EVROPSKO RAČUNSKO SODIŠČE

Sklep Računskega sodišča št. 041-2021 o varnostnih pravilih za varovanje tajnih podatkov EU

EVROPSKO RAČUNSKO SODIŠČE JE –

OB UPOŠTEVANJU člena 13 Pogodbe o Evropski uniji,

OB UPOŠTEVANJU člena 287 Pogodbe o delovanju Evropske unije,

OB UPOŠTEVANJU člena 257 Uredbe (EU, Euratom) 2018/1046 Evropskega parlamenta in Sveta z dne 18. julija 2018 o finančnih pravilih, ki se uporabljajo za splošni proračun Unije,

OB UPOŠTEVANJU člena 1(6) izvedbenih pravil Poslovnika Računskega sodišča (Sklep Računskega sodišča št. 21-2021),

OB UPOŠTEVANJU varnostnih pravil za varovanje tajnih podatkov EU drugih institucij, agencij in organov EU,

OB UPOŠTEVANJU politike Računskega sodišča o informacijski varnosti (DEC 127/15 FINAL) in politike za določanje stopnje tajnosti podatkov (obvestilo uslužbencem 123/2020),

KER ima v skladu s členom 287(3) PDEU Računsko sodišče pravico dostopa do vseh ustreznih dokumentov in informacij, vključno s tajnimi podatki EU, ki jih po svojem mnenju potrebuje za izvajanje svojega mandata, ki se izvaja ob polnem spoštovanju načela lojalnega sodelovanja med institucijami in načela prenosa pristojnosti; tvorec tajnih podatkov EU sicer ne more izpodbijati pravice dostopa do tajnih podatkov EU, ki se zagotavlja s PDEU, vendar lahko od Računskega sodišča zahteva, naj uvede in spoštuje nekatere varnostne ukrepe, kot je podrobneje pojasnjeno v tem dokumentu;

KER za člane Računskega sodišča ter njegove uradnike in druge uslužbence tudi po prenehanju delovnega razmerja velja obveznost glede zaupnosti v skladu s členom 339 PDEU, členom 17 kadrovskih predpisov in akti, sprejetimi na njihovi podlagi;

KER se za obravnavo tajnih podatkov EU zaradi njihove občutljive narave zahteva, da se spoštovanje obveznosti glede zaupnosti zagotovi z ustreznimi varnostnimi ukrepi, s katerimi se lahko zagotovi visoka raven varovanja teh podatkov in ki so enakovredni tistim, ki jih določajo pravila o varovanju tajnih podatkov EU, ki so jih sprejele druge institucije, agencije in organi EU, pri čemer si Računsko sodišče pridržuje pravico, da v primeru, ko meni, da takšni varnostni ukrepi glede na naravo in vrsto tajnih podatkov EU niso upravičeni, ob upoštevanju stopnje tajnosti tajnih podatkov EU poda ustrezne pripombe;

KER morajo varnostni ukrepi za varovanje zaupnosti, celovitosti in razpoložljivosti informacij, posredovanih Računskemu sodišču, ustrezati naravi in vrsti zadevnih informacij;

KER je treba Računskemu sodišču dostop do tajnih podatkov zagotoviti v skladu z načelom potrebe po seznanitvi za izvajanje nalog, ki so mu poverjene s Pogodbama in pravnimi akti, sprejetimi na njuni podlagi;

KER je glede na naravo in občutljivo vsebino nekaterih podatkov primerno, da se določi poseben postopek, v skladu s katerim Računsko sodišče obravnava dokumente, ki vsebujejo tajne podatke EU;

KER mora institucija zagotoviti, da se ta sklep izvaja v skladu z vsemi veljavnimi pravili, zlasti določbami o varstvu osebnih podatkov, fizični varnosti oseb, zgradb in IT ter dostopu javnosti do dokumentov –

SKLENILO:

Člen 1 **Predmet urejanja in področje uporabe**

(1) V tem sklepu so določena osnovna načela in minimalni varnostni standardi za varovanje tajnih podatkov, ki jih Računsko sodišče obravnava pri izvrševanju svojega mandata.

(2) Za namene tega sklepa tajni podatki pomenijo katero koli ali vse naslednje vrste podatkov:

(a) tajni podatki EU, kakor so opredeljeni v varnostnih pravilih drugih institucij, agencij, organov ali uradov EU in imajo eno od naslednjih oznak stopnje tajnosti:

- TRÈS SECRET UE/EU TOP SECRET: podatki in gradivo, katerih nepooblaščeno razkritje bi lahko povzročilo izjemno resno škodo za vitalne interese Evropske unije ali ene ali več držav članic;
- SECRET UE/EU SECRET: podatki in gradivo, katerih nepooblaščeno razkritje bi lahko resno škodovalo vitalnim interesom Evropske unije ali ene ali več držav članic,
- CONFIDENTIEL UE/EU CONFIDENTIAL: podatki in gradivo, katerih nepooblaščeno razkritje bi lahko škodovalo vitalnim interesom Evropske unije ali ene ali več držav članic,
- RESTREINT UE/EU RESTRICTED: podatki in gradivo, katerih nepooblaščeno razkritje bi lahko bilo škodljivo za interese Evropske unije ali ene ali več držav članic;

(b) tajni podatki, ki jih predložijo države članice in imajo nacionalno oznako stopnje tajnosti, ki je enakovredna kateri od stopenj tajnosti, ki se uporabljajo za tajne podatke EU[1], navedene v točki (a);

(c) tajni podatki, ki jih Evropskemu računskemu sodišču predložijo tretje države ali mednarodne organizacije ter imajo oznako stopnje tajnosti, ki je enakovredna kateri od stopenj tajnosti, ki se uporabljajo za tajne podatke EU, navedene v točki (a), v skladu z zadevnimi sporazumi o varnosti tajnih podatkov ali upravnih dogovorih.

(3) Računsko sodišče podatke stopnje RESTREINT UE/EU RESTRICTED obravnava v svojih prostorih in v ta namen sprejme vse potrebne ukrepe varovanja. Poskrbi se, da uslužbenci Računskega sodišča (opomba: v tem dokumentu uporabljeni izrazi, zapisani v slovnični obliki moškega

[1] Glej Sporazum med državami članicami Evropske unije, ki so se sestale v okviru Sveta, o varovanju tajnih podatkov, ki se izmenjujejo v interesu Evropske unije z dne 4. maja 2011 in Prilogo k Sporazumu (UL 2011/C 202/13).

spola, so uporabljeni kot spolno nevtralni), ki morajo dostopati do tajnih podatkov EU višjih stopenj, to storijo v ustreznih prostorih drugih institucij, organov ali agencij EU.

(4) Ta sklep se uporablja za vse oddelke Računskega sodišča in v vseh njegovih prostorih.

(5) Razen kadar se neka določba nanaša ne specifične skupine uslužbencev, se ta sklep uporablja za člane Računskega sodišča, za uslužbence Računskega sodišča, za katere veljajo kadrovski predpisi in pogoji za zaposlitev drugih uslužbencev Evropske unije[2], za nacionalne strokovnjake, napotene na Računsko sodišče, ponudnike storitev in njihove uslužbence, pripravnike in za vse osebe, ki imajo dostop do zgradb ali drugih prostorov Računskega sodišča ali do informacij, ki jih Računsko sodišče upravlja.

(6) Če ni določeno drugače, se določbe o tajnih podatkih EU uporabljajo enako za tajne podatke iz odstavka 2(b) in (c) tega člena.

Člen 2 **Opredelitve pojmov**

V tem sklepu:

(a) „pooblastilo za dostop do tajnih podatkov EU“ pomeni odločitev, ki jo sprejme direktor direktorata Računskega sodišča za kadrovske, finančne in splošne zadeve v skladu z zagotovitvijo pristojnega organa države članice, da se uradnik Računskega sodišča, drugi uslužbenec ali napoten nacionalni strokovnjak lahko pooblasti za dostop do tajnih podatkov EU do določene stopnje tajnosti (CONFIDENTIEL UE/EU CONFIDENTIAL ali višje) in do določenega datuma, če je bila ugotovljena njegova potreba po vedenju in če je bil ustrezno poučen o svoji odgovornosti; ta posameznik je po tem „varnostno preverjen“;

(b) „določitev stopnje tajnosti“ pomeni dodelitev stopnje tajnosti podatkom na podlagi stopnje škodovanja, ki bi ga lahko povzročilo njihovo nepooblaščeno razkritje;

(c) „kriptografski material“ pomeni kriptografske algoritme, kriptografske module strojne in programske opreme ter produkte, vključno s podrobnostmi izvajanja in s tem povezano dokumentacijo, ter šifrirni material;

(d) „preklic stopnje tajnosti“ pomeni odstranitev vsakršne stopnje tajnosti;

(e) „dokument“ pomeni vse shranjene podatke, ne glede na njihovo fizično obliko ali značilnosti;

(f) „znižanje stopnje tajnosti“ pomeni razvrstitev v nižjo stopnjo tajnosti;

(g) „varnostno dovoljenje organizacije“ je uradna izjava katerega koli pristojnega varnostnega organa, da lahko določena organizacija iz varnostnega vidika nudi ustrezno stopnjo varovanja tajnih podatkov EU do določene stopnje tajnosti;

(h) „obravnavanje“ tajnih podatkov EU pomeni vse možne dejavnosti, v katere so vključeni tajni podatki EU skozi celotni življenjski cikel: ustvarjanje, vpis v register, obdelavo, prenašanje, znižanje stopnje tajnosti, preklic tajnosti in uničenje. V zvezi s komunikacijskimi in informacijskimi sistemi zajema tudi njihovo zbiranje, prikaz, razpošiljanje in hrambo;

[2] Uredba št. 31 (EGS) o določitvi Kadrovskih predpisov za uradnike in Pogojev za zaposlitev drugih uslužbencev, kakor je bila spremenjena, UL 01962R0031-01.01.2020-019.003-1 (https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:01962R0031-20200101&qid=1624620186104&from=en).

(i) „imetnik podatkov“ pomeni ustrezno pooblaščenega posameznika, za katerega je ugotovljena potreba po seznanitvi in ki razpolaga s tajnimi podatki ter je zato odgovoren za njihovo varovanje;

(j) „organ za informacijsko varnost“ pomeni uradnika Računskega sodišča za informacijsko varnost, ki lahko naloge iz tega sklepa v celoti ali delno prenese;

(k) „podatek“ pomeni vsak pisni ali ustni podatek, ne glede na vrsto nosilca ali avtorja;

(l) „gradivo“ pomeni vsak medij, nosilec podatkov ali stroj ali oprema;

(m) „organ izvora“ pomeni institucijo, organ ali agencijo EU, državo članico, tretjo državo ali mednarodno organizacijo, v pristojnosti katere so podatki nastali in/ali bili vneseni v strukture EU;

(n) „dovoljenje za dostop do tajnih podatkov“ (PSC) pomeni izjavo pristojnega organa države članice, sprejeto po končani varnostni preiskavi, ki jo opravijo pristojni organi države članice in s katero je potrjeno, da se posameznik lahko pooblasti za dostop do tajnih podatkov EU do določene stopnje (CONFIDENTIEL UE/EU CONFIDENTIAL ali višje) in do določenega datuma, če je bila ugotovljena potreba po njegovi seznanitvi in če je bil ustrezno poučen o svoji odgovornosti;

(o) „potrdilo za dostop do tajnih podatkov“ pomeni potrdilo, ki ga izda direktor direktorata Računskega sodišča za kadrovske, finančne in splošne zadeve in ki dokazuje, da je posameznik imetnik veljavnega dovoljenja ali pooblastila za dostop do tajnih podatkov, ter na katerem je navedena stopnja tajnosti podatkov EU, do katere se lahko posamezniku odobri dostop (CONFIDENTIEL UE/EU CONFIDENTIAL ali višje), obdobje veljavnosti tega dovoljenja ali pooblastila za dostop do tajnih podatkov in datum izteka veljavnosti samega potrdila;

(p) „organ za fizično varnost“ pomeni vodjo varnostne službe Računskega sodišča, ki je odgovoren za izvajanje potrebnih ukrepov za fizično varnost in postopkov za varovanje tajnih podatkov EU;

(q) „urad za vodenje evidenc“ vodi sekretariat Sodišča, nahaja pa se v upravnem območju v pristojnosti direktorja direktorata Računskega sodišča za človeške vire, finance in splošne storitve. Odgovoren je za vstop in izstop podatkov stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje, izmenjanih z Računskim sodiščem;

(r) „register tajnih podatkov EU“ je območje, vzpostavljeno znotraj varovanega območja. Ta register upravlja varnostno preverjen in pooblaščen nadzorni uradnik registra Računskega sodišča. Odgovoren je za vstop in izstop podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, ali enakovredne stopnje, izmenjanih z Računskim sodiščem;

(s) „organ za varnostno akreditacijo“ pomeni direktorja direktorata Računskega sodišča za kadrovske, finančne in splošne zadeve.

Člen 3 Ukrepi za varovanje tajnih podatkov EU

(1) Računsko sodišče zagotovi varovanje vseh tajnih podatkov, ki so mu bili posredovani, na način, ki je sorazmeren s stopnjo tajnosti, ki jo določi organ izvora, in skladno s tem sklepom.

(2) V ta namen Računsko sodišče za obravnavanje tajnih podatkov EU uporablja ukrepe za fizično varnost in po potrebi ukrepe v zvezi z varnostnimi obveznostmi osebja vključno s pooblastili za dostop za identificirane osebe ter ukrepi za varovanje komunikacijskih in informacijskih sistemov. Ti ukrepi so opisani v členih 4 do 6 in se uporabljajo v celotnem življenjskem ciklu tajnih podatkov EU. So sorazmerni s stopnjo tajnosti, obliko in obsegom podatkov ali gradiva, krajem in strukturo objektov, kjer se hranijo tajni podatki EU, ter lokalno oceno grožnje

zlonamernih in/ali kriminalnih dejavnosti, vključno z nevarnostjo vohunstva, sabotaže in terorizma.

(3) Tajni podatki EU se varujejo z ukrepi za fizično varnost, podatki stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje pa se dodatno varujejo z ukrepi v zvezi z varnostnimi obveznostmi osebja.

(4) Tajni podatki EU se lahko posredujejo le osebam v instituciji, ki morajo biti seznanjene z njimi. Imetnik tajnega podatka EU ga mora varovati v skladu s tem sklepom.

(5) Tajni podatki EU se ne smejo razkriti ustno ali pisno. Predhodne ugotovitve, poročila, mnenja, sporočila za javnost in drugi izdelki Računskega sodišča, njegovo spletišče in intranet, ustni prispevki, odgovori na zahteve za dostop do dokumentov[3] ter glasovni ali video posnetki ne smejo vsebovati tajnih podatkov EU ali njihovih izvlečkov ali se nanje sklicevati. Kadar je organ izvora objavil dokumente ali informacije, ki vsebujejo sklic na tajne podatke EU, se ta sklic lahko navede.

(6) Ne glede na odstavek 5 se Računsko sodišče in organ izvora lahko dogovorita, da lahko Računsko sodišče v primeru specifične revizije v dokumentu reproducira ali uporabi elemente tajnih podatkov EU. V takem primeru se dokument Računskega sodišča najprej pošlje organu izvora zadevnih tajnih podatkov EU pred ali med kontradiktornim postopkom. Računsko sodišče in organ izvora se dogovorita, ali naj se dokument Računskega sodišča označi za tajnega. Kadar član Računskega sodišča, ki je poročevalec, meni, da je revizijsko poročilo, ki je bilo v celoti ali delno označeno kot tajno, treba poslati nekaterim naslovnikom v Evropskem parlamentu ali Svetu (ob upoštevanju vseh varnostnih ukrepov v skladu s tem sklepom), je za to potrebno soglasje organa izvora tajnih podatkov. Pravni okvir in postopek za izmenjavo takih dokumentov sta določena v členu 7.

(7) Kadar se zaradi izvajanja mandata Računskega sodišča zahteva širša izmenjava nekaterih elementov tajnega dokumenta ali podatkov, se Računsko sodišče ob ustreznem upoštevanju oznake stopnje tajnosti posvetuje z organom izvora, preden se odloči za uporabo teh elementov ali informacij, če meni, da za to obstaja prevladujoči javni interes. V poročilu se podatki uporabijo samo tako, da ni mogoče škodovati interesu organa izvora. Tega je mogoče ustrezno zaščititi tako, da se organ izvora zaprosi za predložitev pripomb, da bi se dosegel dogovor o načinu anonimizacije, zgostitve ali posploševanja podatkov itd., ob upoštevanju interesov tistih, ki jih objavljeni podatki najbolj zadevajo.

(8) Računsko sodišče tajnih podatkov EU ne posreduje drugi instituciji, agenciji, organu ali uradu EU, državi članici, tretji državi ali mednarodni organizaciji brez predhodnega posvetovanja in izrecnega pisnega soglasja organa izvora.

(9) Razen kadar organ izvora dokumenta stopnje SECRET UE/EU SECRET ali nižje omeji njegovo kopiranje ali prevod, se takšni dokumenti na zahtevo imetnika lahko kopirajo ali prevajajo v skladu s praktičnimi navodili za delo organa Računskega sodišča za informacijsko varnost. Varnostni ukrepi, ki veljajo za izvorni dokument, veljajo tudi za njegove kopije in prevode.

(10) Kadar Računsko sodišče želi, da se za tajni dokument, ki ga je prejelo ali za dostop do katerega je pooblaščeno, zniža stopnja tajnosti ali se ta prekliče, se posvetuje z organom izvora in poizve, ali lahko slednji zagotovi različico dokumenta, za katero je bila stopnja tajnosti znižana ali preklicana.

---

[3] V skladu s Sklepom Računskega sodišča št. 12-2005 o dostopu javnosti do dokumentov Sodišča, kakor je bil spremenjen s Sklepom št. 14-2009 (UL 2009/C 67/1).

Člen 4 **Varnostne obveznosti osebja**

(1) Člani Računskega sodišča so na podlagi svojih funkcij pooblaščeni za dostop do vseh tajnih podatkov EU in za sodelovanje na sestankih, na katerih se tajni podatki EU obravnavajo. Člani se obvestijo o svojih varnostnih obveznostih glede varovanja tajnih podatkov EU in pisno potrdijo svojo odgovornost za varovanje takih podatkov.

(2) Uslužbencu Računskega sodišča, bodisi uradniku bodisi uslužbencu, za katerega veljajo pogoji za zaposlitev drugih uslužbencev, ali napotenemu nacionalnemu strokovnjaku, se dostop do tajnih podatkov EU odobri šele potem, ko:

i. je bila ugotovljena potreba po seznanitvi;

ii. je bil poučen o varnostnih pravilih za varovanje tajnih podatkov EU ter relevantnih varnostnih standardih in smernicah ter je pisno sprejel odgovornost za varovanje teh podatkov;

iii. je bil, v primeru podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, varnostno preverjen in pooblaščen za dostop.

(3) Postopek za določitev, ali se uradniku ali drugemu uslužbencu Računskega sodišča lahko dovoli dostop do podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, ob upoštevanju lojalnosti, integritete in zanesljivosti posameznika ter po pridobitvi zagotovila pristojnih organov države članice iz člena 2(n), se določi v delegiranem sklepu, ki se sprejme v skladu s členom 10(10). Odločitve o odobritvi dostopa sprejme direktor direktorata Računskega sodišča za kadrovske, finančne in splošne zadeve.

(4) Direktor direktorata Računskega sodišča za kadrovske, finančne in splošne zadeve lahko izda potrdilo za dostop do tajnih podatkov, v katerem je določena stopnja tajnosti, za katero se posameznikom lahko odobri dostop do tajnih podatkov EU (CONFIDENTIEL UE/EU CONFIDENTIAL ali višje), obdobje veljavnosti zadevnega pooblastila za dostop in datum poteka njegove veljavnosti.

(5) Sestankov, na katerih se obravnavajo podatki stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, se lahko udeležijo samo osebe s pooblastilom iz odstavka 2(iii) zgoraj in člani Računskega sodišča v skladu z odstavkom 1 zgoraj. Računsko sodišče in organ izvora sprejmeta praktične ureditve za takšne sestanke za vsak primer posebej.

(6) Oddelki Računskega sodišča, ki so odgovorni za organizacijo sestankov, na katerih se obravnavajo podatki stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, pravočasno obvestijo organ za informacijsko varnost o datumih, urah in krajih sestankov ter mu predložijo sezname udeležencev.

(7) Vsak posameznik, ki ima tajne podatke EU brez ustreznega pooblastila in/ali brez dokazane potrebe po seznanitvi, mora to čim prej sporočiti organu za informacijsko varnost in zagotoviti, da so tajni podatki EU varovani, kot je določeno v tem sklepu.

Člen 5 **Ukrepi fizične varnosti za varovanje tajnih podatkov**

(1) „Fizična varnost“ pomeni uporabo fizičnih in tehničnih ukrepov varovanja za preprečitev nepooblaščenega dostopa do tajnih podatkov EU.

(2) Namen ukrepov fizične varnosti je vsiljivcem preprečiti skriven vstop ali vstop na silo, odvrniti, zadržati in odkriti nedovoljena dejanja ter omogočiti ločevanje uslužbencev pri dostopu do

tajnih podatkov EU glede na potrebo po seznanitvi. Ti ukrepi se določijo na podlagi postopka obvladovanja tveganja v skladu s tem sklepom.

(3) Pristojni organ Računskega sodišča za varnost redno pregleduje območja, v katerih se obravnavajo tajni podatki EU ali v katerih se ti hranijo.

(4) Za obravnavanje tajnih podatkov EU in njihovo hrambo se uporabljajo le oprema ali naprave, ki so skladni s pravili, ki se v institucijah, agencijah ali organih EU uporabljajo za varovanje tajnih podatkov EU.

(5) Uslužbenci Računskega sodišča lahko dostopajo do tajnih podatkov EU stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje ali enakovredne stopnje v varovanih območjih izven prostorov Računskega sodišča.

(6) Računsko sodišče lahko sklene sporazum o ravni storitve z drugo institucijo EU v Luxembourgu, da bi se omogočila obravnavanje in hramba podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje v varovanem območju te institucije. Razen z izrecnim dovoljenjem organa izvora se ti tajni podatki EU ne smejo obravnavati ali hraniti v prostorih Računskega sodišča, Računsko sodišče pa jih ne sme kopirati ali prevajati.

(7) Računsko sodišče evidentira podatke stopnje RESTREINT UE/EU RESTRICTED, ki jih prejme. Vpogled v podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje ali enakovredne stopnje izven prostorov Računskega sodišča se iz varnostnih razlogov vpiše v register.

(8) Tajni podatki EU stopnje RESTREINT UE/EU RESTRICTED se lahko hranijo v ustrezno zaklenjenih pisarniških omarah v upravnem območju ali varovanem območju. Tajni podatki EU stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET se v skladu s sporazumom o ravni storitve hranijo v varnostnem vsebniku v varovanem območju druge institucije EU v Luksemburgu.

(9) Kadar tajni podatki EU niso v registru, se med oddelki in prostori prenašajo na naslednji način:

(a) praviloma se tajni podatki EU pošiljajo z elektronskimi sredstvi, ki so zaščiteni s šifrirnimi izdelki, odobrenimi v skladu s členom 6(8);

(b) kadar se tajni podatki EU ne pošiljajo, kot je opisano v točki (a), se posredujejo na nosilcih podatkov (npr. ključi USB, zgoščenke, trdi diski), ki so zaščiteni s šifrirnimi izdelki, odobrenimi v skladu s členom 6(8), ali kot papirna kopija v neprozorni zapečateni ovojnici.

(10) Imetnik lahko tajne podatke stopnje RESTREINT UE/EU RESTRICTED uniči v skladu s pravili o arhiviranju, ki veljajo na Računskem sodišču. Podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje uniči samo nadzorni uradnik registra, in sicer po navodilu imetnika ali pristojnega organa v skladu s pravili o arhiviranju, ki veljajo na Računskem sodišču. Dokumenti stopnje SECRET UE/EU SECRET se uničijo v prisotnosti priče, ki ima dovoljenje za dostop do tajnih podatkov vsaj do stopnje tajnosti dokumenta, ki se uničuje. Nadzorni uradnik registra in priča, kadar mora biti prisotna, podpišeta zapisnik o uničenju, ki se shrani v register. Nadzorni uradnik registra zapisnik o uničenju dokumentov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET hrani vsaj pet let.

(11) Organ za fizično varnost in organ za informacijsko varnost ob upoštevanju lokalnih razmer pripravita skupni načrt za varovanje tajnih podatkov EU v kriznih časih, po potrebi vključno z načrti za uničenje ali evakuacijo v nujnih primerih. Organa izdata navodila, ki se jima zdijo potrebna, da se prepreči, da bi tajni podatki EU prišli v roke nepooblaščenim osebam.

(12) Kadar je treba tajne podatke EU fizično prevažati, Računsko sodišče upošteva ukrepe, ki jih določi organ izvora, da se podatki zavarujejo pred nepooblaščenim razkritjem med prevozom.

(13) Ukrepi fizične varnosti, ki se uporabljajo na upravnih območjih, kjer se obravnavajo in shranjujejo podatki stopnje RESTREINT UE/EU RESTRICTED, so določeni v Prilogi.

Člen 6 **Varovanje tajnih podatkov EU v komunikacijskih in informacijskih sistemih**

(1) Za namene tega člena „komunikacijski in informacijski sistem“ pomeni sistem, ki omogoča obravnavanje tajnih podatkov EU v elektronski obliki. Komunikacijski in informacijski sistem zajema vse sestavne dele, potrebne za njegovo delovanje, tudi infrastrukturo, organizacijo, osebje in informacijske vire.

(2) „Zakoniti uporabnik“ pomeni člana, uradnika, drugega uslužbenca Računskega sodišča ali napotenega nacionalnega strokovnjaka, za katerega je bilo ugotovljeno in potrjeno, da potrebuje dostop do določenega informacijskega sistema.

(3) Računsko sodišče zagotovi, da bodo podatki, ki se obravnavajo v njegovih sistemih, ustrezno varovani, ter da bodo sistemi pod nadzorom zakonitih uporabnikov delovali tako, kot morajo in kadar morajo. Zato se s sistemi zagotavljajo ustrezne stopnje:

- avtentičnosti: zagotovilo, da so podatki pravi in iz zaupanja vrednih virov,
- razpoložljivosti: podatki so dostopni ter na voljo za uporabo na zahtevo pooblaščenega subjekta,
- zaupnosti: podatki se ne razkrijejo nepooblaščenim posameznikom in subjektom ali ne uporabijo v postopkih, v katerih to ni dovoljeno,
- celovitosti: zagotavljanje točnosti in popolnosti sestavnih delov in podatkov,
- nezatajljivosti: zmožnost dokazati, da se je dejanje zgodilo ali da je prišlo do dogodka, tako da tega kasneje ni mogoče zanikati.

To zagotovilo temelji na postopku obvladovanja tveganja. „Tveganje“ pomeni možnost, da se zaradi notranje ali zunanje ranljivosti organizacije ali katerega koli sistema, ki ga uporablja, uresniči določena grožnja, kar lahko škodi organizaciji in njenim opredmetenim ali neopredmetenim sredstvom. Meri se kot kombinacija verjetnosti pojava groženj in njihovega učinka. Postopek obvladovanja tveganja vključuje naslednje stopnje: prepoznavanje groženj in ranljivosti, oceno tveganja, obravnava tveganja, prevzemanje tveganja in obveščanje o tveganju:

- „ocena tveganja“ zajema opredelitev groženj in ranljivosti ter izvedbo s tem povezane analize tveganja, tj. oceno verjetnosti in učinka,
- „obravnava tveganja“ zajema ublažitev tveganja, njegovo odpravo, zmanjšanje (z ustrezno kombinacijo tehničnih, fizičnih, organizacijskih ali postopkovnih ukrepov), prenos ali spremljanje,
- „prevzemanje tveganja“ je odločitev, da se sprejme prisotnost preostalega tveganja, potem ko se je poskušalo tveganje obravnavati,
- „preostalo tveganje“ pomeni tveganje, ki je še vedno prisotno, potem ko so bili izvedeni varnostni ukrepi, saj vseh groženj ni mogoče preprečiti in vseh ranljivosti ni mogoče odpraviti,
- „obveščanje o tveganju“ zajema ozaveščanje skupnosti uporabnikov komunikacijskega in informacijskega sistema o tveganjih, obveščanje organov za odobritev o takih tveganjih in poročanje o takih tveganjih operativnim organom.

(4) Vse elektronske naprave in oprema, ki se uporabljajo za obravnavanje tajnih podatkov EU, so skladne s pravili, ki se uporabljajo za varovanje tajnih podatkov EU. Prednost imajo elektronske

naprave in oprema, ki so že bile akreditirane pri drugi instituciji, agenciji ali organu EU. Naprave morajo biti zajamčeno varne v celotnem življenjskem ciklu.

(5) Komunikacijski in informacijski sistem Računskega sodišča za obravnavanje tajnih podatkov EU akreditira ustrezen organ. Računsko sodišče za to zaprosi za sklenitev sporazuma o ravni storitve z organom za varnostno akreditacijo institucije EU, ki ima pristojnosti za akreditacijo komunikacijskih in informacijskih sistemov, v katerih se obravnavajo tajni podatki EU, da bi prejelo izjavo o akreditaciji za podatke stopnje RESTREINT UE/EU RESTRICTED, ki se lahko obravnavajo v komunikacijskih in informacijskih sistemih Računskega sodišča, ter ustrezne pogoje za delovanje. Sporazum o ravni storitve vsebuje tudi sklic na standarde, ki se uporabljajo za akreditacijski postopek, sklene pa se v skladu s postopkom iz člena 10(3).

(6) Kadar mora Računsko sodišče za svoj komunikacijski in informacijski sistem vzpostaviti lasten postopek akreditacije, se z delegiranim sklepom iz člena 10(10) tega sklepa vzpostavi postopek v skladu s standardi o postopku akreditacije za komunikacijske in informacijske sisteme, v katerih se obravnavajo tajni podatki EU, v drugih institucijah, agencijah in organih EU.

(7) Odgovornost za pripravo akreditacijskih datotek in dokumentacije v skladu z veljavnimi standardi ostane v domeni lastnika komunikacijskega in informacijskega sistema.

(8) Kadar se tajni podatki EU varujejo s šifrirnimi izdelki, Računsko sodišče da prednost izdelkom, ki jih je odobril Svet ali generalni sekretar Sveta v svoji funkciji kot organ za odobritev šifrirnih metod in izdelkov, ali izdelkom, ki so jih za varovanje tajnih podatkov EU odobrile druge institucije, agencije in organi EU.

(9) Podatki stopnje RESTREINT UE/EU RESTRICTED se obravnavajo samo na elektronskih napravah (kot so delovne postaje, tiskalniki, fotokopirni stroji), ki se nahajajo v upravnem območju ali varovanem območju. Elektronske naprave, s katerimi se obravnavajo podatki stopnje RESTREINT UE/EU RESTRICTED, so ločene od drugih računalniških omrežij in varovane z ustreznimi fizičnimi ali tehničnimi ukrepi.

(10) Vsi uslužbenci Računskega sodišča, ki so vključeni v oblikovanje, razvoj, preskušanje, obratovanje, upravljanje ali uporabo komunikacijskih in informacijskih sistemov za obravnavanje tajnih podatkov EU, uradnika za informacijsko varnost obvestijo o vseh morebitnih varnostnih pomanjkljivostih, incidentih in kršitvah v zvezi z varnostjo ali nepooblaščenim razkritjem, ki bi lahko vplivali na varovanje komunikacijskih in informacijskih sistemov in/ali tajnih podatkov EU v njih.

Člen 7 Postopek za izmenjavo tajnih podatkov in omogočanje dostopa do njih

(1) V primeru zakonske obveznosti na podlagi Pogodb ali pravnih aktov, sprejetih na podlagi Pogodb, institucije, agencije, organi in uradi EU ter nacionalni organi na lastno pobudo ali na pisno zahtevo predsednika, člana(-ov) poročevalca(-ev) ali generalnega sekretarja omogočijo Računskemu sodišču dostop do tajnih podatkov EU v skladu s postopkom, opisanim spodaj.

(2) Zahteve za dostop se zadevnim institucijam pošljejo prek urada Računskega sodišča za vodenje evidenc.

(3) Računsko sodišče po potrebi sklene upravni dogovor, v katerem so zajeti praktični vidiki izmenjave tajnih podatkov EU ali enakovrednih informacij.

(4) Računsko sodišče zaradi sklenitve takšnih upravnih dogovorov zagotovi organu izvora vse potrebne informacije o svojem sistemu informacijske varnosti. Po potrebi se lahko organizira ocenjevalni obisk.

(5) Ti upravni dogovori se sklenejo ob polnem spoštovanju načel prenosa pristojnosti in lojalnega sodelovanja iz člena 13 Pogodbe o Evropski uniji. Sklenejo se v skladu s postopkom iz člena 10(4).

(6) Kadar z določeno institucijo, organom ali agencijo EU, tretjo državo ali mednarodno organizacijo ni bil sklenjen upravni dogovor o zagotavljanju tajnih podatkov Računskemu sodišču, slednje podpiše izjavo o zavezi, da bo varovalo prejete tajne podatke.

Člen 8 **Kršitev varovanja tajnosti, izguba ali nepooblaščeno razkritje tajnih podatkov**

(1) Kršitev varovanja tajnosti pomeni posameznikovo dejanje ali opustitev dejanja, ki je v nasprotju z varnostnimi pravili iz tega sklepa in njegovih izvedbenih pravil.

(2) Do nepooblaščenega razkritja pride, če so tajni podatki kot posledica kršitve varovanja tajnosti v celoti ali delno razkriti nepooblaščenim osebam.

(3) O vseh kršitvah ali domnevnih kršitvah varovanja tajnosti se nemudoma obvesti organ za informacijsko varnost Računskega sodišča.

(4) Če je bilo ugotovljeno ali če obstajajo utemeljeni razlogi za domnevo, da so bili tajni podatki EU nepooblaščeno razkriti ali izgubljeni, organ za informacijsko varnost obvesti direktorja direktorata Računskega sodišča za kadrovske, finančne in splošne zadeve ter generalnega sekretarja Računskega sodišča. Direktor direktorata za kadrovske, finančne in splošne zadeve nemudoma obvesti zadevni varnostni organ organa izvora. Zgoraj omenjeni direktor direktorata Računskega sodišča opravi preiskavo ter generalnega sekretarja Računskega sodišča in varnostni organ organa izvora obvesti o rezultatih in ukrepih, sprejetih za preprečitev ponovitve dogodka. Kadar gre za člana Računskega sodišča, je za ukrepanje odgovoren predsednik Računskega sodišča v sodelovanju z generalnim sekretarjem Računskega sodišča.

(5) Uradnikom ali drugim uslužbencem Računskega sodišča, ki so odgovorni za kršitev varnostnih pravil iz tega sklepa in njegovih izvedbenih pravil, se lahko naložijo kazni, določene v kadrovskih predpisih in pogojih za zaposlitev drugih uslužbencev Evropske unije.

(6) Član Računskega sodišča, ki ne ravna v skladu s pravili iz tega sklepa, se lahko kaznuje z ukrepi in kaznimi, določenimi v členu 286(6) Pogodbe.

(7) Zoper vsakega posameznika, ki je odgovoren za izgubo ali nepooblaščeno razkritje tajnih podatkov EU, se lahko uvede disciplinski in/ali kazenski postopek v skladu z veljavnimi zakoni, pravili in predpisi.

Člen 9 **Varnost v primeru zunanjega posredovanja**

(1) Računsko sodišče lahko izvajanje nalog, ki vključujejo ali zahtevajo dostop do tajnih podatkov EU, na podlagi pogodbe naloži izvajalcem, registriranim v državi članici. To se lahko zgodi zlasti v zvezi z vzdrževanjem komunikacijskih in informacijskih sistemov ter računalniškega omrežja.

(2) V primeru zunanjega posredovanja Računsko sodišče sprejme vse potrebne varnostne ukrepe iz odstavka 3 tega člena, vključno z zahtevo po varnostnem dovoljenju organizacije, da se zagotovi, da kandidati in ponudniki varujejo tajne podatke EU med celotnim trajanjem postopka javnega razpisa in postopka javnega naročanja, izvajalci in podizvajalci pa med celotnim trajanjem pogodbe. Javni naročnik zagotovi, da so v pogodbah navedeni minimalni varnostni standardi iz tega sklepa, s čimer se od izvajalcev zahteva, da jih upoštevajo.

(3) Varnostna pravila, postopki javnega naročanja ter predloge in vzorci za izvajalske pogodbe in podizvajalske pogodbe, ki vključujejo dostop do tajnih podatkov EU, obvestila o javnih naročilih, smernice o okoliščinah, v katerih se zahteva varnostno dovoljenje organizacije in dovoljenje osebja za dostop do tajnih podatkov, navodila za varnost programa ali projekta, listine o varnostnih vidikih, obiski ter pošiljanje in prevoz tajnih podatkov EU v okviru takih izvajalskih in podizvajalskih pogodb, so skladni s pravili, predlogami in vzorci, ki jih je Evropska komisija določila za pogodbe s tajnimi podatki v Sklepu Komisije (EU, Euratom) 2015/444 z dne 13. marca 2015 o varnostnih predpisih za varovanje tajnih podatkov EU.

<u>Člen 10</u> Izvajanje sklepa in odgovornosti, povezane z njim

(1) Oddelki Računskega sodišča sprejmejo vse potrebne ukrepe v okviru svojih odgovornosti, da bi zagotovili, da se pri obravnavanju tajnih podatkov EU oziroma kakršnih koli drugih tajnih podatkov ali njihovi hrambi uporabljajo ta sklep in zadevna izvedbena pravila.

(2) Generalni sekretar je organ za imenovanja in organ, pooblaščen za sklepanje pogodb o zaposlitvi vseh uradnikov in drugih uslužbencev. Generalni sekretar lahko na direktorja direktorata za kadrovske, finančne in splošne zadeve prenese odgovornost za izdajo pooblastil za dostop do podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje uradnikom in drugem uslužbencem, za opravljanje funkcije organa za varnostno akreditacijo in za nadzor sekretariata Sodišča v zvezi z obravnavanjem tajnih podatkov EU.

(3) Generalni sekretar je pristojen za sklepanje sporazumov o ravni storitve v zvezi z akreditacijo komunikacijske in informacijske opreme in sistemov Računskega sodišča, uporabo varovanega območja v drugi instituciji EU in zahtevki za izdajo dovoljenj za dostop do tajnih podatkov EU.

(4) Direktor direktorata za kadrovske, finančne in splošne zadeve je pristojen za sklepanje upravnih dogovorov z institucijami, agencijami in drugimi organi EU v zvezi z izmenjavo tajnih podatkov EU, ki jih Računsko sodišče potrebuje za izvajanje svojega mandata. Ta direktor lahko sklene tudi upravne dogovore o varovanju prejetih tajnih podatkov s tretjimi državami ali mednarodnimi organizacijami.

(5) Direktor direktorata za kadrovske, finančne in splošne zadeve je pristojen za podpis izjav o zavezi za varovanje tajnih podatkov EU, ki se predložijo v okviru *ad hoc* posredovanja tajnih podatkov EU v izjemnih primerih.

(6) Uradnik za informacijsko varnost na Računskem sodišču deluje kot organ za informacijsko varnost. Uradnik za informacijsko varnost in osebe, na katere ta prenese vse ali del svojih nalog, imajo ustrezno dovoljenje za dostop do tajnih podatkov. Organ za informacijsko varnost prevzame svoje odgovornosti v tesnem sodelovanju z direktoratom za kadrovske, finančne in splošne zadeve, direktoratom za informatiko, delovno okolje in inovacije ter direktoratom odbora za nadzor kakovosti revizij (glej zlasti člene 4, 6 in 8). Organ za informacijsko varnost je odgovoren tudi za usposabljanje in sestanke v zvezi ozaveščanjem o informacijski varnosti ter za redne inšpekcijske preglede zaradi preverjanja skladnosti s tem sklepom, tudi v primeru zunanjega posredovanja, in vse ukrepe, ki jih je treba sprejeti za zagotovitev skladnosti.

(7) Vodja varnostne službe je odgovoren za ukrepe fizične varnosti (zlasti člen 5).

(8) Urad za vodenje evidenc, ustanovljen v okviru sekretariata Sodišča, je vstopna in izstopna točka za tajne podatke stopnje RESTREINT UE/EU RESTRICTED, ki si jih Računsko sodišče lahko izmenjuje z drugimi institucijami, agencijami in organi EU ter državami članicami. Je tudi vstopna in izstopna točka za enakovredne podatke tretjih držav in mednarodnih organizacij. Urad za vodenje evidenc je organiziran, kot je določeno v delegiranem sklepu. Vodja urada za vodenje evidenc prevzame naslednje glavne odgovornosti:

a) evidentiranje vstopa in izstopa tajnih podatkov stopnje RESTREINT UE/EU RESTRICTED;

b) upravljanje namenskih upravnih območij za evidentiranje obravnavanja tajnih podatkov EU stopnje RESTREINT UE/EU RESTRICTED, njihovega shranjevanja in vpogleda vanje.

(9) V okviru sporazuma o ravni storitve se vzpostavi register o uporabi varovanega območja drugih institucij EU. Ta register, ki ga organizira sekretariat Sodišča pod pristojnostjo direktorja direktorata Računskega sodišča za kadrovske, finančne in splošne zadeve, je vstopna in izstopna točka za podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, ki si jih Računsko sodišče lahko izmenja z drugimi institucijami, agencijami in organi EU ter državami članicami. Je tudi vstopna in izstopna točka za enakovredne podatke tretjih držav in mednarodnih organizacij. Opremljen je z ustreznimi sefi in drugo varnostno opremo, ki je primerna za varovanje podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje. Register je organiziran, kot je določeno v delegiranem sklepu. Nadzorni uradnik registra ima ustrezno dovoljenje za dostop do tajnih podatkov in prevzame naslednje glavne odgovornosti:

(a) vodenje postopkov v zvezi z vpisom v register, ohranjanjem, razmnoževanjem, prevajanjem, razpošiljanjem in odpremljanjem tajnih podatkov EU in vpogledom vanje ter, kadar je primerno, uničevanjem tajnih podatkov EU;

(b) vse druge naloge v zvezi z varovanjem tajnih podatkov EU, opredeljene v delegiranem sklepu.

(10) Upravni odbor sprejme delegirani sklep, s katerim določi izvedbena pravila za ta sklep. Uradnik za informacijsko varnost pripravi smernice za informacijsko varnost. Odbor za kontrolo kakovosti revizij pripravi revizijske smernice.

<u>Člen 11</u> Začetek veljavnosti

Ta sklep začne veljati dan po objavi v Uradnem listu Evropske unije.

V Luxembourgu, 3. junija 2021

Za Evropsko računsko sodišče

Klaus-Heiner Lehne
predsednik

Priloga: UKREPI FIZIČNE VARNOSTI V ZVEZI Z UPRAVNIMI OBMOČJI ZA TAJNE PODATKE EU

PRILOGA

UKREPI FIZIČNE VARNOSTI
V ZVEZI Z UPRAVNIMI OBMOČJI ZA TAJNE PODATKE EU

(1) V tej prilogi so določena pravila za izvajanje člena 5 te odločbe. To so minimalna pravila za fizično varovanje upravnih območij za podatke stopnje RESTREINT UE/EU RESTRICTED na Računskem sodišču: območja, ki so določena za evidentiranje, shranjevanje podatkov stopnje RESTREINT UE/EU RESTRICTED in vpogled vanje.

(2) Namen ukrepov fizične varnosti na upravnih območjih je preprečiti nepooblaščen dostop do teh območij, in sicer tako:

(a) vzpostavi se vidno določen varnostni perimeter, s katerim se omogoča preverjanje posameznikov;

(b) dostop brez spremstva se odobri samo posameznikom, ki jih ustrezno pooblasti organ Računskega sodišča za informacijsko varnost ali drug pristojni organ;

(c) vsi drugi posamezniki imajo ves čas spremstvo ali so pod enakovrednim nadzorom.

(3) Organ Računskega sodišča za informacijsko varnost lahko izjemoma odobri dostop nepooblaščenim osebam, tudi za delo v upravnem območju, če to ne vključuje dostopa do tajnih podatkov EU, ki ostanejo zaklenjeni. Te osebe lahko vstopijo le, če jih spremlja in stalno nadzoruje organ za informacijsko varnost ali nadzorni uradnik za evidence.

(4) Organ za informacijsko varnost določi postopke za upravljanje ključev in/ali nastavitev kombinacij za vsa upravna območja in zavarovano pohištvo. Ti postopki so namenjeni zaščiti pred nepooblaščenim dostopom.

(5) Nastavitve kombinacij si zapomni najmanjše možno število oseb, ki jih morajo poznati. Nastavitve kombinacij za zavarovano pohištvo, ki se uporablja za shranjevanje podatkov stopnje RESTREINT UE/EU RESTRICTED, se spremenijo:

- ob prejemu novega kosa zavarovanega pohištva,
- vsakič ko pride do menjave uslužbenca, ki pozna kombinacijo;
- ob vsakem nepooblaščenem razkritju kombinacije ali sumu razkritja kombinacije;
- po vsaki izvedbi vzdrževanja ali popravilu ključavnice;
- najmanj vsakih 12 mesecev.

(6) Za spoštovanje teh pravil sta odgovorna organ za informacijsko varnost in vodja varnostne službe.