EVROPSKÝ
ÚČETNÍ DVŮR

Rozhodnutí Účetního dvora č. 41-2021 o bezpečnostních pravidlech na ochranu utajovaných informací EU

EVROPSKÝ ÚČETNÍ DVŮR,

S OHLEDEM NA článek 13 Smlouvy o Evropské unii,

S OHLEDEM NA článek 287 Smlouvy o fungování Evropské unie,

S OHLEDEM NA článek 257 nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046 ze dne 18. července 2018, kterým se stanoví finanční pravidla o souhrnném rozpočtu Unie,

S OHLEDEM NA čl. 1 odst. 6 prováděcích předpisů k jednacímu řádu Účetního dvora (rozhodnutí Účetního dvora č. 21-2021),

S OHLEDEM NA bezpečnostní pravidla na ochranu utajovaných informací EU ostatních orgánů, institucí a subjektů EU,

S OHLEDEM NA politiku bezpečnosti informací Účetního dvora (DEC 127/15 FINAL) a jeho politiku klasifikace informací (sdělení zaměstnancům 123/2020),

VZHLEDEM K TOMU, ŽE podle čl. 287 odst. 3 SFEU má Účetní dvůr právo na přístup ke všem relevantním dokumentům a informacím, které jsou podle jeho názoru nezbytné k výkonu jeho mandátu, včetně utajovaných informací EU, přičemž tento přístup je prováděn plně v souladu se zásadou loajální spolupráce mezi orgány a se zásadou svěření pravomocí; toto právo na přístup k utajovaným informacím EU zaručené SFEU nemůže být zpochybněno původcem utajovaných informací EU, přičemž Účetní dvůr může být požádán, aby zavedl a dodržoval určitá bezpečnostní opatření, jak je podrobněji uvedeno v tomto dokumentu;

VZHLEDEM K TOMU, ŽE členové Účetního dvora a jeho úředníci a jiní zaměstnanci jsou vázáni povinností zachovávat důvěrnost informací podle článku 339 SFEU, článku 17 služebního řádu a aktů přijatých na jeho základě, a to i po skončení služebního poměru;

VZHLEDEM K TOMU, ŽE nakládání s utajovanými informacemi EU vyžaduje – v důsledku citlivé povahy těchto informací – dodržování povinnosti důvěrnosti, a to prostřednictvím vhodných bezpečnostních opatření, jež mohou zaručit vysokou úroveň ochrany těchto informací a která jsou rovnocenná opatřením stanoveným pravidly na ochranu utajovaných informací EU přijatými ostatními orgány, institucemi a jinými subjekty EU, přičemž Účetní dvůr si vyhrazuje právo vznést jakékoli připomínky týkající se utajovaných informací EU, pokud se domnívá, že taková bezpečnostní opatření nejsou odůvodněná vzhledem k povaze a

druhu utajovaných informací EU, při současném dodržení stupně utajení utajovaných informací EU;

VZHLEDEM K TOMU, ŽE bezpečnostní opatření na ochranu důvěrnosti, integrity a dostupnosti informací sdělených Účetnímu dvoru musí odpovídat povaze a druhu dotyčných informací;

VZHLEDEM K TOMU, ŽE přístup k utajovaným informacím musí být Účetnímu dvoru poskytnut v souladu se zásadou „potřeby znát utajované informace“, aby mohl plnit úkoly svěřené Smlouvami a právními akty přijatými na základě Smluv;

VZHLEDEM K TOMU, ŽE v důsledku povahy a citlivého obsahu některých informací je vhodné stanovit zvláštní postup pro nakládání s dokumenty obsahujícími utajované informace EU ze strany Účetního dvora;

VZHLEDEM K TOMU, ŽE orgán musí zajistit, aby toto rozhodnutí bylo prováděno v souladu se všemi platnými pravidly, zejména s ustanoveními o ochraně osobních údajů, fyzické bezpečnosti osob, budov a informačních technologií a přístupu veřejnosti k dokumentům;

PŘIJAL TOTO ROZHODNUTÍ:

Článek 1 **Předmět a oblast působnosti**

1. Toto rozhodnutí stanoví základní zásady a minimální bezpečnostní normy pro ochranu utajovaných informací, s nimiž Účetní dvůr nakládá při výkonu svého mandátu.

2. Pro účely tohoto rozhodnutí se utajovanými informacemi rozumí kterékoliv nebo všechny tyto druhy informací:

   a) „Utajované informace EU“ definované v bezpečnostních pravidlech jiných orgánů, institucí nebo jiných subjektů EU, které jsou označeny jedním z těchto stupňů utajení:

   - TRÈS SECRET UE / EU TOP SECRET: informace a materiály, jejichž neoprávněné vyzrazení by mohlo mimořádně závažně poškodit podstatné zájmy Evropské unie nebo jednoho či více členských států;
   - SECRET UE / EU SECRET: informace a materiály, jejichž neoprávněné vyzrazení by mohlo závažně poškodit podstatné zájmy Evropské unie nebo jednoho či více členských států;
   - CONFIDENTIEL UE / EU CONFIDENTIAL: informace a materiály, jejichž neoprávněné vyzrazení by mohlo poškodit podstatné zájmy Evropské unie nebo jednoho či více členských států;
   - RESTREINT UE / EU RESTRICTED: informace a materiály, jejichž neoprávněné vyzrazení by mohlo být nevýhodné pro zájmy Evropské unie nebo jednoho či více členských států.

b) utajované informace poskytnuté členskými státy, které jsou opatřeny vnitrostátním stupněm utajení odpovídajícím některému z označení stupně utajení utajovaných informací EU[1] uvedených v písmenu a);

c) utajované informace poskytnuté Evropskému účetnímu dvoru třetími státy nebo mezinárodními organizacemi, které jsou označeny stupněm utajení rovnocenným označení stupně utajení utajovaných informací EU uvedeným v písmenu a), v souladu s příslušnými dohodami o bezpečnosti informací nebo správními ujednáními.

3. Účetní dvůr nakládá s informacemi se stupněm utajení RESTREINT UE / EU RESTRICTED ve svých prostorách a za tímto účelem přijímá veškerá nezbytná ochranná opatření. Pro zaměstnance Účetního dvora, kteří potřebují přístup k utajovaným informacím EU na vyšším stupni utajení, se přijmou opatření, aby tak učinili ve vhodných prostorách jiných orgánů, institucí nebo subjektů EU.

4. Toto rozhodnutí se vztahuje na všechny útvary a prostory Účetního dvora.

5. S výjimkou případů, kdy se ustanovení týká zvláštních skupin zaměstnanců, se toto rozhodnutí vztahuje na členy Účetního dvora, zaměstnance Účetního dvora, na které se vztahuje služební řád a pracovní řád ostatních zaměstnanců Evropské unie[2], národní odborníky vyslané k Účetnímu dvoru, poskytovatele služeb a jejich zaměstnance, stážisty a všechny osoby s přístupem do budov a jiných nemovitostí Účetního dvora nebo k informacím spravovaným Účetním dvorem.

6. Není-li stanoveno jinak, použijí se ustanovení o utajovaných informacích EU rovnocenným způsobem na utajované informace uvedené v odst. 2 písm. b) a c) tohoto článku.

Článek 2 Definice

Pro účely tohoto rozhodnutí se rozumí:

a) „oprávněním k přístupu k utajovaným informacím EU“ rozhodnutí přijaté ředitelem pro lidské zdroje, finance a obecné služby Účetního dvora na základě ujištění poskytnutého příslušným orgánem členského státu, že úředník Účetního dvora, jiný zaměstnanec nebo národní odborník mohou být zmocněni k přístupu k utajovaným informacím EU až do určitého stupně utajení (CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyššího) a do určitého data, pokud je zjištěno, že tyto informace potřebují znát a že byli řádně informováni o svých povinnostech; tato osoba se pak označuje za „osobu s bezpečnostním oprávněním“;

b) „utajením“ přiřazení stupně utajení informacím na základě stupně újmy, která by mohla být způsobena neoprávněným vyzrazením;

c) „kryptografickými materiály“ šifrovací algoritmy, hardwarové a softwarové kryptografické moduly a prostředky, včetně prováděcích pravidel a související dokumentace, a klíčový materiál;

d) „odtajněním“ odstranění veškerých stupňů utajení;

---

[1] Viz Dohoda mezi členskými státy Evropské unie zasedajícími v Radě o ochraně utajovaných informací vyměňovaných v zájmu Evropské unie ze dne 4. května 2011 a její příloha (Úř. věst. 2011/C 202/13).

[2] Nařízení č. 31 (EHS), kterým se stanoví služební řád úředníků a pracovní řád ostatních zaměstnanců, ve znění pozdějších předpisů, Úř. věst. 01962R0031-01.01.2020-019.003-1 (https://eur-lex.europa.eu/eli/reg/1962/31(1)/2020-01-01).

e) „dokumentem“ jakékoli zaznamenané informace bez ohledu na jejich podobu či fyzickou povahu;

f) „snížením stupně utajení“ označení informace nižším stupněm utajení;

g) „osvědčení o bezpečnostní prověrce zařízení“ správní rozhodnutí příslušného bezpečnostního orgánu, že z bezpečnostního hlediska může zařízení zajistit odpovídající úroveň ochrany utajovaných informací EU s daným stupněm utajení;

h) „nakládáním“ s utajovanými informacemi EU veškeré možné činnosti, jimž mohou být podrobovány utajované informace EU během celého svého životního cyklu: vytváření, evidence, zpracovávání, přenášení, snižování stupně utajení, odtajňování a ničení informací. V souvislosti s komunikačními a informačními systémy tento pojem zahrnuje rovněž jejich shromažďování, zobrazování, přenos a uchovávání;

i) „držitelem“ řádně oprávněná osoba s prokázanou potřebou znát utajované informace, která má utajované informace v držení, a je tudíž odpovědná za jejich ochranu;

j) „orgánem pro bezpečnost informací“ pracovník Účetního dvora pro bezpečnost informací, který může zcela nebo zčásti delegovat úkoly stanovené tímto rozhodnutím;

k) „informacemi“ jakákoli písemná či ústní informace bez ohledu na druh nosiče a její zdroj;

l) „materiálem“ jakékoli médium, datový nosič nebo část technického zařízení či vybavení;

m) „původcem“ orgán, instituce nebo subjekt EU, členský stát, třetí stát nebo mezinárodní organizace, z jejichž pověření byly utajované informace vytvořeny nebo uvedeny do struktur EU;

n) „bezpečnostní prověrkou personálu“ prohlášení příslušného orgánu členského státu, které je vydáno po skončení bezpečnostního řízení vedeného příslušnými orgány členského státu a kterým se osvědčuje, že určité osobě může být za podmínky, že bylo stanoveno, že utajované informace potřebuje znát, a že byla náležitě poučena o svých povinnostech, umožněn přístup k utajovaným informacím EU až do konkrétního stupně utajení (CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyššího) a do konkrétního data;

o) „osvědčením o bezpečnostní prověrce personálu“ osvědčení vydané ředitelem pro lidské zdroje, finance a obecné služby Účetního dvora, v němž se uvádí, že určitá osoba je držitelem platné bezpečnostní prověrky nebo bezpečnostního oprávnění, a které udává, k jakému stupni utajovaných informací EU může být dané osobě umožněn přístup (CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyššímu), dobu platnosti příslušné bezpečnostní prověrky či bezpečnostního oprávnění a datum skončení platnosti vlastního potvrzení;

p) „orgánem pro fyzickou bezpečnost“ vedoucí bezpečnostní služby Účetního dvora, který odpovídá za provádění nezbytných fyzických bezpečnostních opatření a postupů na ochranu utajovaných informací EU;

q) „rejstříkem záznamů“ rejstřík spravovaný sekretariátem Účetního dvora spadající do administrativní oblasti, za kterou odpovídá ředitel Účetního dvora pro lidské zdroje, finance a obecné služby. Odpovídá za vstup a výstup informací se stupněm utajení RESTREINT UE / EU RESTRICTED nebo rovnocenných informací vyměňovaných s Účetním dvorem.

r) „registrem utajovaných informací EU“ oblast vytvořená uvnitř zabezpečené oblasti. Tento registr spravuje na Účetním dvoře vedoucí registru s pověřením a bezpečnostní prověrkou. Odpovídá za vstup a výstup informací se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším nebo rovnocenných informací vyměňovaných s Účetním dvorem.

s) „orgánem pro bezpečnostní akreditaci“ ředitel pro lidské zdroje, finance a obecné služby Účetního dvora.

Článek 3 **Opatření na ochranu utajovaných informací EU**

1. Účetní dvůr zajistí ochranu všech utajovaných informací, které mu byly poskytnuty, způsobem odpovídajícím stupni utajení určenému původcem a v souladu s tímto rozhodnutím.

2. Za tímto účelem Účetní dvůr podmíní nakládání s utajovanými informacemi EU fyzickými a případně personálními bezpečnostními opatřeními, včetně oprávnění k přístupu určených osob a opatření na ochranu komunikačních a informačních systémů. Tato opatření jsou popsána v článcích 4 až 6 a uplatňují se po celou dobu životního cyklu utajovaných informací EU. Musí odpovídat bezpečnostnímu stupni utajení utajovaných informací EU, formě a objemu informací nebo materiálů, umístění a konstrukci zařízení, v nichž jsou utajované informace EU drženy, a na místě vyhodnocené hrozbě zlovolné nebo trestné činnosti, včetně špionáže, sabotáže a terorismu.

3. Utajované informace EU jsou chráněny fyzickými bezpečnostními opatřeními a informace se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším jsou navíc chráněny bezpečnostními opatřeními týkajícími se osob.

4. Utajované informace EU mohou být poskytnuty pouze osobám, které v rámci orgánu potřebují znát utajované informace. Držitel jakékoli utajované informace EU ji musí chránit v souladu s požadavky tohoto rozhodnutí.

5. Utajované informace EU nesmí být zpřístupněny ústně ani písemně. Předběžné připomínky, zprávy, stanoviska, tiskové zprávy a jiné výstupy Účetního dvora, jeho internetové stránky a intranet, ústní vystoupení, odpovědi na žádosti o přístup k dokumentům[3] a hlasové či obrazové záznamy nesmějí obsahovat utajované informace EU ani výtahy z nich ani na ně odkazovat. Pokud však původce zveřejnil dokumenty nebo informace obsahující odkaz na utajované informace EU, může být takový odkaz uveden.

6. Bez ohledu na odstavec 5 se Účetní dvůr a původce mohou dohodnout, že v případě konkrétního auditu může Účetní dvůr reprodukovat nebo použít prvky utajovaných informací EU v dokumentu. V takovém případě je dokument Účetního dvora před řízením o sporných otázkách nebo v jeho průběhu nejprve předložen původci dotčených utajovaných informací EU. V této situaci se Účetní dvůr a původce dohodnou na tom, zda bude dokument vydaný Účetním dvorem označen jako utajený. Považuje-li člen-zpravodaj Účetního dvora za nezbytné předat zprávu o auditu, která zcela nebo zčásti podléhá utajení, některým příjemcům v Evropském parlamentu nebo Radě – a to při zohlednění všech bezpečnostních opatření souvisejících s tímto rozhodnutím –, vyžaduje to souhlas původce utajovaných informací. Právní rámec a postup pro výměnu těchto dokumentů je stanoven v článku 7.

7. Je-li pro výkon mandátu Účetního dvora nutné, aby byly některé prvky utajovaného dokumentu nebo informací šířeny v širším rozsahu, konzultuje při řádném zohlednění stupně utajení dokumentu původce předtím, než se rozhodne použít tyto prvky nebo informace, pokud se domnívá, že pro to existuje převažující veřejný zájem. Informace se ve zprávě použijí pouze takovým způsobem, aby nemohl být poškozen zájem původce. To by mohlo být vhodným způsobem zajištěno tím, že bude původce požádán o vyjádření, aby bylo dosaženo

[3] Podle rozhodnutí Účetního dvora č. 12-2005 o přístupu veřejnosti k dokumentům Účetního dvora, ve znění rozhodnutí č. 14-2009 (Úř. věst. 2009/C 67/1).

dohody o způsobu anonymizace, kondenzace nebo zobecnění informací atd. a aby byly zároveň respektovány zájmy těch, jichž se zveřejněné informace týkají.

8. Účetní dvůr neposkytne utajované informace EU jinému orgánu, agentuře, subjektu nebo úřadu EU, členskému státu, třetímu státu nebo mezinárodní organizaci bez předchozí konzultace a výslovného písemného souhlasu původce.

9. Pokud původce dokumentu se stupněm utajení SECRET UE / EU SECRET nebo nižším nestanovil omezení pro jeho kopie nebo překlad, mohou být tyto dokumenty na žádost držitele a v souladu s praktickými pracovními pokyny orgánu pro bezpečnost informací Účetního dvora kopírovány nebo přeloženy. Bezpečnostní opatření, která se týkají původního dokumentu, se rovněž použijí pro jeho kopie a překlady.

10. Pokud Účetní dvůr potřebuje, aby byl snížen stupeň utajení dokumentu nebo byl odtajněn dokument, který obdržel nebo k němuž má oprávnění k přístupu, obrátí se Účetní dvůr na původce s žádostí, zda může poskytnout verzi dokumentu s nižším stupněm utajení nebo odtajněnou verzi dokumentu.

Článek 4 Personální bezpečnost

1. Členové Účetního dvora jsou z titulu své funkce oprávněni mít přístup ke všem utajovaným informacím EU a účastnit se zasedání, na nichž se s utajovanými informacemi EU nakládá. Členové jsou informováni o svých bezpečnostních povinnostech týkajících se ochrany utajovaných informací EU a písemně potvrdí svou odpovědnost za ochranu těchto informací.

2. Zaměstnanci Účetního dvora, ať již úředníci, zaměstnanci podléhající pracovnímu řádu ostatních zaměstnanců nebo vyslaní národní odborníci, mají přístup k utajovaným informacím EU pouze poté, co:

   i. byla stanovena jejich potřeba znát tyto informace;

   ii. byli informováni o bezpečnostních pravidlech na ochranu utajovaných informací EU a příslušných bezpečnostních normách a pokynech a písemně potvrdili svou odpovědnost za ochranu těchto informací;

   iii. v případě informací se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším prošli bezpečnostní prověrkou a bylo jim uděleno oprávnění k přístupu.

3. Postup pro určení, zda může být úředník nebo jiný zaměstnanec Účetního dvora oprávněn k přístupu k informacím se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším, s ohledem na loajalitu, bezúhonnost a spolehlivost dané osoby a po získání ujištění od příslušných orgánů členského státu podle čl. 2 písm. n), se stanoví v rozhodnutí v přenesené pravomoci přijatém v souladu s čl. 10 odst. 10. Rozhodnutí o udělení povolení k přístupu k informacím přijímá ředitel pro lidské zdroje, finance a obecné služby Účetního dvora.

4. Ředitel pro lidské zdroje, finance a obecné služby Účetního dvora může vydat osvědčení o bezpečnostní prověrce personálu s upřesněním stupně utajení, pro který může být osobám umožněn přístup k utajovaným informacím EU (CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším), doby platnosti příslušného oprávnění k přístupu a data skončení platnosti osvědčení o bezpečnostní prověrce personálu.

5. Zasedání, na nichž se nakládá s informacemi se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším, se mohou účastnit pouze osoby oprávněné podle odst. 2 bodu iii)

a členové Účetního dvora podle odstavce 1. Účetní dvůr a původce přijmou praktická opatření pro tato zasedání případ od případu.

6. Útvary Účetního dvora, které odpovídají za organizaci zasedání, na nichž má být nakládáno s informacemi se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším, včas informují orgán pro bezpečnost informací o datech, časech a místech zasedání a předloží seznamy účastníků.

7. Každá osoba, která má v držení utajované informace EU bez řádného povolení anebo u níž se neprokázalo, že je potřebuje znát, musí co nejdříve tuto situaci oznámit orgánu pro bezpečnost informací a zajistit, aby utajované informace EU byly chráněny v souladu s požadavky tohoto rozhodnutí.

Článek 5 Opatření fyzické bezpečnosti na ochranu utajovaných informací

1. „Fyzickou bezpečností“ se rozumí použití fyzických a technických ochranných opatření k zabránění neoprávněnému přístupu k utajovaným informacím EU.

2. Opatření fyzické bezpečnosti mají znemožnit podloudné nebo násilné vniknutí narušitele, odradit od neoprávněné činnosti a takové činnosti zabránit a odhalit ji a umožnit rozdělení členů personálu, pokud jde o přístup k utajovaným informacím EU, v souladu se zásadou potřeby znát utajované informace. Tato opatření se stanoví na základě postupu řízení rizik v souladu s tímto rozhodnutím.

3. Oblasti, kde se nakládá s utajovanými informacemi EU nebo v nichž se tyto informace uchovávají, podléhají pravidelné kontrole ze strany příslušného bezpečnostního orgánu Účetního dvora.

4. K nakládání s utajovanými informacemi EU a jejich uchovávání se používají pouze vybavení nebo přístroje, které jsou v souladu s pravidly na ochranu utajovaných informací EU platnými v rámci orgánů, institucí nebo subjektů EU.

5. Mimo prostory Účetního dvora mají zaměstnanci Účetního dvora přístup k utajovaným informacím EU se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším nebo rovnocenným stupněm utajení v zabezpečených oblastech.

6. Účetní dvůr může uzavřít dohodu o úrovni služeb s jiným orgánem EU v Lucemburku, aby mohl zpracovávat a uchovávat informace se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším v zabezpečené oblasti tohoto orgánu. Není-li výslovně dohodnuto s původcem, nesmí být s těmito utajovanými informacemi EU nakládáno ani tyto informace nesmí být uchovávány v prostorách Účetního dvora a Účetní dvůr je nesmí kopírovat ani překládat.

7. Účetní dvůr vede evidenci obdržených informací, které mají stupeň utajení RESTREINT UE / EU RESTRICTED. Nahlížení do informací se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším nebo rovnocenným mimo prostory Účetního dvora se z bezpečnostních důvodů eviduje.

8. Utajované informace EU se stupněm utajení RESTREINT UE / EU RESTRICTED mohou být uloženy ve vhodném uzamčeném kancelářském nábytku v administrativní oblasti nebo zabezpečené oblasti. Utajované informace EU se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo SECRET UE / EU SECRET se ukládají na základě dohody o úrovni služeb v bezpečnostním úschovném objektu v zabezpečené oblasti jiného orgánu EU v Lucemburku.

9. Pokud se utajované informace EU nacházejí mimo registr, předávají se mezi útvary a prostory takto:

   a) obecně platí, že utajované informace EU se předávají elektronickými prostředky chráněnými kryptografickými prostředky schválenými v souladu s čl. 6 odst. 8;

   b) nejsou-li utajované informace EU přenášeny způsobem popsaným v písmenu a), přenášejí se pomocí datového nosiče (např. paměťového média USB, CD, pevného disku) chráněného kryptografickými prostředky schválenými v souladu s čl. 6 odst. 8 nebo jako papírová kopie v neprůhledné zapečetěné obálce.

10. Informace se stupněm utajení RESTREINT UE / EU může držitel zničit v souladu s pravidly archivace platnými na Účetním dvoře. Informace se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším může zničit pouze vedoucí registru, je-li k tomu zmocněn držitelem nebo příslušným orgánem v souladu s pravidly pro archivaci platnými na Účetním dvoře. Dokumenty se stupněm utajení SECRET UE / EU SECRET se zničí za přítomnosti svědka s bezpečnostní prověrkou odpovídající alespoň stupni utajení dokumentu, který má být zničen. Vedoucí registru a svědek (v případech, kdy je požadována jeho přítomnost) podepíší záznam o zničení, který se uloží do registru. Vedoucí registru uchovává záznamy o zničení dokumentů se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL a SECRET UE / EU SECRET po dobu nejméně pěti let.

11. Orgán pro fyzickou bezpečnost a orgán pro bezpečnost informací vypracují s přihlédnutím k místním podmínkám společný plán pro zabezpečení utajovaných informací EU v době krize, případně včetně plánů na jejich zničení nebo evakuaci v případě mimořádné události. Vydávají pokyny, které považují za vhodné, aby zabránili tomu, aby se utajované informace EU dostaly do rukou neoprávněných osob.

12. Pokud musí být utajované informace EU přepravovány fyzicky, bude Účetní dvůr dodržovat opatření, která původce informací uložil na jejich ochranu před neoprávněným vyzrazením během přepravy.

13. Opatření fyzické bezpečnosti, která se použijí v administrativních oblastech, v nichž se nakládá s informacemi se stupněm utajení RESTREINT UE / EU RESTRICTED a v nichž se tyto informace uchovávají, jsou stanovena v příloze.

Článek 6 Ochrana utajovaných informací EU v komunikačních a informačních systémech

1. Pro účely tohoto článku se „komunikačním a informačním systémem“ rozumí jakýkoli systém umožňující nakládání s utajovanými informacemi EU v elektronické podobě. Komunikační a informační systém zahrnuje veškerá aktiva potřebná k jeho provozu, včetně infrastruktury, organizace, personálu a informačních zdrojů.

2. „Oprávněným uživatelem“ se rozumí člen Účetního dvora, úředník, jiný zaměstnanec nebo vyslaný národní odborník se zjištěnou a uznanou potřebou přístupu k určitému informačnímu systému.

3. Účetní dvůr poskytne záruku, že jeho systémy budou ve vhodné míře chránit informace, s nimiž nakládají, a že budou fungovat podle potřeby pod kontrolou oprávněných uživatelů. Za tímto účelem zaručí přiměřenou úroveň:

   - autenticity: záruka, že informace jsou autentické a z důvěryhodných zdrojů;
   - dostupnosti: přístupnost a použitelnost informací na žádost oprávněného subjektu;
   - důvěrnosti: skutečnost, že informace se nezpřístupňují neoprávněným osobám a subjektům nebo pro nedovolené účely;

- integrity: zajištění správnosti a úplnosti aktiv a informací;
- nepopiratelnosti: schopnost prokázat zpětně jednání či událost tak, aby dané jednání či událost nemohly být následně popřeny.

Toto ujištění vychází z procesu řízení rizik. „Rizikem“ se rozumí možnost, že v rámci určité hrozby budou zneužita vnitřní a vnější zranitelná místa organizace nebo kteréhokoli ze systémů, jichž využívá, a dojde tak k poškození organizace a jejích hmotných či nehmotných aktiv. Měří se jako kombinace pravděpodobnosti, že k hrozbám dojde, a dopadu těchto hrozeb. Proces řízení rizik sestává z těchto kroků: identifikace hrozeb a zranitelných míst, hodnocení rizika, řešení rizika, přijetí rizika a sdělování rizika.

- „Hodnocení rizika“ spočívá v rozpoznání hrozeb a zranitelných míst a v provádění analýzy souvisejícího rizika, tj. analýzy pravděpodobnosti a dopadu.
- „Řešení rizika“ spočívá ve zmírnění, odstranění, omezení (prostřednictvím vhodné kombinace technických, fyzických, organizačních nebo procedurálních opatření), přenesení nebo monitorování rizika.
- „Přijetím rizika“ se rozumí rozhodnutí, kterým se vyjadřuje souhlas s tím, že po řešení rizika i nadále existuje zbytkové riziko.
- „Zbytkovým rizikem“ se rozumí riziko, které přetrvává poté, co byla zavedena bezpečnostní opatření, neboť nelze čelit všem hrozbám a nelze odstranit všechna zranitelná místa.
- „Sdělování rizika“ spočívá v rozvoji informovanosti o rizicích v rámci skupin uživatelů komunikačních a informačních systémů, v informování schvalovacích orgánů o těchto rizicích a podávání zpráv o těchto rizicích provozním orgánům.

4. Veškerá elektronická zařízení a vybavení používané pro nakládání s utajovanými informacemi EU musí být v souladu s pravidly platnými pro ochranu utajovaných informací EU. Přednost mají elektronické přístroje a vybavení, které již byly akreditovány jiným orgánem, institucí nebo subjektem EU. Zařízení musí být zabezpečena po celou dobu svého životního cyklu.

5. Komunikační a informační systém Účetního dvora pro nakládání s utajovanými informacemi EU musí být akreditován příslušným orgánem. Za tímto účelem uzavře Účetní dvůr dohodu o úrovni služeb s orgánem pro bezpečnostní akreditaci orgánu EU, který je schopen akreditovat komunikační a informační systémy nakládající s utajovanými informacemi EU, s cílem získat osvědčení o akreditaci pro informace se stupněm utajení RESTREINT UE / EU RESTRICTED, s nimiž lze nakládat v komunikačním a informačním systému Účetního dvora, a pro odpovídající provozní podmínky. Dohoda o úrovni služeb rovněž odkazuje na normy, které se mají použít pro akreditační řízení, a uzavírá se postupem podle čl. 10 odst. 3.

6. V případě, že Účetní dvůr potřebuje zavést vlastní akreditační postup pro svůj komunikační a informační systém, stanoví se tento postup v rozhodnutí v přenesené pravomoci uvedeném v čl. 10 odst. 10 tohoto rozhodnutí v souladu s normami pro akreditační řízení pro komunikační a informační systémy nakládající s utajovanými informacemi EU v jiných orgánech, institucích a subjektech EU.

7. Odpovědnost za přípravu akreditačních podkladů a dokumentace v souladu s platnými normami nese výhradně vlastník komunikačního a informačního systému.

8. Jsou-li utajované informace EU chráněny kryptografickými prostředky, dává Účetní dvůr přednost prostředkům schváleným Radou nebo generálním tajemníkem Rady jako schvalovacím orgánem pro kryptografickou ochranu, případně prostředkům schváleným jinými orgány, institucemi a jinými subjekty EU na ochranu utajovaných informací EU.

9. S informacemi se stupněm utajení RESTREINT UE / EU RESTRICTED se nakládá pouze na elektronických zařízeních (jako jsou pracovní stanice, tiskárny, kopírovací stroje), která se

nacházejí v administrativní oblasti nebo zabezpečené oblasti. Elektronická zařízení, která zpracovávají informace se stupněm utajení RESTREINT UE / EU RESTRICTED, jsou oddělena od jiných počítačových sítí a chráněna vhodnými fyzickými nebo technickými opatřeními.

10. Všichni zaměstnanci Účetního dvora, kteří se podílejí na navrhování, vývoji, testování, provozu, řízení nebo využívání komunikačních a informačních systémů nakládajících s utajovanými informacemi EU, oznámí pracovníkovi pro bezpečnost informací veškeré potenciální bezpečnostní nedostatky, incidenty, narušení bezpečnosti nebo ohrožení, které mohou mít dopad na ochranu komunikačních a informačních systémů anebo utajovaných informací EU v nich uložených.

Článek 7 Postup výměny utajovaných informací a umožnění přístupu k nim

1. Orgány, instituce, subjekty a úřady EU a vnitrostátní orgány, pokud jsou povinny tak učinit na základě Smluv nebo právních aktů přijatých na základě Smluv, poskytnou z vlastního podnětu nebo na písemnou žádost předsedy, člena-zpravodaje či členů-zpravodajů nebo generálního tajemníka Účetnímu dvoru přístup k utajovaným informacím EU podle níže uvedeného postupu.

2. Žádosti o přístup se dotčeným orgánům zasílají prostřednictvím rejstříku záznamů Účetního dvora.

3. V případě potřeby uzavře Účetní dvůr správní ujednání upravující praktické aspekty výměny utajovaných informací EU nebo rovnocenných informací.

4. Pro účely uzavření těchto správních ujednání poskytne Účetní dvůr původci veškeré nezbytné informace o svém systému informační bezpečnosti. V případě potřeby může být uspořádána hodnoticí návštěva.

5. Tato správní ujednání se uzavírají v plném souladu se zásadami svěření pravomocí a loajální spolupráce stanovenými v článku 13 Smlouvy o Evropské unii. Uzavírají se postupem podle čl. 10 odst. 4.

6. Pokud neexistuje správní ujednání s daným orgánem, institucí nebo subjektem EU, třetím státem nebo mezinárodní organizací o poskytování utajovaných informací Účetnímu dvoru, podepisuje Účetní dvůr prohlášení o závazku chránit obdržené utajované informace.

Článek 8 Narušení bezpečnosti, ztráta nebo ohrožení utajovaných informací

1. Porušením bezpečnosti se rozumí jednání nebo opomenutí jednotlivce, které je v rozporu s bezpečnostními pravidly stanovenými v tomto rozhodnutí a v prováděcích pravidlech k němu.

2. K ohrožení dochází, pokud byly utajované informace EU v důsledku narušení bezpečnosti zcela nebo zčásti zpřístupněny neoprávněným osobám.

3. Jakékoli narušení bezpečnosti nebo podezření z narušení bezpečnosti se neprodleně oznámí orgánu pro bezpečnost informací Účetního dvora.

4. Je-li známo nebo existuje-li důvodné podezření, že došlo k ohrožení nebo ztrátě utajovaných informací EU, informuje orgán pro bezpečnost informací ředitele lidských zdrojů, financí a obecných služeb a generálního tajemníka Účetního dvora. Ředitel pro lidské zdroje, finance a obecné služby neprodleně informuje příslušný bezpečnostní orgán původce. Výše uvedený ředitel Účetního dvora provede šetření a informuje generálního tajemníka Účetního dvora a

bezpečnostní orgán původce o výsledcích šetření a o opatřeních přijatých s cílem zabránit opakování situace. Jedná-li se o člena Účetního dvora, odpovídá za přijetí opatření ve spolupráci s generálním tajemníkem Účetního dvora předseda Účetního dvora.

5. Každý úředník nebo zaměstnanec Účetního dvora, který je odpovědný za porušení bezpečnostních pravidel stanovených v tomto rozhodnutí a v prováděcích pravidlech k němu, podléhá sankcím stanoveným ve služebním řádu a pracovním řádu ostatních zaměstnanců Evropské unie.

6. Každý člen Účetního dvora, který nedodrží podmínky tohoto rozhodnutí, podléhá opatřením a sankcím stanoveným v čl. 286 odst. 6 Smlouvy.

7. Každá osoba, která je odpovědná za ztrátu nebo ohrožení utajovaných informací EU, může být v souladu s platnými právními a správními předpisy vystavena disciplinárním nebo právním krokům.

Článek 9 Bezpečnost v případě vnějšího zásahu

1. Účetní dvůr může na základě smlouvy svěřit plnění úkolů, které zahrnují utajované informace EU nebo k nim vyžadují přístup, dodavatelům registrovaným v některém členském státě. K tomu může dojít zejména v souvislosti s údržbou komunikačních a informačních systémů a počítačové sítě.

2. V případě vnějšího zásahu přijme Účetní dvůr veškerá nezbytná bezpečnostní opatření uvedená v odstavci 3 tohoto článku, včetně požadavku na osvědčení o bezpečnostní prověrce zařízení, aby zájemci a uchazeči po celou dobu zadávacího řízení a dodavatelé a subdodavatelé po celou dobu trvání smlouvy chránili utajované informace EU. Veřejný zadavatel zajistí, aby byly ve smlouvách uvedeny minimální bezpečnostní normy stanovené v tomto rozhodnutí, aby se zhotovitelům uložila povinnost je dodržovat.

3. Bezpečnostní pravidla, zadávací řízení a šablony a modely smluv a subdodavatelských smluv zahrnujících přístup k utajovaným informacím EU, oznámení o zahájení zadávacího řízení, pokyny ohledně okolností, za nichž se vyžaduje osvědčení o bezpečnostní prověrce zařízení a zaměstnanců, bezpečnostní pokyny k programu nebo projektu, dopisy týkající se bezpečnostních aspektů, návštěvy a přenos a přeprava utajovaných informací EU v rámci těchto smluv a subdodavatelských smluv musí být v souladu s pravidly, šablonami a modely stanovenými Evropskou komisí pro utajované smlouvy v rozhodnutí Komise (EU, Euratom) 2015/444 ze dne 13. března 2015 o bezpečnostních pravidlech na ochranu utajovaných informací EU.

Článek 10 Provádění rozhodnutí a související povinnosti

1. Útvary Účetního dvora přijmou v rámci své odpovědnosti veškerá nezbytná opatření, aby při nakládání s utajovanými informacemi EU nebo jinými utajovanými informacemi nebo při jejich uchovávání uplatňovaly toto rozhodnutí a příslušná prováděcí pravidla.

2. Generální tajemník je orgánem oprávněným ke jmenování a orgánem oprávněným uzavírat pracovní smlouvy pro všechny úředníky a ostatní zaměstnance. Generální tajemník může na ředitele oddělení lidských zdrojů, financí a generálních služeb přenést odpovědnost za udělování oprávnění úředníkům a zaměstnancům k přístupu k informacím se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším, za výkon své funkce orgánu pro bezpečnostní akreditaci a za dohled nad sekretariátem Účetního dvora, pokud jde o nakládání s utajovanými informacemi EU.

3. Generální tajemník je oprávněn uzavírat dohody o úrovni služeb týkající se akreditace komunikačního a informačního vybavení a systémů Účetního dvora, využívání zabezpečené oblasti v jiném orgánu EU a postupu pro žádosti o bezpečnostní prověrku personálu pro přístup k utajovaným informacím EU.

4. Ředitel pro lidské zdroje, finance a obecné služby je oprávněn uzavírat správní ujednání s orgány, institucemi a jinými subjekty EU o výměně utajovaných informací EU, které Účetní dvůr potřebuje k plnění svého mandátu. Tento ředitel může rovněž uzavírat správní ujednání se třetími státy nebo mezinárodními organizacemi o ochraně obdržených utajovaných informací.

5. Ředitel pro lidské zdroje, finance a obecné služby je oprávněn podepsat jakékoli prohlášení o závazku na ochranu utajovaných informací EU, které má být poskytnuto v souvislosti s výjimečným *ad hoc* poskytováním utajených informací.

6. Pracovník pro bezpečnost informací Účetního dvora jedná jako orgán pro bezpečnost informací. Pracovník pro bezpečnost informací a osoby, na které deleguje všechny své úkoly nebo jejich část, musí mít příslušnou bezpečnostní prověrku. Orgán pro bezpečnost informací přebírá své povinnosti v úzké spolupráci s ředitelstvím pro lidské zdroje, finance a obecné služby, ředitelstvím pro informace, pracovní prostředí a inovace a s ředitelstvím výboru pro řízení kvality auditu (viz zejména články 4, 6 a 8). Orgán pro bezpečnost informací je rovněž odpovědný za školení a informační schůzky týkající se bezpečnosti informací a za pravidelné kontroly za účelem ověření souladu s tímto rozhodnutím, a to i v případě vnějšího zásahu a jakýchkoli opatření, která mají být přijata k zajištění souladu s tímto rozhodnutím.

7. Vedoucí bezpečnostní služby odpovídá za fyzická bezpečnostní opatření (zejména článek 5).

8. Vstupním a výstupním místem pro informace se stupněm utajení RESTREINT UE / EU RESTRICTED, které si Účetní dvůr může vyměňovat s jinými orgány, institucemi a jinými subjekty EU a členskými státy, je rejstřík záznamů zřízený v rámci sekretariátu Účetního dvora. Jedná se rovněž o vstupní a výstupní místo pro rovnocenné informace třetích států a mezinárodních organizací. Organizace rejstříku záznamů je stanovena v rozhodnutí v přenesené pravomoci. Referent rejstříku záznamů má tyto hlavní povinnosti:

   a) eviduje vstupy a výstupy informací se stupněm utajení RESTREINT UE / EU RESTRICTED;

   b) spravuje vyhrazené administrativních oblastí pro evidenci nakládání s utajovanými informacemi EU se stupněm utajení RESTREINT UE / EU RESTRICTED, jejich uchovávání a nahlížení do nich.

9. Na základě dohody o úrovni služeb se zřizuje registr pro využívání zabezpečené oblasti jiného orgánu EU. Tento registr zřízený sekretariátem Účetního dvora a podléhající řediteli Účetního dvora pro lidské zdroje, finance a obecné služby je vstupním a výstupním místem pro informace se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším, které si Účetní dvůr může vyměňovat s ostatními orgány, institucemi a jinými subjekty EU a členskými státy. Jedná se rovněž o vstupní a výstupní místo pro rovnocenné informace třetích států a mezinárodních organizací. Je vybaven vhodnými trezory a jiným bezpečnostním vybavením vhodným pro ochranu informací se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším. Organizace registru je stanovena v rozhodnutí v přenesené pravomoci. Vedoucí registru má příslušnou bezpečnostní prověrku a má tyto hlavní povinnosti:

   a) řídí operace týkající se evidence, nahlížení, uchovávání, reprodukce, překladu, přenosu, odesílání a případně zničení utajovaných informací EU;

   b) plní další úkoly související s ochranou utajovaných informací EU vymezených v rozhodnutí v přenesené pravomoci.

10. Administrativní výbor přijme rozhodnutí v přenesené pravomoci, kterým se stanoví prováděcí pravidla k tomuto rozhodnutí. Pracovník pro bezpečnost informací vypracuje pokyny pro bezpečnost informací. Výbor pro řízení kvality auditu vypracuje pokyny pro audit.

Článek 11 **Vstup v platnost**

Toto rozhodnutí vstupuje v platnost prvním dnem po vyhlášení v Úředním věstníku Evropské unie.

V Lucemburku dne 3. června 2021.

Za Účetní dvůr

Klaus-Heiner Lehne
předseda

Příloha: OPATŘENÍ FYZICKÉ BEZPEČNOSTI TÝKAJÍCÍ SE ADMINISTRATIVNÍCH OBLASTÍ PRO UTAJOVANÉ INFORMACE EU

PŘÍLOHA

OPATŘENÍ FYZICKÉ BEZPEČNOSTI TÝKAJÍCÍ SE ADMINISTRATIVNÍCH OBLASTÍ PRO UTAJOVANÉ INFORMACE EU

1. Tato příloha obsahuje prováděcí pravidla k článku 5 rozhodnutí. Jedná se o minimální pravidla pro fyzickou ochranu administrativních oblastí pro informace se stupněm utajení RESTREINT UE / EU RESTRICTED na Účetním dvoře: prostory určené pro zaznamenávání a uchovávání informací se stupněm utajení RESTREINT UE / EU RESTRICTED a pro nahlížení do nich.

2. Účelem opatření fyzické bezpečnosti v administrativních oblastech je zabránit neoprávněnému přístupu do těchto oblastí takto:

   a) musí být viditelně vymezen obvod, který umožní kontrolu osob;

   b) přístup bez doprovodu je umožněn pouze osobám řádně zmocněným orgánem pro bezpečnost informací Účetního dvora nebo jiným příslušným orgánem;

   c) pro všechny jiné osoby je třeba zajistit nepřetržitý doprovod nebo rovnocenná kontrolní opatření.

3. Orgán pro bezpečnost informací Účetního dvora může výjimečně povolit přístup neoprávněným osobám, a to i za účelem práce v administrativní oblasti, pokud to nevyžaduje přístup k utajovaným informacím EU, které zůstávají uzamčené. Tyto osoby mohou vstupovat pouze v doprovodu orgánu pro bezpečnost informací nebo vedoucího rejstříku záznamů a pod jeho stálým dohledem.

4. Orgán pro bezpečnost informací stanoví postupy pro správu klíčů anebo nastavení kombinací pro všechny administrativní oblasti a bezpečný nábytek. Účelem těchto postupů je zabránit neoprávněnému přístupu.

5. Nastavení kombinací zná zpaměti co nejmenší možný počet osob, které je potřebují znát. Nastavení kombinací bezpečného nábytku používaného pro uchovávání informací se stupněm utajení RESTREINT UE / EU RESTRICTED se mění takto:

   - po přijetí nového kusu bezpečného nábytku,
   - kdykoli se změní personál, který kombinaci zná,
   - pokud došlo k vyzrazení nastavení nebo existuje podezření, že k takovémuto vyzrazení došlo,
   - pokud zámek prošel údržbou nebo opravou,
   - nejméně každých 12 měsíců.

6. Za dodržování těchto pravidel odpovídají orgán pro bezpečnost informací a vedoucí bezpečnostní služby.