EUROPEJSKI
TRYBUNAŁ
OBRACHUNKOWY

Decyzja Trybunału Obrachunkowego nr 41-2021 w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE

EUROPEJSKI TRYBUNAŁ OBRACHUNKOWY,

UWZGLĘDNIAJĄC art. 13 Traktatu o Unii Europejskiej,

UWZGLĘDNIAJĄC art. 287 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE),

UWZGLĘDNIAJĄC art. 257 rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 z dnia 18 lipca 2018 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii,

UWZGLĘDNIAJĄC art. 1 ust. 6 decyzji Trybunału Obrachunkowego nr 21-2021 ustanawiającej przepisy wykonawcze do regulaminu Trybunału Obrachunkowego,

UWZGLĘDNIAJĄC przepisy bezpieczeństwa dotyczące ochrony informacji niejawnych UE obowiązujące w innych instytucjach, agencjach i organach UE,

UWZGLĘDNIAJĄC politykę Trybunału dotyczącą bezpieczeństwa informacji (dokument DEC 127/15 FINAL) oraz politykę klasyfikacji informacji (komunikat do personelu nr 123/2020),

MAJĄC NA UWADZE, że zgodnie z art. 287 ust. 3 TFUE Trybunał Obrachunkowy ma prawo uzyskać dostęp do wszelkich dokumentów i informacji niezbędnych w jego mniemaniu do wykonania powierzonych mu uprawnień, w tym do informacji niejawnych UE (EUCI), przy czym należy zapewnić pełne przestrzeganie zasady lojalnej współpracy między instytucjami i zasady przyznania kompetencji, a także mając na uwadze, że prawo dostępu do EUCI zagwarantowane postanowieniami TFUE nie może być kwestionowane przez wytwórcę takich informacji, choć Trybunał Obrachunkowy może zostać poproszony o wprowadzenie i przestrzeganie określonych środków bezpieczeństwa, które bardziej szczegółowo omówiono w niniejszym dokumencie;

MAJĄC NA UWADZE, że członkowie Trybunału Obrachunkowego, jak również zatrudnieni w nim urzędnicy i inni pracownicy są związani, również po zaprzestaniu pełnienia swoich funkcji, obowiązkiem zachowania poufności zgodnie z art. 339 TFUE, art. 17 regulaminu pracowniczego i aktami przyjętymi na mocy tych przepisów prawnych;

MAJĄC NA UWADZE, że ze względu na poufny charakter EUCI korzystanie z tych informacji wymaga, by przestrzeganie obowiązku zachowania poufności zagwarantowano przez odpowiednie środki bezpieczeństwa zapewniające wysoki poziom ochrony tych informacji, równoważne środkom wprowadzonym na mocy zasad dotyczących ochrony EUCI przyjętych przez inne instytucje, agencje i organy Unii, przy czym jeśli Trybunał uzna, że jakikolwiek z tych środków

bezpieczeństwa nie jest uzasadniony w kontekście charakteru i rodzaju danych EUCI, zastrzega sobie prawo do zgłoszenia uwag, które uzna za stosowne, przestrzegając jednocześnie klauzuli tajności przyznanej określonym EUCI;

MAJĄC NA UWADZE, że środki bezpieczeństwa mające zapewnić ochronę poufności, integralności i dostępności informacji przekazywanych Trybunałowi Obrachunkowego muszą być odpowiednie w świetle charakteru i rodzaju tych informacji;

MAJĄC NA UWADZE, że należy zapewnić Trybunałowi Obrachunkowemu dostęp do informacji niejawnych w oparciu o zasadę wiedzy koniecznej, tak aby umożliwić mu wykonywanie zadań powierzonych na mocy Traktatów i aktów prawnych przyjętych na podstawie Traktatów;

MAJĄC NA UWADZE, że zważywszy na charakter pewnych informacji i zawarte w nich wrażliwe treści należy ustanowić specjalną procedurę dotyczącą korzystania w Trybunale Obrachunkowym z dokumentów zawierających EUCI;

MAJĄC NA UWADZE, że instytucja musi zagwarantować, iż niniejsza decyzja zostanie wdrożona zgodnie z wszystkimi obowiązującymi przepisami, w szczególności przepisami dotyczącymi ochrony danych osobowych, bezpieczeństwa fizycznego osób, budynków i systemów informatycznych oraz publicznego dostępu do dokumentów;

PRZYJMUJE NASTĘPUJĄCĄ DECYZJĘ:

Artykuł 1 – Przedmiot i zakres

1) W niniejszej decyzji określa się podstawowe zasady i minimalne standardy bezpieczeństwa dotyczące ochrony informacji niejawnych przetwarzanych przez Trybunał Obrachunkowy przy wykonywaniu powierzonych mu uprawnień.

2) Do celów decyzji informacje niejawne oznaczają dowolny lub wszystkie z wymienionych niżej rodzajów informacji:

   a) informacje niejawne Unii Europejskiej (EUCI) zgodnie z definicjami zawartymi w zasadach bezpieczeństwa innych instytucji, agencji, organów lub jednostek organizacyjnych UE, które zostały opatrzone jedną z następujących klauzul tajności:

      - TRÈS SECRET UE/EU TOP SECRET: informacje i materiały, których nieuprawnione ujawnienie mogłoby wyrządzić wyjątkowo poważną szkodę podstawowym interesom Unii Europejskiej lub co najmniej jednego państwa członkowskiego;
      - SECRET UE/EU SECRET: informacje i materiały, których nieuprawnione ujawnienie mogłoby poważnie zaszkodzić podstawowym interesom Unii Europejskiej lub co najmniej jednego państwa członkowskiego;
      - CONFIDENTIEL UE/EU CONFIDENTIAL: informacje i materiały, których nieuprawnione ujawnienie mogłoby zaszkodzić podstawowym interesom Unii Europejskiej lub co najmniej jednego państwa członkowskiego;
      - RESTREINT UE/EU RESTRICTED: informacje i materiały, których nieuprawnione ujawnienie mogłoby być niekorzystne dla interesów Unii Europejskiej lub co najmniej jednego państwa członkowskiego;

b) informacje niejawne przekazane przez państwa członkowskie i opatrzone krajową klauzulą tajności równoważną jednej z klauzul tajności stosowanych w przypadku EUCI[1], wymienionych w lit. a);

c) informacje niejawne przekazane Europejskiemu Trybunałowi Obrachunkowemu przez państwa trzecie lub organizacje międzynarodowe, opatrzone klauzulą tajności równoważną jednej z klauzul tajności stosowanych w przypadku EUCI, wymienionych w lit. a), zgodnie z odpowiednimi porozumieniami w sprawie bezpieczeństwa informacji lub porozumieniami administracyjnymi.

3) Trybunał Obrachunkowy przetwarza informacje opatrzone klauzulą tajności RESTREINT UE/EU RESTRICTED w swojej siedzibie i w tym celu stosuje wszelkie niezbędne środki ochrony. Na potrzeby pracowników Trybunału Obrachunkowego, którzy muszą uzyskać dostęp do EUCI opatrzonych wyższą klauzulą tajności, wypracowane zostaną odpowiednie rozwiązania, tak aby mogli oni zapoznać się z tymi informacjami w odpowiednich obiektach innych instytucji, organów lub agencji UE.

4) Niniejszą decyzję stosuje się do wszystkich działów i obiektów składających się na siedzibę Trybunału Obrachunkowego.

5) Z wyjątkiem przypadków, gdy dany przepis dotyczy konkretnych grup pracowników, niniejsza decyzja ma zastosowanie do członków Trybunału Obrachunkowego, pracowników Trybunału Obrachunkowego objętych regulaminem pracowniczym i warunkami zatrudnienia innych pracowników Unii Europejskiej[2], ekspertów krajowych oddelegowanych do Trybunału Obrachunkowego, dostawców usług i ich pracowników, stażystów oraz do wszystkich innych osób mających dostęp do budynków i innych aktywów Trybunału Obrachunkowego lub do informacji przetwarzanych przez Trybunał Obrachunkowy.

6) O ile nie wskazano inaczej, przepisy dotyczące EUCI stosują się w jednakowy sposób do informacji niejawnych, o których mowa w ust. 2 lit. b) i c) niniejszego artykułu.

Artykuł 2 – Definicje

Do celów niniejszej decyzji:

a) „upoważnienie do dostępu do EUCI" oznacza decyzję Dyrektora Dyrekcji ds. Kadr, Finansów i Usług Ogólnych Trybunału Obrachunkowego podjętą na podstawie zapewnienia udzielonego przez właściwy organ państwa członkowskiego, że dany urzędnik Trybunału Obrachunkowego, inny pracownik lub oddelegowany ekspert krajowy – o ile ustalono jego potrzeby dostępu w ramach zasady wiedzy koniecznej i został on odpowiednio poinformowany o ciążących na nim obowiązkach – może uzyskać dostęp do EUCI do określonego poziomu klauzuli tajności (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższego) i aż do określonej daty. O osobie takiej mówi się, że jest „upoważniona w zakresie bezpieczeństwa";

b) „opatrzenie klauzulą tajności" oznacza przypisanie informacjom określonego poziomu klauzuli tajności w zależności od rozmiaru szkód, jakie mogłoby spowodować nieuprawnione ujawnienie tych informacji;

---

[1] Zob. umowa z 4 maja 2011 r. między państwami członkowskimi Unii Europejskiej, zebranymi w Radzie, w sprawie ochrony informacji niejawnych wymienianych w interesie Unii Europejskiej i załącznik do tej umowy (Dz.U. 2011/C 202/13).

[2] Rozporządzenie Rady nr 31 (EWG) ustanawiające regulamin pracowniczy urzędników i warunki zatrudnienia innych pracowników, z późniejszymi zmianami, Dz.U. 01962R0031-1.1.2020-019.003-1 (https://eur-lex.europa.eu/eli/reg/1962/31 (1)/2020-01-01).

c) „materiał kryptograficzny” oznacza algorytmy kryptograficzne, sprzęt i oprogramowanie kryptograficzne, a także produkty zawierające szczegóły stosowania i związaną z nim dokumentację, a także klucze;

d) „zniesienie klauzuli tajności” oznacza zniesienie wszelkiej klauzuli tajności;

e) „dokument” oznacza każdą zapisaną informację, niezależnie od jej postaci fizycznej lub cech;

f) „obniżenie klauzuli tajności” oznacza obniżenie poziomu klauzuli tajności;

g) „świadectwo bezpieczeństwa przemysłowego” oznacza wydane w trybie administracyjnym oświadczenie właściwego organu do spraw bezpieczeństwa, że z punktu widzenia bezpieczeństwa dany obiekt jest w stanie zapewnić odpowiedni poziom ochrony EUCI na określonym poziomie klauzuli tajności;

h) „korzystanie” z EUCI oznacza wszelkie możliwe działania, jakim mogą być poddawane EUCI w całym cyklu życia, i obejmuje tworzenie, rejestrowanie, przetwarzanie, przenoszenie, obniżenie odnośnej klauzuli tajności, zniesienie klauzuli tajności i zniszczenie informacji. W odniesieniu do systemów teleinformatycznych pojęcie to obejmuje również gromadzenie, wyświetlanie, przesyłanie i przechowywanie EUCI;

i) „posiadacz” oznacza odpowiednio uprawnioną osobę, której potrzeby w ramach zasady wiedzy koniecznej zostały ustalone i w której posiadaniu znajdują się informacje niejawne, w związku z czym odpowiada ona za ochronę tych informacji;

j) „organ do spraw bezpieczeństwa informacji” oznacza urzędnika Trybunału Obrachunkowego do spraw bezpieczeństwa informacji, który może delegować w całości lub części, realizację zadań określonych w niniejszej decyzji;

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

l) „materiały” oznaczają dowolny nośnik informacji, nośnik danych lub urządzenie bądź sprzęt;

m) „wytwórca” oznacza instytucję, organ lub agencję UE, państwo członkowskie, państwo trzecie lub organizację międzynarodową, w ramach właściwości której wytworzono informacje lub wprowadzono je do struktur UE;

n) „poświadczenie bezpieczeństwa osobowego” (PBO) oznacza zaświadczenie właściwego organu państwa członkowskiego wydawane po zakończeniu postępowania sprawdzającego prowadzonego przez właściwe organy państwa członkowskiego. Stanowi ono potwierdzenie, że dana osoba – o ile ustalono potrzeby dostępu tej osoby w ramach zasady wiedzy koniecznej i została ona odpowiednio poinstruowana o zakresie swoich obowiązków – może uzyskać dostęp do EUCI do określonego poziomu klauzuli tajności (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższego) aż do określonej daty;

o) „zaświadczenie potwierdzające posiadanie poświadczenia bezpieczeństwa osobowego” (ZPBO) oznacza zaświadczenie wydane przez Dyrektora Dyrekcji ds. Kadr, Finansów i Usług Ogólnych Trybunału Obrachunkowego, potwierdzające, że dana osoba posiada ważne poświadczenie bezpieczeństwa lub upoważnienie w zakresie bezpieczeństwa, oraz zawierające informację o poziomie klauzuli tajności EUCI, do których dana osoba może uzyskać dostęp (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższy), okresie ważności danego poświadczenia bezpieczeństwa lub upoważnienia w zakresie bezpieczeństwa oraz dacie ważności samego zaświadczenia;

p) „organ do spraw bezpieczeństwa fizycznego” oznacza szefa służb ochrony Trybunału Obrachunkowego, który jest odpowiedzialny za wdrożenie środków i procedur w zakresie bezpieczeństwa fizycznego niezbędnych do zapewnienia ochrony EUCI;

q) „kancelaria informacji zastrzeżonych” jest zarządzana przez Sekretariat Trybunału. Jest zlokalizowana w strefie administracyjnej i podlega Dyrektorowi Dyrekcji ds. Kadr, Finansów i Usług Ogólnych Trybunału Obrachunkowego. Kancelaria ta odpowiada za odbiór i przekazywanie informacji opatrzonych klauzulą tajności RESTREINT UE/EU RESTRICTED lub równoważną w ramach wymian informacji prowadzonych przez Trybunał;

r) „kancelaria informacji tajnych” oznacza strefę wydzieloną w obrębie strefy bezpieczeństwa. Kancelarią informacji tajnych zarządza urzędnik kontroli kancelarii informacji tajnych w Trybunale Obrachunkowym posiadający odpowiednie poświadczenie bezpieczeństwa i upoważnienie. Kancelaria odpowiada za odbiór i przekazywanie informacji opatrzonych klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą bądź informacji opatrzonych równoważnymi klauzulami w ramach wymian informacji prowadzonych przez Trybunał;

s) „organ do spraw akredytacji bezpieczeństwa” oznacza Dyrektora Dyrekcji ds. Kadr, Finansów i Usług Ogólnych Trybunału Obrachunkowego.

Artykuł 3 – Środki służące ochronie EUCI

1) Trybunał Obrachunkowy zapewnia ochronę wszystkich przekazanych mu informacji niejawnych współmierną do klauzuli tajności określonej przez wytwórcę tych informacji i zgodnie z niniejszą decyzją.

2) W tym celu Trybunał Obrachunkowy obejmuje korzystanie z EUCI odpowiednimi środkami w zakresie bezpieczeństwa fizycznego i – w stosownych przypadkach – osobowego, w tym upoważnieniami do dostępu przyznawanymi osobom wskazanym z imienia i nazwiska oraz środkami służącymi ochronie systemów teleinformatycznych. Środki te opisano w art. 4–6 niniejszej decyzji. Mają one zastosowanie na wszystkich etapach cyklu życia EUCI. Środki te są współmierne do klauzuli tajności przyznanej danym EUCI, formy i ilości informacji lub materiałów, lokalizacji i konstrukcji obiektów, w których EUCI są przechowywane, oraz wyników oceny ryzyka dotyczącej tego, czy w danym miejscu mogą być podejmowane działania w złych zamiarach lub działalność przestępcza, w tym działalność szpiegowska, sabotażowa lub terrorystyczna.

3) EUCI są chronione za pomocą środków w zakresie bezpieczeństwa fizycznego, natomiast informacje opatrzone klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą są chronione dodatkowo za pomocą środków w zakresie bezpieczeństwa osobowego.

4) EUCI mogą być udostępniane w obrębie instytucji wyłącznie osobom, którym są one potrzebne zgodnie z zasadą wiedzy koniecznej. Posiadacz jakiegokolwiek elementu EUCI jest zobowiązany zapewnić jego stosowną ochronę zgodnie z niniejszą decyzją.

5) EUCI nie można ujawniać ustnie ani na piśmie. Opracowane przez Trybunał uwagi wstępne, sprawozdania, opinie, komunikaty prasowe oraz inne publikacje, strona internetowa i intranetowa Trybunału, wypowiedzi ustne przedstawicieli Trybunału i odpowiedzi na wnioski o dostęp do dokumentów[3], a także nagrania głosowe i wideo nie mogą zawierać EUCI bądź fragmentów EUCI ani zawierać odniesień do tychże. Niemniej jeśli wytwórca opublikował dokumenty lub informacje zawierające odniesienie do danych EUCI, można wspomnieć o tym odniesieniu.

6) Bez uszczerbku dla przepisów ust. 5 Trybunał Obrachunkowy i wytwórca informacji mogą uzgodnić, że w odniesieniu do konkretnej kontroli Trybunał Obrachunkowy może przedstawić

[3] Zgodnie z decyzją nr 12/2005 Trybunału Obrachunkowego w sprawie publicznego dostępu do dokumentów Trybunału Obrachunkowego, zmienioną decyzją nr 14/2009 (Dz.U. 2009/C 67/1).

lub wykorzystać elementy EUCI w dokumencie. W takim przypadku dokument sporządzony przez Trybunał Obrachunkowy jest w pierwszej kolejności przesyłany do wytwórcy danych EUCI przed rozpoczęciem lub w trakcie postępowania kontradyktoryjnego. Następnie Trybunał Obrachunkowy i wytwórca informacji uzgadniają, czy dokument opracowany przez Trybunał powinien zostać opatrzony klauzulą tajności. Jeśli członek sprawozdawca Trybunału Obrachunkowego uzna za konieczne, by przesłać całość lub część sprawozdania z kontroli, które zostało opatrzone klauzulą tajności, określonym odbiorcom w Parlamencie Europejskim i Radzie – po uwzględnieniu wszystkich środków bezpieczeństwa wynikających z niniejszej decyzji – takie przesłanie sprawozdania wymaga zgody ze strony wytwórcy danych informacji niejawnych. Odnośne ramy prawne i procedurę wymiany takich dokumentów określono w art. 7.

7) W przypadku gdy wykonanie zadań powierzonych Trybunałowi Obrachunkowemu wymaga, by pewne elementy dokumentów lub informacji niejawnych zostały udostępnione szerszemu gronu odbiorców, Trybunał – po należytym uwzględnieniu przyznanej klauzuli tajności – zasięga opinii wytwórcy tych informacji, a następnie podejmuje decyzję o ewentualnym wykorzystaniu tych elementów lub informacji, jeśli uzna, że takie postępowanie jest zgodne z nadrzędnym interesem publicznym. Informacje można wykorzystać w sprawozdaniu wyłącznie w taki sposób, który nie może zaszkodzić interesom wytwórcy informacji. Przed taką szkodą można się odpowiednio zabezpieczyć, zwracając się do wytwórcy informacji o przedstawienie uwag w celu osiągnięcia porozumienia co do sposobu anonimizacji, streszczenia, uogólnienia itd. przedmiotowych informacji przy jednoczesnym poszanowaniu interesów tych podmiotów, których te publikowane informacje w pierwszym rzędzie dotyczą.

8) Trybunał Obrachunkowy nie udostępnia EUCI innej instytucji, agencji, organowi lub jednostce organizacyjnej UE, państwu członkowskiemu, państwu trzeciemu lub organizacji międzynarodowej, nie zasięgnąwszy uprzednio opinii wytwórcy tych informacji i nie otrzymawszy wyraźnej pisemnej zgody.

9) O ile wytwórca dokumentu opatrzonego klauzulą tajności SECRET UE / EU SECRET lub niższą nie nałożył ograniczeń w zakresie powielania lub tłumaczenia, dokumenty takie mogą być powielane lub tłumaczone na wniosek posiadacza i zgodnie z praktycznymi instrukcjami dotyczącymi sposobu pracy przyjętymi przez organ do spraw bezpieczeństwa informacji w Trybunale Obrachunkowym. Środki bezpieczeństwa, które mają zastosowanie do oryginalnego dokumentu, mają również zastosowanie do jego kopii i tłumaczeń.

10) Jeśli Trybunał Obrachunkowy otrzymał dokument niejawny lub prawo dostępu do takiego dokumentu, ale potrzebuje wersji tego dokumentu z obniżoną lub zniesioną klauzulą tajności, zwraca się do wytwórcy dokumentu z pytaniem, czy może on udostępnić taką wersję.

Artykuł 4 – Bezpieczeństwo osobowe

1) Z uwagi na pełnione funkcje członkowie Trybunału Obrachunkowego są uprawnieni do dostępu do wszystkich EUCI i do uczestniczenia w spotkaniach, na których korzysta się z EUCI. Członkowie muszą zostać poinformowani o ciążących na nich obowiązkach w zakresie bezpieczeństwa dotyczących ochrony EUCI i potwierdzić na piśmie, że zapoznali się ze swoimi obowiązkami w zakresie ochrony takich informacji.

2) Personelowi Trybunału Obrachunkowego – zarówno urzędnikom, jak i pracownikom objętym warunkami zatrudnienia innych pracowników oraz oddelegowanym ekspertom krajowym – przyznaje się dostęp do EUCI wyłącznie po tym, jak:

   i. określono potrzeby danej osoby w ramach zasady wiedzy koniecznej;

ii. została ona poinformowana o przepisach bezpieczeństwa służących ochronie EUCI oraz odnośnych standardach i wytycznych dotyczących bezpieczeństwa i potwierdziła na piśmie, że zapoznała się z ciążącymi na niej obowiązkami w zakresie ochrony takich informacji;

iii. w przypadku informacji niejawnych z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą – otrzymała ona poświadczenie bezpieczeństwa i przyznano jej upoważnienie do dostępu.

3) Procedura pozwalająca ustalić, czy urzędnik lub inny pracownik Trybunału Obrachunkowego może otrzymać upoważnienie do dostępu do informacji opatrzonych klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą, zostanie określona w decyzji delegowanej przyjętej zgodnie z art. 10 ust. 10. W procedurze tej uwzględnia się lojalność, uczciwość i wiarygodność danej osoby, a przeprowadza się ją po otrzymaniu odnośnego zapewnienia ze strony właściwych organów państwa członkowskiego, jak wskazano w art. 2 lit. n). Decyzje dotyczące udzielenia upoważnienia do dostępu podejmuje Dyrektor Dyrekcji ds. Kadr, Finansów i Usług Ogólnych Trybunału Obrachunkowego.

4) Dyrektor Dyrekcji ds. Kadr, Finansów i Usług Ogólnych Trybunału Obrachunkowego może wydać ZPBO, określające poziom klauzuli tajności EUCI, do których danej osobie można umożliwić dostęp (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższy), okres ważności odpowiedniego upoważnienia do dostępu oraz datę ważności samego zaświadczenia.

5) W spotkaniach, na których korzysta się z informacji opatrzonych klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą, mogą uczestniczyć jedynie osoby posiadające upoważnienie do dostępu, o którym mowa w ust. 2 pkt (iii) powyżej, oraz członkowie Trybunału Obrachunkowego zgodnie z ust. 1 powyżej. Trybunał Obrachunkowy i wytwórca informacji dokonują wspólnie praktycznych ustaleń dotyczących takich spotkań, indywidualnie dla każdego przypadku.

6) Działy Trybunału Obrachunkowego odpowiedzialne za organizowanie spotkań, na których mają być wykorzystywane informacje opatrzone klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą, informują organ do spraw bezpieczeństwa informacji z odpowiednim wyprzedzeniem o dacie i godzinie oraz miejscu spotkania, a także przekazują listę uczestników.

7) Każda osoba, która znajduje się w posiadaniu EUCI, lecz nie posiada należytego upoważnienia lub potwierdzonej potrzeby w ramach zasady wiedzy koniecznej, musi możliwie jak najszybciej poinformować o zaistniałej sytuacji organ do spraw bezpieczeństwa informacji i zapewnić ochronę EUCI zgodnie z wymogami niniejszej decyzji.

Artykuł 5 – Środki bezpieczeństwa fizycznego mające na celu ochronę informacji niejawnych

1) „Bezpieczeństwo fizyczne” oznacza stosowanie fizycznych i technicznych środków ochrony, aby zapobiec nieuprawnionemu dostępowi do EUCI.

2) Środki bezpieczeństwa fizycznego mają zapobiegać wtargnięciu osoby nieupoważnionej w sposób niezauważony lub z użyciem siły, powstrzymać od podjęcia nieuprawnionych działań, udaremnić je i wykryć oraz umożliwić podział pracowników pod względem potrzeb dostępu do EUCI zgodnie z zasadą wiedzy koniecznej. Środki te określa się na podstawie procedury zarządzania ryzykiem, zgodnie z niniejszą decyzją.

3) Pomieszczenia, gdzie przetwarzane są lub przechowywane EUCI, poddawane są regularnym inspekcjom przez właściwy organ Trybunału Obrachunkowego do spraw bezpieczeństwa.

4) Do przetwarzania EUCI i przechowywania takich informacji stosuje się wyłącznie sprzęt lub urządzenia spełniające odnośne wymogi dotyczące ochrony EUCI obowiązujące w instytucjach, agencjach lub organach UE.

5) Pracownicy Trybunału mogą uzyskać dostęp do EUCI opatrzonych klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą bądź opatrzonych równoważnymi klauzulami tajności w strefach bezpieczeństwa znajdujących się poza siedzibą Trybunału.

6) Trybunał Obrachunkowym może zawrzeć umowę o gwarantowanym poziomie usług z inną instytucją UE z siedzibą w Luksemburgu, aby móc korzystać z informacji opatrzonych klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą i takie informacje przechowywać w strefie bezpieczeństwa tej instytucji. Z takich EUCI nie można korzystać na terenie siedziby Trybunału, nie mogą one też być w siedzibie Trybunału przechowywane ani przez Trybunał powielane lub tłumaczone, chyba że wytwórca informacji udzieli wyraźnej zgody.

7) Trybunał Obrachunkowy rejestruje otrzymane informacje opatrzone klauzulą tajności RESTREINT UE/EU RESTRICTED. Ze względów bezpieczeństwa rejestruje się również przypadki dostępu poza siedzibą Trybunału do informacji opatrzonych klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą bądź równoważną klauzulą tajności.

8) EUCI opatrzone klauzulą tajności RESTREINT UE/EU RESTRICTED mogą być przechowywane w odpowiednim do tego celu zamkniętym meblu biurowym w strefie administracyjnej lub strefie bezpieczeństwa. EUCI opatrzone klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET przechowywane są zgodnie z zapisami umowy o gwarantowanym poziomie usług w zabezpieczonej szafie w strefie bezpieczeństwa innej instytucji UE z siedzibą w Luksemburgu.

9) Poza kancelarią EUCI przekazywane są między poszczególnymi działami i siedzibami w następujący sposób:

   a) co do zasady EUCI są przekazywane drogą elektroniczną chronioną przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z art. 6 ust. 8;

   b) jeśli nie stosuje się metody opisanej w lit. a), EUCI są przekazywane za pomocą nośników danych (np. pamięć USB, płyty kompaktowe, twarde dyski) chronionych przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z art. 6 ust. 8 bądź w formie papierowej w zapieczętowanej nieprzejrzystej kopercie.

10) Informacje opatrzone klauzulą tajności RESTREINT UE/EU RESTRICTED mogą zostać zniszczone przez posiadacza, przy poszanowaniu zasad dotyczących archiwizacji obowiązujących w Trybunale Obrachunkowym. Informacje opatrzone klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą są niszczone wyłącznie przez urzędnika kontroli kancelarii informacji tajnych na polecenie posiadacza informacji lub właściwego organu zgodnie z zasadami dotyczącymi archiwizacji obowiązującymi w Trybunale Obrachunkowym. Dokumenty opatrzone klauzulą tajności SECRET UE/EU SECRET są niszczone w obecności świadka posiadającego poświadczenie bezpieczeństwa na poziomie odpowiadającym co najmniej poziomowi klauzuli tajności dokumentu, który ma zostać zniszczony. Urzędnik kontroli kancelarii informacji tajnych oraz świadek, w przypadkach gdy jego obecność jest wymagana, podpisują protokół zniszczenia, który zostaje włączony do dokumentacji kancelarii informacji tajnych. Urzędnik kontroli kancelarii informacji tajnych przechowuje rejestr zniszczonych dokumentów z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET przez co najmniej pięć lat.

11) Organ do spraw bezpieczeństwa fizycznego i organ do spraw bezpieczeństwa informacji sporządzają wspólnie dostosowany do lokalnych uwarunkowań plan ochrony EUCI w sytuacji kryzysowej, obejmujący w razie potrzeby plany zniszczenia tych informacji lub ewakuacji na

wypadek wystąpienia nadzwyczajnych okoliczności. Organy te wydają odnośne instrukcje, które uznają za odpowiednie, aby zapobiec dostaniu się EUCI w niepowołane ręce.

12) W przypadku gdy EUCI muszą zostać fizycznie przeniesione, Trybunał Obrachunkowy przestrzega środków narzuconych przez wytwórcę informacji w celu zapewnienia ochrony EUCI przed nieuprawnionym dostępem podczas transportu.

13) W załączniku do niniejszej decyzji określono środki bezpieczeństwa fizycznego mające zastosowanie w strefach administracyjnych, w których korzysta się z informacji opatrzonych klauzulą tajności RESTREINT UE/EU RESTRICTED i gdzie takie informacje się przechowuje.

Artykuł 6 – Ochrona EUCI w systemach teleinformatycznych

1) Do celów niniejszego artykułu „system teleinformatyczny” oznacza dowolny system umożliwiający korzystanie z EUCI w formie elektronicznej. System teleinformatyczny obejmuje wszystkie zasoby niezbędne do jego funkcjonowania, w tym infrastrukturę, organizację, pracowników oraz zasoby informatyczne.

2) „Uprawniony użytkownik” z kolei oznacza członka Trybunału Obrachunkowego, urzędnika, innego pracownika lub oddelegowanego eksperta krajowego, w przypadku których ustalono i potwierdzono potrzebę uzyskania dostępu do określonego systemu informatycznego.

3) Trybunał Obrachunkowy gwarantuje, że stosowane przez niego systemy zapewnią we właściwym zakresie ochronę informacji, które są przez te systemy przetwarzane, i będą działać tak jak powinny i kiedy powinny, pod kontrolą uprawnionych użytkowników. W tym celu wspomniane systemy gwarantują odpowiednie poziomy:

- autentyczności – gwarancja, że informacje są prawdziwe i pochodzą z rzetelnych źródeł;
- dostępności – cecha polegająca na tym, że informacje są dostępne i gotowe do wykorzystania na wniosek uprawnionego podmiotu;
- poufności – cecha polegająca na tym, że informacje nie są ujawniane nieupoważnionym osobom lub podmiotom ani do celów nieuprawnionego przetwarzania;
- integralności – cecha polegająca na zachowywaniu poprawności i kompletności zasobów i informacji;
- niezaprzeczalności – możliwość udowodnienia, że działanie lub wydarzenie miało miejsce, aby następnie nie można było zaprzeczyć wystąpieniu tego działania lub wydarzenia.

Gwarancja ta opiera się na procesie zarządzania ryzykiem. „Ryzyko” oznacza w tym kontekście prawdopodobieństwo, że dane zagrożenie wykorzysta podatność danej organizacji lub jakiegokolwiek systemu przez nią używanego na zagrożenia wewnętrzne lub zewnętrzne i przez to wyrządzi szkodę tej organizacji i jej zasobom materialnym lub niematerialnym. Ryzyko mierzone jest jako połączenie prawdopodobieństwa wystąpienia zagrożeń oraz ich skutków. Na proces zarządzania ryzykiem składają się następujące etapy: identyfikacja zagrożeń i podatności, ocena ryzyka, zmniejszanie ryzyka, akceptacja ryzyka i informowanie o ryzyku.

- „Ocena ryzyka” polega na określeniu zagrożeń i podatności oraz przeprowadzeniu odpowiedniej analizy ryzyka, tj. oceny prawdopodobieństwa wystąpienia zagrożeń i ich skutków.
- „Zmniejszanie ryzyka” polega na łagodzeniu, usuwaniu lub redukowaniu ryzyka (przy pomocy odpowiedniego połączenia środków technicznych, fizycznych, organizacyjnych lub proceduralnych), jego przenoszeniu lub monitorowaniu.
- „Akceptacja ryzyka” jest decyzją o zaakceptowaniu dalszego występowania określonego ryzyka rezydualnego po zmniejszeniu ryzyka.

- „Ryzyko rezydualne” oznacza ryzyko, które pozostaje po wdrożeniu środków bezpieczeństwa z uwagi na to, że nie można przeciwdziałać wszystkim zagrożeniom i że nie każdą podatność można wyeliminować.
- „Informowanie o ryzyku” polega na upowszechnianiu wiedzy o ryzyku wśród społeczności użytkowników systemu teleinformatycznego, na informowaniu organów zatwierdzających o takim ryzyku i na składaniu sprawozdań z takiego ryzyka organom operacyjnym.

4) Wszystkie urządzenia i sprzęt elektroniczny stosowane do przetwarzania EUCI muszą być zgodne z zasadami mającymi zastosowanie do ochrony EUCI. Pierwszeństwo w tym względzie przyznaje się sprzętowi i urządzeniom elektronicznym, które już uzyskały akredytację innej instytucji, agencji lub organu UE. Urządzenia muszą być objęte gwarancjami bezpieczeństwa przez cały cykl życia.

5) System teleinformatyczny stosowany przez Trybunał Obrachunkowy do celów korzystania z EUCI musi być akredytowany przez odpowiedni organ. W tym celu Trybunał Obrachunkowy zawrze umowę o gwarantowanym poziomie usług z organem do spraw akredytacji bezpieczeństwa instytucji UE, który ma zdolność do akredytowania systemów teleinformatycznych przetwarzających EUCI, aby uzyskać świadectwo akredytacji potwierdzające, że informacje opatrzone klauzulą tajności RESTREINT UE/EU RESTRICTED mogą być przetwarzane w systemach teleinformatycznych Trybunału Obrachunkowego, i określające odpowiednie warunki działania tego systemu. W umowie zostaną również wskazane standardy mające zastosowanie w toku procesu akredytacji. Umowa zostanie zawarta zgodnie z procedurą określoną w art. 10 ust. 3.

6) Jeśli pojawi się potrzeba ustanowienia przez Trybunał Obrachunkowy własnego procesu akredytacji systemów teleinformatycznych Trybunału, proces ten zostanie określony na mocy decyzji delegowanej, o której mowa w art. 10 ust. 10 niniejszej decyzji, zgodnie ze standardami dotyczącymi procesu akredytacji systemów teleinformatycznych przetwarzających EUCI obowiązującymi w innych instytucjach, agencjach i organach UE.

7) Pełna odpowiedzialność za przygotowanie dokumentacji akredytacyjnej zgodnie z obowiązującymi standardami spoczywa na właścicielu systemu teleinformatycznego.

8) W przypadku gdy EUCI są chronione za pomocą produktów kryptograficznych, Trybunał Obrachunkowy przyznaje pierwszeństwo produktom zatwierdzonym przez Radę lub Sekretarza Generalnego Rady działającego w charakterze organu do spraw zatwierdzania produktów kryptograficznych lub – w pozostałych przypadkach – produktom zatwierdzonym przez inne instytucje, agencje i organy UE na potrzeby ochrony EUCI.

9) Z informacji opatrzonych klauzulą tajności RESTREINT UE/EU RESTRICTED korzysta się na urządzeniach elektronicznych (takich jak stacje robocze, drukarki, fotokopiarki) wyłącznie, jeśli znajdują się one w strefie administracyjnej lub w strefie bezpieczeństwa. Urządzenia elektroniczne przetwarzające informacje opatrzone klauzulą tajności RESTREINT UE/EU RESTRICTED muszą być oddzielone od innych sieci komputerowych i chronione za pomocą odpowiednich środków fizycznych lub technicznych.

10) Wszyscy pracownicy Trybunału Obrachunkowego zaangażowani w projektowanie, budowę, testowanie, funkcjonowanie i stosowanie systemów teleinformatycznych, w których przetwarzane są EUCI, lub zarządzanie takimi systemami zgłaszają urzędnikowi do spraw bezpieczeństwa informacji wszelkie ewentualne uchybienia w zakresie bezpieczeństwa, incydenty, naruszenia lub przypadki narażenia na szwank bezpieczeństwa, które mogą mieć wpływ na ochronę tych systemów lub znajdujących się w nich EUCI.

Artykuł 7 – Procedura wymiany informacji niejawnych i umożliwiania dostępu do nich

1) W przypadku gdy instytucje, agencje, organy i jednostki organizacyjne UE lub organy krajowe są prawnie zobowiązane na mocy Traktatów lub aktów przyjętych na podstawie Traktatów do zapewnienia Trybunałowi Obrachunkowemu dostępu do EUCI, zapewniają one taki dostęp z własnej inicjatywy lub na pisemny wniosek Prezesa Trybunału, członka sprawozdawcy lub Sekretarza Generalnego zgodnie z procedurą opisaną poniżej.

2) Wszystkie wnioski o dostęp do takich informacji są przesyłane do określonej instytucji za pośrednictwem kancelarii informacji zastrzeżonych Trybunału Obrachunkowego.

3) W razie potrzeby Trybunał Obrachunkowy zawiera porozumienie administracyjne regulujące praktyczne kwestie związane z wymianą EUCI lub informacji o równoważnym statusie.

4) W celu zawarcia takich porozumień administracyjnych Trybunał Obrachunkowy udostępnia wytwórcy wszystkie niezbędne informacje dotyczące stosowanego w Trybunale systemu w zakresie bezpieczeństwa informacji. W razie potrzeby istnieje możliwość zorganizowania wizytacji.

5) Wspomniane porozumienia administracyjne są zawierane przy zachowaniu pełnej zgodności z zasadą przyznania kompetencji i zasadą lojalnej współpracy określonymi w art. 13 Traktatu o Unii Europejskiej. Zawiera się je zgodnie z procedurą określoną w art. 10 ust. 4.

6) W przypadku gdy z daną instytucją, organem lub agencją UE, państwem trzecim lub organizacją międzynarodową nie zawarto żadnego porozumienia administracyjnego na temat przekazywania informacji niejawnych Trybunałowi Obrachunkowemu, Trybunał podpisuje oświadczenie, w którym zobowiązuje się do ochrony otrzymanych informacji niejawnych.

Artykuł 8 – Naruszenie bezpieczeństwa, utrata lub narażenie na szwank bezpieczeństwa informacji niejawnych

1) Naruszenie zasad bezpieczeństwa oznacza działanie określonej osoby lub zaniechanie przez nią działania, które jest sprzeczne z zasadami bezpieczeństwa określonymi w niniejszej decyzji i powiązanych przepisach wykonawczych.

2) Narażenie na szwank bezpieczeństwa ma miejsce, gdy w wyniku naruszenia zasad bezpieczeństwa EUCI w całości lub w części zostały ujawnione osobom nieupoważnionym.

3) O każdym podejrzeniu lub przypadku naruszenia zasad bezpieczeństwa powiadamia się niezwłocznie organ Trybunału Obrachunkowego do spraw bezpieczeństwa informacji.

4) W przypadkach, gdy wiadomo lub istnieją racjonalne podstawy do podejrzeń, że bezpieczeństwo EUCI zostało narażone na szwank lub że informacje takie zostały utracone, organ do spraw bezpieczeństwa informacji powiadamia Dyrektora Dyrekcji ds. Kadr, Finansów i Usług Ogólnych Trybunału Obrachunkowego. Dyrektor ten z kolei niezwłocznie powiadamia organ do spraw bezpieczeństwa wytwórcy informacji. Przeprowadza również stosowne dochodzenie, a następnie informuje Sekretarza Generalnego Trybunału Obrachunkowego i organ do spraw bezpieczeństwa wytwórcy informacji o wynikach dochodzenia i środkach wdrożonych, aby zapobiec powtórzeniu się takiej sytuacji w przyszłości. W przypadkach, gdy dana sprawa dotyczy członka Trybunału Obrachunkowego, odpowiedzialność za podjęcie działań spoczywa na Prezesie Trybunału Obrachunkowego, który działa we współpracy z Sekretarzem Generalnym Trybunału.

5) Każdy urzędnik lub inny pracownik Trybunału Obrachunkowego odpowiedzialny za naruszenie przepisów bezpieczeństwa określonych w niniejszej decyzji i powiązanych przepisach wykonawczych podlega karom zgodnie z regulaminem pracowniczym i warunkami zatrudnienia innych pracowników Unii Europejskiej.

6) Każdy członek Trybunału Obrachunkowego, który nie przestrzega zapisów niniejszej decyzji, podlega środkom i karom przewidzianym w art. 286 ust. 6 Traktatu.

7) Każda osoba odpowiedzialna za utratę EUCI lub za narażenie na szwank bezpieczeństwa takich informacji może podlegać postępowaniu dyscyplinarnemu lub sądowemu zgodnie z mającymi zastosowanie przepisami ustawowymi, zasadami i przepisami wykonawczymi.

Artykuł 9 – Bezpieczeństwo w przypadku interwencji zewnętrznej

1) Trybunał Obrachunkowy może powierzyć na mocy stosownej umowy wykonanie zadań, które obejmują dostęp do EUCI lub takiego dostępu wymagają, wykonawcom zarejestrowanym w państwach członkowskich. Do takiej sytuacji może dość w szczególności w związku z utrzymaniem systemów teleinformatycznych i sieci komputerowej.

2) W przypadku interwencji zewnętrznej Trybunał Obrachunkowy podejmuje wszystkie konieczne środki bezpieczeństwa, o których mowa w ust. 3 niniejszego artykułu, w tym zwraca się o świadectwo bezpieczeństwa przemysłowego w celu zagwarantowania ochrony EUCI przez kandydatów i oferentów w trakcie procedury przetargowej i postępowania o udzielenie zamówienia, a następnie przez wykonawców i podwykonawców przez cały okres realizacji zamówienia. Instytucja zamawiająca dopilnowuje, by minimalne standardy bezpieczeństwa przewidziane w niniejszej decyzji zostały wspomniane w umowach, tak aby zobowiązać wykonawców do ich przestrzegania.

3) Zasady bezpieczeństwa, zasady postępowań o udzielenie zamówienia oraz szablony i modele umów i umów podwykonawstwa stosowane w przypadkach obejmujących dostęp do EUCI, odnośne ogłoszenia o zamówieniu, wytyczne co do okoliczności, w których wymagane jest poświadczenie bezpieczeństwa przemysłowego lub osobowego, instrukcje bezpieczeństwa programu lub projektu, dokumenty określające aspekty bezpieczeństwa, wizyty, a także przesyłanie i transport EUCI w ramach takich umów i umów podwykonawstwa muszą być zgodne z zasadami, wzorami i modelami określonymi przez Komisję Europejską w odniesieniu do umów niejawnych w decyzji Komisji (UE, Euratom) 2015/444 z dnia 13 marca 2015 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE.

Artykuł 10 – Wdrożenie niniejszej decyzji i związane z tym obowiązki

1) Poszczególne działy Trybunału Obrachunkowego podejmują wszelkie niezbędne działania leżące w zakresie ich odpowiedzialności, aby zapewnić stosowanie niniejszej decyzji i odpowiednich przepisów wykonawczych przy korzystaniu z EUCI lub jakichkolwiek innych informacji niejawnych bądź ich przechowywaniu.

2) Organem powołującym i organem uprawnionym do zawierania umów zatrudnienia w przypadku wszystkich urzędników i innych pracowników jest Sekretarz Generalny. Sekretarz Generalny może powierzyć Dyrektorowi Dyrekcji ds. Kadr, Finansów i Usług Ogólnych Trybunału Obrachunkowego odpowiedzialność w zakresie udzielania urzędnikom i innym pracownikom upoważnienia do dostępu do informacji opatrzonych klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą, w zakresie sprawowania funkcji organu do spraw akredytacji bezpieczeństwa oraz w zakresie nadzoru nad Sekretariatem Trybunału, jeśli chodzi o korzystanie z EUCI.

3) Sekretarz Generalny jest właściwy do zawierania umów o gwarantowanym poziomie usług dotyczących akredytacji urządzeń i systemów teleinformatycznych Trybunału Obrachunkowego, wykorzystania strefy bezpieczeństwa w innej instytucji UE oraz procedury wnioskowania o poświadczenia bezpieczeństwa osobowego na potrzeby uzyskania dostępu do EUCI.

4) Dyrektor Dyrekcji ds. Kadr, Finansów i Usług Ogólnych jest z kolei właściwy do zawierania porozumień administracyjnych z instytucjami, agencjami i innymi organami UE w odniesieniu do wymiany EUCI, które są Trybunałowi Obrachunkowemu niezbędne do realizowania powierzonych mu zadań. Dyrektor ten może również zawierać porozumienia administracyjne z państwami trzecimi i organizacjami międzynarodowymi w sprawie ochrony wszelkich otrzymanych informacji niejawnych.

5) Dyrektor Dyrekcji ds. Kadr, Finansów i Usług Ogólnych jest właściwy do podpisywania wszelkich oświadczeń, w których Trybunał zobowiązuje się do ochrony EUCI. Oświadczenia te przedstawia się w kontekście wyjątkowego udostępniania EUCI *ad hoc*.

6) Funkcję organu do spraw bezpieczeństwa informacji pełni urzędnik Trybunału Obrachunkowego do spraw bezpieczeństwa informacji. Urzędnik ten oraz osoby, którym powierzy on całość lub część swoich zadań, powinni posiadać odpowiednie poświadczenie bezpieczeństwa. Organ do spraw bezpieczeństwa informacji wypełnia powierzone mu obowiązki w ścisłej współpracy z Dyrekcją ds. Kadr, Finansów i Usług Ogólnych, Dyrekcją ds. Informacji, Środowiska Pracy i Innowacji oraz Dyrekcją Komitetu ds. Jakości Kontroli (zob. w szczególności art. 4, 6 i 8). Organ do spraw bezpieczeństwa informacji odpowiada również za szkolenia i spotkania mające na celu upowszechnianie wiedzy w zakresie bezpieczeństwa informacji, a także za przeprowadzanie okresowych inspekcji w celu sprawdzenia zgodności z niniejszą decyzją, w tym w odniesieniu do zewnętrznej interwencji. Odpowiada również za wszelkie środki, które należy zastosować w celu zapewnienia takiej zgodności.

7) Szef służb ochrony odpowiada za środki bezpieczeństwa fizycznego (wspomniane w szczególności w art. 5).

8) Kancelaria informacji zastrzeżonych utworzona w Sekretariacie Trybunału pełni funkcję punktu, który odpowiada za odbiór i przekazywanie informacji opatrzonych klauzulą tajności RESTREINT UE/EU RESTRICTED w ramach wymian informacji, jakie Trybunał Obrachunkowy może prowadzić z innymi instytucjami, agencjami i organami UE oraz państwami członkowskimi. Pełni również funkcję punktu, który odpowiada za odbiór i przekazywanie informacji pochodzących z państw trzecich i organizacji międzynarodowych opatrzonych równoważnymi klauzulami. Sposób organizacji kancelarii informacji zastrzeżonych określa się w decyzji delegowanej. Na urzędniku odpowiedzialnym za tę kancelarię spoczywają następujące główne obowiązki:

   a) rejestrowanie odbioru i przekazania informacji opatrzonych klauzulą tajności RESTREINT UE/EU RESTRICTED;

   b) zarządzanie strefami administracyjnymi wyodrębnionymi na potrzeby rejestrowania operacji wykorzystywania, przechowywania i sprawdzania EUCI opatrzonych klauzulą tajności RESTREINT UE/EU RESTRICTED.

9) Kancelarię informacji tajnych tworzy się na mocy postanowień umowy o gwarantowanym poziomie usług dotyczącej wykorzystania strefy bezpieczeństwa innej instytucji UE. Kancelaria informacji tajnych zorganizowana przez Sekretariat Trybunału i podlegająca Dyrektorowi Dyrekcji ds. Kadr, Finansów i Usług Ogólnych pełni funkcję punktu, który odpowiada za odbiór i przekazywanie informacji opatrzonych klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą w ramach wymian informacji, jakie Trybunał Obrachunkowy może prowadzić z innymi instytucjami, agencjami i organami UE oraz państwami członkowskimi. Pełni również

funkcję punktu, który odpowiada za odbiór i przekazywanie informacji pochodzących z państw trzecich i organizacji międzynarodowych opatrzonych równoważnymi klauzulami. Jest wyposażona w odpowiednie sejfy i inne urządzenia bezpieczeństwa odpowiednie do zapewnienia ochrony informacji opatrzonych klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą. Sposób organizacji kancelarii informacji tajnych określa się w decyzji delegowanej. Urzędnik kontroli kancelarii informacji tajnych musi posiadać odpowiednie poświadczenie bezpieczeństwa. Spoczywają na nim następujące główne obowiązki:

a) zarządzanie czynnościami związanymi z rejestracją, sprawdzaniem, konserwacją, powielaniem, tłumaczeniem, przesyłaniem, wysyłaniem i – w odpowiednich przypadkach – niszczeniem EUCI;

b) wszelkie inne zadania związane z ochroną EUCI określone w decyzji delegowanej.

10) Komitet Administracyjny przyjmuje decyzję delegowaną ustanawiającą przepisy wykonawcze do niniejszej decyzji. Urzędnik do spraw bezpieczeństwa informacji ustanawia wytyczne w zakresie bezpieczeństwa informacji. Z kolei Komitet ds. Jakość Kontroli sporządza odnośne wytyczne w zakresie kontroli.

Artykuł 11 – Wejście w życie

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

Sporządzono w Luksemburgu, 3 czerwca 2021 r.

W imieniu Europejskiego Trybunału Obrachunkowego

Klaus-Heiner Lehne
Prezes

Załącznik – ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO DOTYCZĄCE STREF ADMINISTRACYJNYCH, W KTÓRYCH KORZYSTA SIĘ Z EUCI

ZAŁĄCZNIK

ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO DOTYCZĄCE STREF ADMINISTRACYJNYCH, W KTÓRYCH KORZYSTA SIĘ Z EUCI

1) Niniejszy załącznik zawiera zasady dotyczące wykonania art. 5 decyzji. Ustanawia się w nim minimalne standardy dotyczące stref administracyjnych w Trybunale Obrachunkowym, w których korzysta się z informacji opatrzonych klauzulą tajności RESTREINT UE/EU RESTRICTED. Są to strefy, które wydzielono na potrzeby rejestrowania, przechowywania i sprawdzania informacji opatrzonych klauzulą tajności RESTREINT UE/EU RESTRICTED.

2) Celem środków bezpieczeństwa fizycznego stosowanych w strefach administracyjnych jest zapobieżenie nieuprawnionemu dostępowi do tych stref w następujący sposób:

   a) wyraźnie określa się granicę umożliwiającą kontrolę osób;

   b) dostęp bez eskorty umożliwia się tylko osobom, które są odpowiednio upoważnione przez organ Trybunału Obrachunkowego do spraw bezpieczeństwa informacji lub każdy inny właściwy organ;

   c) wszystkim innym osobom przez cały czas towarzyszy eskorta lub poddaje się je równorzędnej kontroli.

3) Organ Trybunału Obrachunkowego do spraw bezpieczeństwa informacji może na zasadzie wyjątku udzielić dostępu osobom nieupoważnionym, w tym na potrzeby pracy w strefie administracyjnej, o ile nie wiąże się to z możliwością dostępu do EUCI, które pozostają zamknięte na klucz. Takie osoby mogą wejść do odnośnych stref wyłącznie w towarzystwie i pod stałym nadzorem organu do spraw bezpieczeństwa informacji lub urzędnika kontroli kancelarii informacji zastrzeżonych.

4) Organ do spraw bezpieczeństwa informacji określa procedury zarządzania kluczami i kodami do wszystkich stref administracyjnych i szaf zabezpieczonych. Procedury te służą ochronie przed nieuprawnionym dostępem.

5) Kody zostają powierzone do zapamiętania jak najmniejszej liczbie osób, dla których znajomość tych kodów jest niezbędna. Kody do zabezpieczonych szaf, w których przechowywane są informacje opatrzone klauzulą tajności RESTREINT UE/EU RESTRICTED, zostają zmienione:

   - w przypadku otrzymania nowej szafy zabezpieczonej;
   - przy każdej zmianie pracowników znających kod;
   - każdorazowo w przypadku rzeczywistego lub domniemanego narażenia na szwank bezpieczeństwa danego kodu;
   - gdy zamek poddano konserwacji lub naprawie;
   - nie rzadziej niż co 12 miesięcy.

6) Organ do spraw bezpieczeństwa informacji i szef służb ochrony odpowiadają za zapewnienie zgodności z niniejszymi zasadami.