostępnione przez właściwy organ innego państwa członkowskiego mogą być przekazywane podmiotom prywatnym tylko wtedy, gdy:

a) właściwy organ państwa członkowskiego, z którego uzyskano odnośne dane, wyraził zgodę na ich przekazanie zgodnie ze swoim prawem krajowym;

b) nie istnieje żaden szczególny uzasadniony interes osoby, której dotyczą dane, zapobiegający przekazaniu; oraz

c) w szczególnych przypadkach przekazanie danych ma dla właściwego organu, który przekazuje dane podmiotowi prywatnemu, zasadnicze znaczenie, z uwagi na:

(i) wykonywanie zadań przyznanych mu zgodnie z prawem;

(ii) zapobieganie przestępstwom, ich wykrywanie lub ściganie lub wykonywanie sankcji karnych;

(iii) zażegnanie bezpośredniego i poważnego zagrożenia bezpieczeństwa publicznego; lub

(iv) zapobieżenie poważnemu naruszeniu praw osób fizycznych.

2. Właściwy organ przekazujący dane podmiotowi prywatnemu informuje go o celach, do jakich dane te mogą zostać wyłącznie wykorzystane.

Artykuł 15

Informacje udzielane na wniosek właściwego organu

Na wniosek właściwego organu, który przekazał lub udostępnił dane osobowe, odbiorca informuje ten organ o ich przetwarzaniu.

Artykuł 16

Informacje przeznaczone dla osoby, której dotyczą dane

1. Państwa członkowskie zapewniają, aby ich właściwe organy informowały zgodnie z prawem krajowym osobę, której dotyczą dane, o gromadzeniu lub przetwarzaniu jej danych osobowych.

2. Jeżeli dane osobowe zostały przekazane lub udostępnione między państwami członkowskimi, każde państwo członkowskie może zgodnie z przepisami swojego prawa krajowego, o których mowa w ust. 1, zwrócić się do tego drugiego państwa członkowskiego z prośbą o nieinformowanie osoby, której dotyczą dane. W takim przypadku to drugie państwo członkowskie nie informuje osoby, której dotyczą dane, bez uprzedniej zgody tego pierwszego państwa członkowskiego.

Artykuł 17

Prawo dostępu

1. Każda osoba, której dotyczą dane, ma prawo otrzymać, na wniosek wyrażony w rozsądnych odstępach czasu, bez ograniczeń i bez nadmiernego opóźnienia lub nadmiernie wysokich kosztów:

a) przynajmniej potwierdzenie ze strony administratora danych lub krajowego organu nadzoru, czy odnoszące się do niej dane zostały przekazane lub udostępnione, oraz informacje o odbiorcy lub kategoriach odbiorców, którym dane zostały ujawnione, a także powiadomienie o tym, które dane są przetwarzane; lub

b) przynajmniej potwierdzenie ze strony krajowego organu nadzoru, że dokonano wszystkich koniecznych weryfikacji.

2. Państwa członkowskie mogą przyjmować środki ustawodawcze ograniczające dostęp do informacji, o których mowa w ust. 1 lit. a), jeżeli takie ograniczenie, z należytym uwzględnieniem uzasadnionego interesu odnośnej osoby, stanowi konieczny i proporcjonalny środek:

a) pozwalający uniknąć przeszkód w urzędowych lub prawnych śledztwach, dochodzeniach lub postępowaniach;

b) pozwalający uniknąć niekorzystnego wpływu na zapobieganie przestępstwom, ich ściganie, wykrywanie lub karanie lub na wykonywanie sankcji karnych;

c) służący ochronie bezpieczeństwa publicznego;

d) służący ochronie bezpieczeństwa narodowego;

e) służący ochronie osoby, której dotyczą dane, oraz praw i wolności innych osób.

3. Każda odmowa lub ograniczenie dostępu zostaje przedstawione na piśmie osobie, której dotyczą dane. Równocześnie przedstawia się jej podstawy faktyczne lub prawne, na których opiera się decyzja. Od ich przedstawienia można odstąpić w przypadkach, o których mowa w ust. 2 lit. a)–e). We wszystkich tych przypadkach poucza się osobę, której dotyczą dane, o możliwości wniesienia odwołania do właściwego krajowego organu nadzoru, organu sądowego lub sądu.

Artykuł 18

Prawo do uzyskania korekty danych, ich usunięcia lub zablokowania do nich dostępu

1. Osoba, której dotyczą dane, ma prawo oczekiwać, że administrator danych wywiąże się ze swoich obowiązków określonych w art. 4, 8 i 9, dotyczących korygowania, usuwania danych osobowych i blokowania do nich dostępu, a które to obowiązki wynikają z niniejszej decyzji ramowej. Państwa członkowskie decydują, czy osoba, której dotyczą dane, może dochodzić tego prawa bezpośrednio u administratora danych czy za pośrednictwem właściwego krajowego organu nadzoru. Jeżeli administrator danych odmówi skorygowania, usunięcia danych lub zablokowania do nich dostępu, odmowę tę należy przekazać osobie, której dotyczą dane, na piśmie oraz poinformować ją o możliwościach składania zażaleń lub korzystania ze środków odwoławczych przewidzianych prawem krajowym. Po rozpatrzeniu zażalenia lub środka odwoławczego informuje się osobę, której dotyczą dane, czy administrator danych działał właściwie. Państwa członkowskie mogą także postanowić, że osoba, której dotyczą dane, zostaje poinformowana przez właściwy krajowy organ nadzoru, że przeprowadzono przegląd.

2. Jeżeli osoba, której dotyczą dane, kwestionuje ścisłość jakiegoś elementu swoich danych osobowych, i o ścisłości tego elementu nie można rozstrzygnąć, w odniesieniu do tego elementu można wstawić odnośnik.

Artykuł 19

Prawo do odszkodowania

1. Każda osoba, która poniosła szkodę w wyniku niezgodnej z prawem operacji przetwarzania danych lub w wyniku innego czynu niezgodnego z przepisami krajowymi przyjętymi zgodnie z niniejszą decyzją ramową, jest uprawniona do otrzymania odszkodowania za wyrządzoną szkodę od administratora danych lub innego organu właściwego zgodnie z prawem krajowym.

2. Jeżeli dane osobowe zostały przekazane przez właściwy organ innego państwa członkowskiego, odbiorca, ponosząc zgodnie z prawem krajowym odpowiedzialność wobec poszkodowanego, nie może na swoją obronę powoływać się na zarzut nieścisłości otrzymanych danych. Jeżeli odbiorca wypłaci odszkodowanie za szkodę spowodowaną korzystaniem z nieprawidłowo przekazanych danych, właściwy organ, które dane te przekazał, zwraca odbiorcy kwotę wypłaconego odszkodowania, uwzględniając ewentualne błędy leżące po stronie odbiorcy.

Artykuł 20

Środki odwoławcze

Bez uszczerbku dla możliwości skorzystania z administracyjnych środków odwoławczych, jakie mogą być przewidziane przed skierowaniem sprawy do organu sądowego, osoba, której dotyczą dane, ma prawo do skorzystania ze środka odwoławczego w przypadku naruszenia jej praw zagwarantowanych obowiązującym prawem krajowym.

Artykuł 21

Poufność przetwarzania danych

1. Każda osoba, które ma dostęp do danych osobowych objętych zakresem stosowania niniejszej decyzji ramowej, może przetwarzać te dane tylko wtedy, gdy jest pracownikiem właściwego organu lub gdy działa na jego polecenie, chyba że obowiązek przetwarzania wynika z mocy prawa.

2. Osoby pracujące we właściwym organie państwa członkowskiego podlegają wszystkim przepisom o ochronie danych, które obowiązują dany właściwy organ.

Artykuł 22

Bezpieczeństwo przetwarzania danych

1. Państwa członkowskie określają, że właściwe organy muszą wdrożyć odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed ich przypadkowym lub nielegalnym zniszczeniem, przypadkową utratą, modyfikacją, nieuprawnionym ujawnieniem lub dostępem do nich — w szczególności gdy przetwarzanie wiąże się z przekazywaniem danych za pomocą sieci lub z udostępnianiem ich przez udzielenie bezpośredniego zautomatyzowanego dostępu do nich — oraz przed wszelkimi innymi niedozwolonymi formami przetwarzania; należy przy tym uwzględnić zwłaszcza ryzyko wiążące się z przetwarzaniem i charakterem danych podlegających ochronie. Biorąc pod uwagę poziom rozwoju techniki i koszty ich wdrożenia, środki takie muszą zapewniać poziom bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem i charakterem danych podlegających ochronie.

2. W zakresie zautomatyzowanego przetwarzania danych każde państwo członkowskie wdraża środki przeznaczone do:

a) uniemożliwienia osobom nieuprawnionym dostępu do infrastruktury przetwarzania danych, wykorzystywanej do przetwarzania danych osobowych (kontrola dostępu do infrastruktury);

b) zabezpieczenia przed nieuprawnionym odczytem, kopiowaniem, modyfikowaniem lub usuwaniem nośników danych (kontrola nośników danych);

c) uniemożliwienia nieuprawnionego wprowadzania danych i nieuprawnionego studiowania, zmieniania lub usuwania przechowywanych danych osobowych (kontrola przechowywania danych);

d) uniemożliwienia korzystania z systemów zautomatyzowanego przetwarzania danych przez osoby nieuprawnione, używające sprzętu do przekazywania danych (kontrola użytkowników);

e) zapewnienia, aby osoby uprawnione do korzystania z systemu zautomatyzowanego przetwarzania danych miały dostęp wyłącznie do danych objętych posiadanym przez siebie upoważnieniem (kontrola dostępu do danych);

f) zapewnienia możliwości zweryfikowania i stwierdzenia, jakim organom dane osobowe zostały lub mogą zostać przesłane lub udostępnione za pomocą sprzętu do przekazywania danych (kontrola przesyłania danych);

g) zapewnienia możliwości następczego zweryfikowania i stwierdzenia, jakie dane osobowe zostały wprowadzone do systemów automatycznego przetwarzania danych, kiedy i przez kogo (kontrola wprowadzania danych);

h) przeciwdziałania nieautoryzowanemu odczytowi, kopiowaniu, modyfikowaniu lub usuwaniu danych osobowych podczas przekazywania danych osobowych lub podczas przenoszenia nośników danych (kontrola transportu);

i) zapewnienia przywrócenia zainstalowanego systemu w przypadku awarii (przywracalność); oraz

j) zapewnienia wykonywania przez system swoich funkcji i zgłaszania występujących w nich błędów (niezawodność) oraz zapewnienia zapobieżenia uszkodzeniom przechowywanych danych spowodowanym błędnym działaniem systemu (integralność).

3. Państwa członkowskie określają, że przetwarzający dane mogą zostać wyznaczeni wyłącznie, jeżeli gwarantują wdrożenie wymaganych środków technicznych i organizacyjnych zgodnie z ust. 1 oraz przestrzegają zasad określonych w art. 21. Nadzór nad przetwarzającym dane jest sprawowany w tym względzie przez właściwy organ.

4. Przetwarzający dane może przetwarzać dane osobowe jedynie na podstawie aktu prawnego lub pisemnej umowy.

Artykuł 23

Uprzednie konsultacje

Państwa członkowskie zapewniają, aby — przed przetworzeniem danych osobowych, które będą stanowić część mającego powstać nowego zbioru danych — przeprowadzono konsultacje z właściwymi krajowymi organami nadzoru, jeżeli:

a) przetwarzane mają być szczególne kategorie danych, o których mowa w art. 6; lub

b) sposób przetwarzania, w szczególności stosowanie nowych technologii, mechanizmów lub procedur, niesie ze sobą określone ryzyko dla podstawowych praw i wolności osoby, której dotyczą dane, a zwłaszcza jej prywatności.

Artykuł 24

Sankcje

Państwa członkowskie przyjmują odpowiednie środki w celu zapewnienia pełnego wdrożenia przepisów niniejszej decyzji ramowej oraz określają w szczególności skuteczne, proporcjonalne i odstraszające sankcje za naruszenie przepisów przyjmowanych zgodnie z niniejszą decyzją ramową.

Artykuł 25

Krajowe organy nadzoru

1. Każde państwo członkowskie określa, że co najmniej jeden organ władzy publicznej odpowiada za prowadzenie doradztwa i monitorowania w zakresie stosowania na jego terytorium przepisów przyjętych przez państwa członkowskie zgodnie z niniejszą decyzją ramową. Powierzone funkcje organy te wypełniają w sposób całkowicie niezależny.

2. Każdemu organowi nadaje się w szczególności:

a) uprawnienia dochodzeniowe, takie jak prawo do dostępu do danych, które stanowią przedmiot operacji przetwarzania, oraz prawo do gromadzenia wszelkich informacji potrzebnych mu do wykonywania swoich funkcji nadzorczych;

b) skuteczne uprawnienia interwencyjne — takie jak wydawanie opinii przed przeprowadzeniem operacji przetwarzania danych oraz zapewnienie odpowiedniej publikacji takich opinii; nakazywanie blokady dostępu do danych, ich usunięcia lub zniszczenia; nakładanie czasowego lub ostatecznego zakazu przetwarzania danych; wydawanie administratorowi danych ostrzeżeń lub upomnień lub przekazywanie sprawy parlamentowi państwa członkowskiego lub innym instytucjom politycznym;

c) uprawnienie do podejmowania postępowań prawnych w przypadku naruszenia krajowych przepisów przyjętych na mocy niniejszej decyzji ramowej lub do powiadamiania organów sądowych o takich naruszeniach. Od decyzji organu nadzoru, stanowiących podstawę skargi, przysługuje odwołanie do sądu.

3. Każdy organ nadzoru rozpatruje wnioski złożone przez dowolną osobę, dotyczące ochrony jej praw i swobód w odniesieniu do przetwarzania danych osobowych. Daną osobę powiadamia się o wyniku rozpatrzenia wniosku.

4. Państwa członkowskie określają, że pracownicy i urzędnicy organów nadzoru podlegają tym samym przepisom o ochronie danych, które obowiązują dany właściwy organ, oraz — nawet po upływie ich okresu zatrudnienia — obowiązkowi zachowania tajemnicy zawodowej w odniesieniu do informacji poufnych, do których mieli dostęp.

Artykuł 26

Stosunek względem umów z państwami trzecimi

Niniejsza decyzja ramowa nie narusza istniejących obowiązków i zobowiązań państw członkowskich lub Unii wynikających z dwu- lub wielostronnych umów z państwami trzecimi obowiązujących w dniu przyjęcia niniejszej decyzji ramowej.

W ramach wykonywania tych umów przekazywanie danych osobowych otrzymanych od innego państwa członkowskiego państwu trzeciemu odbywa się z poszanowaniem, odpowiednio, art. 13 ust. 1 lit. c) lub art. 13 ust. 2.

Artykuł 27

Ocena

1. Do dnia 27 listopada 2013 r. państwa członkowskie składają Komisji sprawozdania na temat krajowych środków zastosowanych w celu zapewnienia pełnego przestrzegania niniejszej decyzji ramowej, a zwłaszcza na temat przepisów, które muszą być przestrzegane już na etapie gromadzenia danych. Komisja bada w szczególności wpływ tych przepisów na zakres zastosowania niniejszej decyzji ramowej określony w art. 1 ust. 2.

2. W terminie jednego roku Komisja składa Parlamentowi Europejskiemu i Radzie sprawozdanie z wyników oceny, o której mowa w ust. 1, i załącza do niego odpowiednie propozycje zmian do niniejszej decyzji ramowej.

Artykuł 28

Związek z uprzednio przyjętymi aktami Unii

Jeżeli akty, które przyjęto na podstawie tytułu VI Traktatu o Unii Europejskiej przed wejściem w życie niniejszej decyzji ramowej i które regulują wymianę danych osobowych między państwami członkowskimi lub dostęp wyznaczonych organów państw członkowskich do systemów informacyjnych utworzonych zgodnie z Traktatem ustanawiającym Wspólnotę Europejską, wprowadziły szczegółowe warunki korzystania z takich danych przez otrzymujące je państwo członkowskie, to warunki te są nadrzędne względem przepisów niniejszej decyzji ramowej dotyczących korzystania z danych, które przekazało lub udostępniło inne państwo członkowskie.

Artykuł 29

Wdrożenie

1. Państwa członkowskie podejmują niezbędne środki w celu wykonania przepisów niniejszej decyzji ramowej przed dniem 27 listopada 2010 r.

2. W tym samym terminie państwa członkowskie przekazują Sekretariatowi Generalnemu Rady i Komisji tekst przepisów przenoszących obowiązki nałożone na nie na mocy niniejszej decyzji ramowej do ich prawa krajowego, oraz informacje o organach nadzoru, o których mowa w art. 25. Na podstawie sprawozdania opracowanego przez Komisję w oparciu o te informacje Rada ocenia przed dniem 27 listopada 2011 r., w jakim zakresie państwa członkowskie wykonały przepisy niniejszej decyzji ramowej.

Artykuł 30

Wejście w życie

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

Sporządzono w Brukseli, dnia 27 listopada 2008 r.

W imieniu Rady
M. ALLIOT-MARIE
Przewodniczący