DECYZJA SĄDU (UE) 2016/2387

z dnia 14 września 2016 r.

w sprawie zasad bezpieczeństwa mających zastosowanie do informacji lub materiałów przedstawionych na podstawie art. 105 § 1 lub § 2 regulaminu postępowania

SĄD,

uwzględniając regulamin postępowania, w szczególności jego art. 105 § 11,

a także mając na uwadze, co następuje:

(1) Zgodnie z art. 105 §§ 1 i 2 regulaminu postępowania strona główna sporu może – z własnej inicjatywy lub w wyniku środka dowodowego przyjętego przez Sąd – przedstawić informacje lub materiały mające wpływ na bezpieczeństwo Unii Europejskiej, jej państwa członkowskiego lub państw członkowskich lub też na utrzymywanie przez nie stosunków międzynarodowych. Paragrafy 3–10 tego przepisu przewidują tryb postępowania mający zastosowanie do takich informacji lub materiałów.

(2) Zważywszy na wrażliwy i poufny charakter odnośnych informacji lub materiałów, wprowadzenie w życie trybu ustanowionego w art. 105 regulaminu postępowania wymaga wprowadzenia odpowiednich rozwiązań w zakresie bezpieczeństwa mających na celu zapewnienie wysokiego poziomu ochrony tych informacji lub materiałów.

(3) We wskazanym powyżej celu rozwiązania w zakresie bezpieczeństwa powinny mieć zastosowanie do wszystkich informacji lub materiałów przedstawionych na podstawie art. 105 § 1 lub § 2 regulaminu postępowania, które są informacjami niejawnymi Unii Europejskiej lub w odniesieniu do których przedstawiająca je strona główna sygnalizuje, że ich przekazanie przeciwnej stronie głównej zaszkodziłoby bezpieczeństwu Unii lub jej państw członkowskich lub też utrzymywaniu przez nie stosunków międzynarodowych, także w sytuacji gdy wspomniane informacje lub materiały nie są informacjami niejawnymi Unii Europejskiej.

(4) W celu zapewnienia wysokiego poziomu ochrony tych informacji lub tych materiałów podstawowe zasady i minimalne normy bezpieczeństwa owych informacji lub materiałów są wzorowane na zasadach i normach mających zastosowanie do ochrony informacji niejawnych SECRET UE/EU SECRET zgodnie z przepisami instytucji Unii w dziedzinie ochrony informacji niejawnych Unii Europejskiej (EUCI), w szczególności z przepisami przyjętymi przez Radę Unii Europejskiej, Parlament Europejski i Komisję Europejską.

(5) Informacje lub materiały przedstawione na podstawie art. 105 § 1 lub § 2 regulaminu postępowania zostają opatrzone swoistym dla Trybunału Sprawiedliwości Unii Europejskiej oznaczeniem, zwanym „FIDUCIA", określającym tryb bezpieczeństwa, który się do nich stosuje na wszystkich etapach postępowania przed Sądem oraz – w przypadku odwołania – przed Trybunałem Sprawiedliwości. Opatrzenie oznaczeniem FIDUCIA i usunięcie tego oznaczenia nie mają wpływu na klasyfikację informacji przekazanych Sądowi.

(6) Dostęp do informacji FIDUCIA zapewnia się z poszanowaniem zasady ograniczonego dostępu,

POSTANAWIA:

Artykuł 1

Definicje

Do celów niniejszej decyzji:

a) „organ bezpieczeństwa" oznacza organ odpowiedzialny za bezpieczeństwo Trybunału Sprawiedliwości Unii Europejskiej wyznaczony przez tę instytucję, który to organ może delegować, w całości lub w części, wykonanie zadań przewidzianych w niniejszej decyzji;

b) „biuro FIDUCIA" oznacza biuro Trybunału Sprawiedliwości Unii Europejskiej zapewniające zarządzanie informacjami FIDUCIA;

c) „posiadacz" oznacza osobę należycie upoważnioną i spełniającą zasadę ograniczonego dostępu, znajdującą się w posiadaniu informacji FIDUCIA i w związku z tym odpowiedzialną za ich ochronę;

d) „dokument" oznacza każdą informację, bez względu na jej formę fizyczną lub cechy charakterystyczne;

e) „informacja" oznacza każdą informację pisemną lub ustną, niezależnie od jej nośnika lub autora;

f) „informacje niejawne Unii Europejskiej" (EUCI) oznaczają wszelkie informacje lub materiały objęte klauzulą tajności Unii Europejskiej na podstawie przepisów mających zastosowanie w tej dziedzinie w instytucjach Unii, którym to informacjom lub materiałom nadano jedną z następujących klauzul tajności:

— TRÈS SECRET UE/EU TOP SECRET,

— SECRET UE/EU SECRET,

— CONFIDENTIEL UE/EU CONFIDENTIAL,

— RESTREINT UE/EU RESTRICTED;

g) „informacja FIDUCIA" oznacza każdą informację noszącą oznaczenie FIDUCIA;

h) „przetwarzanie" informacji FIDUCIA oznacza wszelkie działania, których przedmiotem mogą być informacje FIDUCIA na wszystkich etapach postępowania przed Sądem i najpóźniej do upływu terminu wskazanego w art. 56 akapit pierwszy statutu Trybunału Sprawiedliwości Unii Europejskiej. Obejmują one zatem ich rejestrację, przeglądanie, wytwarzanie, powielanie, przechowywanie, zwracanie i niszczenie.

Artykuł 2

Przedmiot i zakres stosowania

1. Niniejsza decyzja określa podstawowe zasady i minimalne normy bezpieczeństwa służące ochronie informacji FIDUCIA w ramach postępowania przed Sądem i najpóźniej do upływu terminu wskazanego w art. 56 akapit pierwszy statutu Trybunału Sprawiedliwości Unii Europejskiej.

2. Te podstawowe zasady i minimalne normy bezpieczeństwa mają zastosowanie do każdej informacji FIDUCIA, podobnie jak do wszelkiego wykorzystania pisemnego lub ustnego, jak również do kopii, które w stosownym przypadku sporządza się zgodnie z zasadami bezpieczeństwa ustalonymi w niniejszej decyzji.

Artykuł 3

Zasady dotyczące składania i zwracania informacji lub materiałów

W celu stosowania mechanizmu przewidzianego w niniejszej decyzji:

— strona główna informuje sekretariat Sądu o dniu złożenia informacji lub materiałów na podstawie art. 105 § 1 lub § 2 regulaminu postępowania,

— strona główna – w obecności przedstawiciela sekretariatu – jest zobowiązana złożyć informacje lub materiały na podstawie art. 105 § 1 lub § 2 regulaminu postępowania w biurze FIDUCIA w godzinach przyjęć interesantów przez sekretariat,

— strona główna, która przedstawiła informacje lub materiały na podstawie art. 105 § 1 lub § 2 regulaminu postępowania, jest zobowiązana odebrać je w biurze FIDUCIA w obecności przedstawiciela sekretariatu, jeżeli nie wyraża zgody na ich przekazanie na podstawie art. 105 § 4 wspomnianego regulaminu, niezwłocznie po ich usunięciu zgodnie z art. 105 § 7 tego samego regulaminu lub niezwłocznie po upływie terminu wskazanego w art. 56 akapit pierwszy statutu Trybunału Sprawiedliwości Unii Europejskiej, chyba że wniesiono odwołanie w tym terminie,

— jeżeli w terminie wskazanym w art. 56 akapit pierwszy statutu Trybunału Sprawiedliwości Unii Europejskiej wniesiono odwołanie od orzeczenia Sądu, informacje lub materiały przedstawione w ramach tej sprawy na podstawie art. 105 § 1 lub § 2 regulaminu postępowania udostępnia się Trybunałowi Sprawiedliwości. W tym celu sekretarz Sądu, niezwłocznie po otrzymaniu informacji o istnieniu tego odwołania, kieruje pismo do sekretarza Trybunału Sprawiedliwości, informując go o udostępnieniu Trybunałowi Sprawiedliwości odnośnych informacji lub materiałów. Sekretarz Sądu informuje jednocześnie organ bezpieczeństwa, że odnośne informacje lub materiały winny zostać udostępnione Trybunałowi Sprawiedliwości bez fizycznego przemieszczenia tych informacji lub materiałów. Informacja ta jest odnotowywana przez biuro FIDUCIA. Strona główna, która przedstawiła te informacje lub materiały, jest zobowiązana odebrać je w biurze FIDUCIA w obecności przedstawiciela sekretariatu Trybunału Sprawiedliwości niezwłocznie po doręczeniu orzeczenia kończącego postępowanie odwoławcze, chyba że sprawa zostanie przekazana do ponownego rozpoznania przez Sąd,

— w przypadku przekazania sprawy do Sądu Trybunał Sprawiedliwości udostępnia Sądowi odnośne informacje lub materiały niezwłocznie po doręczeniu orzeczenia kończącego postępowanie odwoławcze. W tym celu sekretarz Trybunału Sprawiedliwości kieruje pismo do sekretarza Sądu, informując go o udostępnieniu odnośnych informacji lub materiałów Sądowi. Sekretarz Trybunału Sprawiedliwości informuje jednocześnie organ bezpieczeństwa, że odnośne informacje lub materiały winny zostać udostępnione Sądowi bez fizycznego przemieszczenia tych informacji lub materiałów. Informacja ta jest odnotowywana przez biuro FIDUCIA. Strona główna, która przedstawiła te informacje lub materiały, jest zobowiązana odebrać je w biurze FIDUCIA w obecności przedstawiciela sekretariatu Sądu niezwłocznie po upływie terminu wskazanego w art. 56 akapit pierwszy statutu Trybunału Sprawiedliwości Unii Europejskiej, chyba że wniesiono odwołanie w tym terminie.

Artykuł 4

Oznaczenie FIDUCIA

1. Oznaczenie FIDUCIA jest nadawane przez biuro FIDUCIA wszystkim informacjom lub materiałom przedstawionym zgodnie z art. 105 § 1 lub § 2 regulaminu postępowania.

2. Oznaczenie FIDUCIA jest także nadawane przez biuro FIDUCIA każdej informacji, która przejmuje w całości lub w części treść informacji lub materiałów przedstawionych zgodnie z art. 105 § 1 lub § 2 regulaminu postępowania, jak również każdej kopii takich informacji lub materiałów.

3. Oznaczenie FIDUCIA jest także nadawane przez biuro FIDUCIA sporządzanym przez biuro FIDUCIA na podstawie niniejszej decyzji dokumentom lub rejestrom, których nieuprawnione ujawnienie mogłoby zaszkodzić bezpieczeństwu Unii, jej państwa członkowskiego lub państw członkowskich lub też utrzymywaniu przez nie stosunków międzynarodowych.

4. Oznaczenie FIDUCIA umieszcza się w widoczny sposób na wszystkich stronach i nośnikach informacji FIDUCIA.

5. Opatrzenie oznaczeniem FIDUCIA i usunięcie tego oznaczenia na warunkach określonych w załączniku III nie mają wpływu na klasyfikację informacji przekazanych Sądowi.

Artykuł 5

Ochrona informacji FIDUCIA

1. Ochrona informacji FIDUCIA odpowiada ochronie zapewnianej w przypadku EUCI SECRET UE/EU SECRET zgodnie z przepisami mającymi zastosowanie w instytucjach Unii w dziedzinie ochrony EUCI.

2. Posiadacz wszelkich informacji FIDUCIA jest zobowiązany do ich ochrony zgodnie z niniejszą decyzją.

Artykuł 6

Zarządzanie ryzykiem dla bezpieczeństwa

1. Zarządzanie ryzykiem naruszenia informacji FIDUCIA przebiega w ramach procesu analizowania ryzyka mającego na celu określenie znanych rodzajów ryzyka naruszenia zasad bezpieczeństwa, zdefiniowanie środków bezpieczeństwa służących zmniejszeniu tego ryzyka do akceptowalnego poziomu zgodnie z podstawowymi zasadami i minimalnymi normami bezpieczeństwa przedstawionymi w niniejszej decyzji oraz stosowanie tych środków. Skuteczność takich środków jest stale oceniana przez organ bezpieczeństwa.

2. Środki bezpieczeństwa służące ochronie informacji FIDUCIA na wszystkich etapach postępowania przed Sądem i najpóźniej do upływu terminu wskazanego w art. 56 akapit pierwszy statutu Trybunału Sprawiedliwości Unii Europejskiej są proporcjonalne w szczególności do formy i obszerności odnośnych informacji lub materiałów, otoczenia i struktury pomieszczeń biura FIDUCIA oraz do dokonywanej na szczeblu lokalnym oceny zagrożenia wystąpienia działań realizowanych w złych zamiarach lub działalności przestępczej, w tym działalności szpiegowskiej, sabotażowej lub terrorystycznej.

3. Wewnętrzny plan awaryjny Trybunału Sprawiedliwości Unii Europejskiej uwzględnia potrzebę ochrony informacji FIDUCIA podczas sytuacji nadzwyczajnych w celu zapobieżenia nieuprawnionemu dostępowi do informacji, ich nieuprawnionemu ujawnieniu bądź utracie ich integralności lub dostępności.

4. W wewnętrznym planie awaryjnym Trybunału Sprawiedliwości Unii Europejskiej przewidziane są środki zapobiegawcze i naprawcze służące zminimalizowaniu skutków poważnych niedopatrzeń lub incydentów związanych z przetwarzaniem informacji FIDUCIA oraz z ich przechowywaniem.

Artykuł 7

Środki bezpieczeństwa w odniesieniu do osób

1. Dostęp do informacji FIDUCIA można przyznać jedynie osobom, które:

— spełniają zasadę ograniczonego dostępu,

— z zastrzeżeniem ust. 2 niniejszego artykułu zostały upoważnione do dostępu do informacji FIDUCIA, oraz

— zostały poinstruowane o ciążących na nich obowiązkach.

2. Sędziów Sądu uznaje się za upoważnionych, ze względu na pełnione przez nich funkcje, do dostępu do informacji FIDUCIA.

3. W załączniku I zostaje doprecyzowana procedura mająca na celu ustalenie, czy urzędnik lub inny pracownik Trybunału Sprawiedliwości Unii Europejskiej – z uwagi na jego lojalność, rzetelność i wiarygodność – może zostać upoważniony do dostępu do informacji FIDUCIA.

4. Przed przyznaniem dostępu do informacji FIDUCIA, a następnie w regularnych odstępach czasu wszystkie zainteresowane osoby są instruowane o obowiązkach, które na nich ciążą w zakresie ochrony informacji FIDUCIA zgodnie z niniejszą decyzją, i uznają te obowiązki na piśmie.

Artykuł 8

Bezpieczeństwo fizyczne

1. „Bezpieczeństwo fizyczne" oznacza stosowanie fizycznych i technicznych środków ochrony, aby zapobiec nieuprawnionemu dostępowi do informacji FIDUCIA.

2. Środki bezpieczeństwa fizycznego mają na celu zapobieżenie wtargnięciu osoby nieupoważnionej do pomieszczeń biura FIDUCIA w sposób niezauważony lub z użyciem siły, powstrzymanie od podejmowania nieuprawnionych działań, udaremnienie i wykrycie takich działań oraz umożliwienie odróżnienia osób upoważnionych od osób nieupoważnionych do dostępu do informacji FIDUCIA zgodnie z zasadą ograniczonego dostępu. Środki te są określane na podstawie procesu zarządzania ryzykiem.

3. Środki bezpieczeństwa fizycznego stosuje się w odniesieniu do pomieszczeń biura FIDUCIA, w których są przetwarzane i przechowywane informacje FIDUCIA. Środki te mają na celu zapewnienie ochrony odpowiadającej ochronie, z której korzystają EUCI SECRET UE/EU SECRET zgodnie z przepisami mającymi zastosowanie w instytucjach Unii w dziedzinie ochrony EUCI. Informacje FIDUCIA nie mogą być ani przechowywane, ani przeglądane poza pomieszczeniami biura FIDUCIA stworzonymi w tym celu w obrębie zabezpieczonej strefy.

4. Do ochrony informacji FIDUCIA stosuje się wyłącznie sprzęt lub urządzenia zgodne z przepisami mającymi zastosowanie w instytucjach Unii w dziedzinie ochrony EUCI.

5. Przepisy dotyczące wykonania niniejszego artykułu znajdują się w załączniku II.

Artykuł 9

Zarządzanie informacjami FIDUCIA

1. „Zarządzanie informacjami FIDUCIA" polega na stosowaniu środków administracyjnych mających na celu ochronę informacji FIDUCIA na wszystkich etapach postępowania przed Sądem i najpóźniej do upływu terminu wskazanego w art. 56 akapit pierwszy statutu Trybunału Sprawiedliwości Unii Europejskiej oraz kontrolę, która ma pomóc w zapobieganiu zamierzonemu lub przypadkowemu narażeniu na szwank bezpieczeństwa tych informacji lub ich utracie i w wykrywaniu takich przypadków.

2. Środki zarządzania informacjami FIDUCIA dotyczą w szczególności rejestracji, przeglądania, wytwarzania, powielania, przechowywania, zwracania i niszczenia informacji FIDUCIA.

3. Biuro FIDUCIA rejestruje informacje FIDUCIA w chwili ich otrzymania oraz przed jakimkolwiek przetworzeniem tych informacji.

4. Pomieszczenia biura FIDUCIA są poddawane regularnym inspekcjom przeprowadzanym przez organ bezpieczeństwa.

5. Przepisy dotyczące wykonania niniejszego artykułu znajdują się w załączniku III.

Artykuł 10

Ochrona informacji FIDUCIA przetwarzanych drogą elektroniczną

1. Systemy teleinformatyczne (komputery i urządzenia końcowe) wykorzystywane do przetwarzania informacji FIDUCIA znajdują się w pomieszczeniach biura FIDUCIA. Są one odizolowane od wszystkich sieci informatycznych.

2. Stosuje się środki bezpieczeństwa w celu ochrony sprzętu informatycznego wykorzystywanego do przetwarzania informacji FIDUCIA przed narażeniem na szwank bezpieczeństwa tych informacji z powodu niezamierzonych emisji elektromagnetycznych (środki bezpieczeństwa odpowiadające środkom praktykowanym w odniesieniu do EUCI SECRET UE/EU SECRET zgodnie z przepisami mającymi zastosowanie w instytucjach Unii w dziedzinie ochrony EUCI).

3. Systemy teleinformatyczne podlegają akredytacji udzielanej przez organ bezpieczeństwa, który upewnia się, że odpowiadają one przepisom mającym zastosowanie w instytucjach Unii w dziedzinie ochrony EUCI.

4. Przepisy dotyczące wykonania niniejszego artykułu znajdują się w załączniku IV.

Artykuł 11

Bezpieczeństwo w przypadku interwencji zewnętrznej

1. „Bezpieczeństwo w przypadku interwencji zewnętrznej" oznacza stosowanie środków mających zapewnić ochronę informacji FIDUCIA przez wykonawców, którzy mają interweniować w ramach konserwacji systemów teleinformatycznych odizolowanych od sieci informatycznej, lub w trakcie interwencji wymagającej pilnego przemieszczenia informacji FIDUCIA w celu umieszczenia ich w bezpiecznym miejscu.

2. Organ bezpieczeństwa może powierzyć wykonanie zadań wiążących się z dostępem lub wymagających dostępu do informacji FIDUCIA wykonawcom zarejestrowanym w państwie członkowskim zgodnie z zawartą z nimi umową.

3. Organ bezpieczeństwa zapewnia, by minimalne normy bezpieczeństwa przewidziane w niniejszej decyzji i wymienione w umowie były przestrzegane przy udzielaniu zamówień.

4. Pracownicy wykonawcy mogą uzyskać dostęp do informacji FIDUCIA dopiero po upoważnieniu ich przez organ bezpieczeństwa na podstawie poświadczenia bezpieczeństwa osobowego wydanego przez krajową władzę bezpieczeństwa lub każdy inny właściwy organ bezpieczeństwa zgodnie z krajowymi przepisami ustawowymi lub wykonawczymi.

5. Przepisy dotyczące wykonania niniejszego artykułu znajdują się w załączniku V.

Artykuł 12

Brak cyfrowego rozpowszechniania, przekazywania i wymiany informacji FIDUCIA

1. Informacje FIDUCIA w żadnym wypadku nie są rozpowszechniane w postaci cyfrowej.

2. Sąd nie przekazuje informacji FIDUCIA ani instytucjom, organom, jednostkom organizacyjnym lub agencjom Unii, ani państwom członkowskim, ani też innym stronom sporu, ani osobom trzecim.

Artykuł 13

Naruszenie zasad bezpieczeństwa i narażenie na szwank bezpieczeństwa informacji FIDUCIA

1. Naruszenie zasad bezpieczeństwa następuje w wyniku działania określonej osoby lub zaniechania przez nią działania, sprzecznego z przepisami bezpieczeństwa określonymi w niniejszej decyzji.

2. Narażenie na szwank bezpieczeństwa informacji FIDUCIA ma miejsce, gdy w wyniku naruszenia zasad bezpieczeństwa takie informacje w całości lub w części zostają ujawnione osobom nieupoważnionym lub osobom nieuznawanym za upoważnione.

3. O każdym zaistniałym lub domniemanym przypadku naruszenia zasad bezpieczeństwa powiadamia się niezwłocznie organ bezpieczeństwa.

4. W przypadkach gdy wiadomo lub istnieją racjonalne podstawy do podejrzeń, że bezpieczeństwo informacji FIDUCIA zostało narażone na szwank lub że informacje takie zostały utracone, organ bezpieczeństwa w ścisłej współpracy z prezesem i sekretarzem Sądu podejmuje wszelkie stosowne środki zgodnie z mającymi zastosowanie przepisami w celu:

a) poinformowania strony głównej, która przedstawiła odnośne informacje lub materiały;

b) zwrócenia się do właściwego organu o wszczęcie administracyjnego postępowania wyjaśniającego;

c) dokonania oceny potencjalnych szkód wyrządzonych bezpieczeństwu Unii, jej państwa członkowskiego lub państw członkowskich lub też utrzymywaniu przez nie stosunków międzynarodowych;

d) zapobiegnięcia powtarzaniu się podobnych przypadków; oraz

e) powiadomienia właściwych organów o podjętych działaniach.

5. Każda osoba odpowiedzialna za naruszenie zasad bezpieczeństwa określonych w niniejszej decyzji może podlegać sankcjom dyscyplinarnym zgodnie z odpowiednimi przepisami. Każda osoba odpowiedzialna za narażenie na szwank bezpieczeństwa informacji FIDUCIA lub za ich utratę może podlegać sankcjom dyscyplinarnym lub można wszcząć przeciwko niej postępowanie sądowe zgodnie z odpowiednimi przepisami.

Artykuł 14

Organizacja bezpieczeństwa w Sądzie

1. Biuro FIDUCIA obejmuje ochroną informacje FIDUCIA zgodnie z niniejszą decyzją.

2. Organ bezpieczeństwa jest odpowiedzialny za prawidłowe stosowanie niniejszej decyzji. W tym celu organ bezpieczeństwa:

a) stosuje politykę bezpieczeństwa Trybunału Sprawiedliwości Unii Europejskiej i dokonuje okresowo jej przeglądu;

b) kontroluje stosowanie niniejszej decyzji przez biuro FIDUCIA;

c) w stosownym przypadku zleca – w okolicznościach przewidzianych w art. 13 – wszczęcie postępowania wyjaśniającego w sprawie każdego zaistniałego lub domniemanego przypadku utraty informacji FIDUCIA;

d) przeprowadza okresowe inspekcje zabezpieczeń służących ochronie informacji FIDUCIA w pomieszczeniach biura FIDUCIA.

Artykuł 15

Praktyczne zasady dotyczące wykonania

Praktyczne zasady dotyczące wykonania niniejszej decyzji zostają ustalone przez organ bezpieczeństwa w porozumieniu z sekretarzem Sądu.

Artykuł 16

Wejście w życie

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

Sporządzono w Luksemburgu dnia 14 września 2016 r.

Sekretarz	*Prezes*
E. COULON	M. JAEGER

ZAŁĄCZNIK I

ŚRODKI BEZPIECZEŃSTWA W ODNIESIENIU DO OSÓB

1. Niniejszy załącznik zawiera przepisy dotyczące wykonania art. 7 decyzji.

2. Do sekretarza Sądu należy sporządzenie wykazu – w odniesieniu do tej instytucji i w ściśle koniecznym zakresie – stanowisk wymagających dostępu do informacji FIDUCIA, co wiąże się zatem z tym, że urzędnicy i inni pracownicy zajmujący dane stanowiska w Sądzie powinni być upoważnieni do dostępu do informacji FIDUCIA.

3. W celu udzielenia upoważnienia do dostępu do informacji FIDUCIA biuro FIDUCIA przekazuje ankietę bezpieczeństwa wypełnioną przez zainteresowanego urzędnika lub innego pracownika krajowej władzy bezpieczeństwa państwa członkowskiego, którego obywatelem jest dana osoba, lub każdemu innemu właściwemu organowi krajowemu, wskazanym w przepisach mających zastosowanie w instytucjach Unii w dziedzinie ochrony EUCI (zwanym dalej „właściwą KWB"), i zwraca się z wnioskiem o przeprowadzenie postępowania sprawdzającego w odniesieniu do poziomu klauzuli tajności SECRET UE/EU SECRET.

4. Po zakończeniu postępowania sprawdzającego, które podlega przepisom ustawowym i wykonawczym obowiązującym w danym państwie członkowskim, właściwa KWB powiadamia biuro FIDUCIA o wyniku takiego postępowania.

5. Jeżeli w wyniku postępowania sprawdzającego właściwa KWB uzyskała pewność, że nie istnieją żadne niekorzystne informacje, które mogłyby podważać lojalność, rzetelność i wiarygodność danej osoby, właściwy organ powołujący może udzielić tej osobie upoważnienia do dostępu do informacji FIDUCIA.

6. Jeżeli w wyniku postępowania sprawdzającego nie uzyskano pewności, o której mowa w pkt 5 powyżej, organ powołujący powiadamia o tym fakcie daną osobę. W takim przypadku biuro FIDUCIA, zgodnie z poleceniem organu powołującego, może zwrócić się do właściwej KWB o przedstawienie wszelkich dalszych wyjaśnień, których organ ten może udzielić zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Jeżeli wynik postępowania sprawdzającego zostanie potwierdzony, nie udziela się upoważnienia do dostępu do informacji FIDUCIA.

7. Upoważnienie do dostępu do informacji FIDUCIA jest ważne przez okres pięciu lat. Zostaje ono cofnięte, gdy dana osoba opuszcza stanowisko wymagające dostępu do informacji FIDUCIA lub gdy organ powołujący uważa, że istnieją powody uzasadniające cofnięcie upoważnienia.

8. Upoważnienie do dostępu do informacji FIDUCIA może zostać odnowione zgodnie z procedurą określoną w pkt 3–5 powyżej.

9. Biuro FIDUCIA prowadzi rejestr upoważnień do dostępu do informacji FIDUCIA.

10. Jeżeli biuro FIDUCIA znajdzie się w posiadaniu informacji o ryzyku naruszenia zasad bezpieczeństwa przez osobę będącą posiadaczem upoważnienia do dostępu do informacji FIDUCIA, biuro FIDUCIA powiadamia o tym właściwą KWB i organ powołujący może zawiesić dostęp do informacji FIDUCIA lub cofnąć upoważnienie do dostępu do tych informacji.

11. W nagłych przypadkach organ powołujący może – po konsultacji z właściwą KWB oraz z zastrzeżeniem, że wynik wstępnego sprawdzenia nie wykazał niekorzystnych informacji – udzielić zainteresowanym urzędnikom i innym pracownikom tymczasowego upoważnienia do dostępu do informacji FIDUCIA. Takie tymczasowe upoważnienie zachowuje ważność do momentu zakończenia postępowania, o którym mowa w pkt 3–5 powyżej, nie może ono jednak przekraczać okresu sześciu miesięcy od dnia złożenia do właściwej KWB wniosku o przeprowadzenie postępowania sprawdzającego.

12. Przed przyznaniem dostępu do informacji FIDUCIA osoby do tego upoważnione uczestniczą w szkoleniu, którego celem jest umożliwienie im wykonywania ciążących na nich obowiązków związanych z przetwarzaniem informacji FIDUCIA. Upoważnienie do dostępu do informacji FIDUCIA staje się skuteczne dopiero po tym szkoleniu i pisemnym uznaniu obowiązków.

ZAŁĄCZNIK II

BEZPIECZEŃSTWO FIZYCZNE

I. WSTĘP

1. Niniejszy załącznik zawiera przepisy dotyczące wykonania art. 8 decyzji. Określa on minimalne wymogi w zakresie fizycznej ochrony pomieszczeń biura FIDUCIA, w których są przetwarzane i przechowywane informacje FIDUCIA.

2. Środki bezpieczeństwa fizycznego mają na celu zapobieżenie nieuprawnionemu dostępowi do informacji FIDUCIA poprzez:

   a) zapewnienie właściwego przetwarzania i przechowywania informacji FIDUCIA;

   b) umożliwienie odróżnienia osób upoważnionych od osób nieupoważnionych do dostępu do informacji FIDUCIA zgodnie z zasadą ograniczonego dostępu;

   c) powstrzymanie od nieuprawnionych działań, ich udaremnianie i wykrywanie; oraz

   d) uniemożliwienie lub opóźnienie wtargnięcia osób nieupoważnionych w sposób niezauważony lub z użyciem siły do pomieszczeń biura FIDUCIA.

3. Środki bezpieczeństwa fizycznego dobiera się na podstawie oceny zagrożeń dla informacji FIDUCIA. Środki te uwzględniają otoczenie i strukturę pomieszczeń biura FIDUCIA. Organ bezpieczeństwa określa stopień bezpieczeństwa, jaki należy osiągnąć w przypadku każdego z poniższych środków fizycznych:

   a) ogrodzenie, które chroni granice strefy wymagającej ochrony;

   b) system sygnalizacji włamania i napadu połączony ze stanowiskiem dowodzenia i bezpieczeństwa Trybunału Sprawiedliwości Unii Europejskiej;

   c) system kontroli dostępu przeprowadzanej za pomocą środków elektronicznych lub środków elektromechanicznych oraz dokonywanej przez pracowników ochrony;

   d) przeszkoleni i nadzorowani pracownicy ochrony, którzy zostali upoważnieni do dostępu do informacji FIDUCIA;

   e) system dozoru wizyjnego obsługiwany przez pracowników ochrony i połączony z systemem sygnalizacji włamania i napadu oraz z systemem kontroli dostępu;

   f) oświetlenie ochronne zapewniające skuteczny bezpośredni nadzór lub za pośrednictwem systemu dozoru wizyjnego;

   g) wszelkie inne stosowne środki fizyczne służące powstrzymaniu od nieuprawnionego dostępu lub wykrywaniu takiego dostępu, zapobieganiu przeglądaniu, utracie informacji FIDUCIA lub narażeniu na szwank ich bezpieczeństwa.

II. POMIESZCZENIA, W KTÓRYCH SĄ PRZECHOWYWANE I PRZEGLĄDANE INFORMACJE FIDUCIA

Utworzenie fizycznie chronionych pomieszczeń, w których są przechowywane i przeglądane informacje FIDUCIA

4. Tworzy się zabezpieczone pomieszczenia w celu przechowywania i przeglądania informacji FIDUCIA. Informacje FIDUCIA mogą być przechowywane i przeglądane wyłącznie w pomieszczeniach biura FIDUCIA, które są zgodne pod wszelkimi względami z przepisami mającymi zastosowanie w instytucjach Unii w dziedzinie ochrony EUCI.

5. We wspomnianych pomieszczeniach informacje FIDUCIA są przechowywane w zabezpieczonych szafach, które także są zgodne pod wszelkimi względami z przepisami mającymi zastosowanie w instytucjach Unii w dziedzinie ochrony EUCI.

6. Do pomieszczeń biura FIDUCIA nie można wnieść żadnego systemu komunikacyjnego (telefonu lub innego urządzenia elektronicznego).

7. Lokal zebrań biura FIDUCIA jest chroniony przed podsłuchem. Jest on regularnie poddawany inspekcjom bezpieczeństwa elektronicznego.

Dostęp do pomieszczeń, w których są przechowywane i przeglądane informacje FIDUCIA

8. Dostęp do pomieszczeń biura FIDUCIA jest kontrolowany za pomocą umożliwiających identyfikację drzwi bezpieczeństwa objętych dozorem wizyjnym.

9. Osoby, które zostały upoważnione do dostępu do informacji FIDUCIA, i osoby uznawane za upoważnione mogą wejść do pomieszczeń biura FIDUCIA w celu przeglądania informacji FIDUCIA w okolicznościach, o których mowa w art. 7 ust. 1 i 2 niniejszej decyzji.

10. Organ bezpieczeństwa może wyjątkowo wydać upoważnienie do dostępu osobom nieupoważnionym, których interwencja w pomieszczeniach biura FIDUCIA jest niezbędna, z zastrzeżeniem jednak, że dostęp do tych pomieszczeń nie będzie się wiązać z dostępem do informacji FIDUCIA, które pozostaną niewidoczne w zabezpieczonych szafach. Dostęp tych osób może mieć miejsce tylko w towarzystwie i pod stałym nadzorem osoby z biura FIDUCIA, która została upoważniona do dostępu do informacji FIDUCIA.

11. Każde wejście do pomieszczeń biura FIDUCIA jest zapisywane w rejestrze dostępu. Rejestr ten jest prowadzony na stanowisku pracy znajdującym się w tych pomieszczeniach. Wykorzystywany w tym celu system teleinformatyczny jest zgodny z wymogami bezpieczeństwa określonymi w art. 10 decyzji oraz w załączniku IV.

12. Środki ochrony regulujące pisemne wykorzystanie informacji FIDUCIA znajdują zastosowanie do przypadków ustnego wykorzystania tych samych informacji.

III. KONTROLA KLUCZY I KODÓW WYKORZYSTYWANYCH DO OCHRONY INFORMACJI FIDUCIA

13. Organ bezpieczeństwa określa procedury zarządzania kluczami i kodami do pomieszczeń biura FIDUCIA i zabezpieczonych szaf. Procedury te chronią przed nieuprawnionym dostępem.

14. Kody są zapamiętywane przez jak najmniejszą liczbę osób, którym ich znajomość jest niezbędna. Kody do zabezpieczonych szaf, w których są przechowywane informacje FIDUCIA, są zmieniane:

    a) w przypadku otrzymania nowej szafy;

    b) przy każdej zmianie pracowników znających kod;

    c) w każdym przypadku, gdy następuje rzeczywiste lub domniemane narażenie na szwank bezpieczeństwa informacji;

    d) gdy zamek poddano konserwacji lub naprawie;

    e) nie rzadziej niż co 12 miesięcy.

15. Sprzęt techniczny przeznaczony do fizycznej ochrony informacji FIDUCIA jest zgodny z przepisami mającymi zastosowanie w instytucjach Unii w dziedzinie ochrony EUCI. Organ bezpieczeństwa jest odpowiedzialny za przestrzeganie tych przepisów.

16. Sprzęt techniczny jest poddawany regularnym inspekcjom i regularnej konserwacji. Podczas konserwacji uwzględnia się wyniki inspekcji, aby zapewnić dalsze optymalne działanie sprzętu.

17. Podczas każdej inspekcji przeprowadza się ocenę skuteczności poszczególnych środków bezpieczeństwa oraz całego systemu bezpieczeństwa.

ZAŁĄCZNIK III

ZARZĄDZANIE INFORMACJAMI FIDUCIA

I. WSTĘP

1. Niniejszy załącznik zawiera przepisy dotyczące wykonania art. 9 decyzji. Określa on środki administracyjne służące ochronie informacji FIDUCIA na wszystkich etapach postępowania przed Sądem i najpóźniej do upływu terminu wskazanego w art. 56 akapit pierwszy statutu Trybunału Sprawiedliwości Unii Europejskiej oraz ich kontroli, co ma pomóc w zapobieganiu zamierzonemu lub przypadkowemu narażeniu na szwank bezpieczeństwa tych informacji lub ich utracie i w wykrywaniu takich przypadków.

II. REJESTR INFORMACJI FIDUCIA

2. Ustanawia się rejestr informacji FIDUCIA. Rejestr ten jest prowadzony przez biuro FIDUCIA na stanowisku pracy znajdującym się w pomieszczeniach biura FIDUCIA. System teleinformatyczny wykorzystywany do celów prowadzenia tego rejestru jest zgodny z wymogami bezpieczeństwa określonymi w art. 10 decyzji oraz w załączniku IV.

III. REJESTRACJA INFORMACJI FIDUCIA

3. Do celów niniejszej decyzji rejestracja ze względów bezpieczeństwa (zwana dalej „rejestracją") oznacza stosowanie procedur umożliwiających rejestrowanie etapów cyklu życia informacji FIDUCIA, w tym jej zniszczenia.

4. Rejestrację informacji FIDUCIA zapewnia biuro FIDUCIA.

5. Biuro FIDUCIA przyznaje automatycznie oznaczenie FIDUCIA informacjom lub materiałom przedstawionym na podstawie art. 105 § 1 lub § 2 regulaminu postępowania. Biuro FIDUCIA rejestruje informację FIDUCIA w rejestrze informacji FIDUCIA.

6. Biuro FIDUCIA sporządza raport załączany do rejestru informacji FIDUCIA, określając w nim dokładnie okoliczności otrzymania informacji. Informacja ta jest następnie przetwarzana zgodnie z zasadami określonymi w poprzednim punkcie.

7. Rejestracja, zgodnie z pkt 5 i 6, informacji FIDUCIA w rejestrze informacji FIDUCIA odbywa się bez uszczerbku dla rejestracji do celów postępowania dokonywanej przez osoby, które zostały upoważnione do dostępu do informacji FIDUCIA w sekretariacie.

IV. ZARZĄDZANIE INFORMACJAMI FIDUCIA

Oznaczanie

8. W przypadku gdy EUCI lub każda inna informacja, w odniesieniu do której podnosi się, że jej przekazanie zaszkodziłoby bezpieczeństwu Unii, jej państwa członkowskiego lub państw członkowskich lub też utrzymywaniu przez nie stosunków międzynarodowych, zostaje przedstawiona w ramach art. 105 § 1 lub § 2 regulaminu postępowania, biuro FIDUCIA nadaje jej oznaczenie FIDUCIA.

9. Oznaczenie FIDUCIA wskazuje się jasno i prawidłowo na każdej części dokumentu, bez względu na formę, w jakiej występuje dana informacja: formę papierową, audio, elektroniczną lub inną.

Wytwarzanie informacji FIDUCIA

10. Tylko osoba, która została upoważniona do dostępu do informacji FIDUCIA, lub osoba uznawana za upoważnioną może wytwarzać informacje FIDUCIA, o których mowa w art. 4 ust. 2 i 3 niniejszej decyzji.

11. Każdą wytworzoną informację FIDUCIA biuro FIDUCIA rejestruje w rejestrze informacji FIDUCIA.

12. Każda wytworzona informacja FIDUCIA podlega całości przepisów dotyczących przetwarzania informacji FIDUCIA, które to przepisy zostały ustanowione w niniejszej decyzji i jej załącznikach.

Usunięcie oznaczenia FIDUCIA

13. Informacje FIDUCIA tracą swoje oznaczenie w dwóch przypadkach:

a) gdy strona główna, która przedstawiła informację FIDUCIA, wyraża zgodę na jej przekazanie przeciwnej stronie głównej, pierwotnie przekazana informacja, jak również wszystkie informacje wytworzone na podstawie tej informacji tracą oznaczenie FIDUCIA;

b) gdy informacja FIDUCIA zostaje zwrócona stronie głównej, która ją przedstawiła.

14. Usunięcie oznaczenia FIDUCIA jest dokonywane przez biuro FIDUCIA, które rejestruje to usunięcie w rejestrze informacji FIDUCIA.

15. Usunięcie oznaczenia FIDUCIA nie oznacza zniesienia klauzul tajności EUCI.

V. KOPIE INFORMACJI FIDUCIA

16. Informacje FIDUCIA nie są kopiowane, chyba że jest to niezbędne. W takim przypadku kopie są sporządzane przez biuro FIDUCIA, które je numeruje i rejestruje.

17. Kopie podlegają całości przepisów bezpieczeństwa ustanowionych w niniejszej decyzji i jej załącznikach.

VI. NISZCZENIE INFORMACJI FIDUCIA

18. Jeżeli informacje lub materiały przedstawione zgodnie z art. 105 § 1 lub § 2 regulaminu postępowania zostają zwrócone stronie głównej, która je przedstawiła, wszystkie informacje obejmujące w całości lub w części treść takich informacji lub materiałów, jak również ewentualnie sporządzone kopie zostają zniszczone.

19. Zniszczenia informacji FIDUCIA, o którym mowa w pkt 18, dokonuje biuro FIDUCIA, z użyciem metod zgodnych z przepisami mającymi zastosowanie w instytucjach Unii w dziedzinie ochrony EUCI, aby uniemożliwić ich całkowite lub częściowe odtworzenie.

20. Zniszczenia informacji FIDUCIA, o którym mowa w pkt 18, dokonuje się w obecności świadka, który został upoważniony do dostępu do informacji FIDUCIA.

21. Biuro FIDUCIA sporządza protokół zniszczenia.

22. Protokół zniszczenia załącza się do rejestru informacji FIDUCIA. Kopię tego protokołu przekazuje się stronie głównej, która przedstawiła dany dokument.

ZAŁĄCZNIK IV

OCHRONA INFORMACJI FIDUCIA PRZETWARZANYCH DROGĄ ELEKTRONICZNĄ

1. Niniejszy załącznik zawiera przepisy dotyczące wykonania art. 10.

2. Informacje FIDUCIA mogą być przetwarzane jedynie na urządzeniach elektronicznych (stanowiskach pracy, drukarkach, fotokopiarkach), które nie są podłączone do sieci informatycznej i które znajdują się w pomieszczeniach biura FIDUCIA.

3. Wszystkie urządzenia elektroniczne wykorzystywane do przetwarzania informacji FIDUCIA są zgodne z przepisami mającymi zastosowanie w instytucjach Unii w dziedzinie ochrony EUCI. Zapewnia się bezpieczeństwo tych urządzeń na wszystkich etapach ich życia.

4. Wszelkie możliwe połączenia z Internetem i z innymi narzędziami (LAN, WLAN, Bluetooth itd.) są stale wyłączone.

5. Stanowiska pracy są wyposażone w odpowiednią ochronę antywirusową. Aktualizacji oprogramowania antywirusowego dokonuje się za pomocą CD-ROM-u lub klucza USB używanych wyłącznie w tym celu.

6. Pamięć drukarek i fotokopiarek zostaje wyczyszczona przed każdą operacją konserwacji.

7. Do przetwarzania wniosków o przeprowadzenie postępowania sprawdzającego, o których mowa w załączniku I, używa się wyłącznie produktów kryptograficznych zatwierdzonych zgodnie z przepisami mającymi zastosowanie w instytucjach Unii w dziedzinie ochrony EUCI.

ZAŁĄCZNIK V

BEZPIECZEŃSTWO W PRZYPADKU INTERWENCJI ZEWNĘTRZNEJ

1. Niniejszy załącznik zawiera przepisy dotyczące wykonania art. 11.

2. Wykonawcy mogą mieć dostęp do informacji FIDUCIA wyłącznie w ramach konserwacji systemów teleinformatycznych odizolowanych od sieci informatycznej lub w trakcie interwencji wymagającej pilnego przemieszczenia informacji FIDUCIA w celu umieszczenia ich w bezpiecznym miejscu.

3. Organ bezpieczeństwa opracowuje wytyczne w zakresie interwencji zewnętrznej obejmujące w szczególności poświadczenie bezpieczeństwa wydawane pracownikom wykonawców, jak również treść umów, do których odnosi się niniejszy załącznik.

4. Dokumenty związane z postępowaniami przetargowymi i umowa o konserwację systemów teleinformatycznych odizolowanych od sieci informatycznej noszą oznaczenie FIDUCIA, jeżeli zawierają informacje, których nieuprawnione ujawnienie mogłoby zaszkodzić bezpieczeństwu Unii, jej państwa członkowskiego lub państw członkowskich lub też utrzymywaniu przez nie stosunków międzynarodowych. Dokument określający aspekty bezpieczeństwa stanowiący załącznik do tej umowy zawiera postanowienia zobowiązujące wykonawcę do przestrzegania minimalnych norm określonych w niniejszej decyzji. Nieprzestrzeganie tych minimalnych norm może stanowić wystarczający powód do rozwiązania umowy.

5. Umowa, która wiąże się z interwencjami wymagającymi pilnego przemieszczenia informacji FIDUCIA w celu umieszczenia ich w bezpiecznym miejscu, przewiduje liczbę pracowników ochrony, którzy są zobowiązani dysponować poświadczeniem bezpieczeństwa osobowego. Nie zawiera ona żadnych uściśleń w odniesieniu do procedur, które należy stosować. Umowa ta nie nosi oznaczenia FIDUCIA.

6. Wykonawca nie może zlecić podwykonawcy czynności określonych w zaproszeniu do składania ofert i w umowie wiążącej się z dostępem lub wymagającej dostępu do informacji FIDUCIA.