ODLUKA KOMISIJE (EU) 2022/640

od 7. travnja 2022.

o provedbenim pravilima koja se odnose na uloge i odgovornosti glavnih aktera u području sigurnosti

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 249.,

uzimajući u obzir Odluku Komisije (EU, Euratom) 2015/443 od 13. ožujka 2015. o sigurnosti u Komisiji ([1]),

uzimajući u obzir Odluku Komisije (EU, Euratom) 2015/444 od 13. ožujka 2015. o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a ([2]),

budući da:

(1) Odluke (EU, Euratom) 2015/443 i (EU, Euratom) 2015/444 primjenjuju se na sve službe i prostore Komisije.

(2) Prema potrebi, provedbena pravila za dopunu ili potporu Odluci (EU, Euratom) 2015/444 donose se u skladu s njezinim člankom 60.

(3) Sigurnosne mjere za zaštitu klasificiranih podataka EU-a trebale bi tijekom cijelog životnog ciklusa podataka biti razmjerne, posebice njihovu stupnju tajnosti.

(4) Sigurnosne mjere za zaštitu komunikacijskih i informacijskih sustava u Komisiji utvrđene su u Odluci Komisije (EU, Euratom) 2017/46 ([3]), posebno u članku 3. o načelima informatičke sigurnosti u Komisiji i članku 9. o vlasnicima sustava.

(5) Cilj je provedbenih pravila koja se odnose na uloge i odgovornosti glavnih aktera u području sigurnosti pružiti smjernice o preduvjetima i dužnostima koje su u vezi s tim ulogama utvrđene u odlukama (EU, Euratom) 2015/443 i (EU, Euratom) 2015/444.

(6) U članku 36. stavku 7. Odluke (EU, Euratom) 2015/444 utvrđen je niz dodatnih funkcija povezanih sa sigurnošću koje treba preuzeti sigurnosno tijelo Komisije. U ovoj se Odluci utvrđuju zadaće povezane s tim funkcijama.

(7) Lokalni službenici za sigurnost i nadzorni službenici registarskog ureda imaju posebne odgovornosti povezane sa zaštitom klasificiranih podataka EU-a u svojim službama u skladu s Odlukom (EU, Euratom) 2015/444.

(8) Komisija je 4. svibnja 2016. donijela odluku ([4]) kojom je člana Komisije nadležnog za sigurnosna pitanja ovlastila da u ime Komisije i pod njezinom odgovornošću donese provedbena pravila propisana člankom 60. Odluke (EU, Euratom) 2015/444; slijedom toga 13. travnja 2021. član Komisije nadležan za sigurnosna pitanja donio je u ime Komisije i pod njezinom odgovornošću odluku ([5]) o daljnjem delegiranju tih provedbenih pravila glavnom direktoru Glavne uprave za ljudske resurse i sigurnost,

([1]) SL L 72, 17.3.2015., str. 41.
([2]) SL L 72, 17.3.2015., str. 53.
([3]) Odluka Komisije (EU, Euratom) 2017/46 od 10. siječnja 2017. o sigurnosti komunikacijskih i informacijskih sustava u Europskoj komisiji (SL L 6, 11.1.2017., str. 40.).
([4]) Odluka Komisije C(2016) 2797 od 4. svibnja 2016. o ovlaštenju povezanom sa sigurnošću.
([5]) Odluka Komisije C(2021) 2684 final od 13. travnja 2021. o odobravanju daljnjeg delegiranja ovlasti dodijeljenih Odlukom Komisije C(2016) 2797 o ovlaštenju povezanom sa sigurnošću.

DONIJELA JE OVU ODLUKU:

POGLAVLJE 1.

Opće odredbe

Članak 1.

Predmet i područje primjene

1. Ovom se Odlukom utvrđuju uloge i odgovornosti glavnih aktera u području sigurnosti koji su odgovorni za zaštitu klasificiranih podataka EU-a u Komisiji na temelju odluka (EU, Euratom) 2015/443 i (EU, Euratom) 2015/444.

2. Ova Odluka primjenjuje se na sve službe Komisije i u svim prostorima Komisije.

POGLAVLJE 2.

Glavna uprava za ljudske resurse i sigurnost

Članak 2.

Sigurnosno tijelo Komisije

1. Direktor Uprave za sigurnost u Glavnoj upravi za ljudske resurse i sigurnost jest sigurnosno tijelo Komisije (Commission Security Authority, CSA) iz članka 7. Odluke (EU, Euratom) 2015/444.

2. U skladu s člancima od 3. do 7. ove Odluke CSA obavlja funkcije u sljedećim područjima kako su utvrđena u Odluci (EU, Euratom) 2015/444:

(a) sigurnost osoblja;

(b) fizička sigurnost;

(c) upravljanje klasificiranim podacima EU-a;

(d) akreditacija svih komunikacijskih i informacijskih sustava (Communication and Information System, CIS) za postupanje s klasificiranim podacima EU-a;

(e) gospodarska sigurnost; i

(f) razmjena klasificiranih podataka.

3. CSA organizira obvezno osposobljavanje za lokalne službenike za sigurnost (LSS) i njihove zamjenike te nadzorne službenike registarskog ureda (Registry Control Officer, RCO) i njihove zamjenike o njihovim odgovornostima i dužnostima.

Članak 3.

Tijelo za informacijsku sigurnost

Tijelo za informacijsku sigurnost odgovorno je za sljedeće aktivnosti povezane sa zaštitom klasificiranih podataka EU-a:

(a) oblikovanje politika zaštite informacijske sigurnosti i sigurnosnih smjernica te praćenje njihove učinkovitosti i primjerenosti;

(b) zaštitu i primjenu tehničkih podataka povezanih s kriptografskim proizvodima;

(c) osiguravanje, prema potrebi, usklađenosti mjera informacijske sigurnosti sa sigurnosnim politikama i politikama javne nabave Komisije;

(d) osiguravanje odabira kriptografskih proizvoda u skladu s politikama kojima se uređuje njihova prihvatljivost i odabir;

(e) savjetovanje s vlasnicima sustava, pružateljima sustava, akterima u području sigurnosti i predstavnicima korisnika o politikama zaštite informacijske sigurnosti i sigurnosnim smjernicama.

Članak 4.

Tijelo za sigurnosnu akreditaciju

1. CSA je odgovoran za akreditaciju sigurnosnih zona koje ispunjavaju zahtjeve iz članka 18. Odluke 2015/444 i CIS-ova za postupanje s klasificiranim podacima EU-a.

2. Službe Komisije prema potrebi se u koordinaciji sa svojim LSS-om i lokalnim službenikom za informacijsku sigurnost (Local Informatics Security Officer, LISO) savjetuju s tijelom za sigurnosnu akreditaciju kad god služba namjerava:

(a) izgraditi sigurnosnu zonu;

(b) uvesti CIS za postupanje s klasificiranim podacima EU-a;

(c) instalirati bilo koju drugu opremu za postupanje s klasificiranim podacima, uključujući za povezivanje s CIS-om treće strane.

Tijelo za sigurnosnu akreditaciju pruža savjete o tim aktivnostima i tijekom planiranja i tijekom izgradnje ili razvoja.

3. U sigurnosnoj zoni ili CIS-u ne smije se postupati s klasificiranim podacima EU-a prije nego što tijelo za sigurnosnu akreditaciju izda akreditaciju za odgovarajući stupanj tajnosti klasificiranih podataka EU-a.

4. Zahtjevi za akreditaciju određene sigurnosne zone uključuju:

(a) odobrenje planova za sigurnosnu zonu;

(b) odobrenje svih ugovora za radove koje izvode vanjski izvođači, uzimajući u obzir odredbe o gospodarskoj sigurnosti, kao što su eventualni zahtjevi za sigurnosne provjere izvođača i njihova osoblja;

(c) posjedovanje svih potrebnih izjava i potvrda o sukladnosti;

(d) fizičku inspekciju sigurnosne zone kako bi se provjerilo jesu li građevinski materijali i metode, kontrole pristupa, zaštitna oprema i svi drugi elementi u skladu sa zahtjevima CSA-a;

(e) provjeru valjanosti mjera protiv elektromagnetskog zračenja za sve tehnički zaštićene sigurnosne zone;

(f) odobrenje sigurnosnih operativnih postupaka za tu sigurnosnu zonu.

5. Zahtjevi za akreditaciju CIS-a za postupanje s klasificiranim podacima EU-a uključuju:

(a) izradu strategije za akreditaciju sustava;

(b) provjeru valjanosti sigurnosnog plana za CIS na temelju pristupa upravljanju rizicima;

(c) provjeru valjanosti sigurnosnih operativnih postupaka za CIS;

(d) provjeru valjanosti sve druge potrebne sigurnosne dokumentacije kako je utvrdilo tijelo za sigurnosnu akreditaciju;

(e) odobrenje svake upotrebe tehnologija šifriranja;

(f) provjeru valjanosti mjera protiv elektromagnetskog zračenja za CIS koji postupa s podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim;

(g) inspekciju CIS-a kako bi se provjerilo jesu li dokumentirane sigurnosne mjere ispravno uvedene.

6. Ako su zahtjevi za akreditaciju ispunjeni, tijelo za sigurnosnu akreditaciju izdaje službeno ovlaštenje za postupanje s klasificiranim podacima EU-a u sigurnosnoj zoni ili CIS-u, i to za navedeni najviši stupanj tajnosti klasificiranih podataka EU-a i na razdoblje do pet godina, ovisno o stupnju tajnosti klasificiranih podataka EU-a s kojima se postupa i povezanim rizicima.

7. Nakon obavijesti o povredi sigurnosti ili znatnoj izmjeni projekta ili sigurnosnih mjera u sigurnosnoj zoni ili CIS-u tijelo za sigurnosnu akreditaciju preispituje i, ako je potrebno, može opozvati ovlaštenje za postupanje s klasificiranim podacima EU-a dok se ne riješe utvrđeni problemi.

Članak 5.

Tijelo za TEMPEST

1. Sigurnosne mjere TEMPEST provode se radi zaštite CIS-a koji postupa s podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim, a mogu se primijeniti i na podatke klasificirane stupnjem tajnosti RESTREINT UE/EU RESTRICTED.

2. Tijelo za TEMPEST odgovorno je za odobravanje mjera poduzetih radi zaštite klasificiranih podataka EU-a od ugroze nenamjernim elektromagnetnim zračenjem.

3. Na zahtjev vlasnika CIS-a koji postupa s klasificiranim podacima EU-a tijelo za TEMPEST izdaje specifikacije za sigurnosne mjere TEMPEST koje odgovaraju stupnju tajnosti podataka.

4. U postupku akreditacije sigurnosnih zona i CIS-ova za postupanje s podacima EU-a klasificiranih stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim tijelo za TEMPEST provodi tehničko ispitivanje i izdaje certifikat TEMPEST nakon njegova uspješnog završetka.

5. U certifikatu TEMPEST navode se barem:

(a) datum ispitivanja;

(b) opis sigurnosnih mjera TEMPEST uz koji su priloženi planovi prostora;

(c) datum isteka certifikata;

(d) sve izmjene koje će certifikat učiniti nevažećim;

(e) potpis tijela za TEMPEST.

6. LSS ili organizator sastanka odgovoran za organizaciju povjerljivog sastanka, u koordinaciji s LSS-om, može od tijela za TEMPEST zatražiti da ispita prostorije za sastanke kako bi se provjerilo jesu li tehnički zaštićene.

Članak 6.

Tijelo za odobravanje kriptomaterijala

1. Tijelo za odobravanje kriptomaterijala odgovorno je za odobravanje primjene tehnologija šifriranja.

2. Tijelo za odobravanje kriptomaterijala izdaje smjernice o zahtjevima za primjenu i odobravanje tehnologija šifriranja.

3. Tijelo za odobravanje kriptomaterijala odobrava primjenu rješenja za šifriranje na temelju zahtjeva vlasnika sustava. Odobrenje se temelji na zadovoljavajućoj ocjeni barem sljedećih elemenata:

(a) sigurnosnih potreba podataka koje treba zaštititi;

(b) pregleda CIS-a koji se primjenjuje u rješenju;

(c) procjene inherentnih i preostalih rizika,

(d) opisa predloženog rješenja;

(e) sigurnosnih operativnih postupaka za rješenje za šifriranje.

4. Tijelo za odobravanje kriptomaterijala vodi registar odobrenih rješenja za šifriranje.

Članak 7.

Tijelo za distribuciju kriptomaterijala

1. Tijelo za distribuciju kriptomaterijala odgovorno je za distribuciju kriptografskog materijala koji se primjenjuje za zaštitu klasificiranih podataka EU-a (uglavnom oprema za šifriranje, kriptografski ključevi, certifikati te povezani autentifikatori) sljedećim dionicima:

(a) korisnicima ili službama unutar Komisije za CIS-ove kojima upravljaju vanjske strane;

(b) korisnicima ili organizacijama izvan Komisije za CIS-ove kojima upravlja Komisija.

2. U skladu s člankom 17. stavkom 3. Odluke 2015/443 tijelo za distribuciju kriptomaterijala može distribuciju kriptografskog materijala trećim stranama delegirati drugim službama.

3. Tijelo za distribuciju kriptomaterijala jamči da se svi kriptografski materijali šalju sigurnim kanalima koji štite od neovlaštenog rukovanja i bilježe dokaze o takvom rukovanju, u skladu sa sigurnosnim pravilima koja se primjenjuju na stupanj tajnosti klasificiranih podataka EU-a koji će se tim materijalima štititi.

4. Tijelo za distribuciju kriptomaterijala daje smjernice LSS-u i, prema potrebi, LISO-u svake službe Komisije koja sudjeluje u proizvodnji, distribuciji ili primjeni kriptografskih materijala.

5. Tijelo za distribuciju kriptomaterijala osigurava uspostavu odgovarajućih sigurnosnih operativnih postupaka za postupak distribucije.

POGLAVLJE 3.

Službe Komisije

Članak 8.

Načelnici službi

1. Svaki načelnik službe imenuje:

(a) LSS-a i jednog ili više zamjenika, prema potrebi, za službu ili kabinet;

(b) RCO-a i jednog ili više zamjenika, prema potrebi, za svaku službu koja vodi registarski ured za klasificirane podatke EU-a;

(c) vlasnika sustava za svaki CIS koji postupa s klasificiranim podacima EU-a.

2. Prije imenovanja LSS-a i njihovih zamjenika te RCO-a i njihovih zamjenika načelnik službe traži odobrenje direktora Uprave za sigurnost Glavne uprave za ljudske resurse i sigurnost.

3. Načelnik službe, savjetujući se s LSS-om, utvrđuje sva radna mjesta za koja je potrebna provjera koja omogućuje pristup klasificiranim podacima EU-a. Kandidati za takva radna mjesta obavješćuju se o obveznoj sigurnosnoj provjeri u postupku zapošljavanja.

4. Načelnik svake službe u čijem se posjedu nalaze klasificirani podaci EU-a odgovoran je za aktiviranje planova za hitno uništavanje i evakuaciju kad je to potrebno. Planovi sadržavaju alternativu za situacije u kojima nije moguće stupiti u kontakt s načelnikom službe.

Članak 9.

Vlasnici CIS-ova koji postupaju s klasificiranim podacima EU-a

1. U okviru projekta za uspostavu CIS-a koji postupa s klasificiranim podacima EU-a vlasnik sustava što prije stupa u kontakt s tijelom za sigurnosnu akreditaciju kako bi se utvrdili relevantni sigurnosni standardi i zahtjevi te pokrenuo postupak sigurnosne akreditacije.

2. Vlasnik sustava osigurava da su sigurnosne mjere u skladu sa zahtjevima tijela za sigurnosnu akreditaciju te da CIS ne postupa s klasificiranim podacima EU-a prije nego što je akreditiran.

3. Vlasnik sustava obraća se tijelu za odobravanje kriptomaterijala kako bi zatražio odobrenje za primjenu bilo koje tehnologije šifriranja. Vlasnici sustava ne smiju primjenjivati tehnologije šifriranja u aktivnim sustavima bez prethodnog odobrenja.

4. Vlasnik sustava savjetuje se s LISO-om svoje službe o pitanjima koja se odnose na sigurnost CIS-ova.

5. Vlasnik sustava najmanje jednom godišnje preispituje sigurnosne mjere koje se primjenjuju na sustav, uključujući sigurnosni plan.

6. Ako se u CIS-u dogodi sigurnosni incident na temelju kojeg se utvrdi da CIS više ne može na odgovarajući način štititi klasificirane podatke EU-a, vlasnik sustava o tome obavješćuje LSS-a i smjesta se obraća tijelu za sigurnosnu akreditaciju radi savjeta o daljnjem postupanju. U tom se slučaju akreditacija može privremeno oduzeti, a sustav se može isključiti dok se ne poduzmu odgovarajuće korektivne mjere.

7. Vlasnik sustava u svakom trenutku pruža tijelu za sigurnosnu akreditaciju punu podršku u obavljanju dužnosti povezanih s akreditacijom CIS-a.

Članak 10.

Operativno tijelo za informacijsku sigurnost

Za svaki CIS operativno tijelo za informacijsku sigurnost:

(a) priprema sigurnosnu dokumentaciju u skladu sa sigurnosnim politikama i smjernicama, prije svega sigurnosni plan, sigurnosne operativne postupke povezane s tim sustavom i kriptografsku dokumentaciju u okviru postupka akreditacije CIS-a;

(b) sudjeluje u odabiru i ispitivanju tehničkih sigurnosnih mjera, uređaja i softvera specifičnih za sustav radi nadzora njihova uvođenja i sigurne instalacije, konfiguracije i održavanja u skladu s odgovarajućom sigurnosnom dokumentacijom;

(c) sudjeluje u odabiru sigurnosnih mjera i uređaja TEMPEST ako se to zahtijeva u sigurnosnom planu te u suradnji s tijelom za TEMPEST osigurava njihovu sigurnu instalaciju i održavanje;

(d) prati uvođenje i primjenu sigurnosnih operativnih postupaka povezanih s radom sustava;

(e) u suradnji s tijelom za distribuciju kriptomaterijala upravlja i postupa s kriptografskim proizvodima radi pravilnog čuvanja kriptografskih materijala i kontroliranih predmeta te, prema potrebi, generiranja kriptografskih varijabli;

(f) provodi sigurnosnu analizu, preglede i ispitivanja, posebno radi izrade relevantnih izvješća o riziku, u skladu sa zahtjevima tijela za sigurnosnu akreditaciju;

(g) pruža osposobljavanje u području informacijske sigurnosti za predmetni CIS;

(h) uvodi i upravlja sigurnosnim mjerama koje se primjenjuju na predmetni CIS.

POGLAVLJE 4.

Lokalni službenik za sigurnost

Članak 11.

Imenovanje lokalnog službenika za sigurnost

1. LSS i njegovi zamjenici dužnosnici su ili članovi privremenog osoblja.

2. Svi LSS-i i njihovi zamjenici posjeduju valjano sigurnosno ovlaštenje za pristup klasificiranim podacima EU-a do stupnja tajnosti SECRET UE/EU SECRET i, prema potrebi, do stupnja tajnosti TRES SECRET UE/EU TOP SECRET. LSS ili njegov zamjenik prije imenovanja pribavlja sigurnosno ovlaštenje.

3. Predstavništva Komisije mogu od CSA-a zatražiti da odobri iznimku od zahtjeva iz stavaka 1. i 2.

Članak 12.

Sigurnosni operativni postupci za sigurnosne zone

1. LSS predmetne službe Komisije priprema sigurnosne operativne postupke za svaku sigurnosnu zonu za koju je odgovoran.

2. LSS osigurava da sigurnosni operativni postupci uključuju sljedeće zahtjeve:

(a) pristup bez pratnje sigurnosnoj zoni tijekom radnog vremena dopušten je samo članovima osoblja s valjanim sigurnosnim ovlaštenjem i utvrđenom potrebom za pristupom dokumentima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim;

(b) pristup bez pratnje sigurnosnoj zoni izvan radnog vremena odobrava se samo LSS-u službe, RCO-ima sigurnosne zone, njihovim zamjenicima i ovlaštenom osoblju Uprave za sigurnost Glavne uprave za ljudske resurse i sigurnost;

(c) uređaji za snimanje i komunikaciju kao što su mobilni telefoni, računala, kamere ili drugi pametni uređaji nisu dopušteni unutar zaštićenih područja bez prethodnog odobrenja CSA-a; svako odstupanje mora se od CSA-a zatražiti unaprijed; LSS je osoba za kontakt;

(d) svi članovi unutarnjeg ili vanjskog osoblja kojima je potreban pristup sigurnosnoj zoni, ali ne ispunjavaju kriterije navedene u točki (a) u stalnoj su pratnji i pod stalnim nadzorom propisno ovlaštenog člana osoblja; svaki takav pristup sigurnosnoj zoni bilježi se u dnevnik koji se vodi na ulazu u sigurnosnu zonu;

(e) LSS osigurava da su sustavi za otkrivanje neovlaštenog pristupa kojima se nadzire sigurnosna zona u svakom trenutku aktivni i pravilno funkcioniraju te upravlja svim povezanim lozinkama, ključevima, PIN-ovima ili drugim mehanizmima za pristup i autentifikaciju;

(f) uzbune u sigurnosnoj zoni prijavljuju se Upravi za sigurnost Glavne uprave za ljudske resurse i sigurnost, koja o tome smjesta obavješćuje LSS-a;

(g) LSS službe u kojoj se nalazi sigurnosna zona vodi evidenciju o svakoj intervenciji nakon uzbune ili sigurnosnog incidenta;

(h) uspostavljaju se postupci za slučaj uzbune ili druge krizne situacije unutar sigurnosne zone, među ostalim za evakuaciju osoblja i pružanje brzog odgovora tima za hitne slučajeve pod nadležnošću CSA-a i, prema potrebi, vanjskih hitnih službi;

(i) LSS o svakoj povredi sigurnosti koja se dogodi unutar sigurnosne zone ili je s njom povezana smjesta izvješćuje CSA kako bi se utvrdio odgovarajući odgovor;

(j) pojedinačni uredi, prostorije i sefovi unutar sigurnosne zone zaključavaju se svaki put kad ih se ostavlja bez nadzora;

(k) članovi osoblja suzdržavaju se od rasprava o klasificiranim podacima na hodnicima ili u drugim zajedničkim prostorijama sigurnosne zone ako se u blizini nalaze neovlašteni pojedinci.

Članak 13.

Sigurnosni ključevi i kombinacije

1. LSS je u cijelosti odgovoran za pravilno rukovanje ključevima i kombinacijama koje se upotrebljavaju u sigurnosnim zonama, za pristup njima te za njihovo pravilno pohranjivanje. Ključevi i kombinacije pohranjuju se u sigurnosnom spremniku i zaštićeni su barem na istoj razini kao i materijal kojem omogućuju pristup.

2. LSS vodi registar sigurnosnih spremnika i trezora te ažurirani popis svih članova osoblja koji tim spremnicima i trezorima smiju pristupiti bez pratnje.

3. LSS vodi registar ključeva za sigurnosne spremnike i trezore u kojem se navode i članovi osoblja kojima su dodijeljeni. Za svaki izdani ključ sastavlja se potvrda o primitku u kojoj se navode identifikacija ključa, primatelj, datum i vrijeme.

4. Ključevi i kombinacije izdaju se samo članovima osoblja za koje je utvrđena nužnost pristupa podacima i kojima je izdano odgovarajuće ovlaštenje za pristup klasificiranim podacima EU-a. LSS preuzima sve ključeve za koje ti uvjeti više nisu ispunjeni.

5. LSS čuva rezervne ključeve i vodi pisanu evidenciju o svakoj postavci kombinacije u pojedinačnim zapečaćenim, netransparentnim, potpisanim i datiranim omotnicama koje dostavlja član osoblja odgovoran za ključeve. Te se omotnice čuvaju u sigurnosnom spremniku klasificiranom stupnjem tajnosti koji odgovara najvišem stupnju tajnosti materijala pohranjenog u odgovarajućem spremniku ili trezoru.

6. Ako su nakon promjene kombinacije ili rotacije ključa na omotnici vidljivi dokazi o neovlaštenom rukovanju ili oštećenju, LSS to smatra sigurnosnim incidentom i o tome smjesta obavješćuje CSA.

7. Postavke kombinacija za sigurnosne spremnike u sigurnosnim zonama mijenjaju se pod nadzorom LSS-a. Kombinacije se ponovno postavljaju najmanje svakih 12 mjeseci i svaki put:

(a) kad se zaprimi novi spremnik ili ugradi nova brava (zadane se kombinacije moraju smjesta promijeniti);

(b) kad postoji sumnja na ugrozu ili je nastupila ugroza;

(c) kad osoba koja posjeduje kombinaciju više ne treba pristup.

8. LSS vodi evidenciju o datumima promjena kombinacije iz stavka 7.

Članak 14.

Planovi za hitnu evakuaciju i uništavanje klasificiranih podataka EU-a

1. LSS pomaže načelniku službe u izradi planova evakuacije i uništavanja klasificiranih podataka EU-a u hitnim slučajevima na temelju smjernica Uprave za sigurnost Glavne uprave za ljudske resurse i sigurnost.

2. LSS poduzima sve što je potrebno da sva oprema potrebna za provedbu planova iz stavka 1. bude lako dostupna i da se održava u ispravnom stanju.

3. LSS zajedno s dužnosnicima imenovanima u planovima iz stavka 1. preispituje stanje pripravnosti planova najmanje svakih 12 mjeseci i poduzima sve mjere potrebne za njihovo ažuriranje.

Članak 15.

Sigurnosna ovlaštenja

1. LSS vodi evidenciju svih radnih mjesta u službi za koja je potrebno sigurnosno ovlaštenje Komisije i članova osoblja zaposlenih na tim radnim mjestima. Obveza posjedovanja sigurnosnog ovlaštenja mora se navesti u oglasu za slobodno radno mjesto u okviru postupka zapošljavanja, a kandidat se o njoj mora obavijestiti na razgovoru.

2. LSS nadzire sve zahtjeve za sigurnosna ovlaštenja za pristup klasificiranim podacima EU-a. LSS je osoba za kontakt u službi i surađuje sa CSA-om u pogledu sigurnosnih ovlaštenja.

3. LSS podnosi zahtjev za pokretanje postupka za pribavljanje sigurnosnog ovlaštenja za predmetnog člana osoblja i osigurava da član osoblja CSA-u bez odgode vrati upitnik u okviru nacionalne sigurnosne provjere.

4. LSS osigurava da članovi osoblja iz službe koji su prošli sigurnosnu provjeru sudjeluju na obveznom informativnom sastanku o klasificiranim podacima EU-a kako bi pribavili sigurnosno ovlaštenje.

5. LSS je u redovitom kontaktu s odjelom za ljudske resurse svoje službe kako bi dobio informacije o svim promjenama na radnim mjestima za koja je potrebno sigurnosno ovlaštenje i o svakoj takvoj promjeni smjesta obavješćuje CSA.

6. LSS obavješćuje CSA o dolasku novog člana osoblja s postojećim uvjerenjem o sigurnosnoj provjeri na radno mjesto na kojem mora biti zaposlen član osoblja sa sigurnosnim ovlaštenjem.

7. LSS provjerava jesu li članovi osoblja u službi dovršili postupak obnove uvjerenja o sigurnosnoj provjeri do propisanog roka. Svaki član osoblja koji odbije dovršiti postupak obvezan je premjestiti se na radno mjesto na kojem ne mora biti zaposlen član osoblja sa sigurnosnim ovlaštenjem.

Članak 16.

Registarski ured za klasificirane podatke EU-a

1. Ako služba ima registarski ured za klasificirane podatke EU-a, LSS nadzire aktivnosti RCO-a koje se odnose na postupanje s klasificiranim podacima EU-a i usklađenost sa sigurnosnim pravilima o zaštiti klasificiranih podataka EU-a.

2. LSS najmanje svakih 12 mjeseci te nakon promjene RCO-a ili njegova zamjenika provodi sljedeće provjere:

(a) provjeru uzorka dokumenata iz registarskog ureda za klasificirane podatke EU-a kako bi se potvrdio njihov status i točnost registra klasificiranih dokumenata;

(b) provjeru uzorka potvrda o primitku i prijenosu koje se odnose na prenošenje klasificiranih podataka EU-a u registarski ured za klasificirane podatke EU-a i iz njega;

(c) provjeru uzorka potvrda o uništavanju.

3. LSS najmanje jednom mjesečno provodi nasumične provjere registra klasificiranih dokumenata i nedavno zaprimljenih klasificiranih dokumenata kako bi se uvjerio da se pravilno registriraju.

4. Sve provjere bilježe se u dnevnik registarskog ureda za klasificirane dokumente.

Članak 17.

Druge odgovornosti povezane sa sigurnošću

Druge odgovornosti LSS-a povezane sa sigurnošću utvrđuju se u sigurnosnoj uputi koja se prvenstveno odnosi na fizičku sigurnost osoba, prostora i druge imovine te podataka.

POGLAVLJE 5.

Nadzorni službenik registarskog ureda

Članak 18.

Imenovanje RCO-a

1. RCO i njegovi zamjenici dužnosnici su ili članovi privremenog osoblja.

2. Svi RCO-i i njihovi zamjenici posjeduju valjano sigurnosno ovlaštenje za pristup klasificiranim podacima EU-a do stupnja tajnosti SECRET UE/EU SECRET i, prema potrebi, do stupnja tajnosti TRES SECRET UE/EU TOP SECRET. RCO ili njegov zamjenik prije imenovanja pribavlja sigurnosno ovlaštenje.

3. Predstavništva Komisije mogu od CSA-a zatražiti da odobri iznimku od zahtjeva iz stavaka 1. i 2.

Članak 19.

Odgovornosti

1. RCO-i informacije klasificirane stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim registriraju u sigurnosne svrhe:

(a) kad stignu u službu Komisije ili je napuste; ili

(b) kad stignu u CIS ili ga napuste.

2. RCO-i registriraju sve događaje u životnom ciklusu svih informacija klasificiranih stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim. RCO-i se usto brinu o vođenju evidencije o svim podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED ili jednakovrijednim stupnjem koji se razmjenjuju s trećim zemljama i međunarodnim organizacijama. To se provodi u koordinaciji s registarskim uredom za klasificirane podatke EU-a kojim upravlja Glavno tajništvo.

3. RCO registrira dokumente klasificirane stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim u registar klasificiranih dokumenata i osigurava da su sigurno pohranjeni u registarskom uredu za klasificirane podatke EU-a.

4. RCO pomaže osoblju Komisije u izradi i slanju podataka klasificiranih stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim.

5. Kad od drugih službi ili vanjskih strana primi dokumente klasificirane stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim, RCO osigurava da se pošiljatelju propisno vrati potvrda o isporuci.

6. Prije nego što članu osoblja omogući pristup klasificiranom dokumentu pohranjenom u registarskom uredu za klasificirane podatke EU-a, RCO provjerava s LSS-om posjeduje li član osoblja sigurnosno ovlaštenje koje je izdao CSA.

7. RCO evidentira sve članove osoblja koji ulaze u registarski ured za klasificirane podatke EU-a i iz njega izlaze, a koji nisu ovlašteni za pristup bez pratnje, te ih prati za vrijeme posjeta.

8. Ako član osoblja iznese dokument iz registarskog ureda za klasificirane podatke EU-a radi uvida, RCO poduzima sve što je potrebno da taj član osoblja bude upoznat s relevantnim kompenzacijskim sigurnosnim mjerama i da vrati dokument čim mu više nije potreban. RCO podsjeća članove osoblja da svaki takav dokument vrate što prije.

9. Ako se klasificirani dokumenti ručno iznose izvan zemlje u kojoj se nalazi registarski ured, registarski ured za klasificirane podatke EU-a izdaje kurirsku potvrdu.

10. Detaljne upute za RCO-e o registraciji klasificiranih dokumenata navode se u sigurnosnoj uputi.

Članak 20.

Smanjenje stupnja tajnosti ili deklasifikacija

RCO pomaže službama iz kojih podaci potječu u postupku pregleda registriranih klasificiranih podataka EU-a kako bi se utvrdilo je li izvorni stupanj tajnosti dokumenta još uvijek primjeren ili ga se može smanjiti ili može li se dokument deklasificirati.

Članak 21.

Uništavanje

1. RCO-i su odgovorni za uništavanje podataka klasificiranih stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i višim na odobren način, prema potrebi u prisutnosti svjedoka koji su prošli sigurnosnu provjeru.

2. RCO-i svako uništavanje podataka klasificiranih stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i višim evidentiraju u registru klasificiranih dokumenata i čuvaju odgovarajuće potvrde o uništavanju u registarskom uredu za klasificirane podatke EU-a.

Članak 22.

Dodatne zadaće

1. RCO pruža svu potrebnu pomoć LSS-u pri provedbi nadzornih aktivnosti u registarskom uredu za klasificirane podatke EU-a.

2. RCO sve sumnjive ili stvarne sigurnosne incidente prijavljuje LSS-u, a on ih zatim prijavljuje CSA-u.

3. RCO registarskog ureda za klasificirane podatke EU-a službe Komisije koja organizira povjerljiv sastanak sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim priprema klasificirane podatke EU-a s kojima će se postupati na sastanku i radi u koordinaciji s organizatorom sastanka kako bi se zajamčilo da se sa svim dokumentima i potvrdama postupa u skladu s relevantnim pravilima.

POGLAVLJE 6.

Završne odredbe

Članak 23.

Transparentnost

O ovoj se Odluci obavješćuje osoblje Komisije i pojedince na koje se odnosi te se ona objavljuje u Službenom listu Europske unije.

Članak 24.

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

Sastavljeno u Bruxellesu 7. travnja 2022.

Za Komisiju,
u ime predsjednice,
Gertrud INGESTAD
Glavna direktorica
Glavna uprava za ljudske resurse i sigurnost