

## III

(Akty przyjęte na mocy Traktatu UE)

## AKTY PRZYJĘTE NA MOCY TYTUŁU VI TRAKTATU UE

## DECYZJA RADY (WE) NR 2008/633/WSiSW

z dnia 23 czerwca 2008 r.

**w sprawie dostępu wyznaczonych organów państw członkowskich i Europolu do Wizowego Systemu Informacyjnego (VIS) do celów jego przeglądania, w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania**

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o Unii Europejskiej, w szczególności jego art. 30 ust. 1 lit. b) i art. 34 ust. 2 lit. c),

uwzględniając wniosek Komisji,

uwzględniając opinię Parlamentu Europejskiego,

a także mając na uwadze, co następuje:

- (1) Decyzja Rady 2004/512/WE z dnia 8 czerwca 2004 r. ustanawiająca Wizowy System Informacyjny (VIS) <sup>(1)</sup> ustanowiła VIS jako system wymiany danych dotyczących wiz pomiędzy państwami członkowskimi. Ustanowienie VIS stanowi jedną z podstawowych inicjatyw podejmowanych w ramach polityk Unii Europejskiej, które służą tworzeniu przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Celem VIS powinna być lepsza realizacja wspólnej polityki wizowej, powinien on także służyć zwiększeniu bezpieczeństwa wewnętrznego i zwalczaniu terroryzmu w jasno określonych i kontrolowanych warunkach.
- (2) Na posiedzeniu w dniu 7 marca 2005 r. Rada przyjęła konkluzje, w których stwierdziła, że „aby w pełni osiągnąć cel, jakim jest poprawa bezpieczeństwa wewnętrznego i walka z terroryzmem”, organy państw członkowskich odpowiedzialne za bezpieczeństwo wewnętrzne powinny mieć zagwarantowany dostęp do VIS „podczas pełnienia przez nie obowiązków związanych z zapobieganiem przestępstwom – w tym aktom i zagrożeniom terrorystycznym – oraz ich wykrywaniem i prowadzeniem odnośnych dochodzeń”, „pod warunkiem że przepisy o ochronie danych osobowych będą ściśle przestrzegane”.

- (3) W zwalczaniu terroryzmu i innych poważnych przestępstw istotne jest dysponowanie przez odpowiednie służby możliwie najbardziej wyczerpującymi i aktualnymi informacjami w ich stosownych dziedzinach. Właściwym służbom krajowym państw członkowskich potrzebne są informacje, jeżeli mają one wypełniać swoje zadania. Informacje zgromadzone w VIS mogą być niezbędne do celów zapobiegania terroryzmowi i poważnym przestępstwom oraz do zwalczania tych zjawisk, i dlatego też powinny one być dostępne dla wyznaczonych organów do celów ich przeglądania, z zastrzeżeniem warunków określonych w niniejszej decyzji.

- (4) Ponadto Rada Europejska stwierdziła, że w odniesieniu do współpracy organów państw członkowskich w dziedzinie ścigania przestępczości transgranicznej, zasadniczą rolę do spełnienia ma Europol przez wspieranie na skalę ogólnounijną prewencji kryminalnej, analiz kryminalnych i prowadzenia dochodzeń. W związku z tym również Europol powinien mieć dostęp do danych zgromadzonych w VIS w ramach swoich zadań i zgodnie z konwencją z dnia 26 lipca 1995 r. w sprawie ustanowienia Europejskiego Urzędu Policji <sup>(2)</sup>.

- (5) Niniejsza decyzja uzupełnia rozporządzenie (WE) nr 767/2008 Parlamentu Europejskiego i Rady z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS) <sup>(3)</sup>, w zakresie w jakim stanowi ona podstawę prawną na mocy tytułu VI Traktatu o Unii Europejskiej dla upoważnienia wyznaczonych organów i Europolu do uzyskania dostępu do VIS.

<sup>(1)</sup> Dz.U. L 213 z 15.6.2004, s. 5.

<sup>(2)</sup> Dz.U. C 316 z 27.11.1995, s. 2. Konwencja ostatnio zmieniona protokołem zmieniającym tę konwencję (Dz.U. C 2 z 6.1.2004, s. 3.

<sup>(3)</sup> Zob. s. 60 niniejszego Dziennika Urzędowego.

- (6) Niezbędne jest wyznaczenie właściwych organów państw członkowskich, jak również centralnych punktów dostępu, które umożliwiają dostęp, oraz prowadzenie wykazu tych jednostek operacyjnych w strukturach wyznaczonych organów, które są uprawnione do dostępu do VIS w szczególnych celach, jakimi są: zapobieganie przestępstwom terrorystycznym i innym poważnym przestępstwom, o których mowa w decyzji ramowej Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi<sup>(1)</sup>, ich wykrywanie i ściganie. Ważne jest zapewnienie, aby odpowiednio upoważniony personel, który ma prawo dostępu do VIS, składał się jedynie z osób zakwalifikowanych według zasady ograniczonego dostępu i mających odpowiednią wiedzę o bezpieczeństwie danych i zasadach ochrony danych.
- (7) Z wnioskami o dostęp do VIS jednostki operacyjne w strukturach wyznaczonych organów powinny występować do centralnych punktów dostępu. Zanim centralne punkty dostępu zrealizują wniosek o dostęp do VIS, powinny one zweryfikować, czy spełnione są wszystkie warunki dostępu. W wyjątkowo pilnych przypadkach centralne punkty dostępu powinny realizować wniosek natychmiast, a dopiero w drugiej kolejności dokonywać weryfikacji.
- (8) Do celów ochrony danych osobowych, w szczególności wykluczenia stałego dostępu do systemu, przetwarzanie danych zgromadzonych w VIS należy dopuścić tylko w indywidualnie rozpatrywanych przypadkach. Takie szczególne przypadki zachodzą zwłaszcza wtedy, kiedy dostęp do celów przeglądania jest związany z określonym wydarzeniem lub z niebezpieczeństwem powiązanim z poważnym przestępstwem, lub z określoną osobą lub określonymi osobami, co do których istnieją poważne podstawy, by sądzić, że popełnią lub popełniły one przestępstwa terrorystyczne lub inne poważne przestępstwa lub że mają one stosowne powiązania z taką osobą lub takimi osobami. Z tego względu wyznaczone organy i Europol powinny przeszukiwać dane zgromadzone w VIS tylko wtedy, gdy mają uzasadnione podstawy pozwalające uznać, że dzięki takiemu przeszukaniu danych zdobędą informacje, które znacznie pomogą im w zapobieganiu poważnym przestępstwom, ich wykryciu lub ściganiu.
- (9) Gdy proponowana decyzja ramowa Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych wejdzie w życie, powinna ona mieć zastosowanie do danych osobowych przetwarzanych zgodnie z niniejszą decyzją. Dopóki jednak przepisy tej decyzji ramowej nie zaczną obowiązywać oraz, aby je uzupełnić, należy przewidzieć odpowiednie uregulowania, które zapewnią konieczną ochronę danych. Każde państwo członkowskie powinno w swoim prawie krajowym zapewnić odpowiedni poziom ochrony danych, który odpowiada przynajmniej poziomowi wynikającemu z Konwencji Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych oraz z odpowiedniego orzecznictwa opartego na art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, a jeżeli dane państwo ratyfikowało protokół dodatkowy z dnia 8 listopada 2001 r. do przywołanej konwencji – poziomowi wynikającemu z tego protokołu, oraz powinno uwzględnić zalecenie nr R (87) 15 Komitetu Ministrów Rady Europy z dnia 17 września 1987 r. o ochronie danych osobowych w sektorze policji.
- (10) Skuteczność kontroli nad stosowaniem niniejszej decyzji powinna być oceniana w regularnych odstępach czasu.
- (11) W związku z tym, że cele niniejszej decyzji, mianowicie określenie obowiązków i warunków regulujących dostęp wyznaczonych organów państw członkowskich i Europolu do danych VIS do celów ich przeglądania, nie mogą być osiągnięte przez państwa członkowskie w wystarczającym stopniu, a z uwagi na zakres i skutki działania mogą być osiągnięte w lepszy sposób na poziomie Unii Europejskiej, Rada może przyjąć środki zgodnie z zasadą pomocniczości, o której mowa w art. 2 Traktatu o Unii Europejskiej i określonej w art. 5 Traktatu ustanawiającego Wspólnotę Europejską. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsza decyzja nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.
- (12) Zgodnie z art. 47 Traktatu o Unii Europejskiej niniejsza decyzja nie narusza kompetencji Wspólnoty Europejskiej, w szczególności jej kompetencji wykonywanych zgodnie z rozporządzeniem (WE) nr 767/2008 i dyrektywą 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<sup>(2)</sup>.
- (13) Niniejsza decyzja stanowi rozwinięcie przepisów dorobku Schengen, w którym Zjednoczone Królestwo nie uczestniczy zgodnie z decyzją Rady 2000/365/WE z dnia 29 maja 2000 r. dotyczącą wniosku Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej o zastosowanie wobec niego niektórych przepisów dorobku Schengen<sup>(3)</sup>. W związku z tym Zjednoczone Królestwo nie uczestniczy w jej przyjęciu, nie jest nią związane ani nie podlega jej stosowaniu.
- (14) Niniejsza decyzja stanowi rozwinięcie przepisów dorobku Schengen, w którym Irlandia nie uczestniczy zgodnie z decyzją Rady 2002/192/WE z dnia 28 lutego 2002 r. dotyczącą wniosku Irlandii o zastosowanie wobec niej niektórych przepisów dorobku Schengen<sup>(4)</sup>. W związku z tym Irlandia nie uczestniczy w jej przyjęciu, nie jest nią związana ani nie podlega jej stosowaniu.

<sup>(1)</sup> Dz.U. L 190 z 18.7.2002, s. 1.

<sup>(2)</sup> Dz.U. L 281 z 23.11.1995, s. 31. Dyrektywa zmieniona rozporządzeniem (WE) nr 1882/2003 (Dz.U. L 284 z 31.10.2003, s. 1).

<sup>(3)</sup> Dz.U. L 131 z 1.6.2000, s. 43.

<sup>(4)</sup> Dz.U. L 64 z 7.3.2002, s. 20.

- (15) Jednak zgodnie z decyzją ramową Rady 2009/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej<sup>(1)</sup> informacje zgromadzone w VIS mogą być przekazywane Zjednoczonemu Królestwu i Irlandii przez właściwe organy tych państw członkowskich, których wyznaczone organy mają dostęp do VIS zgodnie z niniejszą decyzją. Informacje zgromadzone w krajowych rejestrach wizowych Zjednoczonego Królestwa i Irlandii mogą być przekazywane właściwym organom ochrony porządku publicznego pozostałych państw członkowskich. Uzyskanie przez centralne organy Zjednoczonego Królestwa i Irlandii jakiegokolwiek bezpośredniego dostępu do VIS, w obecnych warunkach uczestniczenia tych państw w stosowaniu dorobku Schengen, wymagałoby porozumienia między Wspólnotą a tymi państwami członkowskimi, ewentualnie uzupełnionego innymi przepisami określającymi warunki i tryb takiego dostępu.
- (16) W odniesieniu do Islandii i Norwegii niniejsza decyzja stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy zawartej przez Radę Unii Europejskiej i Republikę Islandii oraz Królestwo Norwegii dotyczącej włączenia tych dwóch państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen<sup>(2)</sup>, objętych obszarem, o którym mowa w art. 1 pkt B decyzji Rady 1999/437/WE<sup>(3)</sup> w sprawie niektórych warunków stosowania tej umowy.
- (17) W odniesieniu do Szwajcarii, niniejsza decyzja stanowi, z wyjątkiem art. 7, rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy podpisanej między Unią Europejską, Wspólnotą Europejską a Konfederacją Szwajcarską w sprawie włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen, objętych obszarem, o którym mowa w art. 1 pkt B decyzji 1999/437/WE w związku z art. 4 ust. 1 decyzji Rady 2004/849/WE<sup>(4)</sup>.
- (18) Niniejsza decyzja, z wyjątkiem art. 6, stanowi akt oparty na dorobku Schengen lub w inny sposób z nim związany w rozumieniu art. 3 ust. 2 Aktu przystąpienia z 2003 r. oraz art. 4 ust. 2 Aktu przystąpienia z 2005 r.
- (19) Niniejsza decyzja nie narusza podstawowych praw i przestrzega zasad uznanych w szczególności w Karcie praw podstawowych Unii Europejskiej,

STANOWI, CO NASTĘPUJE:

#### Artykuł 1

##### Przedmiot i zakres zastosowania

Niniejsza decyzja określa warunki dostępu wyznaczonych organów państw członkowskich i Europejskiego Urzędu Policji

<sup>(1)</sup> Dz.U. L 386 z 18.12.2006, s. 89.

<sup>(2)</sup> Dz.U. L 176 z 10.7.1999, s. 36.

<sup>(3)</sup> Dz.U. L 176 z 10.7.1999, s. 31.

<sup>(4)</sup> Decyzja 2004/849/WE z dnia 25 października 2004 r. w sprawie podpisania w imieniu Unii Europejskiej oraz tymczasowego stosowania niektórych przepisów Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia tego państwa we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen (Dz.U. L 368 z 15.12.2004, s. 26).

(Europol) do Wizowego Systemu Informacyjnego (VIS) do celów jego przeglądania, w celu zapobiegania przestępstwu terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania.

#### Artykuł 2

##### Definicje

1. Do celów niniejszej decyzji stosuje się następujące definicje:
  - a) „Wizowy System Informacyjny (VIS)” oznacza Wizowy System Informacyjny ustanowiony na mocy decyzji 2004/512/WE;
  - b) „Europol” oznacza Europejski Urząd Policji ustanowiony na mocy konwencji z dnia 26 lipca 1995 r. w sprawie ustanowienia Europejskiego Urzędu Policji („konwencja o Europolu”);
  - c) „przestępstwa terrorystyczne” oznaczają przestępstwa w rozumieniu prawa krajowego, które odpowiadają przestępstwom określonym w art. 1–4 decyzji ramowej Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu<sup>(5)</sup> lub są im równoważne;
  - d) „poważne przestępstwa” oznaczają formy przestępczości, które odpowiadają przestępstwom, o którym mowa w art. 2 ust. 2 decyzji ramowej 2002/584/WSiSW, lub są im równoważne;
  - e) „wyznaczone organy” oznaczają organy odpowiedzialne za zapobieganie przestępstwom terrorystycznym lub innym poważnym przestępstwom oraz za ich wykrywanie lub ściganie, wyznaczone przez państwa członkowskie zgodnie z art. 3.
2. Stosuje się również definicje zawarte w rozporządzeniu (WE) nr 767/2008.

#### Artykuł 3

##### Wyznaczone organy i centralne punkty dostępu

1. Państwa członkowskie wyznaczają organy, o których mowa w art. 2 ust. 1 lit. e), upoważnione do dostępu do danych zgromadzonych w VIS zgodnie z niniejszą decyzją.
2. Każde państwo członkowskie prowadzi wykaz wyznaczonych organów. Do dnia 2 grudnia 2008 r. każde państwo członkowskie powiadamia w oświadczeniu Komisję i Sekretariat Generalny Rady o swoich wyznaczonych organach, a w dowolnym czasie może swoje oświadczenie zmienić lub zastąpić je innym oświadczeniem.

<sup>(5)</sup> Dz.U. L 164 z 22.6.2002, s. 3.

3. Każde państwo członkowskie wyznacza centralny(-e) punkt(-y) dostępu umożliwiając(-e) dostęp. Państwa członkowskie mogą wyznaczyć więcej niż jeden centralny punkt dostępu, jeżeli odzwierciedla to ich strukturą organizacyjną i administracyjną zgodnie z ich wymogami konstytucyjnymi lub prawnymi. Do dnia 2 grudnia 2008 r. każde państwo członkowskie informuje w oświadczeniu Komisję i Sekretariat Generalny Rady o swoim(-ich) centralnym(-ych) punkcie(-tach) dostępu, a w dowolnym czasie może swoje oświadczenie zmienić lub zastąpić je innym oświadczeniem.

4. Oświadczenia, o których mowa w ust. 2 i 3, są publikowane przez Komisję w *Dzienniku Urzędowym Unii Europejskiej*.

5. Na szczeblu krajowym każde państwo członkowskie prowadzi wykaz jednostek operacyjnych w strukturach wyznaczonych organów, które są upoważnione do dostępu do VIS za pośrednictwem centralnego(-ych) punktu(-ów) dostępu.

6. Jedynie odpowiednio upoważniony personel jednostek operacyjnych, jak również centralnego(-ych) punktu(-ów) dostępu jest uprawniony do dostępu do VIS zgodnie z art. 4.

#### Artykuł 4

### Tryb dostępu do VIS

1. W przypadku gdy spełnione są warunki określone w art. 5, jednostki operacyjne, o których mowa w art. 3 ust. 5, występują do centralnych punktów dostępu, o których mowa w art. 3 ust. 3, z uzasadnionym wnioskiem pisemnym lub elektronicznym o uzyskanie dostępu do VIS. Po otrzymaniu wniosku o uzyskanie dostępu, centralny(-e) punkt(-y) dostępu sprawdza(-ją), czy spełnione są warunki dostępu określone w art. 5. Jeżeli spełnione są wszystkie warunki dostępu, odpowiednio upoważniony personel centralnego(-ych) punktu(-ów) dostępu realizuje wniosek. Wyszukane w VIS dane są przekazywane jednostkom operacyjnym, o których mowa w art. 3 ust. 5, w sposób nienaruszający bezpieczeństwa tych danych.

2. W wyjątkowo pilnych przypadkach centralny(-e) punkt(-y) dostępu może (mogą) otrzymać wnioski pisemne, elektroniczne lub ustne. W takich przypadkach centralny(-e) punkt(-y) dostępu realizuje(-ją) wniosek natychmiast, a jedynie *ex post* sprawdza(-ją), czy spełnione zostały wszystkie warunki określone w art. 5, w tym, czy zachodził wyjątkowo pilny przypadek. Sprawdzenie *ex post* następuje bez zbędnej zwłoki, po rozpatrzeniu wniosku.

#### Artykuł 5

### Warunki dostępu wyznaczonych organów państw członkowskich do danych zgromadzonych w VIS

1. Wyznaczone organy korzystają z dostępu do VIS w zakresie swoich uprawnień i w przypadku spełnienia następujących warunków:

a) dostęp do celów przeglądania musi być konieczny w celu zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom lub w celu ich wykrywania lub ścigania;

b) dostęp do celów przeglądania musi być w danym przypadku konieczny;

c) istnieją uzasadnione podstawy pozwalające uznać, że przegląd danych zgromadzonych w VIS znacznie przyczyni się do zapobieżenia któremukolwiek z przedmiotowych przestępstw, jego wykrycia lub ścigania;

2. Przeglądanie VIS ogranicza się do wyszukiwania informacji według dowolnej z następujących danych zawartych w dokumentacji wniosku wizowego i podlegających wpisowi do VIS:

a) nazwisko, nazwisko rodowe (poprzednie nazwisko lub nazwiska); imię lub imiona; płeć; data, miejsce i kraj urodzenia;

b) obecne obywatelstwo i obywatelstwo w chwili urodzenia;

c) rodzaj i numer dokumentu podróży, nazwa organu wydającego, data wydania i data upływu ważności;

d) główne miejsce docelowe i długość planowanego pobytu;

e) cel podróży;

f) planowana data przyjazdu i wyjazdu;

g) planowane miejsce pierwszego przekroczenia granicy lub planowana trasa tranzytowa;

h) miejsce zamieszkania;

i) odciski palców;

j) rodzaj wizy i numer naklejki wizowej;

k) dane osoby zapraszającej osobę ubiegającą się o wizę lub mającej ponosić koszty jej utrzymania podczas pobytu.

3. Przeglądanie VIS daje, w razie uzyskania potwierdzenia w systemie, dostęp do wszystkich danych wymienionych w ust. 2 oraz do:

a) wszelkich innych danych pobranych z wniosku wizowego;

b) fotografii;

c) danych wprowadzonych w związku z każdą wizą, która została wydana, której wydania odmówiono, która została unieważniona, cofnięta lub przedłużona.

#### Artykuł 6

### Warunki dostępu wyznaczonych organów państwa członkowskiego, w stosunku do którego rozporządzenie (WE) nr 767/2008 nie stało się jeszcze skuteczne, do danych VIS

1. Wyznaczone organy państwa członkowskiego, w stosunku do którego rozporządzenie (WE) nr 767/2008 nie stało się jeszcze skuteczne, korzystają z dostępu do VIS do celów jego przeglądania w zakresie swoich uprawnień oraz

a) z zastrzeżeniem tych samych warunków, co warunki określone w art. 5 ust. 1; oraz

- b) na podstawie odpowiednie umotywowanego pisemnego lub elektronicznego wniosku skierowanego do wyznaczonego organu tego państwa członkowskiego, do którego rozporządzenie (WE) nr 767/2008 ma zastosowanie; organ ten zwraca się następnie do krajowego(-ych) centralnego(-ych) punktu(-ów) dostępu o przejrzanie danych w VIS.

2. Państwo członkowskie, w stosunku do którego rozporządzenie (WE) nr 767/2008 nie stało się jeszcze skuteczne, udostępnia swoje informacje wizowe państwom członkowskim, do których rozporządzenie ma zastosowanie, w odpowiedzi na odpowiednio uzasadniony pisemny lub elektroniczny wniosek, o ile spełnione są warunki określone w art. 5 ust. 1.

3. Artykuł 8 ust. 1 i 3–6, art. 9 ust. 1, art. 10 ust. 1 i 3, art. 12 oraz art. 13 ust. 1 i 3 stosuje się odpowiednio.

#### Artykuł 7

### Warunki dostępu Europolu do danych VIS

1. Europol korzysta z dostępu do VIS do celów jego przeglądania w granicach swoich uprawnień oraz

- a) w przypadkach koniecznych do wykonywania swoich zadań zgodnie z art. 3 ust. 1 pkt 2 konwencji o Europolu oraz do przeprowadzenia szczególnej analizy, o której mowa w art. 10 konwencji o Europolu; lub
- b) w przypadkach koniecznych do wykonania swoich zadań zgodnie z art. 3 ust. 1 pkt 2 konwencji o Europolu oraz do przeprowadzenia analizy o charakterze ogólnym i strategicznym, o której mowa w art. 10 konwencji o Europolu, pod warunkiem że przed takim przetwarzaniem danych zgromadzonych w VIS Europol dokona ich anonimizacji i zachowa je w formie uniemożliwiającej identyfikację osób, których one dotyczą.

2. Artykuł 5 ust. 2 i 3 stosuje się odpowiednio.

3. Do celów określonych w niniejszej decyzji Europol wyznacza wyspecjalizowaną jednostkę, składającą się z odpowiednio uprawnionych funkcjonariuszy Europolu, która ma pełnić funkcję centralnego punktu dostępu do VIS.

4. Przetwarzanie informacji, które Europol uzyskał dzięki dostępowi do VIS, zależy od zgody państwa członkowskiego, które wprowadziło te dane do VIS. Zgodę taką uzyskuje się za pośrednictwem krajowego oddziału Europolu w tym państwie członkowskim.

#### Artykuł 8

### Ochrona danych osobowych

1. Przetwarzanie danych osobowych, do których uzyskano wgląd na podstawie niniejszej decyzji, podlega poniższym zasadom i prawu krajowemu państwa członkowskiego, które uzyskało wgląd do danych. W odniesieniu do przetwarzania

danych, do których wgląd uzyskano na podstawie niniejszej decyzji, każde państwo członkowskie zapewnia w swoim prawie krajowym odpowiedni poziom ochrony danych, który odpowiada przynajmniej poziomowi wynikającemu z Konwencji Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, a jeżeli dane państwo ratyfikowało protokół dodatkowy z dnia 8 listopada 2001 r. do przywołanej konwencji – poziomowi wynikającemu z tego protokołu, oraz uwzględniła zalecenie nr R (87) 15 Komitetu Ministrów Rady Europy z dnia 17 września 1987 r. o ochronie danych osobowych w sektorze policji.

2. Europol przetwarza dane osobowe na podstawie niniejszej decyzji zgodnie z konwencją o Europolu i przepisami wykonawczymi do niej i jest pod tym względem nadzorowany przez niezależny wspólny organ nadzorczy ustanowiony w art. 24 konwencji.

3. Dane osobowe uzyskane z VIS na podstawie niniejszej decyzji są przetwarzane jedynie w celu zapobiegania przestępstwu terrorystycznemu lub innym poważnym przestępstwom, ich wykrywania, ścigania i dochodzenia.

4. Danych osobowych uzyskanych z VIS na podstawie niniejszej decyzji nie przekazuje ani nie udostępnia się państwom trzecim ani organizacjom międzynarodowym. Jednakże w wyjątkowo pilnych przypadkach dane takie można przekazywać lub udostępniać państwom trzecim lub organizacjom międzynarodowym jedynie w celu zapobiegania przestępstwu terrorystycznemu i innym poważnym przestępstwom i ich wykrywania, oraz na warunkach określonych w art. 5 ust. 1 niniejszej decyzji, za zgodą państwa członkowskiego, które wprowadziło te dane do VIS, oraz zgodnie z prawem krajowym państwa, które dane te przekazuje lub udostępnia. Państwo członkowskie zapewnia zgodnie z prawem krajowym rejestrowanie takich przypadków przekazywania danych i, na żądanie, udostępnia rejestry tych przypadków krajowym organom ochrony danych. Przekazanie danych przez państwo członkowskie, które wprowadziło dane do VIS zgodnie z rozporządzeniem (WE) nr 767/2008 podlega prawu krajowemu tego państwa członkowskiego.

5. Właściwy organ lub właściwe organy, które zgodnie z prawem krajowym sprawują nadzór nad przetwarzaniem danych osobowych przez organy wyznaczone na podstawie niniejszej decyzji, sprawdzają, czy przetwarzanie danych osobowych na podstawie niniejszej decyzji następuje zgodnie z prawem. Państwa członkowskie zapewniają, aby organy te dysponowały zasobami wystarczającymi do wykonania zadań powierzonych im na mocy niniejszej decyzji.

6. Organy, o których mowa w ust. 5, zapewniają, aby przetwarzanie danych na podstawie niniejszej decyzji było co cztery lata poddawane kontroli według międzynarodowych standardów kontroli – jeżeli mają one zastosowanie.

7. Państwa członkowskie i Europol zezwalają właściwemu organowi lub właściwym organom, o których mowa w ust. 2 i 5, na uzyskanie informacji niezbędnych do wykonywania przez nich ich zadań zgodnie z niniejszym artykułem.

8. Przed otrzymaniem upoważnienia do przetwarzania danych przechowywanych w VIS personel organów uprawnionych do dostępu do VIS przechodzi odpowiednie przeszkolenie w zakresie zasad bezpieczeństwa i ochrony danych oraz otrzymuje informacje na temat przestępstw i sankcji z nimi związanych.

#### Artykuł 9

### Bezpieczeństwo danych

1. Odpowiedzialne państwo członkowskie zapewnia bezpieczeństwo danych podczas ich przesyłania wyznaczonym organom i podczas ich odbioru przez te organy.

2. Każde państwo członkowskie podejmuje niezbędne środki bezpieczeństwa w trosce o dane, które mają być wyszukane w VIS zgodnie z niniejszą decyzją i które mają następnie zostać przechowane, w szczególności w celu:

- a) zapewnienia fizycznej ochrony danych, m.in. przez sporządzanie planów awaryjnych służących ochronie infrastruktury krytycznej;
- b) uniemożliwienia nieupoważnionym osobom dostępu do krajowych obiektów, w których państwo członkowskie przechowuje dane (kontrola przy wejściu do obiektu);
- c) zapobieżenia nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych (kontrola nośników danych);
- d) zapobieżenia nieuprawnionemu przeglądaniu, zmienianiu i usuwaniu przechowywanych danych osobowych (kontrola przechowywania);
- e) zapobieżenia nieuprawnionemu przetwarzaniu danych pochodzących z VIS (kontrola przetwarzania danych);
- f) zapewnienia – za pomocą indywidualnych i niepowtarzalnych profili identyfikacyjnych oraz poufnych sposobów dostępu – aby osoby uprawnione do dostępu do VIS miały dostęp wyłącznie do tych danych, które są objęte posiadaniem przez nie upoważnieniem (kontrola dostępu do danych);
- g) zapewnienia, aby wszystkie organy uprawnione do dostępu do VIS tworzyły profile z opisem funkcji i zakresu obowiązków osób upoważnionych do dostępu do danych i do ich przeszukiwania oraz udostępniały te profile krajowym organom nadzorczym, o których mowa w art. 8 ust. 5, bezzwłocznie na ich żądanie (profile personelu);
- h) zapewnienia możliwości weryfikacji i stwierdzenia, jakim organom można przekazywać dane osobowe za pośrednictwem sprzętu do przekazywania danych (kontrola przekazywania danych);

- i) zapewnienia możliwości weryfikacji i stwierdzenia, jakiego rodzaju dane, kiedy, przez kogo i w jakim celu zostały wyszukane w VIS (kontrola zapisu danych);
- j) zapobieżenia nieuprawnionemu odczytywaniu i kopiowaniu danych osobowych, gdy są one przesyłane z VIS, szczególnie dzięki zastosowaniu odpowiednich technik szyfrowania (kontrola transportu);
- k) kontrolowania skuteczności środków bezpieczeństwa, o których mowa w niniejszym ustępie, oraz podejmowania niezbędnych środków organizacyjnych związanych z nadzorem wewnętrznym, aby zapewnić przestrzeganie niniejszej decyzji (samokontrola).

#### Artykuł 10

### Odpowiedzialność

1. Jakakolwiek osoba lub państwo członkowskie, które poniosły szkodę w wyniku bezprawnej operacji przetwarzania danych lub jakiegokolwiek działania niezgodnego z niniejszą decyzją, są uprawnione do otrzymania odszkodowania od państwa członkowskiego, które odpowiada za poniesioną szkodę. To państwo członkowskie jest zwolnione z odpowiedzialności, w całości lub w części, jeżeli udowodni, że nie ponosi odpowiedzialności za zdarzenie powodujące szkodę.

2. Jeżeli niewywiązanie się przez państwo członkowskie z jakiegokolwiek z obowiązków wynikających z niniejszej decyzji spowoduje szkodę w VIS, odpowiada ono za taką szkodę, chyba że, i w zakresie w jakim, inne państwo członkowskie nie podjęło uzasadnionych środków w celu zapobieżenia szkodzie lub zminimalizowaniu jej skutków.

3. Roszczenia o odszkodowanie wobec państwa członkowskiego, o których mowa w ust. 1 i 2, podlegają przepisom prawa krajowego państwa członkowskiego, przeciwko któremu są skierowane.

#### Artykuł 11

### Samokontrola

Państwa członkowskie zapewniają, aby każdy organ uprawniony do dostępu do danych w VIS podjął środki konieczne do zapewnienia przestrzegania niniejszej decyzji i aby współpracował, jeżeli jest to konieczne, z krajowym organem lub krajowymi organami, o których mowa w art. 8 ust. 5.

#### Artykuł 12

### Sankcje

Państwa członkowskie podejmują niezbędne środki w celu zapewnienia karalności wszelkiego niezgodnego z przepisami niniejszej decyzji wykorzystania danych wprowadzonych do VIS za pomocą skutecznych, proporcjonalnych i odstraszających sankcji, w tym za pomocą sankcji administracyjnych lub karnych.

## Artykuł 13

**Przechowywanie danych z VIS w plikach krajowych**

1. Dane pochodzące z VIS można przechowywać w plikach krajowych wyłącznie wtedy, gdy jest to w danym przypadku niezbędne do celów określonych w niniejszej decyzji i gdy jest to zgodne z właściwymi przepisami prawnymi, w tym przepisami o ochronie danych, oraz nie dłużej, niż jest to w danym przypadku konieczne.
2. Ustęp 1 pozostaje bez uszczerbku dla przepisów prawa krajowego państwa członkowskiego dotyczących wprowadzania przez jego wyznaczone organy do plików krajowych danych, które państwo to wprowadziło do VIS zgodnie z rozporządzeniem (WE) nr 767/2008.
3. Wszelkie przypadki wykorzystywania danych w sposób niezgodny z ust. 1 i 2 uznaje się za nadużycie zgodnie z prawem krajowym każdego państwa członkowskiego.

## Artykuł 14

**Prawo do dostępu, skorygowania i usunięcia danych**

1. Prawo osób do dostępu do danych, które ich dotyczą i które uzyskano z VIS zgodnie z niniejszą decyzją, wykonywane jest zgodnie z prawem państwa członkowskiego, w którym osoby te powołują się na to prawo.
2. Jeżeli prawo krajowe tak stanowi, krajowy organ nadzorczy decyduje, czy i w jakim trybie informacje mają być podane do wiadomości.
3. Państwo członkowskie inne niż to, które wprowadziło dane do VIS zgodnie z rozporządzeniem (WE) nr 767/2008, może przekazać informację dotyczącą takich danych tylko wtedy, gdy uprzednio umożliwiło państwu członkowskiemu, które dane wprowadziło, zajęcie stanowiska w tej sprawie.
4. Odmawia się przekazywania informacji osobie, której dotyczą dane, jeżeli odmowa taka jest konieczna, by wykonać uprawnione działanie w związku z tymi danymi lub by chronić prawa i swobody osób trzecich.
5. Każda osoba ma prawo wystąpić o to, by dotyczące jej dane niezgodne ze stanem faktycznym zostały skorygowane, a dotyczące jej dane przechowywane z naruszeniem prawa – usunięte. Jeżeli wyznaczone organy otrzymają taki wniosek lub jeżeli dysponują innymi dowodami wskazującymi, że dane przetwarzane w VIS są niezgodne ze stanem faktycznym, natychmiast powiadamiają o tym organ wizowy tego państwa członkowskiego, które wprowadziło te dane do VIS, a organ ten weryfikuje przedmiotowe dane i, w razie konieczności, niezwłocznie koryguje je lub usuwa zgodnie z art. 24 rozporządzenia (WE) nr 767/2008.
6. Zainteresowany jest informowany możliwie jak najszybciej, a w każdym przypadku nie później niż 60 dni od daty złożenia wniosku o dostęp lub wcześniej, jeżeli prawo krajowe tak stanowi.

7. O działaniach podjętych po skorzystaniu przez zainteresowanego z jego prawa do wystąpienia o korektę i usunięcie danych, informuje się go możliwie jak najszybciej, a w każdym przypadku nie później niż 3 miesiące od daty złożenia przez niego wniosku o korektę lub usunięcie danych lub wcześniej, jeżeli prawo krajowe tak stanowi.

8. W każdym państwie członkowskim każda osoba ma prawo do wszczęcia postępowania lub złożenia skargi we właściwych organach lub sądach tego państwa członkowskiego, które odmówiło jej prawa do dostępu lub prawa do wystąpienia o korektę lub usunięcie danych jej dotyczących, które to prawa są określone w niniejszym artykule.

## Artykuł 15

**Koszty**

Każde państwo członkowskie oraz Europol tworzą i utrzymują na własny koszt infrastrukturę techniczną konieczną do wykonania niniejszej decyzji oraz ponoszą koszty wynikające z dostępu do VIS w celach określonych w niniejszej decyzji.

## Artykuł 16

**Prowadzenie zapisu**

1. Każde państwo członkowskie i Europol zapewniają zapis wszystkich operacji przetwarzania danych, wynikających z dostępu do VIS do celów jego przeglądania zgodnie z niniejszą decyzją, w celach sprawdzenia, czy wyszukiwanie jest dopuszczalne i w celach monitorowania, czy dane przetwarzane są zgodnie z prawem, w celach samokontroli, zapewnienia właściwego funkcjonowania systemu, właściwego poziomu integralności i bezpieczeństwa danych.

W zapisie takim należy wykazać:

- a) dokładny cel uzyskania dostępu do celów przeglądania, o którym mowa w art. 5 ust. 1 lit. a), w tym formę danego przestępstwa terrorystycznego lub innego poważnego przestępstwa, a w przypadku Europolu – dokładny cel uzyskania dostępu do celów przeglądania, o którym mowa w art. 7 ust. 1;
- b) odnośnik do danego pliku krajowego;
- c) datę i dokładną godzinę uzyskania dostępu;
- d) w stosownych przypadkach – zastosowanie trybu, o którym mowa w art. 4 ust. 2;
- e) dane wykorzystane do przeglądania;
- f) rodzaj przejrzanych danych;
- g) zgodnie z przepisami krajowymi lub postanowieniami konwencji o Europolu – oznaczenie identyfikacyjne urzędnika, który przeszukiwał dane, i urzędnika, który zlecił ich przeszukiwanie lub dostarczenie.

2. Zapisy zawierające dane osobowe można wykorzystywać wyłącznie do kontroli ochrony danych pod kątem legalności przetwarzania danych oraz do zapewnienia bezpieczeństwa danych. Jedynie zapisy zawierające dane nieosobowe można wykorzystywać do monitorowania i oceny, o których mowa w art. 17.

3. Zapisy te są chronione odpowiednimi środkami przed dostępem osób nieuprawnionych oraz wykorzystaniem niezgodnym z przeznaczeniem i są usuwane rok po upływie okresu ich przechowywania, o którym mowa w art. 23 ust. 1 rozporządzenia (WE) nr 767/2008, chyba że są one konieczne w procedurach kontroli, o których mowa w ust. 2 niniejszego artykułu, i które są już w toku.

#### Artykuł 17

##### Monitorowanie i ocena

1. Organ zarządzający, o którym mowa w rozporządzeniu (WE) nr 767/2008, zapewnia wprowadzenie systemów pozwalających na monitorowanie funkcjonowania VIS zgodnie z niniejszą decyzją pod względem realizacji celów związanych z wynikami, opłacalnością, bezpieczeństwem i jakością usług,

2. Na potrzeby konserwacji technicznej organ zarządzający ma dostęp do niezbędnych informacji o operacjach przetwarzania danych przeprowadzanych w VIS.

3. Dwa lata po rozpoczęciu funkcjonowania VIS, a następnie co dwa lata, organ zarządzający przedkłada Parlamentowi Europejskiemu, Radzie i Komisji sprawozdanie dotyczące technicznego funkcjonowania VIS zgodnie z niniejszą decyzją. W sprawozdaniu tym należy zawrzeć informacje o sprawności VIS, którą ocenia się w odniesieniu do wskaźników liczbowych określonych pierwotnie przez Komisję, w szczególności potrzeb i korzystania z art. 4 ust. 2.

4. Trzy lata po rozpoczęciu funkcjonowania VIS, a następnie co cztery lata Komisja, opracowuje całościową ocenę VIS zgodnie z niniejszą decyzją. Ocena ta obejmuje analizę osiągniętych wyników w porównaniu z założonymi celami oraz ocenę dalszej zasadności przesłanek przyjęcia niniejszej decyzji,

stosowania niniejszej decyzji w odniesieniu do VIS, bezpieczeństwa systemu oraz wszelkich konsekwencji dla funkcjonowania VIS w przyszłości. Komisja przekazuje sprawozdania z oceny Parlamentowi Europejskiemu i Radzie.

5. Państwa członkowskie i Europol dostarczają organowi zarządzającemu i Komisji informacji niezbędnych do sporządzenia sprawozdań, o których mowa w ust. 3 i 4. Informacje takie nie mogą w żadnym przypadku narażać metod pracy ani ujawniać informacji o źródłach, członkach personelu ani dochodzeniach prowadzonych przez wyznaczone organy.

6. Organ zarządzający dostarcza Komisji informacji niezbędnych do sporządzania ogólnych ocen, o których mowa w ust. 4.

7. W okresie przejściowym, do czasu podjęcia obowiązków przez organ zarządzający, za sporządzanie i przekazywanie sprawozdań, o których mowa w ust. 3, odpowiada Komisja.

#### Artykuł 18

##### Wejście w życie i data stosowania

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

2. Niniejsza decyzja staje się skuteczna z dniem określonym przez Radę po otrzymaniu przez nią powiadomienia Komisji o wejściu w życie rozporządzenia (WE) nr 767/2008 i staniu się przez nie w pełni stosownym.

Sekretariat Generalny Rady publikuje tę datę w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Luksemburgu dnia 23 czerwca 2008 r.

W imieniu Rady

I. JARC

Przewodniczący