DECYZJA KOMISJI

z dnia 4 maja 2010 r.

w sprawie planu bezpieczeństwa dla funkcjonowania wizowego systemu informacyjnego

(2010/260/UE)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 767/2008 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) [1], w szczególności jego art. 32,

a także mając na uwadze, co następuje:

(1) Zgodnie z art. 32 ust. 3 rozporządzenia (WE) nr 767/2008 organ zarządzający podejmie niezbędne środki dla osiągnięcia celów określonych w art. 32 ust. 2 w odniesieniu do funkcjonowania VIS, łącznie z przyjęciem planu bezpieczeństwa.

(2) Zgodnie z art. 26 ust. 4 rozporządzenia (WE) nr 767/2008 w okresie przejściowym, zanim organ zarządzający podejmie swoje obowiązki, Komisja jest odpowiedzialna za zarządzanie operacyjne VIS.

(3) Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady [2] ma zastosowanie do przetwarzania danych osobowych przez Komisję w trakcie pełnienia przez nią obowiązków w zakresie zarządzania operacyjnego VIS.

(4) Zgodnie z art. 26 ust. 7 rozporządzenia (WE) nr 767/2008, jeżeli w okresie przejściowym Komisja deleguje swoje obowiązki, zanim obowiązki podejmie organ zarządzający, Komisja dokłada wszelkich starań, aby delegowanie tych zadań nie wpłynęło niekorzystnie na jakikolwiek ustanowiony prawem Unii Europejskiej system skutecznej kontroli, niezależnie od tego, czy jest to kontrola sprawowana przez Trybunał Sprawiedliwości, Trybunał Obrachunkowy czy przez Europejskiego Inspektora Ochrony Danych.

(5) Po podjęciu obowiązków organ zarządzający powinien określić własny plan bezpieczeństwa w odniesieniu do VIS.

(6) W decyzji Komisji 2008/602/WE z dnia 17 czerwca 2008 r. ustanawiającej architekturę fizyczną i wymogi dotyczące interfejsów krajowych oraz infrastruktury łączności między Centralnym Wizowym Systemem Informacyjnym (VIS) i interfejsami krajowymi w fazie rozwoju [3] przedstawiono niezbędne usługi z zakresu bezpieczeństwa dotyczące sieci na potrzeby VIS.

(7) Zgodnie z art. 27 rozporządzenia (WE) nr 767/2008 główny centralny VIS, sprawujący nadzór techniczny i administrację, mieści się w Strasburgu, we Francji, natomiast rezerwowy centralny VIS, zdolny do zapewnienia wszystkich funkcji głównego centralnego VIS w przypadku jego awarii, mieści się w Sankt Johann im Pongau, w Austrii.

(8) Należy określić funkcje urzędników ds. bezpieczeństwa w celu zapewnienia skutecznego i szybkiego reagowania na zdarzenia zagrażające bezpieczeństwu oraz ich zgłaszania.

(9) Należy ustanowić politykę bezpieczeństwa określającą wszystkie szczegółowe informacje techniczne i organizacyjne zgodnie z przepisami niniejszej decyzji.

(10) Należy określić środki zapewniające odpowiedni poziom bezpieczeństwa funkcjonowania VIS,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot

Niniejsza decyzja ustanawia organizację i środki bezpieczeństwa (plan bezpieczeństwa) w rozumieniu art. 32 ust. 3 rozporządzenia (WE) nr 767/2008.

ROZDZIAŁ II

ORGANIZACJA, OBOWIĄZKI I ZARZĄDZANIE ZDARZENIAMI

Artykuł 2

Zadania Komisji

1. Komisja wdraża środki bezpieczeństwa w odniesieniu do centralnego VIS oraz infrastruktury łączności, o których mowa w niniejszej decyzji, i monitoruje ich skuteczność.

[1] Dz.U. L 218 z 13.8.2008, s. 60.
[2] Dz.U. L 8 z 12.1.2001, s. 1.
[3] Dz.U. L 194 z 23.7.2008, s. 3.

2. Komisja wyznacza spośród swoich urzędników urzędnika ds. bezpieczeństwa systemu. Urzędnika ds. bezpieczeństwa systemu mianuje dyrektor generalny Dyrekcji Generalnej Komisji ds. Sprawiedliwości, Wolności i Bezpieczeństwa. Zadania urzędnika ds. bezpieczeństwa systemu obejmują w szczególności:

a) przygotowanie, aktualizację i przegląd polityki bezpieczeństwa opisanej w art. 7 niniejszej decyzji;

b) monitorowanie skuteczności wdrażania procedur bezpieczeństwa odnośnie do centralnego VIS i infrastruktury łączności;

c) udział w przygotowaniu sprawozdań dotyczących bezpieczeństwa, o których mowa w art. 50 ust. 3 i 4 rozporządzenia (WE) nr 767/2008;

d) koordynację i pomoc w zakresie kontroli i audytów przeprowadzanych przez Europejskiego Inspektora Ochrony Danych, o których mowa w art. 42 rozporządzenia (WE) nr 767/2008;

e) monitorowanie, czy niniejsza decyzja i polityka bezpieczeństwa są odpowiednio i w pełni stosowane przez wszystkich wykonawców, w tym podwykonawców, zaangażowanych w jakikolwiek sposób w zarządzanie VIS i jego funkcjonowanie;

f) prowadzenie wykazu pojedynczych krajowych punktów kontaktowych odnośnie do bezpieczeństwa VIS i udostępnianie go lokalnym urzędnikom ds. bezpieczeństwa centralnego VIS i infrastruktury łączności.

Artykuł 3

Lokalny urzędnik ds. bezpieczeństwa centralnego VIS

1. Nie naruszając art. 8, Komisja wyznacza spośród swoich urzędników lokalnego urzędnika ds. bezpieczeństwa centralnego VIS. Zapobiega się powstawaniu konfliktów interesów między obowiązkami lokalnego urzędnika ds. bezpieczeństwa a wszelkimi innymi obowiązkami służbowymi. Lokalnego urzędnika ds. bezpieczeństwa centralnego VIS mianuje dyrektor generalny Dyrekcji Generalnej Komisji ds. Sprawiedliwości, Wolności i Bezpieczeństwa.

2. Lokalny urzędnik ds. bezpieczeństwa centralnego VIS zapewnia wdrażanie środków bezpieczeństwa, o których mowa w niniejszej decyzji, i przestrzeganie procedur bezpieczeństwa w głównym centralnym VIS. W odniesieniu do rezerwowego centralnego VIS lokalny urzędnik ds. bezpieczeństwa centralnego VIS zapewnia wdrażanie środków bezpieczeństwa, o których mowa w niniejszej decyzji, z wyjątkiem środków, o których mowa w art. 10, oraz przestrzeganie związanych z nimi procedur bezpieczeństwa.

3. Lokalny urzędnik ds. bezpieczeństwa centralnego VIS może przekazać każde ze swoich zadań podlegającym mu pracownikom. Zapobiega się powstawaniu konfliktów interesów między obowiązkami związanymi z wykonywaniem takich zadań a innymi obowiązkami służbowymi. Jeden numer telefonu i adres umożliwiają skontaktowanie się w każdym momencie z lokalnym urzędnikiem ds. bezpieczeństwa lub z podlegającym mu pracownikiem pełniącym dyżur.

4. Lokalny urzędnik ds. bezpieczeństwa centralnego VIS wykonuje zadania wynikające ze środków bezpieczeństwa, które mają zostać podjęte w miejscach, w których znajdują się główny i rezerwowy centralny VIS, w granicach wyznaczonych ust. 1. Zadania te obejmują w szczególności:

a) lokalne zadania operacyjne w zakresie bezpieczeństwa obejmujące kontrole zapór sieciowych, systematyczne testy bezpieczeństwa, przeprowadzanie audytu i sprawozdawczość;

b) monitorowanie efektywności planu ciągłości działania oraz zapewnianie przeprowadzania systematycznych ćwiczeń;

c) zabezpieczanie dowodów dotyczących wszelkich zdarzeń, które mogą mieć wpływ na bezpieczeństwo centralnego VIS lub infrastruktury łączności, oraz zgłaszanie takich zdarzeń urzędnikowi ds. bezpieczeństwa systemu;

d) informowanie urzędnika ds. bezpieczeństwa systemu o potrzebie zmiany polityki bezpieczeństwa;

e) monitorowanie stosowania niniejszej decyzji i polityki bezpieczeństwa przez każdego z wykonawców, w tym podwykonawców, zaangażowanych w jakikolwiek sposób w zarządzanie centralnym VIS i jego funkcjonowanie;

f) dopilnowanie, by pracownicy zapoznali się ze swoimi obowiązkami, i monitorowanie stosowania polityki bezpieczeństwa;

g) monitorowanie zmian w technologii informacyjnej związanych z bezpieczeństwem oraz zapewnianie odpowiedniego przeszkolenia pracowników;

h) przygotowywanie podstawowych informacji i opcji dotyczących ustanawiania, aktualizacji i przeglądu polityki bezpieczeństwa zgodnie z art. 7.

Artykuł 4

Lokalny urzędnik ds. bezpieczeństwa infrastruktury łączności

1. Nie naruszając art. 8, Komisja wyznaczy spośród swoich urzędników lokalnego urzędnika ds. bezpieczeństwa infrastruktury łączności. Zapobiega się powstawaniu konfliktów interesów między obowiązkami lokalnego urzędnika ds. bezpieczeństwa a wszelkimi innymi obowiązkami służbowymi. Lokalnego urzędnika ds. bezpieczeństwa infrastruktury łączności mianuje dyrektor generalny Dyrekcji Generalnej Komisji ds. Sprawiedliwości, Wolności i Bezpieczeństwa.

2. Lokalny urzędnik ds. bezpieczeństwa infrastruktury łączności monitoruje funkcjonowanie infrastruktury łączności oraz zapewnia wdrażanie środków bezpieczeństwa i przestrzeganie procedur bezpieczeństwa.

3. Lokalny urzędnik ds. bezpieczeństwa infrastruktury łączności może przekazać każde ze swoich zadań podlegającym mu pracownikom. Zapobiega się powstawaniu konfliktów interesów między obowiązkami związanymi z wykonywaniem takich zadań a innymi obowiązkami służbowymi. Jeden numer telefonu i adres umożliwiają skontaktowanie się w każdym momencie z lokalnym urzędnikiem ds. bezpieczeństwa lub z podlegającym mu pracownikiem pełniącym dyżur.

4. Lokalny urzędnik ds. bezpieczeństwa infrastruktury łączności wykonuje zadania związane ze środkami bezpieczeństwa dotyczącymi infrastruktury łączności, obejmujące w szczególności:

a) wszelkie zadania operacyjne w zakresie bezpieczeństwa związane z infrastrukturą łączności, takie jak kontrola zapór sieciowych, systematyczne testy bezpieczeństwa, przeprowadzanie audytu i sprawozdawczość;

b) monitorowanie efektywności planu ciągłości działania oraz zapewnianie przeprowadzania systematycznych ćwiczeń;

c) zabezpieczanie dowodów dotyczących wszelkich zdarzeń, które mogą mieć wpływ na bezpieczeństwo infrastruktury łączności lub centralnego VIS lub na systemy krajowe, oraz zgłaszanie takich zdarzeń urzędnikowi ds. bezpieczeństwa systemu;

d) informowanie urzędnika ds. bezpieczeństwa systemu o potrzebie zmiany polityki bezpieczeństwa;

e) monitorowanie stosowania niniejszej decyzji i polityki bezpieczeństwa przez każdego z wykonawców, w tym podwykonawców, zaangażowanych w jakikolwiek sposób w zarządzanie infrastrukturą łączności;

f) dopilnowanie, by pracownicy zapoznali się ze swoimi obowiązkami, i monitorowanie stosowania polityki bezpieczeństwa;

g) monitorowanie zmian w technologii informacyjnej związanych z bezpieczeństwem oraz zapewnianie odpowiedniego przeszkolenia pracowników;

h) przygotowywanie podstawowych informacji i opcji dotyczących ustanawiania, aktualizacji i przeglądu polityki bezpieczeństwa zgodnie z art. 7.

Artykuł 5

Zdarzenia zagrażające bezpieczeństwu

1. Wszelkie wydarzenia, które mają lub mogą mieć wpływ na bezpieczeństwo funkcjonowania VIS oraz mogą spowodować szkody lub straty w tym systemie, uznaje się za zdarzenia zagrażające bezpieczeństwu, w szczególności jeżeli mogło dojść do uzyskania dostępu do danych lub jeżeli została lub mogła zostać naruszona dostępność, integralność lub poufność przedmiotowych danych.

2. W ramach polityki bezpieczeństwa ustanawia się procedury dotyczące przeprowadzania działań naprawczych po zdarzeniu zagrażającym bezpieczeństwu. Zdarzeniami zagrażającymi bezpieczeństwu zarządza się w taki sposób, aby zapewnić szybkie, skuteczne i właściwe reagowanie zgodnie z polityką bezpieczeństwa.

3. Informacje na temat zdarzeń zagrażających bezpieczeństwu, które mają lub mogą mieć wpływ na funkcjonowanie VIS w państwie członkowskim lub na dostępność, integralność i poufność danych wprowadzonych do tego systemu przez państwo członkowskie, przekazuje się temu państwu członkowskiemu. Zdarzenia zagrażające bezpieczeństwu zgłasza się inspektorowi ochrony danych Komisji.

Artykuł 6

Zarządzanie zdarzeniami

1. Wszyscy pracownicy i wykonawcy zaangażowani w rozwijanie i obsługę VIS oraz zarządzanie nim mają obowiązek odnotowywania i zgłaszania odpowiednio urzędnikowi ds. bezpieczeństwa systemu lub lokalnemu urzędnikowi ds. bezpieczeństwa centralnego VIS bądź lokalnemu urzędnikowi ds. bezpieczeństwa infrastruktury łączności wszelkich zaobserwowanych lub podejrzewanych niedociągnięć w zakresie bezpieczeństwa w funkcjonowaniu VIS.

2. W przypadku wykrycia jakichkolwiek zdarzeń, które mają lub mogą mieć wpływ na bezpieczeństwo funkcjonowania VIS, lokalny urzędnik ds. bezpieczeństwa centralnego VIS lub lokalny urzędnik ds. bezpieczeństwa infrastruktury łączności bezzwłocznie informuje o tym urzędnika ds. bezpieczeństwa systemu oraz, w stosownych przypadkach, pojedynczy krajowy punkt kontaktowy ds. bezpieczeństwa VIS, jeżeli taki punkt istnieje w powyższym państwie członkowskim, w formie pisemnej, a w wyjątkowo pilnych przypadkach za pośrednictwem innych dróg komunikacji. Zgłoszenie obejmuje opis zdarzenia zagrażającego bezpieczeństwu, poziom ryzyka, możliwe konsekwencje oraz środki, które podjęto lub które należy podjąć w celu zmniejszenia ryzyka.

3. Lokalny urzędnik ds. bezpieczeństwa centralnego VIS lub, odpowiednio, lokalny urzędnik ds. bezpieczeństwa infrastruktury łączności bezzwłocznie zabezpiecza wszelkie dowody związane ze zdarzeniem zagrażającym bezpieczeństwu. W zakresie dopuszczonym obowiązującymi przepisami dotyczącymi ochrony danych dowody te udostępnia się urzędnikowi ds. bezpieczeństwa systemu na jego wniosek.

4. Wdrożone zostają procedury przekazywania informacji zwrotnych w celu zapewnienia informacji o wynikach po zakończeniu zdarzenia i usunięciu jego skutków.

ROZDZIAŁ III

ŚRODKI BEZPIECZEŃSTWA

Artykuł 7

Polityka bezpieczeństwa

1. Dyrektor generalny Dyrekcji Generalnej ds. Sprawiedliwości, Wolności i Bezpieczeństwa ustanawia i aktualizuje obowiązującą politykę bezpieczeństwa oraz dokonuje jej regularnego przeglądu zgodnie z niniejszą decyzją. W ramach polityki bezpieczeństwa ustanawia się szczegółowe procedury i środki do celów ochrony przed zagrożeniami dla dostępności, integralności i poufności VIS, w tym planowanie na wypadek sytuacji awaryjnych, aby zapewnić odpowiedni poziom bezpieczeństwa określony niniejszą decyzją. Polityka bezpieczeństwa jest zgodna z niniejszą decyzją.

2. Polityka bezpieczeństwa opiera się na ocenie ryzyka. Środki określone w ramach polityki bezpieczeństwa są proporcjonalne do zidentyfikowanych zagrożeń.

3. Aktualizacji oceny ryzyka i polityki bezpieczeństwa dokonuje się, jeżeli jest to niezbędne w wyniku zmian technologicznych, określenia nowych zagrożeń lub jakichkolwiek innych okoliczności. Niezależnie od powyższych czynników dokonuje się rocznego przeglądu polityki bezpieczeństwa w celu zapewnienia jej dostosowania do najnowszej oceny ryzyka lub innych nowo określonych zmian technologicznych, zagrożeń lub innych istotnych okoliczności.

4. Urzędnik ds. bezpieczeństwa systemu przygotowuje politykę bezpieczeństwa w koordynacji z lokalnym urzędnikiem ds. bezpieczeństwa VIS i lokalnym urzędnikiem ds. bezpieczeństwa infrastruktury łączności.

Artykuł 8

Wdrażanie środków bezpieczeństwa

1. Realizację zadań i wymogów określonych w niniejszej decyzji oraz w polityce bezpieczeństwa, w tym zadanie wyznaczenia lokalnego urzędnika ds. bezpieczeństwa, można zlecić lub powierzyć organom prywatnym bądź publicznym.

2. W takim przypadku Komisja w ramach wiążącej prawnie umowy zapewnia całkowitą zgodność z wymogami określonymi w niniejszej decyzji i polityce bezpieczeństwa. W przypadku gdy zadanie wyznaczenia lokalnego urzędnika ds. bezpieczeństwa zostanie delegowane lub zlecone na zewnątrz, Komisja w ramach wiążącej prawnie umowy gwarantuje, że zostaną z nią przeprowadzone konsultacje dotyczące osoby, która ma być wyznaczona na stanowisko lokalnego urzędnika ds. bezpieczeństwa.

Artykuł 9

Kontrola dostępu do infrastruktury

1. W celu ochrony obszarów, na których znajduje się infrastruktura przetwarzania danych, stosuje się obwody bezpieczeństwa obejmujące odpowiednie bariery i kontrole dostępu.

2. W ramach powyższych obwodów określa się strefy bezpieczeństwa w celu ochrony elementów fizycznych (aktywów), w tym sprzętu komputerowego, nośników danych i wyposażenia do zarządzania danymi, planów i innych dokumentów dotyczących VIS oraz biur i innych miejsc pracy pracowników zajmujących się obsługą VIS. Strefy bezpieczeństwa są chronione za pośrednictwem odpowiednich kontroli dostępu w celu zapewnienia wstępu na dany obszar jedynie upoważnionym pracownikom. Pracę w strefach bezpieczeństwa regulują szczegółowe przepisy dotyczące bezpieczeństwa określone w polityce bezpieczeństwa.

3. Zapewnia się fizyczne zabezpieczenia biur, sal i infrastruktury oraz ich instalację. Punkty dostępu, takie jak miejsca dostaw i załadunku, oraz inne punkty, przez które osoby nieupoważnione mogą wejść na dany teren, są kontrolowane i, jeżeli jest to możliwe, oddzielone od infrastruktury przetwarzania danych w celu uniknięcia nieupoważnionego dostępu.

4. Opracowuje się system ochrony fizycznej obwodów bezpieczeństwa przed zniszczeniami wynikającymi z klęsk żywiołowych lub katastrof spowodowanych przez człowieka oraz stosuje się go w sposób proporcjonalny do zagrożenia.

5. Wyposażenie chroni się przed zagrożeniami o charakterze fizycznym i środowiskowym oraz przed możliwościami nieupoważnionego dostępu.

6. Jeżeli Komisja ma dostęp do powyższych informacji, do wykazu, o którym mowa w art. 2 ust. 2 lit. f), dołączy ona pojedynczy punkt kontaktowy do celów monitorowania wdrażania przepisów zawartych w niniejszym artykule na terenie, na którym znajduje się rezerwowy centralny VIS.

Artykuł 10

Kontrola nośników danych i aktywów

1. Nośniki wymienne zawierające dane są chronione przed nieupoważnionym dostępem, niewłaściwym wykorzystaniem lub uszkodzeniem, a ich czytelność jest zapewniana przez cały okres istnienia danych.

2. Nośniki, gdy nie są już potrzebne, są w sposób bezpieczny unieszkodliwiane zgodnie ze szczegółowymi procedurami określonymi w polityce bezpieczeństwa.

3. Dzięki inwentaryzacjom zapewnia się dostępność informacji dotyczących miejsca przechowywania, właściwego okresu przechowywania oraz upoważnień do dostępu.

4. Określa się wszystkie istotne aktywa centralnego VIS i infrastruktury łączności, aby można je było chronić zgodnie z ich znaczeniem. Prowadzony jest aktualny rejestr właściwego wyposażenia IT.

5. Dostępna jest aktualna dokumentacja centralnego VIS i infrastruktury łączności. Powyższą dokumentację chroni się przed nieupoważnionym dostępem.

Artykuł 11

Kontrola przechowywania

1. Podejmuje się odpowiednie środki w celu zapewnienia właściwego przechowywania informacji oraz zapobiegania nieupoważnionemu dostępowi do nich.

2. Wszystkie elementy wyposażenia zawierające nośniki do przechowywania danych są poddawane kontroli przed ich unieszkodliwieniem w celu upewnienia się, że dane szczególnie chronione zostały z nich w całości usunięte lub nadpisane, lub są one w bezpieczny sposób niszczone.

Artykuł 12

Kontrola hasła

1. Wszystkie hasła są przechowywane w bezpieczny sposób i traktowane jako poufne. Jeśli istnieje podejrzenie ujawnienia hasła, należy je bezzwłocznie zmienić lub zablokować konto danego użytkownika. Stosuje się osobiste i niepowtarzalne identyfikatory użytkowników.

2. W polityce bezpieczeństwa określone są procedury logowania i wylogowania mające na celu zapobieganie nieupoważnionemu dostępowi.

Artykuł 13

Kontrola dostępu

1. W polityce bezpieczeństwa określa się formalną procedurę rejestracji pracowników i wykreślania ich z rejestru, która służy do przyznawania lub unieważniania dostępu do sprzętu komputerowego i oprogramowania VIS w ramach centralnego VIS do celów zarządzania operacyjnego. Przydział i wykorzystanie odpowiednich danych uwierzytelniających dostęp (haseł oraz innych właściwych środków) kontroluje się za pomocą formalnego procesu zarządzania określonego w polityce bezpieczeństwa.

2. Dostęp do sprzętu komputerowego i oprogramowania VIS w ramach centralnego VIS:

(i) jest ograniczony do upoważnionych osób;

(ii) jest ograniczony do przypadków, w których można określić cel zgodny z prawem zgodnie z art. 42 i art. 50 ust. 2 rozporządzenia (WE) nr 767/2008;

(iii) nie trwa dłużej, niż jest to niezbędne do celów dostępu, i nie wykracza poza zakres tego celu; oraz

(iv) odbywa się wyłącznie zgodnie z polityką kontroli dostępu, która zostanie określona w ramach polityki bezpieczeństwa.

3. W centralnym VIS wykorzystuje się wyłącznie wyposażenie i oprogramowanie zaakceptowane przez lokalnego urzędnika ds. bezpieczeństwa centralnego VIS. Korzystanie z narzędzi systemowych, które może doprowadzić do przeciążenia systemu oraz aplikacji, jest ograniczone i podlega kontroli. Należy ustanowić procedury dotyczące kontroli instalacji oprogramowania.

Artykuł 14

Kontrola łączności

Infrastruktura łączności jest monitorowana w celu zapewnienia dostępności, integralności i poufności w zakresie wymiany informacji. Dane przesyłane w ramach infrastruktury łączności chronione są za pomocą środków kryptograficznych.

Artykuł 15

Kontrola zapisu danych

Konta osób upoważnionych do dostępu do oprogramowania VIS z centralnego VIS monitoruje lokalny urzędnik ds. bezpieczeństwa centralnego VIS. Korzystanie z tych kont, w tym czas i identyfikator użytkownika, jest rejestrowane.

Artykuł 16

Kontrola transportu

1. W ramach polityki bezpieczeństwa określa się odpowiednie środki, aby zapobiec nieupoważnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas przesyłania danych z lub do VIS i podczas przemieszczania nośników danych. W ramach polityki bezpieczeństwa określa się przepisy dotyczące dopuszczalnych metod wysyłki lub transportu oraz procedur odpowiedzialności za transport elementów i ich dotarcie do miejsca przeznaczenia. Na nośniku danych nie znajdują się żadne inne dane poza tymi, które mają być przesłane.

2. W odniesieniu do usług świadczonych przez osoby trzecie, obejmujących przetwarzanie, łączność, zapewnienie dostępu do infrastruktury przetwarzania danych lub zarządzanie nią bądź dodawanie produktów lub usług do infrastruktury przetwarzania danych, stosuje się odpowiednie zintegrowane kontrole bezpieczeństwa.

Artykuł 17

Bezpieczeństwo infrastruktury łączności

1. Infrastruktura łączności jest odpowiednio zarządzana i kontrolowana, tak, aby chronić ją przed zagrożeniami oraz zapewnić bezpieczeństwo samej infrastruktury łączności i centralnego VIS, w tym danych wymienianych za jego pośrednictwem.

2. Charakterystyka zabezpieczeń, poziomy usług oraz wymogi dotyczące zarządzania w odniesieniu do wszystkich usług sieciowych są określane w umowie o świadczenie usług sieciowych zawieranej z usługodawcą.

3. Oprócz punktów dostępowych VIS ochronie podlegają również dodatkowe usługi wykorzystywane w ramach infrastruktury łączności. Odpowiednie środki są określone w polityce bezpieczeństwa.

Artykuł 18

Monitorowanie

1. Dzienniki rejestrujące informacje, o których mowa w art. 34 ust. 1 rozporządzenia (WE) nr 767/2008, dotyczące wszystkich przypadków, w których uzyskano dostęp do danych osobowych w centralnym VIS lub dokonano przetwarzania takich danych, są bezpiecznie przechowywane i dostępne w miejscu, w którym zlokalizowany jest również główny VIS i rezerwowy VIS, przez okres, o którym mowa w art. 34 ust. 2 rozporządzenia (WE) nr 767/2008.

2. Procedury dotyczące monitorowania funkcjonowania lub błędów infrastruktury przetwarzania informacji są określone w polityce bezpieczeństwa, a wyniki monitorowania poddawane są regularnemu przeglądowi. W stosownych przypadkach podejmuje się odpowiednie działania.

3. Infrastruktura rejestrowania oraz dzienniki są chronione przed ingerencją lub nieupoważnionym dostępem w celu spełnienia wymogów dotyczących gromadzenia i przechowywania dowodów w trakcie okresu ich przechowywania.

Artykuł 19

Środki kryptograficzne

W stosownych przypadkach w celu ochrony informacji stosuje się środki kryptograficzne. Ich zastosowanie wraz z celem i warunkami ich zastosowania muszą zostać uprzednio zatwierdzone przez urzędnika ds. bezpieczeństwa systemu.

ROZDZIAŁ IV

BEZPIECZEŃSTWO ZASOBÓW LUDZKICH

Artykuł 20

Profile personelu

1. Funkcje i zadania osób upoważnionych do dostępu do VIS, w tym do infrastruktury łączności, są określone w polityce bezpieczeństwa.

2. Funkcje i zadania dotyczące bezpieczeństwa, wchodzące w zakres obowiązków pracowników Komisji, wykonawców oraz pracowników biorących udział w zarządzaniu operacyjnym, są określane, dokumentowane i przekazywane osobom, których to dotyczy. Wyżej wymienione funkcje i zadania są określone dla pracowników Komisji w opisie stanowiska pracy oraz jego celach, natomiast dla wykonawców są określone w umowach lub porozumieniach o poziomie usług.

3. Porozumienia o poufności i tajemnicy zawierane są ze wszystkimi osobami, do których nie mają zastosowania przepisy Unii Europejskiej lub państw członkowskich dotyczące usług publicznych. Pracownicy, którzy muszą pracować z danymi VIS, otrzymują odpowiednie zezwolenie lub poświadczenie zgodnie ze szczegółowymi procedurami, które zostaną określone w polityce bezpieczeństwa.

Artykuł 21

Informowanie pracowników

1. Wszyscy pracownicy, a w odpowiednich przypadkach również wykonawcy, przechodzą odpowiednie szkolenie w zakresie wiedzy na temat bezpieczeństwa, wymogów prawnych oraz zasad i procedur w zakresie wymaganym w ramach wykonywanych przez nich zadań.

2. W odniesieniu do zakończenia zatrudnienia lub wygaśnięcia umowy w polityce bezpieczeństwa określono wymogi dotyczące zmiany stanowiska lub zakończenia zatrudnienia dla pracowników i wykonawców, tak aby zapewnić zarządzanie zwrotem aktywów i odbieraniem praw dostępu.

ROZDZIAŁ V

PRZEPIS KOŃCOWY

Artykuł 22

Stosowanie

1. Niniejsza decyzja obowiązuje od dnia określonego przez Komisję zgodnie z art. 48 ust. 1 rozporządzenia (WE) nr 767/2008.

2. Niniejsza decyzja traci moc z dniem podjęcia obowiązków przez organ zarządzający.

Sporządzono w Brukseli dnia 4 maja 2010 r.

W imieniu Komisji

José Manuel BARROSO

Przewodniczący