EUROPSKI
REVIZORSKI
SUD

**Odluka Revizorskog suda br. 41-2021 o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a (EUCI)**

**EUROPSKI REVIZORSKI SUD,**

UZIMAJUĆI U OBZIR članak 13. Ugovora o Europskoj uniji,

UZIMAJUĆI U OBZIR članak 287. Ugovora o funkcioniranju Europske unije (UFEU),

UZIMAJUĆI U OBZIR članak 257. Uredbe (EU, Euratom) 2018/1046 Europskog parlamenta i Vijeća od 18. srpnja 2018. o financijskim pravilima koja se primjenjuju na opći proračun Unije,

UZIMAJUĆI U OBZIR članak 1. stavak 6. pravila za provedbu Poslovnika Revizorskog suda (Odluka Revizorskog suda br. 21-2021),

UZIMAJUĆI U OBZIR sigurnosne propise za zaštitu klasificiranih podataka EU-a koje su utvrdile druge institucije, agencije i tijela EU-a,

UZIMAJUĆI U OBZIR politiku informacijske sigurnosti (DEC 127/15 FINAL) i politiku klasifikacije informacija na Revizorskom sudu (Obavijest za osoblje br. 123/2020),

BUDUĆI DA u skladu s člankom 287. stavkom 3. UFEU-a Revizorski sud ima pravo na pristup svim relevantnim dokumentima i informacijama koje smatra potrebnima za izvršavanje svojih zadaća, uključujući klasificirane podatke EU-a, koje se izvršavaju uz potpuno poštovanje načela lojalne suradnje među institucijama i načela dodjeljivanja; autor klasificiranih podataka EU-a ne može dovesti u pitanje pravo Revizorskog suda na pristup tim podatcima, koje je zajamčeno UFEU-om, ali od Revizorskog suda može se zatražiti da uvede određene sigurnosne mjere i da ih se pridržava, kako je detaljno opisano u ovoj Odluci;

BUDUĆI DA članovi Revizorskog suda te njegovi dužnosnici i ostalo osoblje, čak i nakon odlaska iz službe, moraju poštovati obvezu povjerljivosti u skladu s člankom 339. UFEU-a, člankom 17. Pravilnika o osoblju i aktima donesenima na temelju njih;

BUDUĆI DA je s obzirom na osjetljivu prirodu klasificiranih podataka EU-a pri postupanju s takvim podatcima potrebno zajamčiti poštovanje obveze povjerljivosti primjenom sigurnosnih mjera kojima se može jamčiti visoka razina zaštite tih podataka i koje su istovjetne onima koje su utvrđene propisima o zaštiti klasificiranih podataka EU-a koje su donijele druge institucije, agencije i tijela EU-a, pri čemu se podrazumijeva da Revizorski sud, u slučaju da smatra da takve sigurnosne mjere nisu opravdane s obzirom na prirodu i vrstu klasificiranih podataka EU-a, zadržava pravo na iznošenje svih opažanja koja smatra primjerenima vodeći računa o stupnju tajnosti klasificiranih podataka EU-a;

BUDUĆI DA sigurnosne mjere za zaštitu povjerljivosti, cjelovitosti i dostupnosti informacija dostavljenih Revizorskom sudu moraju biti primjerene prirodi i vrsti predmetnih informacija;

BUDUĆI DA se Revizorskom sudu mora omogućiti pristup klasificiranim podatcima u skladu s načelom nužnosti pristupa informacijama u svrhu obavljanja zadaća koje su mu povjerene Ugovorima i pravnim aktima donesenima na temelju Ugovora;

BUDUĆI DA je s obzirom na prirodu i osjetljiv sadržaj određenih informacija primjereno utvrditi poseban postupak kojim se određuje način na koji Revizorski sud postupa s dokumentima koji sadržavaju klasificirane podatke EU-a;

BUDUĆI DA Revizorski sud mora zajamčiti da se ova Odluka provodi u skladu sa svim primjenjivim pravilima, posebno odredbama o zaštiti osobnih podataka, fizičkoj sigurnosti osoba, zgrada i IT-a te javnom pristupu dokumentima;

**DONIO JE SLJEDEĆU ODLUKU:**

**Članak 1.** **Predmet i područje primjene**

(1) Ovom se Odlukom utvrđuju osnovna načela i minimalni sigurnosni standardi za zaštitu klasificiranih podataka s kojima Revizorski sud postupa u okviru izvršavanja svojih zadaća.

(2) Za potrebe ove Odluke pojam klasificirani podatci označava bilo koju ili sve od sljedećih vrsta podataka:

(a) „klasificirane podatke EU-a” kako su definirani u sigurnosnim propisima drugih institucija, agencija, tijela ili ureda EU-a i koji nose jednu od sljedećih oznaka stupnja tajnosti:

- *TRÈS SECRET UE / EU TOP SECRET*: podatci i materijali čijim se neovlaštenim otkrivanjem može nanijeti iznimno ozbiljna šteta ključnim interesima Europske unije ili jedne ili više država članica;
- *SECRET UE / EU SECRET*: podatci i materijali čijim se neovlaštenim otkrivanjem može nanijeti ozbiljna šteta ključnim interesima Europske unije ili jedne ili više država članica;
- *CONFIDENTIEL UE / EU CONFIDENTIAL*: podatci i materijali čijim se neovlaštenim otkrivanjem može nanijeti šteta ključnim interesima Europske unije ili jedne ili više država članica;
- *RESTREINT UE / EU RESTRICTED*: podatci i materijali čije bi neovlašteno otkrivanje moglo biti nepovoljno za interese Europske unije ili jedne ili više država članica.

(b) klasificirane podatke koje su dostavile države članice i koji nose nacionalnu oznaku stupnja tajnosti koja je istovjetna jednoj od oznaka stupnja tajnosti klasificiranih podataka EU-a[1] navedenih u točki (a);

(c) klasificirane podatke koje su Europskom revizorskom sudu dostavile treće zemlje ili međunarodne organizacije i koji nose oznaku stupnja tajnosti istovjetnu jednoj od oznaka stupnja tajnosti klasificiranih podataka EU-a navedenih u točki (a), u skladu s relevantnim sporazumima o sigurnosti podataka ili administrativnim dogovorima.

[1] Vidjeti Sporazum između država članica Europske unije, koje su se sastale u okviru Vijeća, o zaštiti klasificiranih podataka koji se razmjenjuju u interesu Europske unije od 4. svibnja 2011. i njegov Prilog (SL 2011/C 202/13).

(3) Revizorski sud postupa s podatcima sa stupnjem tajnosti *RESTREINT UE / EU RESTRICTED* u svojim prostorijama i u tu svrhu poduzima sve potrebne zaštitne mjere. U slučajevima u kojima članovi osoblja Revizorskog suda trebaju pristupiti klasificiranim podatcima EU-a viših stupnjeva tajnosti osiguravaju im se uvjeti kako bi to mogli učiniti u odgovarajućim prostorijama drugih institucija, tijela ili agencija.

(4) Ova se Odluka primjenjuje na sve službe i prostorije Revizorskog suda.

(5) Uz iznimku slučajeva u kojima se određena odredba odnosi na posebne skupine osoblja, ova se Odluka primjenjuje na članove Revizorskog suda, osoblje Revizorskog suda na koje se primjenjuju Pravilnik o osoblju i Uvjeti zaposlenja ostalih službenika Europske unije[2], nacionalne stručnjake upućene na rad na Revizorskom sudu, pružatelje usluga i njihovo osoblje, stažiste i sve osobe koje imaju pristup zgradama i drugoj imovini Revizorskog suda ili informacijama kojima upravlja Revizorski sud.

(6) Osim ako je drukčije navedeno, odredbe o klasificiranim podatcima EU-a primjenjuju se na isti način na klasificirane podatke iz stavka 2. točaka (b) i (c) ovog članka.

**Članak 2.** **Definicije**

Za potrebe ove Odluke:

(a) „ovlaštenje za pristup klasificiranim podatcima EU-a” označava odluku koju je ravnatelj Uprave Revizorskog suda za kadrovske poslove, financije i opće usluge donio na temelju potvrde nadležnog tijela države članice da se dužnosniku ili drugom službeniku Revizorskog suda ili upućenom nacionalnom stručnjaku može odobriti pristup klasificiranim podatcima EU-a do određenog stupnja tajnosti (*CONFIDENTIEL UE / EU CONFIDENTIAL* ili višeg) i do određenog datuma pod uvjetom da je za njih utvrđena nužnost pristupa podatcima i da su odgovarajuće upoznati sa svojim odgovornostima. Predmetna osoba u tom se slučaju smatra „sigurnosno ovlaštenom”;

(b) „klasifikacija” označava dodjelu stupnja tajnosti podatcima na temelju stupnja štete koju bi moglo uzrokovati njihovo neovlašteno otkrivanje;

(c) „kriptografski materijal” označava kriptografske algoritme, kriptografske hardverske i softverske module i proizvode, uključujući detalje o primjeni te povezanu dokumentaciju i kriptografske ključeve;

(d) „deklasifikacija” označava uklanjanje svakog stupnja tajnosti;

(e) „dokument” označava svaki zapis podataka bez obzira na njegov oblik ili fizičke značajke;

(f) „smanjenje stupnja tajnosti” označava smanjenje razine stupnja tajnosti;

(g) „uvjerenje o sigurnosnoj provjeri pravne osobe” označava potvrdu koju izdaje nadležno sigurnosno tijelo o tome da, sa stajališta sigurnosti, pravna osoba može pružiti odgovarajuću razinu zaštite klasificiranih podataka EU-a određenog stupnja tajnosti;

(h) „postupanje” s klasificiranim podatcima EU-a označava sve radnje kojima klasificirani podatci EU-a mogu biti izloženi tijekom svojeg životnog ciklusa: izrada, registracija, obrada, prijenos, smanjenje stupnja tajnosti, deklasifikacija i uništavanje. Kada je riječ o komunikacijskim i informacijskim sustavima, to obuhvaća i njihovo prikupljanje, prikaz, slanje i čuvanje;

[2] Uredba br. 31 (EEZ) o utvrđivanju Pravilnika o osoblju za dužnosnike i Uvjeta zaposlenja ostalih službenika, kako je izmijenjena, SL 01 962R0031. – 1..1.2020. – 019..003. – 1. (https://eur-lex.europa.eu/eli/reg/1962/31 (1)/2020. – 01.-01).

(i) „imatelj” označava osobu s odgovarajućim ovlaštenjem za koju je utvrđena nužnost pristupa podatcima i koja raspolaže klasificiranim podatcima te je stoga odgovorna za njihovu zaštitu;

(j) „tijelo za informacijsku sigurnost” označava službenika Revizorskog suda za informacijsku sigurnost koji može u cijelosti ili djelomično delegirati zadaće predviđene ovom Odlukom;

(k) „podatak” označava svaki pismeni ili usmeni podatak, bez obzira na medij ili autora;

(l) „materijal” označava svaki medij, nosač podataka ili dio stroja ili opreme;

(m) „autor” označava instituciju, tijelo ili agenciju EU-a, državu članicu, treću zemlju ili međunarodnu organizaciju u čijoj su nadležnosti podatci izrađeni i/ili uvedeni u strukture EU-a;

(n) „uvjerenje o sigurnosnoj provjeri osobe” označava izjavu koju nadležno tijelo države članice izdaje nakon završetka sigurnosne istrage koju provode nadležna tijela države članice i kojom se potvrđuje da se određenoj osobi može odobriti pristup klasificiranim podatcima EU-a do određenog stupnja tajnosti (*CONFIDENTIEL UE* / *EU CONFIDENTIAL* ili višeg) i do određenog datuma pod uvjetom da je za nju utvrđena nužnost pristupa podatcima i da je odgovarajuće upoznata sa svojim odgovornostima;

(o) „certifikat o sigurnosnoj provjeri osobe” označava certifikat koji izdaje ravnatelj Uprave Revizorskog suda za kadrovske poslove, financije i opće usluge i kojim se utvrđuje da određena osoba ima valjano uvjerenje o sigurnosnoj provjeri ili sigurnosno ovlaštenje te u kojem je naveden stupanj tajnosti klasificiranih podataka EU-a do kojeg se pojedincu može odobriti pristup (*CONFIDENTIEL UE* / *EU CONFIDENTIAL* ili viši), datum valjanosti relevantnog uvjerenja o sigurnosnoj provjeri ili sigurnosnog ovlaštenja te datum isteka samog certifikata;

(p) „tijelo za fizičku sigurnost” označava voditelja službe sigurnosti na Revizorskom sudu koji je odgovoran za provedbu potrebnih mjera i postupaka fizičke sigurnosti za zaštitu klasificiranih podataka EU-a;

(q) „pisarnicom” upravlja tajništvo Suda te je ona smještena u administrativnoj zoni koja je u nadležnosti ravnatelja Uprave Revizorskog suda za kadrovske poslove, financije i opće usluge. Odgovorna je za ulaz i izlaz podataka sa stupnjem tajnosti *RESTREINT UE* / *EU RESTRICTED* ili istovjetnih podataka koji se razmjenjuju s Revizorskim sudom.

(r) „registarski ured za klasificirane podatke EU-a” zona je koja je uspostavljena unutar sigurnosne zone. Registarskim uredom upravlja nadzorni službenik registarskog ureda na Revizorskom sudu koji je prošao sigurnosnu provjeru i koji je za to ovlašten. Odgovoran je za ulaz i izlaz podataka sa stupnjem tajnosti *CONFIDENTIEL UE* / *EU CONFIDENTIAL* ili oznakom višeg stupnja tajnosti ili istovjetnih podataka koji se razmjenjuju s Revizorskim sudom.

(s) „tijelo za sigurnosnu akreditaciju” označava ravnatelja Uprave Revizorskog suda za kadrovske poslove, financije i opće usluge.

**Članak 3.** **Mjere za zaštitu klasificiranih podataka EU-a**

(1) Revizorski sud jamči zaštitu svih klasificiranih podataka koji su mu dostavljeni na način koji je razmjeran stupnju tajnosti koji je odredio njihov autor i u skladu s ovom Odlukom.

(2) U tu svrhu Revizorski sud pri postupanju s klasificiranim podatcima EU-a primjenjuje fizičke i, prema potrebi, sigurnosne mjere u vezi s osobljem, uključujući ovlaštenja za pristup imenovanih osoba te mjere za zaštitu komunikacijskih i informacijskih sustava. Te su mjere opisane u člancima od 4. do 6. i primjenjuju se tijekom cijelog životnog ciklusa klasificiranih podataka EU-a. One moraju biti razmjerne stupnju tajnosti klasificiranih podataka EU-a, obliku

i količini podataka ili materijala, mjestu i konstrukciji objekata u kojima su ti podatci smješteni i lokalno procijenjenoj prijetnji od zlonamjernih i/ili kriminalnih aktivnosti, uključujući špijunažu, sabotažu i terorizam.

(3) Klasificirani podatci EU-a zaštićeni su mjerama fizičke sigurnosti, a podatci sa stupnjem tajnosti *CONFIDENTIEL UE* / *EU CONFIDENTIAL* ili višim stupnjem dodatno su zaštićeni sigurnosnim mjerama u vezi s osobljem.

(4) Klasificirani podatci EU-a mogu se pružiti na uvid isključivo osobama unutar institucije za koje je utvrđena nužnost pristupa tim podatcima. Imatelj bilo kojeg klasificiranog podatka EU-a dužan je zaštititi ga u skladu s ovom Odlukom.

(5) Klasificirani podatci EU-a ne smiju se otkrivati ni usmeno ni pismeno. Preliminarna opažanja, izvješća, mišljenja, priopćenja za medije i drugi dokumenti Revizorskog suda, njegove internetske i intranetske stranice, usmene intervencije, odgovori na zahtjeve za pristup dokumentima[3] te zvučni zapisi i videozapisi ne smiju sadržavati klasificirane podatke EU-a ili njihove izvatke i u njima se ne smije upućivati na takve podatke. Međutim, ako je autor objavio dokumente ili informacije koji sadržavaju upućivanje na klasificirane podatke EU-a, to se upućivanje može navesti.

(6) Neovisno o stavku 5., Revizorski sud i autor mogu dogovoriti da, u slučaju posebne revizije, Revizorski sud može reproducirati ili upotrijebiti elemente klasificiranih podataka EU-a u određenom dokumentu. U tom slučaju taj se dokument Revizorskog suda prvo šalje autoru predmetnih klasificiranih podataka EU-a prije ili tijekom raspravnog postupka. U toj situaciji Revizorski sud i autor dogovaraju hoće li označiti dokument Revizorskog suda klasificiranim. Ako član Revizorskog suda koji ima ulogu izvjestitelja smatra da je izvješće o reviziji koje je u cijelosti ili djelomično klasificirano potrebno dostaviti određenim primateljima u Europskom parlamentu ili Vijeću – vodeći računa o svim sigurnosnim mjerama povezanima s ovom Odlukom – za to je potrebna suglasnost autora klasificiranih podataka. Pravni okvir i postupak za razmjenu takvih dokumenata utvrđeni su u članku 7.

(7) Ako je za izvršavanje zadaća Revizorskog Suda određene elemente klasificiranog dokumenta ili podataka potrebno proslijediti širem krugu primatelja, Revizorski sud, uzimajući u obzir oznaku stupnja tajnosti, savjetuje se s autorom prije donošenja odluke o upotrebi tih elemenata ili podataka u slučaju da smatra da za to postoji prevladavajući javni interes. Podatci se u izvješću upotrebljavaju isključivo na način kojim se ne može naštetiti interesima autora. To bi se moglo zajamčiti na odgovarajući način tako da se od autora zatraži da se očituje u svrhu postizanja dogovora o načinu anonimizacije, sažimanja ili uopćenja podataka i sl. te da se istodobno poštuju interesi onih na koje se objavljeni podatci u prvom redu odnose.

(8) Revizorski sud ne dostavlja klasificirane podatke EU-a drugoj instituciji, agenciji, tijelu ili uredu EU-a, državi članici, trećoj zemlji ili međunarodnoj organizaciji bez prethodnog savjetovanja s autorom i njegove izričite pismene suglasnosti.

(9) Osim ako je autor dokumenta sa stupnjem tajnosti *SECRET UE* / *EU SECRET* ili nižim stupnjem ograničio mogućnost njegova umnožavanja ili prijevoda, takvi se dokumenti mogu umnožavati ili prevoditi na zahtjev imatelja i u skladu s praktičnim radnim uputama tijela za informacijsku sigurnost na Revizorskom sudu. Sigurnosne mjere koje se primjenjuju na izvorni dokument primjenjuju se i na njegove preslike i prijevode.

---

[3] U skladu s Odlukom Revizorskog suda br. 12-2005 o javnom pristupu dokumentima Suda, kako je izmijenjena Odlukom br. 14-2009 (SL 2009/C 67/1).

(10) Ako je Revizorskom sudu potrebno da se za određeni klasificirani dokument koji je zaprimio ili kojem smije pristupiti smanji stupanj tajnosti ili da se on deklasificira, Sud se savjetuje s autorom kako bi upitao može li autor dokumenta dostaviti inačicu dokumenta koja ima niži stupanj tajnosti ili koja je deklasificirana.

**Članak 4.** **Sigurnosne mjere u vezi s osobljem**

(1) Na temelju svojih funkcija članovi Revizorskog suda ovlašteni su imati pristup svim klasificiranim podatcima EU-a i sudjelovati na sastancima na kojima se postupa s takvim podatcima. Članove se informira o njihovim sigurnosnim obvezama u pogledu zaštite klasificiranih podataka EU-a te oni u pismenom obliku potvrđuju svoju odgovornost za zaštitu takvih podataka.

(2) Neovisno o tome je li riječ o dužnosniku, članu osoblja na kojeg se primjenjuju Uvjeti zaposlenja ostalih službenika ili upućenom nacionalnom stručnjaku, pristup klasificiranim podatcima EU-a odobrava se isključivo članovima osoblja Revizorskog suda:

i. za koje je utvrđena nužnost pristupa podatcima;

ii. koji su informirani o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a i relevantnim sigurnosnim standardima i smjernicama i koji su u pismenom obliku potvrdili svoju odgovornost za zaštitu takvih podataka;

iii. u slučaju podataka sa stupnjem tajnosti *CONFIDENTIEL UE* / *EU CONFIDENTIAL* ili višim, koji su prošli sigurnosnu provjeru i dobili ovlaštenje za pristup.

(3) Postupak na temelju kojeg se određuje može li se određenom dužnosniku ili drugom članu osoblja Revizorskog suda odobriti pristup informacijama sa stupnjem tajnosti *CONFIDENTIEL UE* / *EU CONFIDENTIAL* ili višim stupnjem, uzimajući u obzir lojalnost, integritet i pouzdanost pojedinca te nakon dobivanja potvrde od nadležnih tijela države članice kako je navedeno u članku 2. točki (n), utvrđuje se u delegiranoj odluci donesenoj u skladu s člankom 10. stavkom 10. Odluke o davanju ovlaštenja za pristup donosi ravnatelj Uprave Revizorskog suda za kadrovske poslove, financije i opće usluge.

(4) Ravnatelj Uprave Revizorskog suda za kadrovske poslove, financije i opće usluge može izdavati certifikate o sigurnosnoj provjeri osobe navodeći stupanj tajnosti za koji se pojedincima može odobriti pristup klasificiranim podatcima EU-a (*CONFIDENTIEL UE* / *EU CONFIDENTIAL* ili viši stupanj), razdoblje valjanosti odgovarajućeg ovlaštenja za pristup i datum isteka certifikata.

(5) Samo osobe s ovlaštenjem iz stavka 2. točke iii. i članovi Revizorskog suda u skladu sa stavkom 1. mogu sudjelovati na sastancima na kojima se postupa s podatcima sa stupnjem tajnosti *CONFIDENTIEL UE* / *EU CONFIDENTIAL* ili višim stupnjem. Revizorski sud i autor utvrđuju praktične aspekte održavanja takvih sastanaka za svaki pojedini slučaj.

(6) Službe Revizorskog suda koje su odgovorne za organizaciju sastanaka na kojima će se postupati s podatcima sa stupnjem tajnosti *CONFIDENTIEL UE* / *EU CONFIDENTIAL* ili višim stupnjem pravodobno obavješćuju tijelo za informacijsku sigurnost o datumima sastanaka, vremenu i lokacijama te mu dostavljaju popise sudionika.

(7) Svaka osoba koja raspolaže klasificiranim podatcima EU-a bez odgovarajućeg ovlaštenja i/ili dokazane nužnosti pristupa mora to što prije prijaviti tijelu za informacijsku sigurnost i voditi računa o tome da su klasificirani podatci EU-a zaštićeni u skladu s ovom Odlukom.

**Članak 5.** **Mjere fizičke sigurnosti u svrhu zaštite klasificiranih podataka**

(1) „Fizička sigurnost” odnosi se na upotrebu fizičkih i tehničkih zaštitnih mjera za sprječavanje neovlaštenog pristupa klasificiranim podatcima EU-a.

(2) Svrha je mjera fizičke sigurnosti sprječavanje tajnog ili nasilnog ulaska neovlaštenih osoba, odvraćanje od neovlaštenih radnji, njihovo sprječavanje ili otkrivanje te omogućavanje razvrstavanja osoblja s obzirom na pristup klasificiranim podatcima EU-a prema nužnosti pristupa. Te se mjere utvrđuju na temelju postupka upravljanja rizicima, u skladu s ovom Odlukom.

(3) Nadležno sigurnosno tijelo Revizorskog suda provodi redovite inspekcije zona u kojima se postupa s klasificiranim podatcima EU-a ili u kojima se oni čuvaju.

(4) Za postupanje s klasificiranim podatcima EU-a i njihovu pohranu upotrebljavaju se isključivo oprema ili uređaji koji su u skladu s pravilima o zaštiti klasificiranih podataka EU-a koja se primjenjuju unutar institucija, agencija ili tijela EU-a.

(5) Osoblje Revizorskog suda može pristupiti klasificiranim podatcima EU-a sa stupnjem tajnosti *CONFIDENTIEL UE* / *EU CONFIDENTIAL*, višim stupnjem ili istovjetnim stupnjem u sigurnosnim zonama izvan prostorija Revizorskog suda.

(6) Revizorski sud može sklopiti sporazum o razini usluge s drugom institucijom EU-a u Luxembourgu kako bi mogao postupati s podatcima sa stupnjem tajnosti *CONFIDENTIEL UE* / *EU CONFIDENTIAL* ili višim stupnjem i pohranjivati ih u sigurnosnoj zoni te institucije. Osim ako se autor izričito s time složi, s tim klasificiranim podatcima EU-a ne postupa se niti se oni pohranjuju u prostorijama Revizorskog suda te ih Revizorski sud ne umnožava niti prevodi.

(7) Revizorski sud evidentira zaprimljene podatke sa stupnjem tajnosti *RESTREINT UE* / *EU RESTRICTED*. Uvid u informacije sa stupnjem tajnosti *CONFIDENTIEL UE* / *EU CONFIDENTIAL*, višim stupnjem ili istovjetnim stupnjem izvan prostorija Revizorskog suda evidentira se iz sigurnosnih razloga.

(8) Klasificirani podatci EU-a sa stupnjem tajnosti *RESTREINT UE* / *EU RESTRICTED* mogu se pohraniti u primjerenom zaključanom uredskom namještaju u administrativnoj ili sigurnosnoj zoni. Klasificirani podatci EU-a sa stupnjem tajnosti *CONFIDENTIEL UE* / *EU CONFIDENTIAL* ili *SECRET UE* / *EU SECRET* pohranjuju se na temelju sporazuma o razini usluge u sigurnosnom spremniku u sigurnosnoj zoni druge institucije EU-a u Luxembourgu.

(9) U slučajevima u kojima se klasificirani podatci EU-a prenose izvan registarskog ureda, prijenos između odjela i prostorija obavlja se kako je opisano u nastavku:

(a) opće je pravilo da se klasificirani podatci EU-a prenose elektroničkim sredstvima koja su zaštićena kriptografskim proizvodima odobrenima u skladu s člankom 6. stavkom 8.;

(b) ako se ne prenose na način opisan u točki (a), klasificirani podatci EU-a prenose se s pomoću medija za pohranu podataka (npr. USB uređaja, CD-a, tvrdog diska) zaštićenog kriptografskim proizvodima odobrenima u skladu s člankom 6. stavkom 8. ili u obliku papirnatog primjerka u neprozirnoj zapečaćenoj omotnici.

(10) Imatelj može uništiti podatke sa stupnjem tajnosti *RESTREINT UE* / *EU RESTRICED*, u skladu s pravilima o arhiviranju koja se primjenjuju na Revizorskom sudu. Podatke sa stupnjem tajnosti *CONFIDENTIEL UE* / *EU CONFIDENTIAL* ili višim stupnjem uništava nadzorni službenik registarskog ureda, i to isključivo kada to zatraži imatelj ili nadležno tijelo u skladu s pravilima o arhiviranju koja se primjenjuju na Revizorskom sudu. Dokumenti sa stupnjem tajnosti *SECRET UE* / *EU SECRET* uništavaju se u prisutnosti svjedoka s uvjerenjem o sigurnosnoj

provjeri koje odgovara najmanje stupnju tajnosti dokumenta koji se uništava. Nadzorni službenik registarskog ureda i svjedok, ako mora biti prisutan, potpisuju zapisnik o uništenju koji se pohranjuje u registarskom uredu. Nadzorni službenik registarskog ureda čuva evidenciju o uništavanju dokumenata sa stupnjem tajnosti *CONFIDENTIEL UE* / *EU CONFIDENTIAL* i *SECRET UE* / *EU SECRET* najmanje pet godina.

(11) Tijelo za fizičku sigurnost i tijelo za informacijsku sigurnost sastavljaju zajednički plan, uzimajući u obzir lokalne uvjete, za zaštitu klasificiranih podataka EU-a u kriznim situacijama, uključujući, prema potrebi, planove za njihovo uništenje ili evakuaciju u hitnim situacijama. Ta tijela izdaju upute, kako to smatraju primjerenim, s ciljem sprječavanja da klasificirani podatci EU-a dospiju u ruke neovlaštenih osoba.

(12) U slučajevima u kojima postoji potreba za fizičkim prijevozom klasificiranih podataka EU-a Revizorski sud postupa u skladu s mjerama koje je odredio autor u svrhu njihove zaštite od neovlaštenog otkrivanja tijekom prijevoza.

(13) Mjere fizičke sigurnosti koje se primjenjuju u administrativnim zonama u kojima se postupa s podatcima sa stupnjem tajnosti *RESTREINT UE* / *EU RESTRICTED* i u kojima se oni pohranjuju navedene su u Prilogu.

**Članak 6.** **Zaštita klasificiranih podataka EU-a u komunikacijskim i informacijskim sustavima**

(1) Za potrebe ovog članka „komunikacijski i informacijski sustav” označava bilo koji sustav koji omogućuje postupanje s klasificiranim podatcima EU-a u elektroničkom obliku. Komunikacijski i informacijski sustav obuhvaća sva sredstva potrebna za njegovo funkcioniranje, uključujući infrastrukturu, organizaciju, osoblje i informacijske resurse.

(2) „Legitimni korisnik” član je Revizorskog suda, dužnosnik, drugi član osoblja ili upućeni nacionalni stručnjak s utvrđenom i priznatom potrebom za pristupom posebnom informacijskom sustavu.

(3) Revizorski sud pruža jamstvo da će njegovi sustavi u odgovarajućoj mjeri štititi podatke s kojima se u okviru njih postupa i da će funkcionirati onako kako je potrebno i kada je to potrebno, pod nadzorom legitimnih korisnika. U tu svrhu njima se jamče odgovarajuće razine:

- autentičnosti: jamstvo da je podatak istinit i da potječe iz dobronamjernih izvora;
- raspoloživosti: podatci su dostupni i mogu se upotrebljavati na zahtjev ovlaštenog subjekta;
- povjerljivosti: podatci se ne otkrivaju neovlaštenim osobama i subjektima, kao ni u okviru procesa za koje nije izdano ovlaštenje;
- cjelovitosti: štiti se točnost i cjelovitost sredstava i podataka;
- nepobitnosti: sposobnost dokazivanja da se dogodila određena radnja ili da je nastupio određeni događaj na način da to kasnije nije moguće zanijekati.

To se jamstvo temelji na procesu upravljanja rizicima. „Rizik” označava mogućnost da će određena prijetnja dovesti do iskorištavanja unutarnjih i vanjskih slabih točaka organizacije ili bilo kojeg sustava koji organizacija upotrebljava i na taj način naštetiti organizaciji i njezinoj materijalnoj i nematerijalnoj imovini. Mjeri se kao kombinacija vjerojatnosti pojave prijetnji i njihova učinka. Proces upravljanja rizicima sastoji se od sljedećih koraka: prepoznavanje prijetnji i slabih točaka, procjena rizika, postupanje s rizicima, prihvaćanje rizika i obavješćivanje o rizicima.

- „Procjena rizika” obuhvaća prepoznavanje prijetnji i slabih točaka te provedbu pripadajuće analize rizika, tj. procjenu vjerojatnosti pojave i učinka.

- „Postupanje s rizicima” označava ublažavanje, otklanjanje, smanjivanje (odgovarajućom kombinacijom tehničkih, fizičkih, organizacijskih ili proceduralnih mjera), prijenos ili praćenje rizika.
- „Prihvaćanje rizika” odnosi se na odluku kojom se prihvaća da nakon postupanja s rizicima i dalje postoji preostali rizik.
- „Preostali rizik” označava rizik koji ostaje nakon provedbe sigurnosnih mjera, uzimajući u obzir da se ne mogu suzbiti sve prijetnje i ukloniti sve slabe točke.
- „Obavješćivanje o rizicima” sastoji se od razvijanja svijesti o rizicima u zajednici korisnika određenog komunikacijskog i informacijskog sustava, informiranja tijela za odobrenja o tim rizicima i izvješćivanja operativnih tijela o njima.

(4) Svi elektronički uređaji i oprema koji se upotrebljavaju za postupanje s klasificiranim podatcima EU-a moraju biti u skladu s pravilima koja se primjenjuju na zaštitu tih podataka. Prednost se daje elektroničkim uređajima i opremi koje je već akreditirala druga institucija, agencija ili tijelo EU-a. Sigurnost uređaja jamči se tijekom njihova cjelokupnog vijeka trajanja.

(5) Komunikacijski i informacijski sustav Revizorskog suda za postupanje s klasificiranim podatcima EU-a akreditira odgovarajuće tijelo. U tu svrhu Revizorski sud sklapa sporazum o razini usluge s tijelom za sigurnosnu akreditaciju iz jedne od institucija EU-a koja ima mogućnost akreditirati komunikacijski i informacijski sustav u okviru kojeg se postupa s klasificiranim podatcima EU-a s ciljem pribavljanja izjave o akreditaciji za podatke sa stupnjem tajnosti *RESTREINT UE* / *EU RESTRICTED* s kojima se može postupati u okviru informacijskog i komunikacijskog sustava Revizorskog suda, kao i odgovarajućih uvjeta za njegovu upotrebu. U sporazumu o razini usluge također se upućuje na standarde koji se primjenjuju za proces akreditacije te se on sklapa u skladu s postupkom utvrđenim u članku 10. stavku 3.

(6) U slučaju da Revizorski sud treba uspostaviti vlastiti postupak akreditacije za svoj komunikacijski i informacijski sustav delegiranom odlukom iz članka 10. stavka 10. ove Odluke uspostavlja se proces koji je u skladu sa standardima za proces akreditacije komunikacijskih i informacijskih sustava u okviru kojih se postupa s klasificiranim podatcima EU-a u drugim institucijama, agencijama i tijelima EU-a.

(7) Odgovornost za pripremu akreditacijskih spisa i dokumentacije u skladu s važećim standardima u potpunosti snosi vlasnik komunikacijskog i informacijskog sustava.

(8) U slučajevima u kojima se klasificirani podatci EU-a štite kriptografskim proizvodima Revizorski sud daje prednost proizvodima koje je odobrilo Vijeće ili glavni tajnik Vijeća u svojoj ulozi tijela za odobravanje kriptomaterijala ili, u protivnom, proizvodima za zaštitu klasificiranih podataka EU-a koje su odobrile druge institucije, agencije i tijela EU-a.

(9) Za postupanje s podatcima sa stupnjem tajnosti *RESTREINT UE* / *EU RESTRICTED* upotrebljavaju se isključivo elektronički uređaji (kao što su radne stanice, pisači, fotokopirni uređaji) koji se nalaze u administrativnoj zoni ili sigurnosnoj zoni. Elektronički uređaji koji se upotrebljavaju za postupanje s podatcima sa stupnjem tajnosti *RESTREINT UE* / *EU RESTRICTED* odvojeni su od drugih računalnih mreža i zaštićeni odgovarajućim fizičkim ili tehničkim mjerama.

(10) Svi članovi osoblja Revizorskog suda koji su uključeni u oblikovanje, razvoj i testiranje komunikacijskog i informacijskog sustava za postupanje s klasificiranim podatcima EU-a, koji rukuju ili upravljaju tim sustavom ili se njime koriste obavješćuju službenika za informacijsku sigurnost o svim potencijalnim sigurnosnim nedostatcima i incidentima te slučajevima povrede sigurnosti ili ugrožavanja koji bi mogli utjecati na zaštitu tog sustava i/ili klasificiranih podataka EU-a koje on sadržava.

**Članak 7.** **Postupak za razmjenu klasificiranih podataka i omogućavanje pristupa tim podatcima**

(1) U slučajevima u kojima su na temelju Ugovora ili pravnih akata donesenih na temelju Ugovora zakonski obvezni to učiniti, institucije, agencije, tijela i uredi EU-a te nacionalna tijela na vlastitu inicijativu ili na pismeni zahtjev predsjednika Revizorskog suda, člana ili članova izvjestitelja ili glavnog tajnika Revizorskom sudu omogućuju pristup klasificiranim podatcima EU-a u skladu s postupkom u nastavku.

(2) Zahtjevi za pristup šalju se relevantnim institucijama preko pisarnice Revizorskog suda.

(3) Revizorski sud prema potrebi sklapa administrativni dogovor o praktičnim aspektima razmjene klasificiranih podataka EU-a ili jednakovrijednih informacija.

(4) Za potrebe sklapanja takvih administrativnih dogovora Revizorski sud pruža autoru sve potrebne informacije o svojem sustavu informacijske sigurnosti. U slučaju da je to potrebno može se organizirati posjet radi procjene stanja.

(5) Ti administrativni dogovori sklapaju se u cijelosti u skladu s načelima dodjeljivanja i lojalne suradnje iz članka 13. Ugovora o Europskoj uniji. Sklapaju se u skladu s postupkom utvrđenim u članku 10. stavku 4.

(6) U slučajevima u kojima s određenom institucijom tijelom ili agencijom EU-a, trećom državom ili međunarodnom organizacijom nije sklopljen administrativni dogovor o dostavljanju klasificiranih podataka Revizorskom sudu, Revizorski sud potpisuje izjavu o preuzimanju obveze zaštite klasificiranih podataka koje zaprimi.

**Članak 8.** **Povreda sigurnosti, gubitak ili ugrožavanje klasificiranih podataka**

(1) Povreda sigurnosti označava radnju ili propust koji su u suprotnosti sa sigurnosnim propisima utvrđenima ovom Odlukom i njezinim provedbenim pravilima.

(2) Do ugrožavanja dolazi kada su klasificirani podatci EU-a, kao rezultat povrede sigurnosti, djelomično ili u cijelosti otkriveni neovlaštenim osobama.

(3) Svaka povreda ili sumnja na povredu sigurnosti odmah se prijavljuje tijelu Revizorskog suda za informacijsku sigurnost.

(4) U slučajevima u kojima postoji saznanje ili opravdani razlozi za pretpostavku da su klasificirani podatci EU-a ugroženi ili izgubljeni, tijelo za informacijsku sigurnost obavješćuje ravnatelja Uprave za kadrovske poslove, financije i opće usluge i glavnog tajnika Revizorskog suda. Ravnatelj Uprave za kadrovske poslove, financije i opće usluge odmah obavješćuje relevantno sigurnosno tijelo autora. Predmetni ravnatelj Revizorskog suda provodi istragu i obavješćuje glavnog tajnika Revizorskog suda i sigurnosno tijelo autora o rezultatima i mjerama poduzetima kako bi se spriječilo da se ta situacija ponovi. U slučaju da je riječ uključen član Revizorskog suda predsjednik Revizorskog suda odgovoran je za poduzimanje mjera u suradnji s glavnim tajnikom Revizorskog suda.

(5) Na svakog dužnosnika ili drugog člana osoblja Revizorskog suda koji je odgovoran za povredu sigurnosnih propisa utvrđenih u ovoj Odluci i njezinim provedbenim pravilima primjenjuju se sankcije predviđene Pravilnikom o osoblju i Uvjetima zaposlenja ostalih službenika Europske unije.

(6) Na svakog člana Revizorskog suda koji ne postupi u skladu s uvjetima iz ove Odluke primjenjuju se mjere i sankcije predviđene člankom 286. stavkom 6. Ugovora.

(7) Protiv svake osobe odgovorne za gubitak ili ugrožavanje klasificiranih podataka EU-a može se pokrenuti disciplinski i/ili pravni postupak u skladu s važećim zakonima, pravilima i propisima.

**Članak 9.** **Sigurnost u slučaju vanjske intervencije**

(1) Revizorski sud na ugovornoj osnovi može povjeriti izvršenje zadaća koje uključuju ili zahtijevaju pristup klasificiranim podatcima EU-a izvođačima registriranima u državama članicama. Takvi slučajevi posebno mogu biti povezani s održavanjem komunikacijskih i informacijskih sustava i računalne mreže.

(2) U slučaju vanjske intervencije Revizorski sud poduzima sve potrebne sigurnosne mjere iz stavka 3. ovog članka, uključujući zahtijevanje uvjerenja o sigurnosnoj provjeri pravne osobe kako bi se zajamčilo da natjecatelji i ponuditelji štite klasificirane podatke EU-a tijekom trajanja natječaja i postupka javne nabave, kao i izvođači i podizvođači tijekom trajanja ugovora. Javni naručitelj vodi računa o tome da su minimalni sigurnosni standardi predviđeni ovom Odlukom navedeni u ugovorima kako bi se izvođače obvezalo da ih poštuju.

(3) Sigurnosni propisi, postupci javne nabave te predlošci i modeli ugovora i podugovora koji uključuju pristup klasificiranim podatcima EU-a, obavijesti o nadmetanju, smjernice o okolnostima u kojima su potrebna uvjerenja o sigurnosnoj provjeri osoba i pravnih osoba, sigurnosne upute za određeni program ili projekt, dopisi o sigurnosnim aspektima, posjeti te prijenos i prijevoz klasificiranih podataka EU-a u okviru takvih ugovora i podugovora u skladu su s pravilima, predlošcima i modelima koje je Europska komisija utvrdila za klasificirane ugovore u Odluci Komisije (EU, Euratom) 2015/444 od 13. ožujka 2015. o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a.

**Članak 10.** **Provedba Odluke i povezane odgovornosti**

(1) Službe Revizorskog suda poduzimaju sve potrebne mjere u okviru svoje nadležnosti kako bi zajamčile da pri postupanju s klasificiranim podatcima EU-a ili drugim klasificiranim podatcima i pri njihovu čuvanju primjenjuju ovu Odluku i relevantna provedbena pravila.

(2) Glavni tajnik tijelo je za imenovanje i tijelo ovlašteno za sklapanje ugovora o radu za sve dužnosnike i ostalo osoblje. Glavni tajnik može delegirati odgovornost za davanje ovlaštenja dužnosnicima i ostalom osoblju za pristup podatcima sa stupnjem tajnosti *CONFIDENTIEL UE* / *EU CONFIDENTIAL* ili višim stupnjem, za obavljanje svoje funkcije tijela za sigurnosnu akreditaciju te za nadzor nad tajništvom Suda u pogledu postupanja s klasificiranim podatcima EU-a ravnatelju Uprave za kadrovske poslove, financije i opće usluge.

(3) Glavni tajnik nadležan je za sklapanje sporazuma o razini usluge u vezi s akreditacijom komunikacijske i informacijske opreme i sustava Revizorskog suda, upotrebom sigurnosne zone u drugoj instituciji EU-a i postupku za zahtjeve za uvjerenja o sigurnosnoj provjeri osoba za pristup klasificiranim podatcima EU-a.

(4) Ravnatelj Uprave za kadrovske poslove, financije i opće usluge nadležan je za sklapanje administrativnih dogovora s institucijama, agencijama i drugim tijelima EU-a u svrhu razmjene klasificiranih podataka EU-a koji su Revizorskom sudu potrebni za izvršavanje njegovih zadaća. Predmetni ravnatelj također može sklapati administrativne dogovore o zaštiti zaprimljenih klasificiranih podataka s trećim zemljama ili međunarodnim organizacijama.

(5) Ravnatelj Uprave za kadrovske poslove, financije i opće usluge nadležan je za potpisivanje izjave o preuzimanju obveze za zaštitu klasificiranih podataka EU-a koje je potrebno dostaviti u kontekstu iznimnog *ad hoc* otkrivanja.

(6) Službenik Revizorskog suda za informacijsku sigurnost djeluje kao tijelo za informacijsku sigurnost. Službenik za informacijsku sigurnost i osobe kojima djelomično ili u cijelosti delegira svoje zadaće moraju proći odgovarajuću sigurnosnu provjeru. Tijelo za informacijsku sigurnost obavlja svoje dužnosti u bliskoj suradnji s Upravom za kadrovske poslove, financije i opće usluge, Upravom za informacije, radnu okolinu i inovacije te upravom Odbora za kontrolu kvalitete revizija (vidjeti posebno članke 4., 6. i 8.). Tijelo za informacijsku sigurnost ujedno je odgovorno za održavanje sastanaka u svrhu osposobljavanja i razvijanja svijesti o informacijskoj sigurnosti te za provedbu redovitih inspekcija u svrhu provjere usklađenosti s ovom Odlukom, uključujući u slučaju vanjske intervencije, kao i za sve mjere koje je potrebno poduzeti kako bi se zajamčila usklađenost.

(7) Voditelj službe sigurnosti odgovoran je za mjere fizičke sigurnosti (posebice članak 5.).

(8) Pisarnica koja je uspostavljena u okviru tajništva Suda ulazna je i izlazna točka za podatke sa stupnjem tajnosti *RESTREINT UE* / *EU RESTRICTED* koje Revizorski sud može razmjenjivati s drugim institucijama, agencijama i tijelima EU-a te državama članicama. Ona je ujedno ulazna i izlazna točka za istovjetne podatke trećih zemalja i međunarodnih organizacija. Način na koji je organizirana pisarnica utvrđuje se u delegiranoj odluci. Službenik pisarnice preuzima sljedeće glavne odgovornosti:

a) evidentiranje ulaska i izlaska podataka sa stupnjem tajnosti *RESTREINT UE* / *EU RESTRICTED*;

b) upravljanje namjenskom administrativnom zonom za evidentiranje postupanja s klasificiranim podatcima EU-a sa stupnjem tajnosti *RESTREINT UE* / *EU RESTRICTED* te njihovo pohranjivanje i uvid u njih.

(9) Na temelju sporazuma o razini usluge u vezi s upotrebom sigurnosne zone u jednoj od drugih institucija EU-a uspostavlja se registarski ured. Predmetni registarski ured koji organizira tajništvo Suda pod odgovornošću ravnatelja Uprave Revizorskog suda za kadrovske poslove, financije i opće usluge ulazna je i izlazna točka za podatke sa stupnjem tajnosti *CONFIDENTIEL UE* / *EU CONFIDENTIAL* ili višim stupnjem koje Revizorski sud može razmjenjivati s drugim institucijama, agencijama i tijelima EU-a te državama članicama. On je ujedno ulazna i izlazna točka za istovjetne podatke trećih zemalja i međunarodnih organizacija. Opremljen je odgovarajućim sefovima i drugom sigurnosnom opremom prikladnom za zaštitu podataka sa stupnjem tajnosti *CONFIDENTIEL UE* / *EU CONFIDENTIAL* ili višim stupnjem. Način na koji je organiziran registarski ured utvrđuje se u delegiranoj odluci. Nadzorni službenik registarskog ureda mora proći odgovarajuću sigurnosnu provjeru i preuzima sljedeće glavne odgovornosti:

(a) upravljanje operacijama povezanima s bilježenjem klasificiranih podataka EU-a, uvidom u takve podatke te njihovim čuvanjem, umnožavanjem, prevođenjem, prijenosom, slanjem i, u relevantnim slučajevima, uništavanjem;

(b) obavljanje drugih zadataka povezanih sa zaštitom klasificiranih podataka EU-a, a koji su utvrđeni u delegiranoj odluci.

(10) Upravni odbor donosi delegiranu odluku kojom se utvrđuju provedbena pravila za ovu Odluku. Službenik za informacijsku sigurnost utvrđuje smjernice za informacijsku sigurnost. Odbor za kontrolu kvalitete revizija sastavlja smjernice za reviziju.

**Članak 11.** **Stupanje na snagu**

Ova Odluka stupa na snagu sljedećeg dana od dana objave u Službenom listu Europske unije.

Sastavljeno u Luxembourgu 3. lipnja 2021.

Za Revizorski sud

Klaus-Heiner Lehne
*predsjednik*

Prilog: MJERE FIZIČKE SIGURNOSTI U VEZI S ADMINISTRATIVNIM ZONAMA ZA KLASIFICIRANE PODATKE EU-a

***PRILOG***

**MJERE FIZIČKE SIGURNOSTI U VEZI S ADMINISTRATIVNIM ZONAMA ZA KLASIFICIRANE PODATKE EU-a**

(1) Ovaj prilog sadržava pravila za provedbu članka 5. Odluke. Riječ je o minimalnim pravilima za fizičku zaštitu administrativnih zona za podatke sa stupnjem tajnosti *RESTREINT UE* / *EU RESTRICTED* na Revizorskom sudu: zona koje su predviđene za evidentiranje i pohranu klasificiranih podataka sa stupnjem tajnosti RESTREINT UE/EU RESTRICTED i uvid u takve podatke.

(2) Svrha je fizičkih sigurnosnih mjera u administrativnim zonama spriječiti neovlašteni pristup tim zonama kako je opisano u nastavku:

(a) uspostavlja se vidljivo definirani perimetar koji omogućuje provjeru osoba;

(b) pristup bez pratnje odobrava se isključivo pojedincima kojima je tijelo Revizorskog suda za informacijsku sigurnost ili drugo nadležno tijelo dalo odgovarajuće ovlaštenje;

(c) ostale osobe moraju imati stalnu pratnju ili se na njih primjenjuju istovjetne kontrole.

(3) Tijelo Revizorskog suda za informacijsku sigurnost može iznimno odobriti pristup neovlaštenim osobama, među ostalim i za rad u administrativnoj zoni, pod uvjetom da to ne podrazumijeva pristup klasificiranim podatcima EU-a, koji ostaju pod ključem. Takve osobe mogu ući isključivo uz pratnju tijela za informacijsku sigurnost ili nadzornog službenika pisarnice i uz njihov stalni nadzor.

(4) Tijelo za informacijsku sigurnost utvrđuje postupke za upravljanje ključevima i/ili kombinacijama za sve administrativne zone i siguran namještaj. Ti se postupci utvrđuju u svrhu zaštite od neovlaštenog pristupa.

(5) Kombinacije pamti najmanji mogući broj osoba koje ih moraju znati. Kombinacije za siguran namještaj koji se upotrebljava za pohranu podataka sa stupnjem tajnosti *RESTREINT UE* / *EU RESTRICTED* mijenjaju se:

- po primitku novog komada sigurnog namještaja;
- pri svakoj promjeni osoblja koje zna kombinaciju;
- ako je tajnost kombinacije ugrožena ili se sumnja da je ugrožena;
- u slučaju popravka ili održavanja brave;
- najmanje svakih 12 mjeseci.

(6) Tijelo za informacijsku sigurnost i voditelj službe sigurnosti odgovorni su za usklađenost s ovim pravilima.