ISSN 1977-0596

# Službeni list Europske unije

L 274

Hrvatsko izdanje

Zakonodavstvo

Svezak 56.

15. listopada 2013.

Sadržaj



**Cijena: 4 EUR**

HR

Akti čiji su naslovi tiskani običnim slovima su oni koji se odnose na svakodnevno upravljanje poljoprivrednim pitanjima, a općenito vrijede ograničeno razdoblje.

Naslovi svih drugih akata tiskani su masnim slovima, a prethodi im zvjezdica.

II.

*(Nezakonodavni akti)*

# ODLUKE

## ODLUKA VIJEĆA

## od 23. rujna 2013.

## o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a

(2013/488/EU)

VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 240. stavak 3.,

uzimajući u obzir Odluku Vijeća 2009/937/EU od 1. prosinca 2009. o donošenju Poslovnika Vijeća [1], a posebno njezin članak 24.,

budući da:

(1) Kako bi se razvile aktivnosti Vijeća u svim područjima u kojima je potrebno postupati s klasificiranim podacima, primjereno je uspostaviti sveobuhvatni sigurnosni sustav za zaštitu klasificiranih podataka kojim će biti obuhvaćeni Vijeće, njegovo Glavno tajništvo i države članice.

(2) Ova bi se Odluka trebala primjenjivati kada Vijeće, njegova pripremna tijela i Glavno tajništvo Vijeća (GSC) postupaju s klasificiranim podacima EU-a (EUCI-jem).

(3) U skladu s nacionalnim zakonima i propisima i u mjeri u kojoj je to potrebno za funkcioniranje Vijeća, države članice trebale bi poštovati ovu Odluku kada njihova nadležna tijela, osoblje ili ugovaratelji postupaju s klasificiranim podacima EU-a, kako bi svi bili sigurni da je za klasificirane podatke EU-a osigurana jednaka razina zaštite.

(4) Vijeće, Komisija i Europska služba za vanjsko djelovanje (EEAS) zalažu se za primjenu jednakih sigurnosnih standarda za zaštitu klasificiranih podataka EU-a.

(5) Vijeće ističe važnost povezivanja, prema potrebi, Europskog parlamenta i drugih institucija, tijela, ureda ili agencija Unije s načelima, standardima i pravilima za zaštitu klasificiranih podataka nužnih za zaštitu interesa Unije i njezinih država članica.

(6) Vijeće bi trebalo utvrditi odgovarajući okvir za razmjenu klasificiranih podataka EU-a u posjedu Vijeća s drugim institucijama, tijelima, uredima ili agencijama Unije, prema potrebi, u skladu s ovom Odlukom i međuinstitucionalnim dogovorima koji su na snazi.

(7) Tijela i agencije EU-a uspostavljeni na temelju glave V. poglavlja 2. Ugovora o Europskoj uniji (UEU), Europol i Eurojust trebali bi primjenjivati, u kontekstu svoje interne organizacije, osnovna načela i minimalne standarde za zaštitu klasificiranih podataka EU-a utvrđene u ovoj Odluci ako je tako predviđeno u aktu o njihovoj uspostavi.

(8) Na operacije upravljanja krizama uspostavljene na temelju glave V. poglavlja 2. UEU-a i njihovo osoblje trebala bi se primjenjivati sigurnosna pravila koja je donijelo Vijeće u svrhu zaštite klasificiranih podataka EU-a kada je to predviđeno aktom Vijeća o njihovoj uspostavi.

(9) Posebni predstavnici EU-a i članovi njihovih timova trebali bi primjenjivati sigurnosna pravila koja je donijelo Vijeće u svrhu zaštite klasificiranih podataka EU-a kada je tako predviđeno relevantnim aktom Vijeća.

(10) Donošenjem ove Odluke ne dovode se u pitanje članci 15. i 16. Ugovora o funkcioniranju Europske unije (UFEU) te instrumenti kojima se ti članci provode.

(11) Donošenjem ove Odluke ne dovodi se u pitanje postojeća praksa u državama članicama s obzirom na obavješćivanje njihovih nacionalnih parlamenata o aktivnostima Unije.

[1] SL L 325, 11.12.2009., str. 35.

(12) Kako bi se osigurala pravodobna primjena sigurnosnih pravila u pogledu zaštite klasificiranih podataka EU-a s obzirom na pristupanje Republike Hrvatske Europskoj uniji, ova bi Odluka trebala stupiti na snagu na dan objave,

DONIJELO JE OVU ODLUKU:

*Članak 1.*

**Svrha, područje primjene i definicije**

1. Ovom se Odlukom utvrđuju osnovna načela i minimalni standardi sigurnosti za zaštitu klasificiranih podataka EU-a (EUCI).

2. Navedeni minimalni standardi i osnovna načela primjenjuju se na Vijeće i GSC, a države članice ih poštuju u skladu s njihovim nacionalnim zakonima i propisima kako bi svi bili sigurni da je za klasificirane podatke EU-a osigurana jednaka razina zaštite.

3. Za potrebe ove Odluke primjenjuju se definicije navedene u Dodatku A.

*Članak 2.*

**Definicija klasificiranih podataka EU-a, stupnjeva tajnosti i oznaka**

1. „Klasificirani podaci EU-a" (EUCI) znači svaki podatak ili materijal koji je označen stupnjem tajnosti EU-u i čije neovlašteno otkrivanje može uzrokovati različite stupnjeve prijetnje nanošenjem štete interesima Europske unije ili jedne ili više država članica.

2. Klasificirani podaci EU-a klasificiraju se prema sljedećim stupnjevima tajnosti:

(a) TRÈS SECRET UE/EU TOP SECRET podaci i materijali čije neovlašteno otkrivanje može iznimno teško naštetiti bitnim interesima Europske unije ili jedne ili više država članica;

(b) SECRET UE/EU SECRET podaci i materijali čije neovlašteno otkrivanje može teško naštetiti bitnim interesima Europske unije ili jedne ili više država članica;

(c) CONFIDENTIEL UE/EU CONFIDENTIAL podaci i materijali čije neovlašteno otkrivanje može nanijeti štetu bitnim interesima Europske unije ili jedne ili više država članica;

(d) RESTREINT UE/EU RESTRICTED podaci i materijali čije neovlašteno otkrivanje može dovesti u nepovoljan položaj interese Europske unije ili jedne ili više država članica.

3. Klasificirani podaci EU-a moraju biti označeni stupnjem tajnosti u skladu sa stavkom 2. Mogu nositi i dodatne oznake kojima se utvrđuje područje djelatnosti na koje se odnose, određuje onog od kojeg potječu, ograničava distribucija, ograničava uporaba ili naznačuje mogućnost objavljivanja.

*Članak 3.*

**Upravljanje klasifikacijom**

1. Nadležna tijela osiguravaju da su klasificirani podaci EU-a klasificirani na odgovarajući način, da su jasno određeni kao klasificirani podaci i da zadrže svoj stupanj tajnosti samo onoliko dugo koliko je to potrebno.

2. Bez prethodne pisane suglasnosti onog od kojeg potječu, ne smije se smanjiti stupanj tajnosti klasificiranih podataka EU-a, klasificirani se podaci EU-a ne smiju deklasificirati niti se smije promijeniti ili ukloniti ijedna oznaka iz članka 2. stavka 3.

3. Vijeće odobrava sigurnosnu politiku za stvaranje klasificiranih podataka EU-a koja mora obuhvaćati i praktični vodič za klasificiranje.

*Članak 4.*

**Zaštita klasificiranih podataka**

1. Klasificirani podaci EU-a štite se u skladu s ovom Odlukom.

2. Imatelj klasificiranog podatka EU-a odgovoran je za njegovu zaštitu u skladu s ovom Odlukom.

3. Ako države članice uvedu klasificirane podatke s oznakom nacionalnog stupnja tajnosti u strukture ili mreže Unije, Vijeće i GSC štite navedene podatke u skladu sa zahtjevima primjenljivima na klasificirane podatke EU-a na jednakoj razini kako je utvrđeno u tablici ekvivalentnosti stupnjeva tajnosti sadržanoj u Dodatku B.

4. Skup klasificiranih podataka EU-a može nalagati stupanj zaštite koji odgovara višem stupnju tajnosti od njegovih pojedinačnih dijelova.

*Članak 5.*

**Upravljanje sigurnosnim rizicima**

1. Rizikom za klasificirane podatke EU-a upravlja se kao procesom. Cilj je tog procesa utvrđivanje poznatih sigurnosnih rizika, definiranje sigurnosnih mjera za smanjenje takvih rizika na prihvatljivu razinu u skladu s osnovnim načelima i minimalnim standardima navedenima u ovoj Odluci te primjena navedenih mjera u skladu s konceptom dubinske obrane kako je određeno u Dodatku A. Učinkovitost takvih mjera stalno se ocjenjuje.

2. Sigurnosne mjere za zaštitu klasificiranih podataka EU-a moraju tijekom njihova životnog ciklusa biti primjerene njihovu stupnju tajnosti, obliku i opsegu podataka ili materijala, mjestu i konstrukciji objekata u kojima su smješteni klasificirani podaci EU-a i lokalno procijenjenoj prijetnji zlonamjernih i/ili kriminalnih aktivnosti, uključujući špijunažu, sabotažu i terorizam.

3. U kriznim se planovima mora imati na umu potrebu zaštite klasificiranih podataka EU-a u izvanrednim situacijama kako bi se spriječio neovlašteni pristup, otkrivanje ili gubitak cjelovitosti ili dostupnosti.

4. U planove neprekidnosti poslovanja moraju se uključiti preventivne mjere i mjere oporavka kako bi se na najmanju moguću mjeru sveli veliki propusti ili nezgode u postupanju s klasificiranim podacima EU-a i njihovu čuvanju.

*Članak 6.*

**Provedba ove Odluke**

1. Vijeće prema potrebi, na preporuku Sigurnosnog odbora, odobrava sigurnosne politike u kojima su navedene mjere za provedbu ove Odluke.

2. Sigurnosni se odbor na svojoj razini može dogovoriti o sigurnosnim smjernicama kojima će dopuniti ili potkrijepiti ovu Odluku te sve sigurnosne politike koje odobri Vijeće.

*Članak 7.*

**Sigurnost osoblja**

1. Sigurnost osoba je primjena mjera kojima se osigurava odobravanje pristupa klasificiranim podacima EU-a samo pojedincima:

— kojima je nužan pristup podacima,

— koji su, prema potrebi, prošli sigurnosnu provjeru za odgovarajući stupanj, i

— koji su upoznati sa svojim odgovornostima.

2. Postupci za sigurnosnu provjeru osoba oblikovani su tako da se njima utvrđuje može li se pojedinca, s obzirom na njegovu lojalnost, vjerodostojnost i pouzdanost, ovlastiti za pristup klasificiranim podacima EU-a.

3. Svi pojedinci u GSC-u koji zbog svojih dužnosti moraju imati pristup ili moraju postupati s klasificiranim podacima EU-a sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim moraju proći sigurnosnu provjeru za odgovarajući stupanj prije nego što im se omogući pristup takvim klasificiranim podacima EU-a. Te pojedince mora ovlastiti tijelo za imenovanja GSC-a za pristup klasificiranim podacima EU-a do određene razine i do određenog datuma.

4. Osoblje država članica iz članka 15. stavka 3., koje zbog svojih dužnosti može zatrebati pristup klasificiranim podacima EU-a sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim mora proći sigurnosnu provjeru za odgovarajući stupanj ili mora biti na neki drugi način propisno ovlašteno na temelju svojih funkcija, u skladu s nacionalnim zakonima i propisima, prije nego što mu se odobri pristup takvim klasificiranim podacima EU-a.

5. Prije nego što im se odobri pristup klasificiranim podacima EU-a te u pravilnim vremenskim razmacima nakon toga, svi se pojedinci upućuju u svoje odgovornosti povezane sa zaštitom klasificiranih podataka EU-a u skladu s ovom Odlukom te ih moraju prihvatiti.

6. Odredbe za provedbu ovog članka navedene su u Prilogu I.

*Članak 8.*

**Fizička sigurnost**

1. Fizička sigurnost je primjena fizičkih i tehničkih zaštitnih mjera za sprečavanje neovlaštenog pristupa klasificiranim podacima EU-a.

2. Cilj mjera fizičke sigurnosti je sprečavanje tajnog ili nasilnog ulaska neovlaštenih osoba, odvraćanje od neovlaštenih radnji, sprečavanje ili otkrivanje neovlaštenih radnji te omogućavanje razdvajanja osoblja koje pristupa klasificiranim podacima EU-a zbog nužnosti pristupa. Takve se mjere određuju na temelju procesa upravljanja rizicima.

3. Mjere fizičke sigurnosti uspostavljaju se za sve prostorije, zgrade, urede, sobe i druga područja u kojima se postupa s klasificiranim podacima EU-a ili se ondje čuvaju, uključujući područja u kojima su smješteni komunikacijski i informacijski sustavi kako je određeno u članku 10. stavku 2.

4. Područja u kojima se čuvaju klasificirani podaci EU-a sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili više utvrđuju se kao sigurnosne zone u skladu s Prilogom II., a odobrava ih nadležno sigurnosno tijelo.

5. Za zaštitu klasificiranih podataka EU-a sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili više koristi se samo odobrena oprema ili uređaji.

6. Odredbe za provedbu ovog članka navedene su u Prilogu II.

*Članak 9.*

**Upravljanje klasificiranim podacima**

1. Upravljanje klasificiranim podacima primjena je administrativnih mjera za kontrolu klasificiranih podataka EU-a tijekom njihova životnog ciklusa kojima se dopunjuju mjere iz članaka 7., 8. i 10. i pri tome pomaže pri odvraćanju i otkrivanju namjerne ili slučajne ugroze ili gubitka takvih podataka. Takve se mjere posebno odnose na stvaranje, upis, umnožavanje, prevođenje, smanjenje stupnja tajnosti, deklasifikaciju, prijenos i uništavanje klasificiranih podataka EU-a.

2. Podaci klasificirani kao CONFIDENTIEL UE/EU CONFIDENTIAL ili više upisuju se iz sigurnosnih razloga prije distribucije i po primitku. U tu svrhu nadležna tijela u GSC-u i državama članicama uspostavljaju sustav registara. Podaci klasificirani kao TRÈS SECRET UE/EU TOP SECRET upisuju se u predviđene registre.

3. Službe i prostorije u kojima se postupa s klasificiranim podacima EU-a ili se ondje čuvaju podliježu redovitim inspekcijama koje provodi nadležno sigurnosno tijelo.

4. Klasificirani podaci EU-a prosljeđuju se između službi i prostorija izvan fizički zaštićenih područja na sljedeći način:

(a) u pravilu, klasificirani podaci EU-a prenose se elektroničkim sredstvima koja su zaštićena kriptografskim proizvodima odobrenima u skladu s člankom 10. stavkom 6.;

(b) ako se ne uporabe sredstva iz točke (a), klasificirani podaci EU-a prenose se:

i. na elektroničkim medijima (npr. USB-u, CD-u, tvrdom disku) koji su zaštićeni kriptografskim proizvodima odobrenima u skladu s člankom 10. stavkom 6.; ili

ii. u svim drugim slučajevima na način koji je propisalo nadležno sigurnosno tijelo u skladu s odgovarajućim zaštitnim mjerama utvrđenima u Prilogu III.

5. Odredbe za provedbu ovog članka navedene su u prilozima III. i IV.

*Članak 10.*

**Zaštita klasificiranih podataka EU-a koji se obrađuju u komunikacijskim i informacijskih sustavima**

1. Informacijska sigurnost (IA) u području komunikacijskih i informacijskih sustava povjerenje je da će takvi sustavi štititi podatke koje obrađuju i da će funkcionirati onako kako trebaju, kada trebaju i pod kontrolom zakonitih imatelja. Učinkoviti IA osigurava odgovarajuće razine tajnosti, cjelovitosti, dostupnosti, nepobitnosti i autentičnosti. IA se temelji na procesu upravljanja rizicima.

2. „Komunikacijski i informacijski sustav" (CIS) znači svaki sustav koji omogućuje postupanje s podacima u elektroničkom obliku. CIS obuhvaća sva sredstva potrebna za njegov rad, uključujući infrastrukturu, organizaciju, osoblje i informacijske resurse. Ova se Odluka primjenjuje na CIS za postupanje s klasificiranim podacima EU-a (CIS).

3. CIS postupa s klasificiranim podacima EU-a u skladu s konceptom IA-a.

4. Svaki CIS mora proći proces akreditacije. Cilj je akreditacije pribavljanje potvrde da su sve odgovarajuće sigurnosne mjere provedene i da je ostvarena dostatna razina zaštite klasificiranih podataka EU-a i CIS-a u skladu s ovom Odlukom. U izjavi o akreditaciji određuju se najviši stupanj tajnosti podataka s kojima se može postupati u CIS-u i odgovarajući uvjeti.

5. Provode se sigurnosne mjere za zaštitu CIS-a, u kojem se postupa s podacima sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i višim, od ugroze takvih podataka nenamjernim elektromagnetnim zračenjem („sigurnosne mjere TEMPEST"). Takve sigurnosne mjere razmjerne su riziku iskorištavanja i stupnju tajnosti tih podataka.

6. Ako su klasificirani podaci EU-a zaštićeni kriptografskim proizvodima, takvi proizvodi odobravaju se kako slijedi:

(a) tajnost podataka klasificiranih kao SECRET UE/EU SECRET i više zaštićena je kriptografskim proizvodima koje je odobrilo Vijeće u ulozi tijela za odobravanje kriptomaterijala (CAA) na preporuku Sigurnosnog odbora;

(b) tajnost podataka klasificiranih kao CONFIDENTIEL UE/EU CONFIDENTIAL ili RESTREINT UE/EU RESTRICTED zaštićena je kriptografskim proizvodima koje je odobrio glavni tajnik Vijeća („glavni tajnik") u ulozi CAA-a na preporuku Sigurnosnog odbora.

Neovisno o točki (b), unutar nacionalnih sustava država članica povjerljivost klasificiranih podataka EU-a sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili RESTREINT UE/EU RESTRICTED može se zaštititi kriptografskim proizvodima koje je odobrio CAA države članice.

7. Tijekom prijenosa klasificiranih podataka EU-a elektroničkim sredstvima rabe se odobreni kriptografski proizvodi. Neovisno o tom zahtjevu, u izvanrednim se okolnostima ili posebnim tehničkim konfiguracijama navedenima u Prilogu IV. mogu primjenjivati posebni postupci.

8. Nadležna tijela GSC-a, odnosno država članica uspostavljaju sljedeće funkcije IA-a:

(a) tijelo za IA (IAA);

(b) tijelo za TEMPEST (TA);

(c) tijelo za odobravanje kriptomaterijala (CAA);

(d) tijelo za distribuciju kriptomaterijala (CDA).

9. Nadležna tijela GSC-a, odnosno država članica uspostavljaju za svaki sustav:

(a) tijelo za sigurnosnu akreditaciju (SAA);

(b) operativno tijelo za IA.

10. Odredbe za provedbu ovog članka navedene su u Prilogu IV.

*Članak 11.*

**Gospodarska sigurnost**

1. Gospodarska sigurnost je primjena mjera kojima se osigurava da ugovaratelji i podugovaratelji štite klasificirane podatke EU-a u pregovorima prije sklapanja ugovora i tijekom životnog ciklusa klasificiranih ugovora. Takvi ugovori ne smiju uključivati pristup podacima koji su klasificirani kao TRÈS SECRET UE/EU TOP SECRET.

2. GSC može na temelju ugovora povjeriti zadaće koji obuhvaćaju ili uključuju pristup ili postupanje s klasificiranim podacima EU-a ili njihovo čuvanje gospodarskim ili drugim subjektima registriranima u državi članici ili trećoj državi koja je sklopila sporazum ili administrativni dogovor u skladu s člankom 13. stavkom 2. točkama (a) ili (b).

3. GSC, kao tijelo za ugovaranje, osigurava poštovanje minimalnih standarda o gospodarskoj sigurnosti navedenih u ovoj Odluci, i iz ugovora, prilikom sklapanja klasificiranih ugovora s gospodarskim ili drugim subjektima.

4. Nacionalno sigurnosno tijelo (NSA) ili zaduženo sigurnosno tijelo (DSA) ili bilo koje drugo nadležno tijelo svake države članice osigurava, u mjeri u kojoj je to moguće prema nacionalnim zakonima i propisima, da ugovaratelji i podugovaratelji registrirani na njezinom državnom području poduzmu sve odgovarajuće mjere za zaštitu klasificiranih podataka EU-a tijekom pregovora prije sklapanja ugovora i prilikom izvršenja klasificiranog ugovora.

5. NSA, DSA ili bilo koje drugo nadležno sigurnosno tijelo svake države članice osigurava, u skladu s nacionalnim zakonima i propisima, da ugovaratelji ili podugovaratelji koji su registrirani u državi članici i koji sudjeluju u klasificiranim ugovorima ili podugovorima koji zahtijevaju pristup podacima klasificiranima kao CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET unutar svojih prostorija, bilo tijekom izvršenja takvih ugovora ili u fazi prije sklapanja ugovora, posjeduju uvjerenje o sigurnosnoj provjeri pravne osobe (FSC) za odgovarajući stupanj tajnosti.

6. Osoblju ugovaratelja ili podugovaratelja kojem za izvršenje klasificiranog ugovora treba pristup podacima klasificiranima kao CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET odgovarajući NSA, DSA ili bilo koje drugo nadležno sigurnosno tijelo odobrava uvjerenje o sigurnosnoj provjeri osobe (PSC) u skladu s nacionalnim zakonima i propisima te minimalnim standardima utvrđenima u Prilogu I.

7. Odredbe za provedbu ovog članka navedene su u Prilogu V.

*Članak 12.*

**Razmjena klasificiranih podataka EU-a**

1. Vijeće određuje uvjete prema kojima ono može razmjenjivati klasificirane podatke EU-a u njegovu vlasništvu s drugim institucijama, tijelima, uredima, ili agencijama Unije. U tu svrhu može se uspostaviti odgovarajući okvir, uključujući sklapanje međuinstitucionalnih sporazuma ili drugih dogovora, ako je to potrebno.

2. Takvim okvirom jamči se da su klasificirani podaci EU-a zaštićeni na odgovarajući način u skladu sa stupnjem tajnosti te sukladno temeljnim načelima i minimalnim standardima koji su jednaki onima utvrđenima u ovoj Odluci.

*Članak 13.*

**Razmjena klasificiranih podataka s trećim državama i međunarodnim organizacijama**

1. Ako Vijeće utvrdi da postoji potreba za razmjenom klasificiranih podataka EU-a s trećim državama ili međunarodnim organizacijama, u tu se svrhu uspostavlja odgovarajući okvir.

2. Za uspostavljanje takvog okvira i definiranje uzajamnih pravila o zaštiti razmijenjenih klasificiranih podataka:

(a) Unija sklapa sporazume s trećim državama ili međunarodnim organizacijama o sigurnosnim postupcima za razmjenu i zaštitu klasificiranih podataka („sporazumi o sigurnosti podataka”); ili

(b) glavni tajnik može sklapati administrativne dogovore u ime GSC-a u skladu sa stavkom 17. Priloga VI. ako stupanj tajnosti klasificiranih podataka EU-a koji se treba objaviti u pravilu nije viši od RESTREINT UE/EU RESTRICTED.

3. Sporazumi o sigurnosti podataka ili administrativni dogovori iz stavka 2. sadrže odredbe kojima se osigurava odgovarajuća zaštita podataka koje prime treće države ili međunarodne organizacije u skladu s njihovim stupnjem tajnosti i minimalnim standardima koji nisu ništa manje strogi od minimalnih standarda utvrđenih ovom Odlukom.

4. Odluku o objavljivanju klasificiranih podataka EU-a koji potječu od Vijeća trećoj državi ili međunarodnoj organizaciji donosi Vijeće od slučaja do slučaja, u skladu s prirodom i sadržajem takvih podataka, nužnosti primatelja za pristupom podacima i koristi koju će imati Unija. Ako onaj od kojeg potječu klasificirani podaci koji se žele objaviti nije Vijeće, GSC najprije mora zatražiti pisanu suglasnost za objavljivanje od onog od kojeg podaci potječu. Ako se taj ne može utvrditi, Vijeće preuzima odgovornost onog od kojeg podaci potječu.

5. Organiziraju se posjeti za procjenu stanja, kako bi se utvrdila učinkovitost uspostavljenih sigurnosnih mjera u trećoj državi ili međunarodnoj organizaciji za zaštitu dostavljenih ili razmijenjenih klasificiranih podataka EU-a.

6. Odredbe za provedbu ovog članka navedene su u Prilogu VI.

*Članak 14.*

**Povrede sigurnosti i ugroza klasificiranih podataka EU-a**

1. Povreda sigurnosti posljedica je radnje ili propusta pojedinca koji je u suprotnosti sa sigurnosnim propisima utvrđenima ovom Odlukom.

2. Do ugroze klasificiranih podataka EU-a dolazi kada su ti podaci djelomično ili u cijelosti otkriveni neovlaštenim osobama kao rezultat povrede sigurnosti.

3. Svaka povreda ili sumnja u povredu sigurnosti odmah se prijavljuje nadležnom sigurnosnom tijelu.

4. Ako je poznato ili ako postoje opravdani razlozi na temelju kojih se može pretpostaviti da su klasificirani podaci EU-a ugroženi ili izgubljeni, NSA ili drugo nadležno tijelo poduzima sve odgovarajuće mjere u skladu s mjerodavnim zakonima i propisima, kako bi:

(a) obavijestilo onog od kojeg podaci potječu;

(b) osiguralo da istragu predmeta provede osoblje koje nije neposredno povezano s povredom s ciljem utvrđivanja činjenica;

(c) procijenilo moguću štetu nanesenu interesima Unije ili država članica;

(d) poduzelo odgovarajuće mjere za sprečavanje ponovne povrede; i

(e) obavijestilo nadležna tijela o poduzetim mjerama.

5. Protiv svakog pojedinca odgovornog za povredu sigurnosnih propisa utvrđenih ovom Odlukom može se pokrenuti disciplinski postupak u skladu s mjerodavnim pravilima i propisima. Protiv svakog pojedinca odgovornog za ugrozu ili gubitak klasificiranih podataka EU-a pokreće se disciplinski i/ili pravni postupak u skladu s mjerodavnim zakonima, pravilima i propisima.

*Članak 15.*

**Odgovornost za provedbu**

1. Vijeće poduzima sve potrebne mjere, kako bi osiguralo cjelokupnu dosljednost u primjeni ove Odluke.

2. Glavni tajnik poduzima sve potrebne mjere kako bi osigurao da, prilikom postupanja s klasificiranim podacima EU-a ili bilo kojim drugim klasificiranim podacima ili prilikom njihova čuvanja, dužnosnici GSC-a i drugi službenici, osoblje upućeno GSC-u i ugovaratelji GSC-a primjenjuju ovu Odluku u prostorijama kojima se služi Vijeće i unutar GSC-a.

3. Države članice poduzimaju sve odgovarajuće mjere u skladu sa svojim nacionalnim zakonima i propisima kako bi osigurale da prilikom postupanja s klasificiranim podacima EU-a i njihova čuvanja ovu Odluku poštuju:

(a) osoblje stalnih predstavništava država članica u Europskoj uniji i nacionalni predstavnici koji prisustvuju sastancima Vijeća ili njegovih pripremnih tijela ili sudjeluju u drugim aktivnostima Vijeća;

(b) ostalo osoblje u nacionalnim administracijama država članica, uključujući osoblje upućeno tim administracijama, bez obzira na to obavlja li ono svoju službu na državnom području države članice ili u inozemstvu;

(c) ostale osobe u državama članicama koje su, u skladu sa svojim funkcijama, propisno ovlaštene za pristup klasificiranim podacima EU-a; i

(d) ugovaratelji država članica, bez obzira na to jesu li na području države članice ili u inozemstvu.

*Članak 16.*

**Organizacija sigurnosti u Vijeću**

1. U okviru svoje uloge u osiguravanju cjelokupne dosljednosti u primjeni ove Odluke Vijeće odobrava:

(a) sporazume iz članka 13. stavka 2. točke (a);

(b) odluke kojima se odobrava ili daje suglasnost za objavu klasificiranih podataka EU-a koji potječu od Vijeća ili su njegovom posjedu trećim državama i međunarodnim organizacijama, u skladu s načelom pristanka izvora;

(c) godišnji program posjeta radi procjene stanja na preporuku Sigurnosnog odbora za posjete radi procjene službi i prostorija država članica, tijela, agencija i subjekata Unije koji primjenjuju ovu Odluku ili njezina načela te za posjete radi procjene stanja trećim državama i međunarodnim organizacijama, kako bi se utvrdila učinkovitost provedenih mjera za zaštitu klasificiranih podataka EU-a; i

(d) sigurnosne politike predviđene člankom 6. stavkom 1.

2. Glavni tajnik sigurnosno je tijelo GSC-a. U tom svojstvu glavni tajnik:

(a) provodi i preispituje sigurnosnu politiku Vijeća;

(b) koordinira s NSA-ima država članica sva pitanja sigurnosti povezana sa zaštitom klasificiranih podataka koji se odnose na aktivnosti Vijeća;

(c) izdaje dužnosnicima GSC-a, drugim službenicima i upućenim nacionalnim stručnjacima ovlaštenje za pristup podacima sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim, u skladu s člankom 7. stavkom 3.;

(d) prema potrebi, nalaže istrage svake stvarne ugroze ili gubitka ili ako postoji sumnja u ugrozu ili gubitak klasificiranih podataka koji su u posjedu ili potječu od Vijeća te zahtijeva pomoć od nadležnih sigurnosnih tijela u takvim istragama;

(e) poduzima periodične inspekcije sigurnosnih mjera za zaštitu klasificiranih podataka u prostorijama GSC-a;

(f) poduzima periodične posjete radi procjene sigurnosnih mjera za zaštitu klasificiranih podataka EU-a u tijelima, agencijama i subjektima Unije koji primjenjuju ovu Odluku ili njezina načela;

(g) zajedno i u dogovoru s predmetnim NSA-om poduzima periodične procjene sigurnosnih mjera za zaštitu klasificiranih podataka EU-a u službama i prostorijama država članica;

(h) osigurava da se sigurnosne mjere koordiniraju prema potrebi s nadležnim tijelima država članica koja su odgovorna za zaštitu klasificiranih podataka i, prema potrebi, trećim državama ili međunarodnim organizacijama, također i u pogledu prirode prijetnji sigurnosti klasificiranih podataka EU-u i sredstava za zaštitu od njih; i

(i) sklapa administrativne dogovore iz članka 13. stavka 2. točke (b).

Ured za sigurnost GSC-a na raspolaganju je glavnom tajniku i pruža mu pomoć u pogledu navedenih odgovornosti.

3. Za potrebe provedbe članka 15. stavka 3. države članice trebale bi:

(a) odrediti NSA, kako je navedeno u Dodatku C, odgovoran za sigurnosne mjere za zaštitu klasificiranih podataka EU-a, kako bi:

i. klasificirani podaci u posjedu bilo kojeg nacionalnog odjela, tijela ili agencije, bilo javne ili privatne, kod kuće ili u inozemstvu, bili zaštićeni u skladu s ovom Odlukom;

ii. se sigurnosne mjere za zaštitu klasificiranih podataka EU-a povremeno pregledale ili procijenile;

iii. svi pojedinci zaposleni u nacionalnoj administraciji ili pri ugovaratelju kojem se može odobriti pristup podacima klasificiranim kao CONFIDENTIEL UE/EU CONFIDENTIAL ili više prošli odgovarajuću sigurnosnu provjeru ili bili na neki drugi način propisno ovlašteni na temelju svojih funkcija u skladu s nacionalnim zakonima i propisima;

iv. se prema potrebi uspostavili sigurnosni programi radi smanjivanja opasnosti od ugroze ili gubitka klasificiranih podataka EU-a;

v. pitanja sigurnosti koja se odnose na zaštitu klasificiranih podataka EU-a bila usklađena s drugim nadležnim nacionalnim tijelima, uključujući tijela iz ove Odluke; i

vi. se odgovorilo na odgovarajuće zahtjeve za sigurnosnu provjeru, a posebno na one koje su podnijele bilo koja tijela, agencije, subjekti i operacije Unije, uspostavljeni na temelju glave V. poglavlja 2. UEU-a, te posebni predstavnici EU-a (PPEU-i) i njihovi timovi koji primjenjuju ovu Odluku ili njezina načela;

(b) osigurati da njihova nadležna tijela dostave podatke i savjete svojim vladama, a putem njih i Vijeću, o prirodi prijetnji sigurnosti klasificiranih podataka EU-a i sredstvima zaštite od njih.

*Članak 17.*

**Sigurnosni odbor**

1. Ovim se uspostavlja Sigurnosni odbor. On ispituje i ocjenjuje sva sigurnosna pitanja obuhvaćena područjem primjene ove Odluke te prema potrebi daje preporuke Vijeću.

2. Sigurnosni je odbor sastavljen od predstavnika NSA-a država članica, a u njegovu radu sudjeluju predstavnici Komisije i EEAS-a. Njime predsjeda glavni tajnik ili njegov imenovani izaslanik. Sastaje se po uputi Vijeća ili na zahtjev glavnog tajnika ili NSA-a.

Predstavnici tijela, agencija i subjekata Unije koji primjenjuju ovu Odluku ili njezina načela mogu biti pozvani da sudjeluju na sastancima kada se raspravlja o pitanjima koja se na njih odnose.

3. Sigurnosni odbor organizira svoje aktivnosti tako da može davati preporuke za specifična područja sigurnosti. On utvrđuje stručno potpodručje za pitanja IA-a te prema potrebi druga stručna potpodručja. On sastavlja opis poslova za takva potpodručja i prima njihova izvješća o aktivnostima, uključujući, prema potrebi, sve preporuke Vijeću.

*Članak 18.*

**Zamjena prethodne odluke**

1. Ovom se Odlukom stavlja izvan snage i zamjenjuje Odluka Vijeća 2011/292/EU ([1]).

2. Svi klasificirani podaci EU-a klasificirani u skladu s Odlukom Vijeća 2001/264/EZ ([2]) i Odlukom 2011/292/EU i dalje su zaštićeni u skladu s odgovarajućim odredbama ove Odluke.

*Članak 19.*

**Stupanje na snagu**

Ova Odluka stupa na snagu na dan objave u *Službenom listu Europske unije*.

Sastavljeno u Bruxellesu 23. rujna 2013..

*Za Vijeće*
*Predsjednik*
V. JUKNA

([1]) Odluka Vijeća 2011/292/EU od 31. ožujka 2011. o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a (SL L 141, 27.5.2011., str. 17.).

([2]) Odluka Vijeća 2001/264/EZ od 19. ožujka 2001. o donošenju sigurnosnih propisa Vijeća (SL L 101, 11.4.2001., str. 1.).

*PRILOZI*

*PRILOG I.*

Sigurnost osoba

*PRILOG II.*

Fizička sigurnost

*PRILOG III.*

Upravljanje klasificiranim podacima

*PRILOG IV.*

Zaštita klasificiranih podataka EU-a s kojima se postupa u CIS-u

*PRILOG V.*

Gospodarska sigurnost

*PRILOG VI.*

Razmjena klasificiranih podataka s trećim državama i međunarodnim organizacijama

*PRILOG I.*

**SIGURNOST OSOBA**

I. UVOD

1. U ovom se Prilogu određuju odredbe za provedbu članka 7. U njemu se utvrđuju kriteriji na temelju kojih se određuje može li se pojedincu, s obzirom na njegovu lojalnost, vjerodostojnost i pouzdanost, odobriti pristup klasificiranim podacima EU-a te istražni i administrativni postupci kojih se u tu svrhu treba držati.

II. ODOBRAVANJE PRISTUPA KLASIFICIRANIM PODACIMA EU-a

2. Pojedincu se odobrava pristup klasificiranim podacima samo nakon što:

(a) je za njega utvrđena nužnost pristupa podacima;

(b) je upoznat sa sigurnosnim propisima i postupcima za zaštitu klasificiranih podataka EU-a i nakon što je potvrdio svoje odgovornosti povezane sa zaštitom takvih podataka; i

(c) u slučaju podataka sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim:

— nakon što mu je odobren PSC za relevantni stupanj tajnosti ili nakon što je na neki drugi način propisno ovlašten na temelju svojih funkcija u skladu s nacionalnim zakonima i propisima, ili

— u slučaju dužnosnika GSC-a, drugih službenika ili upućenih nacionalnih stručnjaka, njima tijelo za imenovanja GSC-a mora dati ovlaštenje za pristup klasificiranim podacima EU-a do određenog stupnja tajnosti i do određenog datuma, u skladu sa stavcima od 16. do 25. u sljedećem tekstu.

3. Svaka država članica i GSC utvrđuju položaje u svojim strukturama za koje je potreban pristup podacima sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim i stoga zahtijevaju uvjerenje o sigurnosnoj provjeri za odgovarajući stupanj tajnosti.

III. ZAHTJEVI POVEZANI S UVJERENJEM O SIGURNOSNOJ PROVJERI OSOBA

4. Nakon što zaprime propisno ovlašten zahtjev, NSA-i ili druga nadležna nacionalna tijela odgovorna su za osiguravanje provedbe sigurnosnih istraga svojih državljana koji traže pristup podacima klasificiranima kao CONFIDENTIEL UE/EU CONFIDENTIAL ili više. Standardi istrage moraju biti u skladu s nacionalnim zakonima i propisima s ciljem izdavanja PSC-a ili davanja potvrde za pojedinca kojem se treba izdati ovlaštenje za pristup klasificiranim podacima EU-a, prema potrebi..

5. Ako dotični pojedinac boravi na području druge države članice ili treće države, nadležna nacionalna tijela zatražit će pomoć nadležnog tijela države boravišta u skladu s nacionalnim zakonima i propisima. Države članice pomažu jedna drugoj u provedbi sigurnosnih istraga u skladu s nacionalnim zakonima i propisima.

6. Ako je to dopušteno prema nacionalnim zakonima i propisima, NSA-i ili druga nadležna nacionalna tijela mogu provoditi istrage nad stranim državljanima kojima je potreban pristup podacima sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim. Standardi istrage u skladu su s nacionalnim zakonima i propisima.

**Kriteriji sigurnosne istrage**

7. Lojalnost, vjerodostojnost i pouzdanost pojedinca utvrđuje se sigurnosnom istragom u svrhu provođenja sigurnosne provjere za pristup podacima sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim. Nadležno nacionalno tijelo izrađuje opću procjenu na temelju nalaza takve sigurnosne istrage. Temeljni kriteriji koji se u tu svrhu rabe obuhvaćaju, u mjeri u kojoj je to moguće prema nacionalnim zakonima i propisima, ispitivanje je li pojedinac:

(a) počinio ili namjeravao počiniti djelo špijunaže, terorizma, sabotaže, izdaje ili ugrožavanja nacionalne sigurnosti, odnosno urotio se s drugima, pomagao im ili ih poticao pri počinjenju takvog djela;

(b) suradnik ili je bio suradnik špijuna, terorista, sabotera ili pojedinaca za koje se opravdano sumnja da to jesu, odnosno suradnik predstavnika organizacija ili stranih država, uključujući strane obavještajne službe, koji mogu ugroziti sigurnost Unije i/ili država članica, osim ako je takva suradnja bila ovlaštena u okviru službene dužnosti;

(c) član ili je bio član organizacije koja nasilnim, subverzivnim ili drugim nezakonitim sredstvima pokušava, *inter alia*, srušiti vladu države članice, promijeniti ustavni poredak države članice ili promijeniti oblik ili politiku njezine vlade;

(d) podupire ili je podupirao organizaciju opisanu pod točkom (c), odnosno tijesno je povezan ili je bio usko povezan s članovima takvih organizacija;

(e) namjerno uskratio, netočno naveo ili krivotvorio važne podatke, posebno podatke sigurnosne prirode, ili namjerno lagao prilikom popunjavanja upitnika za sigurnosnu provjeru osobe ili tijekom sigurnosnog razgovora;

(f) bio osuđivan za jedno ili više kaznenih djela;

(g) bio ovisan o alkoholu, rabio nedopuštene droge i/ili zlorabio zakonom dopuštene lijekove;

(h) uključen ili je bio uključen u ponašanje koje može uzrokovati rizik od osjetljivosti na ucjenu ili pritisak;

(i) djelovanjem ili govorom pokazao nepoštenje, nelojalnost, nepouzdanost ili nevjerodostojnost;

(j) ozbiljno ili višekratno kršio sigurnosne propise ili je pokušao, odnosno uspio provesti neovlaštenu aktivnost povezanu s komunikacijskim i informacijskim sustavima; i

(k) podložan pritisku (npr. jer je državljanin jedne ili više država koje nisu članice EU-a ili jer ima rođake ili bliske suradnike koji mogu biti podložni stranim obavještajnim službama, terorističkim skupinama ili drugim subverzivnim organizacijama ili pojedincima čiji ciljevi mogu ugroziti sigurnosne interese Unije i/ili država članica).

8. Ako je potrebno i u skladu s nacionalnim zakonima i propisima, financijska i medicinska pozadina pojedinca također se mogu smatrati važnima u sigurnosnoj istrazi.

9. Ako je potrebno i u skladu s nacionalnim zakonima i propisima, ponašanje i okolnosti supružnika, izvanbračnog partnera ili člana uže obitelji također se mogu smatrati važnima u sigurnosnoj istrazi.

**Istražni zahtjevi za pristup klasificiranim podacima EU-a**

*Prva dodjela uvjerenja o sigurnosnoj provjeri*

10. Prvo uvjerenje o sigurnosnoj provjeri za pristup podacima sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET temelji se na sigurnosnoj istrazi koja obuhvaća najmanje 5 godina ili razdoblje od 18. godine do danas, ovisno o tome što je kraće, a koja uključuje sljedeće:

(a) popunjavanje nacionalnog upitnika za sigurnosnu provjeru osobe za stupanj tajnosti klasificiranih podataka EU-a za koje će pojedinac možda trebati pristup; nakon popunjavanja upitnik se prosljeđuje nadležnom sigurnosnom tijelu;

(b) provjeru identiteta/državljanstva/status državljanstva – potvrđuju se datum i mjesto rođenja te provjerava identitet pojedinca. Utvrđuju se prošlo i sadašnje državljanstvo i status državljanstva pojedinca, što uključuje procjenu svake osjetljivosti na pritisak stranih izvora, na primjer zbog prethodnog boravišta ili prethodnih veza; i

(c) provjeru nacionalne i lokalne evidencije – provjerava se evidencija povezana s nacionalnom sigurnošću i središnja kaznena evidencija, ako potonja postoji, i/ili usporediva vladina ili policijska evidencija. Provjerava se evidencija tijela kaznenog progona s nadležnošću na području na kojem pojedinac boravi ili je zaposlen.

11. Prvo uvjerenje o sigurnosnoj provjeri za pristup podacima sa stupnjem tajnosti TRÈS SECRET UE/EU TOP SECRET temelji se na sigurnosnoj istrazi koja obuhvaća najmanje zadnjih 10 godina ili razdoblje od 18. godine do danas, ovisno o tome što je kraće. Ako se razgovori provode kako je navedeno u točki (e), istrage obuhvaćaju najmanje zadnjih 7 godina ili razdoblje od 18. godine do danas, ovisno o tome što je kraće. Uz kriterije navedene u gornjem stavku 7. istražuju se sljedeći elementi, u mjeri u kojoj je to moguće prema nacionalnim zakonima i propisima, prije odobrenja PSC-a za stupanj tajnosti TRÈS SECRET UE/EU TOP SECRET; navedeni se elementi također mogu istražiti prije odobrenja PSC-a za stupanj tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET, kako je propisano nacionalnim zakonima i propisima:

(a) financijski status – traže se podaci o financijama pojedinca kako bi se ocijenila svaka osjetljivost na strane i domaće pritiske zbog ozbiljnih financijskih teškoća ili kako bi se otkrio bilo kakav neobjašnjivi priljev;

(b) obrazovanje – traže se podaci kojima se potvrđuje obrazovanje pojedinca u školama, sveučilištima i drugim obrazovnim institucijama koje je pohađao od 18. rođendana ili u razdoblju koje istražno tijelo smatra primjerenim;

(c) zaposlenje – traže se informacije o sadašnjem i prijašnjem zaposlenju, uz upućivanje na izvore kao što su evidencija o zaposlenju, izvješća o uspješnosti ili učinku te na poslodavce i nadzornike;

(d) služenje vojnog roka – ako je primjenljivo, provjerava se služenje pojedinca u oružanim snagama i način otpuštanja; i

(e) razgovori – ako je propisano i dopušteno prema nacionalnom pravu, s pojedincem se može obaviti razgovor ili razgovori. Razgovori se također obavljaju s drugim pojedincima koji mogu nepristrano ocijeniti pozadinu, aktivnosti, lojalnost, vjerodostojnost i pouzdanost pojedinca. Ako je u nacionalnoj praksi uobičajeno da se od pojedinca koji je predmetom istrage traže preporuke, obavljaju se razgovori i s osobama koje su dale preporuke, osim ako postoje dobri razlozi da se to ne učini.

12. Ako je potrebno i u skladu s nacionalnim zakonima i propisima, mogu se provesti dodatne istrage, kako bi se razradili svi važni podaci dostupni o pojedincu te potkrijepili ili opovrgnuli štetni podaci.

*Obnova uvjerenja o sigurnosnoj provjeri*

13. Nakon izdavanja prvog uvjerenja o sigurnosnoj provjeri i uz uvjet da pojedinac ima neprekinuti radni staž u nacionalnoj administraciji ili GSC-u te stalnu potrebu za pristupom klasificiranim podacima EU-a, uvjerenje o sigurnosnoj provjeri se pregledava u svrhu obnove u vremenskim razmacima ne većim od 5 godina za uvjerenje o sigurnosnoj provjeri za stupanj tajnosti TRÈS SECRET UE/EU TOP SECRET, odnosno 10 godina za uvjerenje o sigurnosnoj provjeri za stupanj tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL, počevši od datuma obavijesti o ishodu zadnje sigurnosne istrage na temelju koje je izdano uvjerenje. Sve sigurnosne istrage za obnovu uvjerenja o sigurnosnoj provjeri obuhvaćaju razdoblje od prethodne takve istrage.

14. U svrhu obnove uvjerenjâ o sigurnosnoj provjeri istražuju se elementi opisani u stavcima 10. i 11.

15. Zahtjevi za obnovu podnose se pravodobno imajući na umu vrijeme potrebno za sigurnosne istrage. Neovisno o tome, ako je nadležni NSA ili drugo nadležno nacionalno tijelo zaprimilo dotični zahtjev za obnovu i odgovarajući upitnik za sigurnosnu provjeru osobe prije isteka uvjerenja o sigurnosnoj provjeri i ako potrebne sigurnosne istrage još nisu završene, nadležno nacionalno tijelo može, ako je to dopušteno prema nacionalnim zakonima i propisima, produljiti valjanost postojećeg uvjerenja o sigurnosnoj provjeri za najviše 12 mjeseci. Ako na kraju ovog razdoblja od 12 mjeseci sigurnosna istraga još nije završena, pojedincu se dodjeljuju dužnosti za koje nije potrebno uvjerenje o sigurnosnoj provjeri.

*Postupci povezani s izdavanjem ovlaštenja u GSC-u*

16. Za dužnosnike i druge službenike u GSC-u, sigurnosno tijelo GSC-a popunjeni upitnik za sigurnosnu provjeru osobe prosljeđuje NSA-u države članice čiji je pojedinac državljanin sa zahtjevom da se provede sigurnosna istraga za stupanj tajnosti klasificiranih podataka EU-a za koje će pojedinac trebati pristup.

17. Ako GSC-u postanu poznati podaci važni za sigurnosnu istragu povezani s pojedincem koji se prijavio za uvjerenje o sigurnosnoj provjeri radi pristupa klasificiranim podacima EU-a, GSC, djelujući u skladu s mjerodavnim pravilima i propisima, o tome obavješćuje nadležni NSA.

18. Po završetku sigurnosne istrage, nadležni NSA obavješćuje sigurnosno tijelo GSC-a o ishodu takve istrage koristeći standardni obrazac za korespondenciju koji propisuje Sigurnosni odbor.

(a) Ako se sigurnosnom istragom potvrdi da nisu poznati nikakvi štetni podaci kojima bi se u pitanje dovela lojalnost, vjerodostojnost i pouzdanost pojedinca, tijelo za imenovanja GSC-a može izdati predmetnom pojedincu ovlaštenje za pristup klasificiranim podacima EU-a do odgovarajućeg stupnja tajnosti i do određenog datuma.

(b) Ako sigurnosna istraga ne rezultira takvom potvrdom, tijelo za imenovanja GSC-a obavješćuje predmetnog pojedinca koji može zatražiti saslušanje pred tijelom za imenovanja. Tijelo za imenovanja može zatražiti od nadležnog NSA-a sva dodatna pojašnjenja koja NSA može dati u skladu sa svojim nacionalnim zakonima i propisima. Ako se ishod potvrdi, ne izdaje se ovlaštenje za pristup klasificiranim podacima EU-a.

19. Sigurnosna istraga zajedno s dobivenim rezultatima podliježe mjerodavnim zakonima i propisima koji su na snazi u predmetnoj državi članici, uključujući one koji se odnose na žalbe. Odluke tijela za imenovanja GSC-a podliježu žalbama u skladu s Pravilnikom o osoblju za dužnosnike Europske unije i Uvjetima zaposlenja ostalih službenika Europske unije utvrđenih Uredbom Vijeća (EEZ, Euratom, EZUČ) br. 259/68 [1] „Pravilnik o osoblju i Uvjeti zaposlenja").

20. Nacionalni stručnjaci, upućeni GSC-u za položaj za koji je potreban pristup klasificiranim podacima EU-a sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i višim, moraju, prije negoli preuzmu svoje dužnosti, sigurnosnom tijelu GSC-a predočiti valjani certifikat o sigurnosnoj provjeri osobe (PSCC) za pristup klasificiranim podacima EU-a, na temelju kojeg tijelo za imenovanja izdaje ovlaštenje za pristup klasificiranim podacima EU-a.

21. GSC će prihvatiti ovlaštenje za pristup klasificiranim podacima EU-a izdano od druge institucije, tijela ili agencije Unije pod uvjetom da je valjano. Ovlaštenje će obuhvaćati sva zaduženja predmetnog pojedinca u GSC-u. Institucija, tijelo ili agencija Unije u kojoj se pojedinac zapošljava obavijestit će nadležni NSA o promjeni poslodavca.

22. Ako pojedinac ne započne službu u roku od 12 mjeseci od obavijesti o ishodu sigurnosne istrage upućene tijelu za imenovanja GSC-a ili ako prekid radnog staža pojedinca traje 12 mjeseci tijekom kojih nije zaposlen u GSC-u ili na položaju u nacionalnoj administraciji države članice, navedeni se ishod upućuje nadležnom NSA-u, kako bi potvrdio da je još uvijek valjan i primjeren.

[1] Uredba Vijeća (EEZ, Euratom, EZUČ) br. 259/68 od 29. veljače 1968. o utvrđivanju Pravilnika o osoblju i Uvjeta zaposlenja ostalih službenika Europskih zajednica i uvođenju posebnih mjera koje se privremeno primjenjuju na dužnosnike Komisije (SL L 56, 4.3.1968., str. 1.).

23. Ako GSC-u postanu poznati podaci o sigurnosnom riziku povezanom s pojedincem koji posjeduje ovlaštenje za pristup klasificiranim podacima EU-a, GSC, djelujući u skladu s mjerodavnim pravilima i propisima, obavješćuje nadležni NSA o tome te može obustaviti pristup klasificiranim podacima EU-a ili oduzeti ovlaštenje za pristup klasificiranim podacima EU-a.

24. Ako NSA obavijesti GSC o povlačenju potvrde izdane u skladu sa stavkom 18. točkom (a) za pojedinca koji posjeduje ovlaštenje za pristup klasificiranim podacima EU-a, tijelo za imenovanja GSC-a može zatražiti svako objašnjenje koje NSA može dati u skladu sa svojim nacionalnim zakonima i propisima. Ako se štetni podaci potvrde, ovlaštenje se oduzima, a pojedincu se onemogućuje pristup klasificiranim podacima EU-a i uklanja se s položaja na kojem je takav pristup moguć ili na kojem bi mogao ugroziti sigurnost.

25. Obavijest o svakoj odluci o oduzimanju ili suspenziji ovlaštenja dužnosnika GSC-a ili drugog službenika za pristup klasificiranim podacima EU-a i, prema potrebi, razlozima takvog postupka upućuje se predmetnom pojedincu, koji može zatražiti saslušanje pred tijelom za imenovanja. Podaci koje je dostavio NSA podliježu mjerodavnim zakonima i propisima koji su na snazi u predmetnoj državi članici, uključujući one koji se odnose na žalbe. Odluke tijela za imenovanja GSC-a podliježu žalbama u skladu s Pravilnikom o osoblju i Uvjetima zaposlenja.

*Evidencija uvjerenja o sigurnosnoj provjeri i ovlaštenja*

26. Svaka država članica i GSC vode evidenciju o PSC-ima i ovlaštenjima izdanim za pristup podacima sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim. Ta evidencija mora sadržavati barem stupanj tajnosti klasificiranih podataka EU-a do kojeg se pojedincu može odobriti pristup, datum uvjerenja o sigurnosnoj provjeri i njegov rok valjanosti.

27. Nadležno sigurnosno tijelo može izdati PSCC u kojemu je naveden stupanj tajnosti klasificiranih podataka EU-a do kojeg se pojedincu može odobriti pristup (CONFIDENTIEL UE/EU CONFIDENTIAL ili viši), datum valjanosti odgovarajućeg PSC-a za pristup klasificiranim podacima EU-a ili ovlaštenje za pristup klasificiranim podacima EU-a i datum isteka samog certifikata.

**Iznimke od zahtjeva povezani s PSC-om**

28. Pristup klasificiranim podacima EU-a za pojedince u državama članicama koji su propisno ovlašteni na temelju svojih funkcija određuje se u skladu s nacionalnim zakonima i propisima; takve se pojedince upućuje u njihove sigurnosne obveze u pogledu zaštite klasificiranih podataka EU-a.

## IV. OBRAZOVANJE I PODIZANJE SVIJESTI O SIGURNOSTI

29. Svi pojedinci, kojima je izdano uvjerenje o sigurnosnoj provjeri, u pisanom obliku potvrđuju da su razumjeli svoje obveze u pogledu zaštite klasificiranih podataka EU-a i posljedice ugroze klasificiranih podataka EU-a. Država članica, odnosno GSC, čuva evidenciju o takvoj pisanoj potvrdi prema potrebi.

30. Sve pojedince koji imaju ovlaštenje za pristup ili od kojih se zahtijeva postupanje s klasificiranim podacima EU-a na početku se upozorava, a zatim ih se periodično upućuje u sigurnosne prijetnje te su dužni odgovarajućim sigurnosnim tijelima odmah prijaviti svaki pokušaj približavanja ili aktivnost koju smatraju sumnjivom ili neuobičajenom.

31. Sve pojedince koji prestanu obavljati dužnosti za koje je potreban pristup klasificiranim podacima EU-a upoznaje se s njihovim obvezama u pogledu s daljnje zaštite klasificiranih podataka EU-a, a ako je potrebno, to potvrđuju i u pisanom obliku.

## V. IZNIMNE OKOLNOSTI

32. Ako je to dopušteno prema nacionalnim zakonima i propisima, na temelju uvjerenja o sigurnosnoj provjeri koje je izdalo nadležno nacionalno tijelo države članice za pristup nacionalnim klasificiranim podacima nacionalnim se dužnosnicima, u ograničenom razdoblju do izdavanja PSC-a za pristup klasificiranim podacima EU-a, može dopustiti pristup klasificiranim podacima EU-a do jednakog stupnja tajnosti navedenog u tablici ekvivalentnosti u Dodatku B ako je takav privremeni pristup u interesu Unije. NSA-i obavješćuju Sigurnosni odbor ako prema nacionalnim zakonima i propisima takav privremeni pristup klasificiranim podacima EU-a nije dopušten.

33. Zbog hitnosti, ako je to propisno opravdano interesima službe i do završetka potpune sigurnosne istrage, tijelo za imenovanja GSC-a može, nakon savjetovanja s NSA-om države članice čije je pojedinac državljanin i ovisno o ishodu prethodnih provjera kojima se provjerava nepostojanje štetnih podataka, izdati privremeno ovlaštenje dužnosnicima GSC-a i drugim službenicima za pristup klasificiranim podacima EU-a za posebnu funkciju. Takva privremena ovlaštenja valjana su najviše 6 mjeseci i njima se ne dopušta pristup podacima klasificiranima kao TRÈS SECRET UE/EU TOP SECRET. Svi pojedinci kojima je izdano privremeno ovlaštenje u pisanom obliku potvrđuju da su razumjeli svoje obveze u pogledu zaštite klasificiranih podataka EU-a i posljedice ugroze klasificiranih podataka EU-a. GSC čuva evidenciju o takvim pisanim potvrdama.

34. Ako se pojedinac upućuje na položaj za koji je potrebno uvjerenje o sigurnosnoj provjeri s jednim stupnjem tajnosti višim od PSC-a koji pojedinac trenutačno posjeduje, moguće je privremeno zaduženje uz uvjet da:

(a) nadređeni pojedincu u pisanom obliku opravda nužnu potrebu za pristupom klasificiranim podacima EU-a;

(b) je pristup ograničen na specifične pojedinosti iz klasificiranih podataka EU-a potrebne za zadaću;

(c) pojedinac posjeduje valjani PSC ili ovlaštenje za pristup klasificiranim podacima EU-a;

(d) je pokrenuta mjera za ishođenje ovlaštenja za razinu pristupa potrebnu za položaj;

(e) je nadležno tijelo u zadovoljavajućoj mjeri provjerilo je li pojedinac ozbiljno ili višekratno kršio sigurnosne propise;

(f) je nadležno tijelo potvrdilo upućivanje pojedinca na položaj; i

(g) se u odgovarajućem registru ili podregistru čuva evidencija o iznimci, uključujući opis podataka za koje je odobren pristup.

35. Gore opisani postupak primjenjuje se za jednokratni pristup klasificiranim podacima EU-a sa stupnjem tajnosti za jedan viši od onog za koji je pojedinac prošao sigurnosnu provjeru. Taj se postupak ne smije primjenjivati učestalo.

36. U vrlo iznimnim okolnostima, kao što su misije u neprijateljskom okruženju ili u vrijeme povećanja međunarodne napetosti kada hitne mjere to zahtijevaju, posebno radi spašavanja života, države članice i glavni tajnik mogu odobriti, ako je moguće u pisanom obliku, pristup podacima sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET pojedincima koji ne posjeduju potrebno uvjerenje o sigurnosnoj provjeri, uz uvjet da je takvo dopuštenje apsolutno nužno i da nema nikakve opravdane sumnje u lojalnost, vjerodostojnost i pouzdanost predmetnog pojedinca. Vodi se evidencija o takvom dopuštenju u kojoj su opisani podaci za koje je odobren pristup.

37. U slučaju podataka klasificiranih kao TRÈS SECRET UE/EU TOP SECRET, hitni je pristup ograničen na građane Unije kojima je odobren pristup nacionalnom ekvivalentu podataka sa stupnjem tajnosti TRÈS SECRET UE/EU TOP SECRET ili podacima klasificiranima kao SECRET UE/EU SECRET.

38. Sigurnosni se odbor obavješćuje o slučajevima primjene postupka navedenog u stavcima 36. i 37.

39. Ako su nacionalnim zakonima i propisima država članica propisana stroža pravila u pogledu privremenih ovlaštenja, privremenih zaduženja, jednokratnog pristupa ili hitnog pristupa pojedinaca klasificiranim podacima, postupci predviđeni u ovom odjeljku provode se samo u okviru ograničenja utvrđenih mjerodavnim nacionalnim zakonima i propisima.

40. Sigurnosni odbor prima godišnje izvješće o primjeni postupaka navedenih u ovom odjeljku.

VI. SUDJELOVANJE NA SASTANCIMA VIJEĆA

41. U skladu sa stavkom 28., pojedinci upućeni na sudjelovanje na sastancima Vijeća ili pripremnih tijela Vijeća na kojima se raspravlja o podacima sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim, mogu sudjelovati samo nakon potvrde statusa pojedinca u vezi uvjerenja o sigurnosnoj provjeri. Za delegate nadležna tijela prosljeđuju PSCC ili drugi dokaz o uvjerenju o sigurnosnoj provjeri Uredu za sigurnost GSC-a ili ga iznimno može predočiti predmetni delegat. Prema potrebi, može se koristiti konsolidirani popis imena s odgovarajućim dokazom o uvjerenju o sigurnosnoj provjeri.

42. Ako je pojedincu koji zbog svojih dužnosti sudjeluje na sastancima Vijeća ili pripremnih tijela Vijeća iz sigurnosnih razloga oduzet PSC za pristup klasificiranim podacima EU-a, nadležno tijelo o tome obavješćuje GSC.

VII. MOGUĆI PRISTUP KLASIFICIRANIM PODACIMA EU-a

43. Kuriri, zaštitari i pratnja moraju proći sigurnosnu provjeru za odgovarajuću razinu ili drugu vrstu odgovarajuće istrage u skladu s nacionalnim zakonima ili propisima, moraju se uputiti u sigurnosne postupke za zaštitu klasificiranih podataka EU-a i u njihove dužnosti povezane sa zaštitom takvih podataka koji su im povjereni.

*PRILOG II.*

## FIZIČKA SIGURNOST

I. UVOD

1. U ovom se Prilogu određuju odredbe za provedbu članka 8. U njemu se utvrđuju minimalni zahtjevi za fizičku zaštitu prostorija, zgrada, ureda, soba i drugih područja u kojima se postupa s klasificiranim podacima EU-a ili se čuvaju, uključujući područja u kojima je smješten CIS.

2. Mjere fizičke sigurnosti namijenjene su sprečavanju neovlaštenog pristupa klasificiranim podacima EU-a tako da se:

   (a) osigura pravilno postupanje s klasificiranim podacima EU-a i njihovo čuvanje;

   (b) omogući razdvajanje osoblja u smislu pristupa klasificiranim podacima EU-a na temelju nužnosti pristupa podacima za obavljanje poslova iz djelokruga te, prema potrebi, s obzirom na njihovu sigurnosnu provjeru;

   (c) odvraćaju, sprečavaju i otkrivaju neovlaštene radnje; i

   (d) onemogući ili odgodi tajni ili nasilni ulazak neovlaštenih osoba.

II. ZAHTJEVI I MJERE POVEZANE S FIZIČKOM SIGURNOŠĆU

3. Mjere fizičke sigurnosti odabiru se na temelju procjene prijetnje koju provode nadležna tijela. GSC i države članice primjenjuju proces upravljanja rizicima za zaštitu klasificiranih podataka EU-a u svojim prostorijama kako bi osigurali razinu fizičke zaštite razmjernu procijenjenim rizicima. U procesu upravljanja rizicima u obzir se uzimaju svi važni čimbenici, a posebno:

   (a) stupanj tajnosti klasificiranih podataka EU-a;

   (b) oblik i opseg klasificiranih podataka EU-a, imajući na umu da velike količine ili zbirka klasificiranih podataka EU-a mogu zahtijevati primjenu strožih mjera zaštite;

   (c) okruženje i struktura zgrada ili područja u kojima su smješteni klasificirani podaci EU-a; i

   (d) procijenjena prijetnja od obavještajnih službi, čiji su cilj Unija ili države članice te od sabotaže, terorista, subverzivnih ili drugih kriminalnih aktivnosti.

4. Primjenjujući koncept dubinske obrane, nadležno sigurnosno tijelo određuje odgovarajuću kombinaciju mjera fizičke zaštite koje će se provesti. One mogu obuhvaćati jednu ili više sljedećih mjera:

   (a) rubna prepreka: fizička prepreka kojom se brani granica nekog područja za koje je potrebna zaštita;

   (b) sustavi za otkrivanje neovlaštenog ulaska (IDS): IDS se može rabiti za poboljšanje razine zaštite koju osigurava rubna prepreka ili u sobama i zgradama umjesto zaštitarskog osoblja ili kao pomoć njemu;

   (c) kontrola pristupa: kontrola pristupa može se provoditi na lokaciji, u zgradi ili zgradama na lokaciji ili u područjima ili sobama unutar zgrade. Kontrolu može provoditi zaštitarsko osoblje i/ili recepcionar pomoću elektroničkih ili elektromehaničkih sredstava ili bilo kojih drugih fizičkih sredstava;

   (d) zaštitarsko osoblje: može se zaposliti zaštitarsko osoblje koje je obučeno pod nadzorom i koje je, prema potrebi, prošlo odgovarajuću sigurnosnu provjeru, kako bi se, *inter alia*, odvratili pojedinci koji planiraju tajni neovlašteni ulazak;

   (e) televizija zatvorenog kruga (CCTV): zaštitarsko osoblje može rabiti CCTV za provjeru incidenata i dojava IDS-a na velikim lokacijama ili unutar perimetara;

   (f) sigurnosna rasvjeta: sigurnosna se rasvjeta može rabiti za odvraćanje mogućih neovlaštenih osoba te za osvjetljavanje potrebno za učinkovit nadzor koji izravno provodi zaštitarsko osoblje ili koji se neizravno provodi putem CCTV sustava; i

   (g) sve druge odgovarajuće mjere fizičke zaštite namijenjene odvraćanju od ili otkrivanju neovlaštenog pristupa ili sprečavanju gubitka ili oštećivanja klasificiranih podataka EU-a.

5. Nadležno tijelo može biti ovlašteno za provođenje pretrage prilikom ulaska i izlaska s ciljem odvraćanja od neovlaštenog unosa materijala ili neovlaštenog odnošenja klasificiranih podataka EU-a iz prostorija ili zgrada.

6. Ako postoji opasnost od uvida u klasificirane podatke EU-a, čak i slučajno, poduzimaju se odgovarajuće mjere za suzbijanje opasnosti.

7. Za nove se objekte zahtjevi u pogledu fizičke sigurnosti i njihove funkcionalne specifikacije definiraju u okviru planiranja i projektiranja objekata. U postojećim se objektima zahtjevi u pogledu fizičke sigurnosti provode u najvećoj mogućoj mjeri.

III. OPREMA ZA FIZIČKU ZAŠTITU KLASIFICIRANIH PODATAKA EU-a

8. Pri nabavi opreme (kao što su sigurnosni spremnici, uništavači papira, brave za vrata, elektronički sustavi za kontrolu pristupa, IDS, sustavi uzbunjivanja) za fizičku zaštitu klasificiranih podataka EU-a, nadležno sigurnosno tijelo osigurava da oprema ispunjava odobrene tehničke norme i minimalne zahtjeve.

9. Tehničke specifikacije opreme koja služi za fizičku zaštitu klasificiranih podataka EU-a navedene su u sigurnosnim smjernicama koje odobrava Sigurnosni odbor.

10. Sigurnosni se sustavi pregledavaju u pravilnim vremenskim razmacima, a oprema se redovito održava. Radovi održavanja u skladu su s ishodom inspekcija kako bi se osigurao daljnji optimalni rad opreme.

11. Učinkovitost pojedinačnih sigurnosnim mjera i cjelokupnog sigurnosnog sustava ponovno se ocjenjuje tijekom svake inspekcije.

IV. FIZIČKI ZAŠTIĆENA PODRUČJA

12. Za fizičku zaštitu klasificiranih podataka EU-a utvrđene su dvije vrste fizički zaštićenih područja ili njihovih nacionalnih ekvivalenata:

(a) administrativne zone; i

(b) sigurnosne zone (uključujući tehnički zaštićene sigurnosne zone).

U ovoj se Odluci svako upućivanje na administrativne zone i sigurnosne zone, uključujući tehnički zaštićene sigurnosne zone, smatra i upućivanjem na njihove nacionalne ekvivalente.

13. Nadležno sigurnosno tijelo određuje da određeno područje ispunjava zahtjeve te ga se stoga može odrediti kao administrativnu zonu, sigurnosnu zonu ili tehnički zaštićenu sigurnosnu zonu.

14. Za administrativne zone:

(a) uspostavlja se vidljivo utvrđeni perimetar koji omogućuje provjeru pojedinaca i, ako je moguće, vozila;

(b) pristup bez pratnje odobrava se samo pojedincima koje je propisno ovlastilo nadležno tijelo; i

(c) svi drugi pojedinci stalno imaju pratnju ili podliježu jednakim kontrolama.

15. Za sigurnosne zone:

(a) uspostavlja se vidljivo utvrđen i zaštićen perimetar kroz koji se nadziru svi ulasci i izlasci pomoću propusnice ili sustava prepoznavanja osoba;

(b) pristup bez pratnje odobrava se samo pojedincima koji su prošli sigurnosnu provjeru i koji su posebno ovlašteni za ulazak u područje na temelju nužnosti pristupa podacima; i

(c) svi drugi pojedinci stalno imaju pratnju ili podliježu jednakim kontrolama.

16. Ako ulazak u sigurnosnu zonu praktički predstavlja izravan pristup klasificiranim podacima sadržanima u toj zoni, primjenjuju se dodatni zahtjevi:

(a) mora biti jasno naveden najviši stupanj tajnosti podataka koji se uobičajeno čuvaju u zoni;

(b) svi posjetitelji moraju zatražiti posebno ovlaštenje za ulazak u zonu, moraju stalno imati pratnju i moraju proći odgovarajuću sigurnosnu provjeru, osim ako su poduzeti koraci kojima se onemogućuje svaki pristup klasificiranim podacima EU-a.

17. Sigurnosne zone zaštićene od prisluškivanja označene su kao tehnički zaštićene sigurnosne zone. Primjenjuju se sljedeći dodatni zahtjevi:

(a) takve zone opremljene su IDS-om, zaključane su kada u njima nema nikog i pod zaštitom kada je netko u njima. Svi se ključevi nadziru u skladu s odjeljkom VI.;

(b) nadziru se svi materijali i osobe koji ulaze u takve zone;

(c) u takvim se zonama redovito provode fizičke i/ili tehničke inspekcije na zahtjev nadležnog sigurnosnog tijela. Takve se inspekcije također provode nakon svakog neovlaštenog ulaska ili sumnje u takav ulazak; i

(d) u takvim zonama ne smije biti neovlaštenih komunikacijskih linija, neovlaštenih telefona ili drugih neovlaštenih komunikacijskih uređaja i električne ili elektroničke opreme.

18. Neovisno o točki (d) stavka 17., prije uporabe u zonama u kojima se održavaju sastanci ili obavlja posao koji obuhvaća podatke klasificirane kao SECRET UE/EU SECRET ili više i u kojima je prijetnja klasificiranim podacima EU-a ocijenjena kao visoka, sve komunikacijske uređaje i električnu ili elektroničku opremu najprije ispituje nadležno sigurnosno tijelo s ciljem sprečavanja slučajnog ili nedopuštenog prijenosa razumljivih podataka pomoću takve opreme izvan perimetra sigurnosne zone.

19. Sigurnosne zone u kojima nema osoblja na dužnosti 24 sata dnevno pregledavaju se, prema potrebi, na kraju redovitog radnog vremena i u nasumičnim vremenskim razmacima izvan redovitog radnog vremena, osim ako je postavljen IDS.

20. Sigurnosne zone i tehnički zaštićene sigurnosne zone mogu se uspostaviti privremeno unutar administrativne zone za tajne sastanke ili u druge slične svrhe.

21. Za svaku se sigurnosnu zonu sastavljaju sigurnosno-operativni postupci kojima se određuju:

(a) stupanj tajnosti klasificiranih podataka EU-a s kojima se može postupati i koji se mogu čuvati u zoni;

(b) mjere nadzora i zaštitne mjere koje je potrebno održavati;

(c) pojedinci ovlašteni za pristup zoni bez pratnje, na temelju nužnosti pristupa podacima i sigurnosne provjere;

(d) prema potrebi, postupci za pratnju ili zaštitu klasificiranih podataka EU-a ako se ovlašćuju bilo koji drugi pojedinci za pristup zoni; i

(e) sve druge odgovarajuće mjere i postupci.

22. Unutar sigurnosnih zona moraju biti izgrađeni trezori. Nadležno sigurnosno tijelo odobrava zidove, podove, stropove, prozore i vrata koja se mogu zaključati, koji osiguravaju zaštitu jednaku sigurnosnom spremniku odobrenom za čuvanje klasificiranih podataka EU-a istog stupnja tajnosti.

V. FIZIČKE MJERE ZAŠTITE ZA POSTUPANJE S KLASIFICIRANIM PODACIMA EU-a I NJIHOVO ČUVANJE

23. S klasificiranim podacima EU-a sa stupnjem tajnosti RESTREINT UE/EU RESTRICTED može se postupati:

(a) u sigurnosnoj zoni;

(b) u administrativnoj zoni uz uvjet da su klasificirani podaci EU-a zaštićeni od pristupa neovlaštenih pojedinaca; ili

(c) izvan sigurnosne ili administrativne zone uz uvjet da imatelj prenosi klasificirane podatke EU-a u skladu sa stavcima od 28. do 41. Priloga III. i da se obvezao poštovati kompenzacijske mjere utvrđene u sigurnosnim uputama koje izdaje nadležno sigurnosno tijelo s ciljem zaštite klasificiranih podataka EU-a od pristupa neovlaštenih osoba.

24. Klasificirani podaci EU-a sa stupnjem tajnosti RESTREINT UE/EU RESTRICTED čuvaju se u primjerenom zaključanom uredskom namještaju u administrativnoj ili sigurnosnoj zoni. Privremeno se mogu čuvati izvan sigurnosne ili administrativne zone uz uvjet da se imatelj obvezao poštovati kompenzacijske mjere utvrđene u sigurnosnim uputama koje izdaje nadležno sigurnosno tijelo.

25. S klasificiranim podacima EU-a sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET može se postupati:

(a) u sigurnosnoj zoni;

(b) u administrativnoj zoni uz uvjet da su klasificirani podaci EU-a zaštićeni od pristupa neovlaštenih pojedinaca; ili

(c) izvan sigurnosne ili administrativne zone uz uvjet da imatelj:

i. prenosi klasificirane podatke EU-a u skladu sa stavcima od 28. do 41. Priloga III.;

ii. obvezao se poštovati kompenzacijske mjere utvrđene u sigurnosnim uputama koje izdaje nadležno sigurnosno tijelo s ciljem zaštite klasificiranih podataka EU-a od pristupa neovlaštenih osoba;

iii. stalno drži klasificirane podatke EU-a pod osobnom kontrolom; i

iv. ako su dokumenti u papirnom obliku, obavijestio je o tome nadležni registar.

26. Klasificirani podaci EU-a sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET čuvaju se u sigurnosnoj zoni ili u sigurnosnom spremniku ili u trezoru.

27. S klasificiranim podacima EU-a sa stupnjem tajnosti TRÈS SECRET UE/EU TOP SECRET postupa se u sigurnosnoj zoni.

28. Klasificirani podaci EU-a sa stupnjem tajnosti TRÈS SECRET UE/EU TOP SECRET čuvaju se u sigurnosnoj zoni uz jedan od sljedećih uvjeta:

(a) u sigurnosnom spremniku u skladu sa stavkom 8. uz najmanje jednu od sljedećih dodatnih kontrola:

i. stalnu zaštitu ili provjeru koju provodi zaštitarsko osoblje ili osoblje na dužnosti koje je prošlo sigurnosnu provjeru;

ii. odobren IDS u kombinaciji sa zaštitarskim osobljem za odziv;

(b) u trezoru opremljenom IDS-om u kombinaciji sa zaštitarskim osobljem za odziv.

29. Pravila kojima se uređuje prijenos klasificiranih podataka EU-a izvan fizički zaštićenih područja određena su u Prilogu III.

VI. KONTROLA KLJUČEVA I KOMBINACIJA ZA ZAŠTITU KLASIFICIRANIH PODATAKA EU-a

30. Nadležno sigurnosno tijelo određuje postupke za upravljanje ključevima i postavkama kombinacija za urede, sobe, trezore i sigurnosne spremnike. Takvi postupci predstavljaju zaštitu od neovlaštenog pristupa.

31. Postavke kombinacija pamti najmanji mogući broj pojedinaca koji ih moraju znati. Postavke kombinacija za sigurnosne spremnike i trezore u kojima se čuvaju klasificirani podaci EU-a mijenjaju se:

(a) prilikom primitka novog spremnika;

(b) pri svakoj promjeni osoblja koje zna kombinaciju;

(c) pri svakoj pojavi ugroze ili sumnje u ugrozu;

(d) u slučaju popravka ili održavanja brave i

(e) najmanje svakih 12 mjeseci.

*PRILOG III.*

## UPRAVLJANJE KLASIFICIRANIM PODACIMA

I. UVOD

1. U ovom se Prilogu određuju odredbe za provedbu članka 9. U njemu se utvrđuju upravne mjere za kontrolu klasificiranih podataka EU-a tijekom njihova životnog ciklusa, radi lakšeg odvraćanja i otkrivanja namjerne ili slučajne ugroze ili gubitka takvih podataka.

II. UPRAVLJANJE KLASIFIKACIJOM

**Klasifikacija i oznake**

2. Podaci se klasificiraju ako je potrebna zaštita u pogledu njihove tajnosti.

3. Onaj od kojeg potječu klasificirani podaci EU-a odgovoran je za utvrđivanje stupnja tajnosti u skladu s odgovarajućim smjernicama za klasifikaciju te za početno širenje podataka.

4. Stupanj tajnosti klasificiranih podataka EU-a određuje se u skladu s člankom 2. stavkom 2. i pozivom na sigurnosnu politiku koja se odobrava u skladu s člankom 3. stavkom 3.

5. Stupanj tajnosti mora biti jasno i pravilno naveden, bez obzira na to jesu li klasificirani podaci EU-a u papirnatom, usmenom, elektroničkom ili nekom drugom obliku.

6. Pojedinačni dijelovi određenog dokumenta (npr. stranice, stavci, odjeljci, prilozi, dodaci i privici) mogu zahtijevati drugačiju klasifikaciju te stoga moraju biti označeni na odgovarajući način, uključujući dijelove pohranjene u elektroničkom obliku.

7. Cjelokupni stupanj tajnosti dokumenta ili spisa mora biti najmanje jednako visok kao njegova komponenta s najvišim stupnjem tajnosti. Ako se uređuju podaci iz različitih izvora, konačni se proizvod pregledava kako bi se utvrdio njegov cjelokupni stupanj tajnosti jer mu se može odrediti viši stupanj tajnosti od onog koji imaju njegovi sastavni dijelovi.

8. Ako je to moguće, dokumenti koji sadržavaju dijelove s različitim stupnjevima tajnosti strukturiraju se tako da se dijelovi s različitim stupnjevima tajnosti mogu lako utvrditi i prema potrebi odvojiti.

9. Stupanj tajnosti pisma ili napomene koji obuhvaćaju privitke mora biti jednak najvišem stupnju tajnosti njihovih privitaka. Onaj od kojeg podaci potječu jasno navodi koji je stupanj tajnosti pisma ili napomene kada se odvoji od privitaka koristeći odgovarajuće oznake, npr.:

CONFIDENTIEL UE/EU CONFIDENTIAL

Bez privitka(-taka) RESTREINT UE/EU RESTRICTED

**Oznake**

10. Uz jednu od oznaka stupnja tajnosti navedenih u članku 2. stavku 2. klasificirani podaci EU-a mogu nositi dodatne oznake kao što su:

(a) oznaka kojom se određuje onaj od kojeg podaci potječu;

(b) sva upozorenja, šifre ili akronimi kojima se navodi područje djelovanja na koje se dokument odnosi, posebna distribucija prema nužnosti pristupa podacima ili ograničenja uporabe;

(c) oznake o mogućnosti objavljivanja; ili

(d) ako je primjenjivo, datum ili posebni događaj nakon kojeg se stupanj tajnosti može smanjiti ili se podaci mogu deklasificirati.

**Skraćene oznake stupnja tajnosti**

11. Mogu se rabiti standardizirane skraćene oznake stupnja tajnosti kojima se navodi stupanj tajnosti pojedinačnih stavaka u tekstu. Kratice ne zamjenjuju potpunu oznaku stupnja tajnosti.

12. U klasificiranim podacima EU-a mogu se koristiti sljedeće standardne kratice kojima se označuje stupanj tajnosti odjeljaka ili dijelova teksta kraćih od jedne stranice:

| | |
|---|---|
| TRÈS SECRET UE/EU TOP SECRET | TS-UE/EU-TS |
| SECRET UE/EU SECRET | S-UE/EU-S |
| CONFIDENTIEL UE/EU CONFIDENTIAL | C-UE/EU-C |
| RESTREINT UE/EU RESTRICTED | R-UE/EU-R |

**Stvaranje klasificiranih podataka EU-a**

13. Prilikom stvaranja klasificiranog dokumenta EU-a:

(a) svaka stranica mora biti jasno označena stupnjem tajnosti;

(b) svaka stranica mora biti numerirana;

(c) dokument mora imati referentni broj i predmet koji sam za sebe nije klasificirani podatak, osim ako je označen kao takav;

(d) dokument mora biti označen datumom; i

(e) dokumenti klasificirani kao SECRET UE/EU SECRET ili iznad moraju imati broj preslika na svakoj stranici ako se distribuiraju u nekoliko primjeraka.

14. Ako se stavak 13. ne može primijeniti na klasificirane podatke EU-a, poduzimaju se druge odgovarajuće mjere u skladu sa sigurnosnim smjernicama koje se utvrđuju u skladu s člankom 6. stavkom 2.

**Smanjivanje stupnja tajnosti i deklasifikacija klasificiranih podataka EU-a**

15. U trenutku njihova stvaranja onaj od kojeg podaci potječu navodi, ako je to moguće, a posebno za podatke klasificirane kao RESTREINT UE/EU RESTRICTED, može li se stupanj tajnosti klasificiranih podataka EU-a smanjiti, odnosno mogu li se oni deklasificirati na određeni datum ili nakon određenog događaja.

16. GSC redovito pregledava klasificirane podatke EU-a u svojem posjedu kako bi utvrdio primjenjuje li se još uvijek stupanj tajnosti. GSC uspostavlja sustav za pregled stupnja tajnosti klasificiranih podataka EU-a koji potječu od njega najmanje svakih pet godina. Takav pregled nije neophodan ako je onaj od kojeg podaci potječu na početku naveo da će se stupanj tajnosti podataka automatski smanjiti ili da će se podaci deklasificirati te ako su podaci u skladu s tim označeni.

III. UPIS KLASIFICIRANIH PODATAKA EU-a U SIGURNOSNE SVRHE

17. Za svaki se organizacijski subjekt u sklopu GSC-a i nacionalnih administracija država članica u kojem se postupa s klasificiranim podacima EU-a određuje odgovorni registar, kako bi se osiguralo postupanje s klasificiranim podacima EU-a u skladu s ovom Odlukom. Registri se uspostavljaju kao sigurnosne zone kako je određeno u Prilogu II.

18. Za potrebe ove Odluke, upis u sigurnosne svrhe („upis") znači primjenu postupaka za bilježenje životnog ciklusa materijala, uključujući njegovo širenje i uništavanje.

19. Svi materijali klasificirani kao CONFIDENTIEL UE/EU CONFIDENTIAL i više upisuju se u određene registre kada stignu u organizacijski subjekt ili iz njega odlaze.

20. Središnji registar u sklopu GSC-a čuva evidenciju o svim klasificiranim podacima koje su Vijeće i GSC objavili trećim državama i međunarodnim organizacijama, te o svim klasificiranim podacima primljenim od trećih zemalja ili međunarodnih organizacija.

21. U slučaju CIS-a, postupak upisa provodi se kroz procese unutar samog CIS-a.

22. Vijeće odobrava sigurnosnu politiku o upisu klasificiranih podataka EU-a u sigurnosne svrhe.

**Registri za podatke klasificirane kao TRÈS SECRET UE/EU TOP SECRET**

23. U državama članicama i GSC-u određuje se registar koji djeluje kao središnje tijelo za primanje i slanje podataka klasificiranih kao TRÈS SECRET UE/EU TOP SECRET. Prema potrebi, mogu se odrediti podregistri za postupanje s takvim podacima u svrhu njihova upisa.

24. Takvi podregistri ne smiju izravno prenositi dokumente klasificirane kao TRÈS SECRET UE/EU TOP SECRET u druge podregistre istog središnjeg registra za podatke klasificirane kao TRÈS SECRET UE/EU TOP SECRET ili izvan njega bez izričitog pisanog odobrenja potonjeg.

IV. UMNOŽAVANJE I PREVOĐENJE KLASIFICIRANIH DOKUMENATA EU-a

25. Dokumenti klasificirani kao TRÈS SECRET UE/EU TOP SECRET ne smiju se umnožavati ili prevoditi bez prethodne pisane suglasnosti onog od kojeg podaci potječu.

26. Ako onaj od kojeg potječu dokumenti klasificirani kao SECRET UE/EU SECRET ili niže nije odredio upozorenja u pogledu umnožavanja ili prijevoda, takvi se dokumenti mogu umnožavati ili prevoditi prema uputi imatelja.

27. Sigurnosne mjere primjenjive na izvorni dokument primjenjuju se i na njegove preslike i prijevode.

V. PRIJENOS KLASIFICIRANIH PODATAKA EU-a

28. Prijenos klasificiranih podataka EU-a podliježe zaštitnim mjerama određenim u stavcima od 30. do 41. Ako se klasificirani podaci prenose na elektroničkim medijima i neovisno o članku 9. stavku 4., zaštitne mjere navedene u nastavku mogu se dopuniti odgovarajućim tehničkim protumjerama koje je propisalo nadležno sigurnosno tijelo, kako bi se umanjio rizik od gubitka ili ugroze.

29. Nadležna sigurnosna tijela u GSC-u i državama članicama izdaju upute o prijenosu klasificiranih podataka EU-a u skladu s ovom Odlukom.

**Unutar zgrade ili kompleksa zgrada**

30. Klasificirani podaci EU-a koji se prenose unutar zgrade ili kompleksa zgrada moraju biti pokriveni kako bi se spriječilo promatranje njihova sadržaja.

31. Podaci klasificirani kao TRÈS SECRET UE/EU TOP SECRET prenose se unutar zgrade ili kompleksa zgrada u zaštićenoj omotnici na kojoj je navedeno samo ime adresata.

**Unutar Unije**

32. Klasificirani podaci EU-a koji se prenose između zgrada ili prostorija unutar EU-a zapakirani su tako da su zaštićeni od neovlaštenog otkrivanja.

33. Podaci sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET prenose se unutar Unije na jedan od sljedećih načina:

(a) po vojnom, vladinom ili diplomatskom kuriru, ovisno o slučaju;

(b) ručno, uz sljedeće uvjete:

i. da su klasificirani podaci EU-a stalno u posjedu nositelja, osim ako su pohranjeni u skladu sa zahtjevima navedenima u Prilogu II.;

ii. da se klasificirani podaci EU-a putem ne otvaraju i da se ne čitaju na javnim mjestima;

iii. pojedinci su upoznati sa svojim odgovornostima u pogledu sigurnosti; i

iv. pojedincima se prema potrebi osigurava kurirska potvrda;

(c) poštanskom službom ili komercijalnom kurirskom službom uz sljedeće uvjete:

i. da ju je odobrio nadležni NSA u skladu s nacionalnim zakonima i propisima; i

ii. da služba primjenjuje odgovarajuće mjere zaštite u skladu s minimalnim zahtjevima utvrđenim u sigurnosnim smjernicama u skladu s člankom 6. stavkom 2.

U slučaju prijenosa iz jedne države članice u drugu, odredbe točke (c) ograničene su na podatke stupnja tajnosti do CONFIDENTIEL UE/EU CONFIDENTIAL.

34. Podaci sa stupnjem tajnosti RESTREINT UE/EU RESTRICTED mogu se također prenositi poštanskom službom ili komercijalnom kurirskom službom. Kurirska potvrda nije potrebna za prijenos takvih podataka.

35. Materijal klasificiran kao CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET (npr. oprema ili strojevi) koji se ne može prenositi sredstvima navedenima u stavku 33., prevoze komercijalni prijevoznici kao teret u skladu s Prilogom V.

36. Podaci klasificirani kao TRÈS SECRET UE/EU TOP SECRET prenose se između zgrada ili prostorija unutar Unije po vojnom, vladinom ili diplomatskom kuriru, ovisno o slučaju.

**Iz Unije na državno područje treće države**

37. Klasificirani podaci koji se iz Unije prenose na državno područje treće države zapakirani su tako da su zaštićeni od neovlaštenog otkrivanja.

38. Podaci klasificirani kao CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET prenose se iz Unije na državno područje treće države na jedan od sljedećih načina:

(a) po vojnom ili diplomatskom kuriru;

(b) ručno, uz sljedeće uvjete:

i. da je na paketu službeni pečat ili da je zapakiran na način kojim se naznačuje kako je riječ o službenoj pošiljci koja ne prolazi carinsku ili sigurnosnu provjeru;

ii. da pojedinci nose kurirsku potvrdu kojom se identificira paket i koja pojedince ovlašćuje za nošenje paketa;

iii. da su klasificirani podaci EU-a stalno u posjedu nositelja, osim ako su pohranjeni u skladu sa zahtjevima navedenim u Prilogu II.;

iv. da se klasificirani podaci EU-a putem ne otvaraju i da se ne čitaju na javnim mjestima; i

v. da su pojedinci upoznati sa svojim odgovornostima u pogledu sigurnosti.

39. Prijenos podataka sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET koje je Unija objavila trećoj državi ili međunarodnoj organizaciji udovoljava odgovarajućim odredbama sporazuma o sigurnosti podataka ili administrativnog dogovora u skladu s člankom 13. stavkom 2. točkama (a) ili (b).

40. Podaci klasificirani kao RESTREINT UE/EU RESTRICTED mogu se također prenositi poštanskom službom ili komercijalnom kurirskom službom.

41. Podaci klasificirani kao TRÈS SECRET UE/EU TOP SECRET prenose se iz Unije na državno područje treće države po vojnom ili diplomatskom kuriru.

VI. UNIŠTAVANJE KLASIFICIRANIH PODATAKA EU-a

42. Klasificirani dokumenti EU-a koji više nisu potrebni mogu se uništiti ne dovodeći u pitanje mjerodavna pravila i propise o arhiviranju.

43. Dokumente koji podliježu upisu u skladu s člankom 9. stavkom 2. uništava odgovorni registar prema uputi imatelja ili nadležnog tijela. Očevidnici i drugi podaci o upisu ažuriraju se u skladu s tim.

44. Dokumenti klasificirani kao SECRET UE/EU SECRET ili TRÈS SECRET UE/EU TOP SECRET uništavaju se u nazočnosti svjedoka koji je prošao sigurnosnu provjeru najmanje za stupanj tajnosti dokumenta koji se uništava.

45. Tajnik i svjedok, ako je potrebna nazočnost potonjeg, potpisuju potvrdu o uništavanju koja se pohranjuje u registru. Registar čuva potvrde o uništavanju dokumenata klasificiranih kao TRÈS SECRET UE/EU TOP SECRET najmanje 10 godina, a dokumenata klasificiranih kao CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET najmanje pet godina.

46. Klasificirani dokumenti, uključujući dokumente klasificirane kao RESTREINT UE/EU RESTRICTED, uništavaju se na načine koji ispunjavaju odgovarajuće standarde EU-a ili jednake standarde ili koje su odobrile države članice u skladu s nacionalnim tehničkim normama radi sprečavanja rekonstrukcije u cijelosti ili djelomično.

47. Računalni nosači podataka koji su se koristili za klasificirane podatke EU-a uništavaju se u skladu sa stavkom 37. Priloga IV.

48. U hitnim slučajevima, ako postoji neposredna opasnost od neovlaštenog otkrivanja, imatelj uništava klasificirane podatke EU-a tako da se ne mogu djelomično ili u cijelosti rekonstruirati. O izvanrednom uništenju upisanih klasificiranih podataka EU-a obavješćuje se onaj od kojeg potječu ti podaci i izvorni registar.

VII. POSJETI RADI PROCJENE STANJA

49. Pojam „posjet radi procjene stanja" rabi se dalje u tekstu te podrazumijeva:

(a) inspekcije ili posjete radi procjene stanja u skladu s člankom 9. stavkom 3. i člankom 16. stavkom 2. točkama (e), (f) i (g); ili

(b) posjet radi procjene stanja u skladu s člankom 13. stavkom 5.,

s ciljem ocjenjivanja učinkovitosti provedenih mjera za zaštitu klasificiranih podataka EU-a.

50. Posjeti radi procjene stanja provode kako bi se, *inter alia*:

(a) osiguralo poštovanje potrebnih minimalnih standarda za zaštitu klasificiranih podataka EU-a utvrđenih ovom Odlukom;

(b) naglasila važnost sigurnosti i učinkovitog upravljanja rizicima unutar subjekata u kojima se provodi inspekcija;

(c) preporučile protumjere za ublažavanje specifičnog učinka gubitka tajnosti, cjelovitosti ili dostupnosti klasificiranih podataka; i

(d) ojačali tekući obrazovni programi i programi za podizanje svijesti o sigurnosti koje provode sigurnosna tijela.

51. Prije završetka svake kalendarske godine Vijeće za sljedeću godinu donosi program posjeta radi procjene stanja predviđen člankom 16. stavkom 1. točkom (c). Stvarni datumi svakog posjeta radi procjene stanja određuju se u dogovoru s predmetnim tijelom ili agencijom Unije, državom članicom, trećom državom ili međunarodnom organizacijom.

**Posjeti radi procjene stanja**

52. Posjeti radi procjene stanja provode se s ciljem provjere mjerodavnih pravila, propisa i postupaka u subjektu koji se posjećuje te kako bi se provjerilo jesu li prakse subjekta u skladu s osnovnim načelima i minimalnim standardima utvrđenima ovom Odlukom i odredbama kojima se uređuje razmjena klasificiranih podataka s tim subjektom.

53. Posjeti radi procjene stanja provode se u dvije faze. Prije samog posjeta organizira se, prema potrebi, pripremni sastanak s predmetnim subjektom. Nakon pripremnog sastanka tim za procjenu, u dogovoru s predmetnim subjektom, utvrđuje podrobni program posjeta radi procjene stanja kojim su obuhvaćena sva područja sigurnosti. Tim za procjenu stanja trebao bi imati pristup svim lokacijama na kojima se postupa s klasificiranim podacima EU-a, a posebno registrima i točkama pristupa CIS-u.

54. Posjeti radi procjene stanja nacionalnim administracijama, trećim državama i međunarodnim organizacijama provode se u potpunoj suradnji s dužnosnicima subjekta, treće države ili međunarodne organizacije koja se posjećuje.

55. Posjeti radi procjene stanja tijelima, agencijama i subjektima Unije koji primjenjuju ovu Odluku ili njezina načela provode se uz pomoć stručnjaka NSA-a na čijem se državnom području nalazi tijelo ili agencija.

56. Za posjete radi procjene stanja tijelima, agencijama i subjektima Unije koji primjenjuju ovu Odluku ili njezina načela te trećim državama i međunarodnim organizacijama može se tražiti pomoć i doprinos stručnjaka NSA-a u skladu s detaljnim rješenjima koje treba dogovoriti Sigurnosni odbor.

**Izvješća**

57. Na kraju posjeta radi procjene stanja posjećenom subjektu predstavljaju se glavni zaključci i preporuke. Nakon toga sastavlja se izvješće o posjetu radi procjene stanja. Ako su predložene korektivne mjere i preporuke, doneseni se zaključci moraju dovoljno podrobno potkrijepiti u izvješću. Izvješće se prosljeđuje odgovarajućem tijelu posjećenog subjekta.

58. Za posjete radi procjene stanja provedene u nacionalnim administracijama država članica:

(a) nacrt izvješća o procjeni prosljeđuje se predmetnom NSA-u koji provjerava točnost činjenica te sadrži li izvješće podatke sa stupnjem tajnosti višim od RESTREINT UE/EU RESTRICTED; i

(b) osim ako predmetni NSA države članice zabrani opću distribuciju, izvješća o procjeni prosljeđuju se Sigurnosnom odboru. Izvješće je klasificirano kao RESTREINT UE/EU RESTRICTED.

Sigurnosno tijelo GSC-a (Ured za sigurnost) odgovorno je za pripremu redovitog izvješća u kojem se ističu lekcije naučene iz posjeta radi procjene stanja provedenih u državama članicama u određenom razdoblju i pregledanih od strane Sigurnosnog odbora.

59. Izvješće o posjetima trećim državama i međunarodnim organizacijama radi procjene stanja dostavlja se Sigurnosnom odboru. Izvješće je klasificirano najmanje kao RESTREINT UE/EU RESTRICTED. Sve korektivne radnje provjeravaju se tijekom sljedećeg posjeta te se o njima izvješćuje Sigurnosni odbor.

60. Za posjete radi procjene stanja bilo kojim tijelima, agencijama, i subjektima Unije koji primjenjuju ovu Odluku ili njezina načela, izvješća o posjetima radi procjene stanja dostavljaju se Sigurnosnom odboru. Nacrt izvješća o posjetu radi procjene stanja prosljeđuje se predmetnoj agenciji ili tijelu koje provjerava točnost činjenica te sadrži li izvješće podatke sa stupnjem tajnosti višim od RESTREINT UE/EU RESTRICTED. Sve korektivne radnje provjeravaju se tijekom sljedećeg posjeta te se o njima izvješćuje Sigurnosni odbor.

61. Sigurnosno tijelo GSC-a provodi redovite inspekcije organizacijskih subjekata GSC-a u svrhe utvrđene u stavku 50.

**Kontrolna lista**

62. Sigurnosno tijelo GSC-a (Ured za sigurnost) sastavlja i ažurira kontrolnu listu stavki koje se provjeravaju tijekom posjeta radi procjene stanja. Ta se kontrolna lista prosljeđuje Sigurnosnom odboru.

63. Podaci za popunjavanje kontrolne liste dobivaju se posebno tijekom posjeta od rukovodstva za sigurnost subjekta koji se pregledava. Nakon što je popunjena podrobnim odgovorima, kontrolna se lista klasificira u dogovoru s pregledanim subjektom. Ona ne čini dio izvješća o inspekciji.

*PRILOG IV.*

**ZAŠTITA KLASIFICIRANIH PODATAKA EU-a S KOJIMA SE POSTUPA U CIS-u**

I. UVOD

1. U ovom se Prilogu određuju odredbe za provedbu članka 10.

2. Sljedeća svojstva i pojmovi IA-a bitni su za sigurnost i pravilno funkcioniranje aktivnosti u CIS-u:

Autentičnost: jamstvo da je podatak pravi i da potječe iz dobronamjernih izvora,

Dostupnost: svojstvo da ovlašteni subjekt na zahtjev može pristupiti podatku i koristiti ga,

Tajnost: svojstvo da se podatak ne otkriva neovlaštenim pojedincima, subjektima ili procesima,

Cjelovitost: svojstvo očuvanja točnosti i potpunosti podataka i imovine,

Nepobitnost: sposobnost dokazivanja da se dogodila određena radnja ili da je nastupio određeni događaj tako da ga poslije nije moguće zanijekati.

II. NAČELA INFORMACIJSKE SIGURNOSTI

3. Odredbe navedene u nastavku čine osnovu sigurnosti svakog CS-a u kojem se postupa s klasificiranim podacima EU-a. Podrobni zahtjevi za provedbu ovih odredaba određeni su u sigurnosnim politikama i sigurnosnim smjernicama za IA.

**Upravljanje sigurnosnim rizicima**

4. Upravljanje sigurnosnim rizicima sastavni je dio definiranja, razvoja, rada i održavanja CIS-a. Upravljanje rizicima (procjena, postupanje, prihvaćanje i obavješćivanje) je proces koji se ponavlja i provodi zajedno s predstavnicima vlasnika sustava, tijela za projekte, operativnih tijela i tijela za sigurnosno odobrenje uz primjenu provjerenog, transparentnog i potpuno razumljivog procesa procjene rizika. Područje primjene CIS-a i njegovih sastavnih dijelova mora biti jasno određeno od samog početka procesa procjene rizika.

5. Nadležna tijela pregledavaju moguće prijetnje CIS-u i održavaju ažurirane i točne procjene prijetnji koje odražavaju trenutačno radno okruženje. Neprestano ažuriraju svoje znanje o pitanjima osjetljivosti i periodično pregledavaju procjene osjetljivosti kako bi držala korak s promjenljivim okruženjem informacijskih tehnologija (IT).

6. Cilj postupanja s rizicima je primjena skupa sigurnosnih mjera koja će rezultirati zadovoljavajućom ravnotežom između zahtjeva imatelja, troškova i preostalog sigurnosnog rizika.

7. Posebni zahtjevi, opseg i stupanj podrobnosti koje je odredio nadležni SAA za akreditaciju CIS-a razmjerni su procijenjenom riziku, uzimajući u obzir važne čimbenike, uključujući stupanj tajnosti klasificiranih podataka EU-a s kojima se postupa u CIS-u. Akreditacija obuhvaća službenu izjavu o preostalom riziku koju daje odgovorno tijelo i time prihvaća preostali rizik.

**Sigurnost tijekom životnog ciklusa CIS-a**

8. Osiguravanje sigurnosti je zahtjev koji je na snazi tijekom cijelog životnog ciklusa CIS-a, od njegova pokretanja do povlačenja iz uporabe.

9. Uloga i međudjelovanje svakog činitelja uključenog u CIS-u pogledu njegove sigurnosti određuju se za svaku fazu životnog ciklusa.

10. Svaki CIS, uključujući njegove tehničke i netehničke sigurnosne mjere, podliježe sigurnosnom testiranju tijekom procesa akreditacije, kako bi se osigurala odgovarajuća razina sigurnosti i provjerilo je li ispravno proveden, integriran i konfiguriran.

11. Sigurnosne procjene, inspekcije i pregledi provode se periodično tijekom rada i održavanja CIS-a i ako nastupe izvanredne okolnosti.

12. Sigurnosna dokumentacija za CIS razrađuje se tijekom životnog ciklusa CIS-a kao sastavni dio procesa upravljanja promjenama i konfiguracijom.

**Najbolja praksa**

13. GSC i države članice surađuju na razvoju najbolje prakse za zaštitu klasificiranih podataka EU-a s kojima se postupa u CIS-u. U smjernicama za najbolje prakse navedene su tehničke, fizičke, organizacijske i postupovne sigurnosne mjere za CIS koje su dokazano učinkovite u suzbijanju navedenih prijetnji i osjetljivosti.

14. Zaštita klasificiranih podataka EU-a s kojima se postupa u CIS-u oslanja se na iskustvo koje su subjekti uključeni u IA stekli unutar i izvan Unije.

15. Širenje i naknadna provedba najboljih praksi pomaže u postizanju jednake razine sigurnosti za različite CIS-eve kojima upravljaju GSC i države članice i u kojima se postupa s klasificiranim podacima EU-a.

**Dubinska obrana**

16. Kako bi se ublažio rizik za CIS, provodi se niz tehničkih i netehničkih sigurnosnih mjera organiziranih kao višestruki slojevi obrane. Navedeni slojevi obuhvaćaju:

(a) *odvraćanje:* sigurnosne mjere namijenjene odvraćanju neprijatelja od planiranja napada na CIS;

(b) *sprečavanje:* sigurnosne mjere namijenjene ometanju ili zaustavljanju napada na CIS;

(c) *otkrivanje:* sigurnosne mjere namijenjene otkrivanju pojave napada na CIS;

(d) *otpornost:* sigurnosne mjere namijenjene ograničavanju učinka napada na najmanji skup podataka ili sastavnih dijelova CIS-a i sprečavanju daljnje štete; i

(e) *oporavak:* sigurnosne mjere namijenjene ponovnoj uspostavi sigurne situacije za CIS.

Stupanj strogoće takvih sigurnosnih mjera određuje se nakon procjene rizika.

17. NSA ili drugo nadležno tijelo osigurava:

(a) primjenu kibernetičkih obrambenih sposobnosti s ciljem odgovora na prijetnje koje mogu prelaziti organizacijske i državne granice; i

(b) koordinaciju odgovora i razmjenu podataka o navedenim prijetnjama, incidentima i povezanim rizicima (sposobnost odgovora na izvanredne situacije u području računarstva).

**Načelo minimalnosti i najmanjih povlastica**

18. Radi izbjegavanja nepotrebnih rizika provode se samo bitne funkcionalnosti, uređaji i usluge kako bi se zadovoljili operativni zahtjevi.

19. Korisnicima CIS-a i automatiziranim procesima daju se pristup, povlastice ili ovlaštenja koja su im potrebna za obavljanje zadaća kako bi se ograničila svaka šteta nastala kao rezultat nezgoda, pogrešaka ili neovlaštene uporabe resursa CIS-a.

20. Postupci upisa koje provodi CIS provjeravaju se, prema potrebi, u okviru procesa akreditacije.

**Svijest o informacijskoj sigurnosti**

21. Svijest o rizicima i raspoloživim sigurnosnim mjerama prva je linija obrane sigurnosti CIS-a. Cjelokupno osoblje uključeno u životni ciklus CIS-a, uključujući imatelje, mora posebno razumjeti:

(a) da sigurnosni propusti mogu nanijeti znatnu štetu CIS-u;

(b) moguću štetu za druge koja može proizići iz međusobne povezanosti i uzajamne ovisnosti; i

(c) osobnu obveznost i odgovornost za sigurnost CIS-a u skladu sa svojim ulogama unutar sustava i procesa.

22. Kako bi se osiguralo razumijevanje odgovornosti u pogledu sigurnosti, obrazovanje o IA-u i obuka za podizanje svijesti o IA-u obvezni su za cjelokupno uključeno osoblje, uključujući više rukovodstvo i korisnike CIS-a.

**Ocjenjivanje i odobravanje proizvoda za IT sigurnost**

23. Potreban stupanj povjerenja u sigurnosne mjere, definiran kao razina sigurnosti, određuje se nakon ishoda procesa procjene rizika i u skladu s mjerodavnim sigurnosnim politikama i sigurnosnim smjernicama.

24. Razina sigurnosti provjerava se uporabom međunarodno priznanih ili nacionalno odobrenih procesa i metodologija. Navedeno ponajprije obuhvaća ocjenjivanje, kontrole i reviziju.

25. Kriptografske proizvode za zaštitu klasificiranih podataka EU-a ocjenjuje i odobrava nacionalni CAA države članice.

26. Prije no što se preporuče Vijeću ili glavnom tajniku za odobravanje u skladu s člankom 10. stavkom 6., takvi kriptografski proizvodi moraju uspješno proći drugo ocjenjivanje koje provodi odgovarajuće kvalificirano tijelo (AQUA) države članice koje nije uključeno u projektiranje ili proizvodnju opreme. Stupanj detalja potreban u drugom ocjenjivanju ovisi o najvišem predviđenom stupnju tajnosti klasificiranih podataka EU-a koji će se štiti navedenim proizvodima. Vijeće odobrava sigurnosnu politiku za ocjenjivanje i odobravanje kriptografskih proizvoda.

27. Ako je opravdano posebnim operativnim razlozima, Vijeće ili glavni tajnik mogu, prema potrebi i na preporuku Sigurnosnog odbora, ukinuti zahtjeve iz stavaka 25. i 26. ovog Priloga i dati privremeno odobrenje za određeno razdoblje u skladu s postupkom utvrđenim u članku 10. stavku 6.

28. Vijeće, postupajući po preporuci Sigurnosnog odbora, može prihvatiti postupak ocjenjivanja, odabira i odobravanja kriptografskih proizvoda treće države ili međunarodne organizacije i u skladu s time utvrditi da su takvi kriptografski proizvodi odobreni za zaštitu klasificiranih podataka EU-a objavljenih u toj trećoj državi ili međunarodnoj organizaciji.

29. AQUA je CAA države članice koja je, na temelju kriterija koje je utvrdilo Vijeće, ovlaštena za provođenje drugog ocjenjivanja kriptografskih proizvoda za zaštitu klasificiranih podataka EU-a.

30. Vijeće odobrava sigurnosnu politiku za kvalifikaciju i odobravanje nekriptografskih proizvoda za IT sigurnost.

**Slanje unutar sigurnosnih i administrativnih zona**

31. Neovisno o odredbama ove Odluke, ako je slanje klasificiranih podataka EU-a ograničeno na sigurnosne zone ili administrativne zone, može se uporabiti prijenos u nešifriranom obliku ili šifriranje na nižoj razini na temelju ishoda procesa upravljanja rizicima i ovisno o odobrenju SAA-a.

**Sigurno međusobno povezivanje CIS-a**

32. Za potrebe ove Odluke međusobno povezivanje znači izravno povezivanje dvaju ili više IT sustava u svrhu razmjene podataka i drugih informacijskih resursa (npr. komunikacije) u jednom ili više smjerova.

33. CIS sa svim međusobno povezanim IT sustavima postupa kao da su nepouzdani i provodi mjere zaštite radi kontrole razmjene klasificiranih podataka.

34. Za svako međusobno povezivanje CIS-a s drugim IT sustavom moraju se ispuniti sljedeći zahtjevi:

(a) poslovne ili operativne zahtjeve povezane s takvim međusobnim povezivanjem navode i odobravaju nadležna tijela;

(b) međusobno se povezivanje podvrgava procesu upravljanja rizicima i akreditacije i zahtijeva odobrenje nadležnog SAA-a; i

(c) na perimetru svakog CIS-a provode se usluge zaštite granice (BPS).

35. Nema međusobnog povezivanja između akreditiranog CIS-a i nezaštićene ili javne mreže, osim ako CIS ima odobreni BPS instaliran u tu svrhu između CIS-a i nezaštićene ili javne mreže. Sigurnosne mjere za takvo međusobno povezivanje pregledava nadležni IAA i odobrava nadležni SAA.

Ako se nezaštićena ili javna mreža rabi samo za prijenos i ako su podaci kodirani pomoću kriptografskog proizvoda odobrenog u skladu s člankom 10., takvo se povezivanje ne smatra međusobnim povezivanjem.

36. Zabranjeno je izravno ili kaskadno međusobno povezivanje CIS-a s akreditacijom za postupanje s podacima klasificiranim kao TRÈS SECRET UE/EU TOP SECRET s nezaštićenom ili javnom mrežom.

**Mediji za pohranu podataka**

37. Mediji za pohranu podataka uništavaju se u skladu s postupcima koje je odobrilo nadležno sigurnosno tijelo.

38. Računalni mediji za pohranu podataka ponovno se rabe, njihov se stupanj tajnosti smanjuje ili deklasificira u skladu sa sigurnosnim smjernicama koje se utvrđuju u skladu s člankom 6. stavkom 2.

**Izvanredne okolnosti**

39. Neovisno o odredbama ove Odluke, dolje opisani posebni postupci mogu se primjenjivati u izvanrednoj situaciji, na primjer, u vrijeme prijeteće ili stvarne krize, sukoba, rata ili u izvanrednim operativnim okolnostima.

40. Klasificirani podaci EU-a mogu se slati pomoću kriptografskih proizvoda odobrenih za niži stupanj tajnosti ili bez kodiranja uz suglasnost nadležnog tijela ako bi zbog bilo kakve odgode mogla nastati šteta koja je, jasno, veća od štete uzrokovane otkrivanjem klasificiranih podataka i ako:

(a) pošiljatelj i primatelj nemaju potrebnu opremu za kodiranje ili nemaju opremu za kodiranje; i

(b) klasificirani se materijal ne može prenijeti na vrijeme drugim sredstvima.

41. Klasificirani podaci preneseni u okolnostima navedenima u stavku 39. nemaju nikakve oznake ili pokazatelje prema kojima se razlikuju od podataka koji nisu klasificirani ili koji se mogu zaštiti raspoloživim kriptografskim proizvodom. Primatelja se bez odgode obavješćuje o stupnju tajnosti drugim sredstvima.

42. Ako se primjenjuje stavak 39., nadležnom se tijelu i Sigurnosnom odboru podnosi naknadno izvješće.

III. FUNKCIJE I NADLEŽNA TIJELA ZA INFORMACIJSKU SIGURNOST

43. U državama članicama i GSC-u utvrđuju se sljedeće funkcije IA-a. Navedene funkcije ne zahtijevaju pojedinačne organizacijske subjekte. One imaju odvojene mandate. Međutim, navedene funkcije te njihove pripadajuće odgovornosti mogu se kombinirati ili integrirati u isti organizacijski subjekt ili podijeliti na različite organizacijske subjekte uz uvjet da se spriječi pojava unutarnjih sukoba interesa.

**Information Assurance Authority (tijelo za informacijsku sigurnosti)**

44. IAA je odgovoran za:

(a) razvoj sigurnosnih politika i sigurnosnih smjernica za IA te praćenje njihove učinkovitosti i primjerenosti;

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

(c) osiguravanje da mjere IA-a odabrane za zaštitu klasificiranih podataka EU-a udovoljavaju mjerodavnim politikama kojima se uređuje njihova prihvatljivost i odabir;

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

(e) koordinaciju obuke i podizanja svijesti o IA-u;

(f) savjetovanje s pružateljem sustava, sigurnosnim činiocima i predstavnicima korisnika u pogledu sigurnosnih politika i sigurnosnih smjernica za IA; i

(g) osiguravanje da stručno potpodručje Sigurnosnog odbora za pitanja IA-a na raspolaganju ima odgovarajuće stručno znanje.

**TEMPEST Authority (tijelo TEMPEST-a)**

45. Tijelo TEMPEST-a (TA) odgovorno je za osiguravanje usklađenosti CIS-a s politikama i smjernicama za TEMPEST. Ono odobrava protumjere TEMPEST-a za instalacije i proizvode za zaštitu klasificiranih podataka EU-a do određenog stupnja tajnosti u njihovu operativnom okruženju.

**Crypto Approval Authority (tijelo za odobravanje kriptomaterijala)**

46. Tijelo za odobravanje kriptomaterijala (CAA) odgovorno je za osiguravanje usklađenosti kriptografskih proizvoda s nacionalnom kriptografskom politikom ili kriptografskom politikom Vijeća. Ono daje odobrenja za kriptografske proizvode za zaštitu klasificiranih podataka EU-a do određenog stupnja tajnosti u njihovu operativnom okruženju. U pogledu država članica CAA je dodatno odgovoran za ocjenjivanje kriptografskih proizvoda.

**Crypto Distribution Authority (tijelo za distribuciju kriptomaterijala)**

47. Tijelo za distribuciju kriptomaterijala (CDA) odgovorno je za:

(a) upravljanje kriptomaterijalom EU-a i vođenje evidencije o njemu;

(b) osiguravanje provedbe odgovarajućih postupaka i uspostavljanja kanala za vođenje evidencije o cjelokupnom kriptomaterijalu EU-a, sigurno postupanje s njime, njegovo čuvanje i distribuciju; i

(c) osiguravanje prijenosa kriptomaterijala EU-a pojedincima ili službama koje ih koriste ili od njih.

**Security Accreditation Authority (tijelo za sigurnosnu akreditaciju)**

48. Za svaki je sustav SAA odgovoran za:

(a) osiguravanje usklađenosti CIS-a s mjerodavnim sigurnosnim politikama i sigurnosnim smjernicama, davanje izjave o odobrenju za CIS za postupanje s klasificiranim podacima EU-a do određenog stupnja tajnosti u njihovu operativnom okruženju, navođenje odredaba i uvjeta akreditacije i kriterija prema kojima je potrebno ponovno odobrenje;

(b) utvrđivanje procesa akreditacije u skladu s mjerodavnim politikama i jasno navođenje uvjeta odobrenja za CIS pod njegovom nadležnošću;

(c) određivanje strategije za sigurnosnu akreditaciju u kojoj se navodi stupanj podrobnosti za proces akreditacije razmjeran potrebnoj razini sigurnosti;

(d) ispitivanje i odobravanje dokumentacije povezane sa sigurnošću, uključujući izjave o upravljanju rizicima i preostalom riziku, izjave o sigurnosnim zahtjevima za specifični sustav („SSRS-ovi”), dokumentaciju o provjeri provedbe sigurnosti i sigurnosno-operativne postupke (dalje u tekstu „SecOP-i”), i osiguravanje njegove usklađenosti sa sigurnosnim propisima i politikama Vijeća;

(e) provjeru provedbe sigurnosnih mjera povezanih s CIS-om kroz poduzimanje ili sponzoriranje sigurnosnih procjena, inspekcija ili pregleda;

(f) određivanje sigurnosnih zahtjeva (npr. razina sigurnosne provjere osoba) za osjetljive položaje povezane s CIS-om;

(g) poticanje odabira odobrenih kriptografskih i TEMPEST proizvoda koji se rabe za zaštitu CIS-a;

(h) odobravanje, ili prema potrebi, sudjelovanje u zajedničkom odobravanju međusobnog povezivanja CIS-a s drugim CIS-om; i

(i) savjetovanje s pružateljem sustava, sigurnosnim činiocima i predstavnicima korisnika u pogledu upravljanja sigurnosnim rizicima, a posebno preostalim rizikom, te odredbama i uvjetima izjave o odobrenju.

49. SAA GSC-a odgovoran je za akreditaciju svih CIS-ova koji rade u nadležnosti GSC-a.

50. Nadležni SAA države članice odgovoran je za akreditaciju CIS-a i njegovih sastavnih dijelova koji rade u nadležnosti države članice.

51. Zajednički odbor za sigurnosnu akreditaciju (SAB) odgovoran je za akreditaciju CIS-a u nadležnosti tijela za sigurnosnu akreditaciju GSC-a i tijela za sigurnosnu akreditaciju država članica. Sastavljen je od predstavnika SAA-a iz svake države članice, a u njegovu radu sudjeluje predstavnik tijela za sigurnosnu akreditaciju Komisije. Drugi subjekti s čvorovima na CIS-u pozivaju se na sudjelovanje kada se raspravlja o navedenom sustavu.

SAB-om predsjeda predstavnik tijela za sigurnosnu akreditaciju GSC-a. SAB donosi odluke konsenzusom predstavnika SAA-a u institucijama, država članicama i drugim subjektima s čvorovima na CIS-u. O svojim aktivnostima periodično izvješćuje Sigurnosni odbor i obavješćuje ga o svim izjavama o akreditaciji.

**Operativno tijelo za informacijsku sigurnost**

52. Za svaki sustav operativno tijelo za IA odgovorno je za:

(a) izradu sigurnosne dokumentacije u skladu sa sigurnosnim politikama i sigurnosnim smjernicama, a posebno SSRS uključujući izjavu o preostalom riziku, SecOP-e i plan kriptomaterijala u okviru procesa akreditacije CIS-a;

(b) sudjelovanje u odabiru i ispitivanju tehničkih sigurnosnih mjera za specifični sustav, uređaja i softvera radi nadzora njihove provedbe i osiguravanja njihove sigurne instalacije, konfiguracije i održavanja u skladu s odgovarajućom sigurnosnom dokumentacijom;

(c) sudjelovanje u odabiru sigurnosnih TEMPEST mjera i uređaja ako se zahtijeva u SSRS-u i osiguravanje njihove sigurne instalacije i održavanja u suradnji s TA-om;

(d) praćenje provedbe i primjene SecOP-a i, prema potrebi, delegiranje sigurnosno-operativnih odgovornosti na vlasnika sustava;

(e) upravljanje i postupanje s kriptografskim proizvodima, osiguravanje čuvanja kriptomaterijala i kontroliranih predmeta te, prema potrebi, osiguravanje stvaranja kriptografskih varijabli;

(f) pregledavanje i ispitivanje sigurnosnih analiza, a posebno za izradu odgovarajućih izvješća o rizicima u skladu sa zahtjevima SAA-a;

(g) osiguravanje obuke o IA-u za specifični CIS; i

(h) provedbu i upravljanje sigurnosnim mjerama za specifični CIS.

*PRILOG V.*

## GOSPODARSKA SIGURNOST

I. UVOD

1. U ovom se Prilogu određuju odredbe za provedbu članka 11. U njemu se utvrđuju opće sigurnosne odredbe koje se primjenjuju na gospodarske ili druge subjekte u pregovorima prije sklapanja ugovora i tijekom životnog ciklusa ugovora koje sklopi GSC.

2. Vijeće odobrava smjernice o gospodarskoj sigurnosti u kojima se posebno podrobno opisuju zahtjevi povezani s FSC-ovima, pismima o sigurnosnim aspektima (SAL-ovi), posjetima, slanju i prijenosu klasificiranih podataka EU-a.

II. SIGURNOSNI ELEMENTI U KLASIFICIRANOM UGOVORU

**Vodič za stupnjeve tajnosti (SCG)**

3. Prije pokretanja natječaja ili sklapanja ugovora, GSC kao tijelo za ugovaranje određuje stupanj tajnosti svakog podataka koji će se dati ponuditeljima i ugovarateljima, kao i stupanj tajnosti svakog podatka koji će stvoriti ugovaratelj. U tu svrhu GSC priprema SCG koji će se koristiti za izvršenje ugovora.

4. Za određivanje stupnja tajnosti različitih elemenata klasificiranog ugovora primjenjuju se sljedeća načela:

(a) prilikom pripreme SCG-a GSC uzima u obzir sve važne sigurnosne aspekte, uključujući stupanj tajnosti dodijeljen podacima koje je onaj od kojeg podaci potječu dostavio i odobrio za uporabu u ugovoru;

(b) ukupni stupanj tajnosti ugovora ne može biti manji od najvećeg stupnja tajnosti bilo kojeg od njegovih elemenata; i

(c) gdje je to bitno, GSC se povezuje s NSA-om/DSA-om države članice ili bilo kojim drugim predmetnim nadležnim sigurnosnim tijelom u slučaju svake promjene koja se odnosi na klasifikaciju podataka koje je stvorio ugovaratelj ili koji su dostavljeni ugovaratelju tijekom izvršenja ugovora i prilikom naknadnih promjena SCG-a.

**Pismo o sigurnosnim aspektima (SAL)**

5. U SAL-u su opisani sigurnosni zahtjevi specifični za ugovor. Prema potrebi, SAL sadrži SCG i čini sastavni dio klasificiranog ugovora ili podugovora.

6. SAL sadrži odredbe kojima se od ugovaratelja i/ili podugovaratelja zahtijeva poštovanje minimalnih standarda utvrđenih ovom Odlukom. Nepoštovanje minimalnih standarda može biti dovoljan razlog za prekid ugovora.

**Sigurnosni naputci za program/projekt (PSI)**

7. Ovisno o opsegu programa ili projekata koji uključuju pristup klasificiranim podacima EU-a, postupanje s njima ili njihovo čuvanje, tijelo za ugovaranje određeno za upravljanje programom ili projektom može pripremiti poseban PSI. PSI zahtijeva odobrenje NSA-ova/DSA-ova države članice ili drugog nadležnog sigurnosnog tijela koje sudjeluje u PSI-ju i može sadržavati dodatne sigurnosne zahtjeve.

III. UVJERENJE O SIGURNOSNOJ PROVJERI PRAVNE OSOBE (FSC)

8. FSC odobrava NSA ili DSA ili bilo koje drugo nadležno sigurnosno tijelo države članice kako bi naznačio da, u skladu s nacionalnim zakonima i propisima, gospodarski ili drugi subjekt može zaštititi klasificirane podatke EU-a s odgovarajućim stupnjem tajnosti (CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET) unutar svojih objekata. Predočuje se GSC-u, kao tijelu za ugovaranje, prije nego što se ugovaratelju ili podugovaratelju ili mogućem ugovaratelju ili podugovaratelju dostave klasificirani podaci EU-a ili mu se odobri pristup njima.

9. Prilikom izdavanja FSC-a nadležni NSA ili DSA kao minimum:

(a) ocjenjuje integritet gospodarskog ili drugog subjekta;

(b) ocjenjuje vlasništvo, kontrolu ili mogući nedopušteni utjecaj koji se može smatrati sigurnosnim rizikom;

(c) provjerava je li gospodarski ili bilo koji drugi subjekt uspostavio sigurnosni sustav u objektu kojim su obuhvaćene sve odgovarajuće sigurnosne mjere potrebne za zaštitu podataka ili materijala klasificiranih kao CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET u skladu sa zahtjevima utvrđenima ovom Odlukom;

(d) provjerava je li utvrđen sigurnosni status rukovodstva, vlasnika i zaposlenika kojima je potreban pristup podacima klasificiranim kao CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET u skladu sa zahtjevima utvrđenim ovom Odlukom; i

(e) provjerava je li gospodarski ili bilo koji drugi subjekt imenovao službenika za sigurnost koji odgovara rukovodstvu za provedbu sigurnosnih obveza unutar takvog subjekta.

10. Gdje je to važno, GSC, kao tijelo za ugovaranje, obavješćuje odgovarajući NSA/DSA ili drugo nadležno sigurnosno tijelo o tome da je potreban FSC u fazi prije sklapanja ugovora ili za izvršenje ugovora. FSC ili PSC je potreban u fazi prije sklapanja ugovora ako se klasificirani podaci EU-a sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET moraju dostaviti tijekom procesa nadmetanja.

11. Tijelo za ugovaranje ne sklapa klasificirani ugovor s najboljim ponuditeljem prije nego što primi potvrdu od NSA-a/DSA-a ili drugog nadležnog sigurnosnog tijela države članice u kojoj je predmetni ugovaratelj ili podugovaratelj registriran da je, prema potrebi, izdan odgovarajući FSC.

12. NSA/DSA ili drugo nadležno sigurnosno tijelo koje je izdalo FSC obavješćuje GSC kao tijelo za ugovaranje o promjenama koje utječu na FSC. Za podugovor se na odgovarajući način obavješćuje NSA/DSA ili bilo koje drugo nadležno sigurnosno tijelo.

13. Ako nadležni NSA/DSA ili drugo nadležno sigurnosno tijelo ukine FSC, GSC kao tijelo za ugovaranje ima dovoljan razlog za raskid klasificiranog ugovora ili isključivanje ponuditelja iz nadmetanja.

IV. KLASIFICIRANI UGOVORI I PODUGOVORI

14. Ako se klasificirani podaci EU-a dostave ponuditelju u fazi prije sklapanja ugovora, poziv za podnošenje ponude mora sadržavati odredbu kojom se ponuditelja koji ne dostavi ponudu ili ne bude izabran obvezuje na vraćanje svih klasificiranih dokumenata unutar određenog vremenskog razdoblja.

15. Nakon sklapanja klasificiranog ugovora ili podugovora, GSC, kao tijelo za ugovaranje, obavješćuje NSA/DSA ili drugo nadležno sigurnosno tijelo ugovaratelja ili podugovaratelja o sigurnosnim odredbama klasificiranog ugovora.

16. Kada se takvi ugovori raskidaju, GSC, kao tijelo za ugovaranje (i/ili NSA/DSA ili bilo koje drugo nadležno sigurnosno tijelo, prema potrebi, za podugovor), odmah obavješćuje NSA/DSA ili drugo nadležno sigurnosno tijelo države članice u kojoj je registriran ugovaratelj ili podugovaratelj.

17. U pravilu se od ugovaratelja ili podugovaratelja zahtijeva da po raskidu klasificiranog ugovora ili podugovora tijelu za ugovaranje vrati sve klasificirane podatke EU-a u svojem posjedu.

18. Posebne odredbe za raspolaganje klasificiranim podacima EU-a tijekom izvršenja ugovora ili nakon njegova prestanka utvrđuju se u SAL-u.

19. Ako je ugovaratelj ili podugovaratelj ovlašten za zadržavanje klasificiranih podataka EU-a po prestanku ugovora, ugovaratelj ili podugovaratelj dužan je i dalje poštovati minimalne standarde sadržane u ovoj Odluci te štititi tajnost klasificiranih podataka EU-a.

20. Uvjeti uz koje ugovaratelj može sklopiti podugovor određuju se u pozivu za podnošenje ponude i ugovoru.

21. Ugovaratelj je dužan od GSC-a, kao tijela za ugovaranje, pribaviti dopuštenje prije podugovaranja dijela klasificiranog ugovora. Ne može se sklopiti podugovor s gospodarskim ili drugim subjektima registriranima u državi koja nije članica EU-a i koja nije sklopila sporazum o sigurnosti podataka s Unijom.

22. Ugovaratelj je odgovoran i osigurava da su sve aktivnosti podugovaranja poduzete u skladu s minimalnim standardima utvrđenim ovom Odlukom i ne smije dostavljati klasificirane podatke EU-a podugovaratelju bez prethodne pisane suglasnosti tijela za ugovaranje.

23. Što se tiče klasificiranih podataka EU-a koje je stvorio ili s kojima postupa ugovaratelj ili podugovaratelj, tijelo za ugovaranje ostvaruje prava koja pripadaju onom od kojeg podaci potječu.

V. POSJETI POVEZANI S KLASIFICIRANIM UGOVORIMA

24. Ako GSC, osoblje ugovaratelja ili podugovaratelja trebaju pristup podacima klasificiranima kao CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET u prostorijama jednih ili drugih za izvršenje klasificiranog ugovora, posjeti se organiziraju u dogovoru s predmetnim NSA-om/DSA-om ili drugim nadležnim sigurnosnim tijelom. Međutim, u kontekstu posebnih projekata, NSA/DSA može također dogovoriti postupak za izravnu organizaciju takvog posjeta.

25. Svi posjetitelji moraju imati odgovarajući PSC te nužnost pristupa podacima za pristup klasificiranim podacima EU-a povezanim s ugovorom s GSC-om.

26. Posjetiteljima se omogućava pristup samo klasificiranim podacima EU-a koji se odnose na svrhu njihova posjeta.

VI. SLANJE I PRIJENOS KLASIFICIRANIH PODATAKA EU-a

27. Što se tiče slanja klasificiranih podataka EU-a elektroničkim sredstvima, primjenjuju se odgovarajuće odredbe članka 10. i Priloga IV.

28. Što se tiče prijenosa klasificiranih podataka EU-a, primjenjuju se odgovarajuće odredbe Priloga III. u skladu s nacionalnim zakonima i propisima.

29. Za prijevoz klasificiranih podataka kao tereta primjenjuju se sljedeća načela prilikom određivanja sigurnosnih mjera:

(a) sigurnost se osigurava u svim fazama prijevoza od mjesta podrijetla do konačnog odredišta;

(b) stupanj zaštite dodijeljen pošiljci određuje se na temelju najvišeg stupnja tajnosti materijala sadržanog u pošiljci;

(c) poduzetnici koji obavljaju prijevoz moraju pribaviti FSC za odgovarajuću razinu. U takvim slučajevima osoblje koje postupa s pošiljkom mora proći sigurnosnu provjeru u skladu s Prilogom I.;

(d) prije prekograničnog kretanja materijala klasificiranog kao CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET pošiljatelj sastavlja plan prijevoza koji odobrava predmetni NSA/DSA ili bilo koje drugo nadležno sigurnosno tijelo;

(e) putovanja moraju biti od točke do točke u mjeri u kojoj je to moguće te moraju završiti što je prije moguće s obzirom na okolnosti; i

(f) kadgod je to moguće, pravci bi trebali prolaziti samo kroz države članice. Pravci bi trebali prolaziti kroz države koje nisu države članice samo ako ih je odobrio NSA/DSA ili bilo koje drugo nadležno sigurnosno tijelo država pošiljatelja i primatelja.

VII. PRIJENOS KLASIFICIRANIH PODATAKA EU-a UGOVARATELJIMA SMJEŠTENIM U TREĆIM DRŽAVAMA

30. Klasificirani se podaci EU-a prenose ugovarateljima i podugovarateljima smještenima u trećim državama u skladu sa sigurnosnim mjerama dogovorenima između GSC-a, kao tijela za ugovaranje, i NSA-a/DSA-a predmetne treće države u kojoj je ugovaratelj registriran.

VIII. PODACI KLASIFICIRANI KAO RESTREINT UE/EU RESTRICTED

31. GSC, kao tijelo za ugovaranje, prema potrebi ima pravo, u suradnji s NSA-om/DSA-om države članice, provoditi inspekcije objekata ugovaratelja/podugovaratelja na temelju ugovornih odredaba kako bi provjerio jesu li uspostavljene odgovarajuće sigurnosne mjere za zaštitu klasificiranih podataka EU-a sa stupnjem tajnosti RESTREINT UE/EU RESTRICTED u skladu sa zahtjevima iz ugovora.

32. U mjeri u kojoj je to potrebno prema nacionalnim zakonima i propisima, GSC, kao tijelo za ugovaranje, obavješćuje NSA-ovi/DSA-ovi ili bilo koje drugo nadležno sigurnosno tijelo o ugovorima ili podugovorima koji sadrže podatke klasificirane kao RESTREINT UE/EU RESTRICTED.

33. FSC ili PSC za ugovaratelje ili podugovaratelje i njihovo osoblje nije potreban za ugovore sklopljene s GSC-om koji sadrže podatke klasificirane kao RESTREINT UE/EU RESTRICTED.

34. GSC, kao tijelo za ugovaranje, ispituje odgovore na poziv za sudjelovanje u natječaju za ugovore koji zahtijevaju pristup podacima klasificiranima kao RESTREINT UE/EU RESTRICTED, neovisno o bilo kojem zahtjevu povezanom s FSC-om ili PSC-om prema nacionalnim zakonima i propisima.

35. Uvjeti pod kojima ugovaratelj može sklopiti podugovor moraju biti u skladu sa stavkom 21.

36. Ako ugovor uključuje postupanje s podacima klasificiranima kao RESTREINT UE/EU RESTRICTED u CIS-u kojim upravlja ugovaratelj, GSC, kao tijelo za ugovaranje, osigurava da su u ugovoru ili svakom podugovoru navedeni nužni tehnički i upravni zahtjevi u pogledu akreditacije CIS-a razmjerni procijenjenom riziku, uzimajući u obzir sve važne čimbenike. Tijelo za ugovaranje i nadležni NSA/DSA dogovaraju područje primjene akreditacije takvog CIS-a.

*PRILOG VI.*

**RAZMJENA KLASIFICIRANIH PODATAKA S TREĆIM DRŽAVAMA I MEĐUNARODNIM ORGANIZACIJAMA**

I. UVOD

1. U ovom se Prilogu određuju odredbe za provedbu članka 13.

II. OKVIRI KOJIMA SE UREĐUJE RAZMJENA KLASIFICIRANIH PODATAKA

2. Ako Vijeće utvrdi postojanje dugoročne potrebe za razmjenom klasificiranih podataka,

— sklapa se sporazum o sigurnosti podataka, ili

— se sklapa administrativni dogovor,

u skladu s člankom 13. stavkom 2. i odjeljcima III. i IV. te na temelju preporuke Sigurnosnog odbora.

3. Ako se klasificirani podaci EU-a izrađeni za potrebe operacije ZSOP-a dostavljaju trećim državama ili međunarodnim organizacijama koje sudjeluju u takvoj operaciji i ako ne postoji ni jedan od okvira iz stavka 2., u skladu s odjeljkom V. razmjena klasificiranih podataka EU-a s trećom zemljom ili međunarodnom organizacijom koja sudjeluje u operaciji uređuje se:

— okvirnim sporazumom o sudjelovanju,

— *ad hoc* sporazumom o sudjelovanju, ili

— u nedostatku gore navedenog, *ad hoc* administrativnim dogovorom.

4. U nedostatku okvira iz stavaka 2. i 3. i ako je donesena odluka o objavi klasificiranih podataka EU-a trećoj državi ili međunarodnoj organizaciji iznimno i *ad hoc* u skladu s odjeljkom VI., od predmetne se treće države ili međunarodne organizacije traže pisana jamstva kojima se osigurava zaštita svih klasificiranih podataka EU-a objavljenih trećoj državi ili međunarodnoj organizaciji u skladu s osnovnim načelima i minimalnim standardima navedenim u ovoj Odluci.

III. SPORAZUMI O SIGURNOSTI PODATAKA

5. Sporazumima o sigurnosti podataka utvrđuju se osnovna načela i minimalni standardi kojima se uređuje razmjena klasificiranih podataka između Unije i treće države ili međunarodne organizacije.

6. Sporazumima o sigurnosti podataka predviđena je tehnička organizacija provedbe koju dogovaraju nadležna sigurnosna tijela mjerodavnih institucija i tijela Unije i nadležno sigurnosno tijelo predmetne treće države ili međunarodne organizacije. Pri takvoj se organizaciji uzima u obzir razina zaštite predviđena sigurnosnim propisima, strukturama i postupcima uspostavljenim u predmetnoj trećoj državi ili međunarodnoj organizaciji. Organizaciju provedbe odobrava Sigurnosni odbor.

7. Na temelju sporazuma o sigurnosti podataka, nijedan se klasificirani podatak EU-a ne smije razmjenjivati elektroničkim sredstvima, osim ako je to izričito predviđeno sporazumom ili odgovarajućom tehničkom organizacijom provedbe.

8. Kada Vijeće sklopi sporazum o sigurnosti podataka, kod svake se stranke određuje registar kao glavna točka ulaska i izlaska za razmjenu klasificiranih podataka.

9. Kako bi se ocijenila učinkovitost sigurnosnih propisa, struktura i postupaka u predmetnoj trećoj državi ili međunarodnoj organizaciji, provode se posjeti radi procjene stanja u međusobnom dogovoru s predmetnom državom članicom ili međunarodnom organizacijom. Takvi posjeti radi procjene stanja provode se u skladu s odgovarajućim odredbama Priloga III. i tijekom njih se ocjenjuju:

(a) mjerodavni regulatorni okvir za zaštitu klasificiranih podataka;

(b) sva posebna obilježja sigurnosne politike i način na koji je sigurnost organizirana u trećoj državi ili međunarodnoj organizaciji koja mogu utjecati na stupanj tajnosti klasificiranih podataka koji se mogu razmjenjivati;

(c) stvarno uspostavljene sigurnosne mjere i postupci; i

(d) postupci za sigurnosnu provjeru za stupanj tajnosti klasificiranih podataka EU-a koji se objavljuju.

10. Tim koji provodi posjet za procjenu stanja u ime Unije procjenjuje jesu li sigurnosni propisi i postupci u predmetnoj trećoj državi ili međunarodnoj organizaciji primjereni za zaštitu klasificiranih podataka EU-a s određenim stupnjem tajnosti.

11. Nalazi takvih posjeta navode se u izvješću na temelju kojeg Sigurnosni odbor određuje najviši stupanj tajnosti klasificiranih podataka EU-a koji se mogu razmjenjivati u papirnatom obliku, a prema potrebi u elektroničkom, s predmetnom trećom strankom, kao i sve posebne uvjete kojima se uređuje razmjena s navedenom strankom.

12. Mora se učiniti sve kako bi se organizirao posjet predmetnoj trećoj državi ili međunarodnoj organizaciji za potpunu procjenu sigurnosti prije no što Sigurnosni odbor odobri organizaciju provedbe, kako bi se utvrdila priroda i učinkovitost uspostavljenog sigurnosnog sustava. Međutim, ako to nije moguće, Sigurnosni odbor prima što potpunije izvješće od Ureda za sigurnost GSC-a na temelju raspoloživih podataka, kojim se Sigurnosni odbor obavješćuje o primjenljivim sigurnosnim propisima i načinu na koji je sigurnost organizirana u predmetnoj trećoj državi ili međunarodnoj organizaciji.

13. Prije stvarne objave klasificiranih podataka EU-a predmetnoj trećoj državi ili međunarodnoj organizaciji, Sigurnosnom odboru prosljeđuje se izvješće o posjetu radi procjene stanja ili, u slučaju da takvo izvješće ne postoji, izvješće iz stavka 12., za koje on mora utvrditi da je zadovoljavajuće.

14. Nadležna sigurnosna tijela institucija i tijela Unije priopćuju trećoj državi ili međunarodnoj organizaciji datum od kojeg, na temelju sporazuma, Unija može objaviti klasificirane podatke EU-a, te najviši stupanj tajnosti klasificiranih podataka EU-a koji se mogu razmjenjivati u papirnatom obliku ili elektroničkim sredstvima.

15. Popratni posjeti radi procjene stanja poduzimaju se prema potrebi, a posebno ako:

(a) treba povisiti stupanj tajnosti za klasificirane podatke EU-a koji se mogu objaviti;

(b) je Unija obaviještena da je došlo do bitnih izmjena u sigurnosnim mjerama treće države ili međunarodne organizacije koje bi mogle utjecati na način na koji ona štiti klasificirane podatke EU-a; ili

(c) je došlo do ozbiljnog incidenta koji je uključivao neovlašteno otkrivanje klasificiranih podatka EU-a.

16. Nakon stupanja sporazuma o sigurnosti podataka na snagu i nakon razmjene podataka s predmetnom trećom državom ili međunarodnom organizacijom, Sigurnosni odbor može odlučiti promijeniti najviši stupanj tajnosti klasificiranih podataka EU-a koji se mogu razmjenjivati u papirnatom obliku ili elektroničkim sredstvima, a posebno s obzirom na bilo koji prateći posjet za procjenu stanja.

IV. ADMINISTRATIVNI DOGOVORI

17. Ako postoji dugoročna potreba za razmjenom podataka čiji stupanj tajnosti u pravilu nije viši od RESTREINT UE/EU RESTRICTED s trećom državom ili međunarodnom organizacijom i ako je Sigurnosni odbor utvrdio da predmetna stranka nema dovoljno razvijen sigurnosni sustav za sklapanje sporazuma o sigurnosti podataka, glavni tajnik može, uz uvjet da Vijeće to odobri, u ime GSC-a sklopiti administrativni dogovor s nadležnim tijelima predmetne treće države ili međunarodne organizacije.

18. Ako je zbog hitnih operativnih razloga potrebno brzo uspostaviti okvir za razmjenu klasificiranih podataka, Vijeće iznimno može odlučiti o sklapanju administrativnog dogovora za razmjenu podataka višeg stupnja tajnosti.

19. Administrativni dogovor u pravilu ima oblik razmjene pisama.

20. Prije stvarne objave klasificiranih podataka EU-a u predmetnoj trećoj državi ili međunarodnoj organizaciji provodi se posjet radi procjene stanja iz stavka 9., a Sigurnosnom odboru prosljeđuje se izvješće ili, u slučaju da takvo izvješće ne postoji, izvješće iz stavka 12., za koje on mora utvrditi da je zadovoljavajuće.

21. Nijedan klasificirani podatak EU-a ne smije se na temelju administrativnog dogovora razmjenjivati elektronskim putem, osim ako je tako izričito navedeno u dogovoru.

V. RAZMJENA KLASIFICIRANIH PODATAKA U OKVIRU OPERACIJA ZSOP-a

22. Okvirnim sporazumima o sudjelovanju uređuje se sudjelovanje trećih zemalja ili međunarodnih organizacija u operacijama ZSOP-a. Takvi sporazumi uključuju odredbe o objavi klasificiranih podataka EU-a izrađenih za potrebe operacija ZSOP-a trećim državama ili međunarodnim organizacijama koje u njima sudjeluju. Najviši stupanj tajnosti klasificiranih podataka EU-a koji se mogu razmjenjivati je RESTREINT UE/EU RESTRICTED za civilne operacije ZSOP-a i CONFIDENTIEL UE/EU CONFIDENTIAL za vojne operacije ZSOP-a, osim ako je drukčije utvrđeno odlukom kojom se određuje svaka operacija ZSOP-a.

23. *Ad hoc* sporazumi o sudjelovanju sklopljeni za određenu operaciju ZSOP-a obuhvaćaju odredbe o objavi klasificiranih podataka EU-a izrađenih za potrebe navedene operacije trećoj državi ili međunarodnoj organizaciji koja u njoj sudjeluje. Najviši stupanj tajnosti klasificiranih podataka EU-a koji se mogu razmjenjivati je RESTREINT UE/EU RESTRICTED za civilne operacije ZSOP-a i CONFIDENTIEL UE/EU CONFIDENTIAL za vojne operacije ZSOP-a, osim ako je drukčije utvrđeno odlukom kojom se određuje svaka operacija ZSOP-a.

24. Ako ne postoji sporazum o sigurnosti podataka i prije sklapanja sporazuma o sudjelovanju, objava klasificiranih podataka EU-a izrađenih za potrebe operacije trećoj državi ili međunarodnoj organizaciji koja sudjeluje u operaciji uređuje se administrativnim dogovorom koji sklapa visoki predstavnik ili podložno odluci o *ad hoc* objavi u skladu s odjeljkom VI. Klasificirani podaci EU-a razmjenjuju se u okviru takvog sporazuma samo u predviđenom razdoblju sudjelovanja treće države ili međunarodne organizacije. Najviši stupanj tajnosti klasificiranih podataka EU-a koji se mogu razmjenjivati je RESTREINT UE/EU RESTRICTED za civilne operacije ZSOP-a i CONFIDENTIEL UE/EU CONFIDENTIAL za vojne operacije ZSOP-a, osim ako je drukčije utvrđeno odlukom kojom se određuje svaka operacija ZSOP-a.

25. Odredbama o klasificiranim podacima koje će se uključiti u okvirne sporazume o sudjelovanju, *ad hoc* sporazume o sudjelovanju i *ad hoc* administrativne dogovore iz stavaka od 22. do 24. predviđeno je da predmetna treća država ili međunarodna organizacija osigurava da će njezino osoblje upućeno bilo kojoj operaciji štititi klasificirane podatke EU-a u skladu sa sigurnosnim propisima Vijeća i daljnjim smjernicama koje izdaju nadležna tijela, uključujući zapovjedni lanac operacije.

26. Ako Unija i sudjelujuća treća država ili međunarodna organizacija naknadno sklope sporazum o sigurnosti podataka, sporazum o sigurnosti podataka zamjenjuje odredbe o razmjeni klasificiranih podataka utvrđene u svakom okvirnom sporazumu o sudjelovanju, *ad hoc* sporazumu o sudjelovanju ili *ad hoc* administrativnom dogovoru u pogledu razmjene klasificiranih podataka EU-a i postupanja s njima.

27. Na temelju okvirnog sporazuma o sudjelovanju, *ad hoc* sporazuma o sudjelovanju ili *ad hoc* administrativnog dogovora nije dopuštena razmjena klasificiranih podataka EU-a elektroničkim sredstvima s trećom državom ili međunarodnom organizacijom, osim ako je izričito navedeno u predmetnom sporazumu ili dogovoru.

28. Klasificirani podaci EU-a izrađeni za potrebe operacije ZSOP-a mogu se otkriti osoblju koje su treće države ili međunarodne organizacije uputile toj operaciji u skladu sa stavcima od 22. do 27. Kada se takvo osoblje ovlašćuje za pristup klasificiranim podacima EU-a u prostorijama ili CIS-u operacije ZSOP-a, primjenjuju se mjere (uključujući vođenje evidencije o otkrivenim klasificiranim podacima EU-a) za ublažavanje rizika od gubitka ili ugroze. Takve su mjere određene u odgovarajućim dokumentima o planiranju ili misijama.

29. Ako ne postoji sporazum o sigurnosti podataka, u slučaju posebne ili neodgodive operativne potrebe, objava klasificiranih podataka EU-a državi domaćinu na čijem se državnom području provodi operacija ZSOP-a može se urediti administrativnim dogovorom koji sklapa visoki predstavnik. Navedena je mogućnost predviđena odlukom kojom se utvrđuje operacija ZSOP-a. Klasificirani podaci EU-a objavljeni u takvim okolnostima ograničeni su na podatke izrađene za potrebe operacije ZSOP-a i imaju stupanj tajnosti ne viši od RESTREINT UE/EU RESTRICTED, osim ako je u odluci kojom se utvrđuje operacija ZSOP-a utvrđen viši stupanj tajnosti. U okviru takvog administrativnog dogovora država domaćin obvezuje se zaštititi klasificirane podatke EU-a u skladu s minimalnim standardima koji nisu ništa manje strogi od standarda utvrđenih ovom Odlukom.

30. Ako ne postoji sporazum o sigurnosti podataka, objava klasificiranih podataka EU-a relevantnim trećim državama ili međunarodnim organizacijama koje ne sudjeluju u operaciji ZSOP-a može se urediti administrativnim dogovorom koji sklapa visoki predstavnik.. Prema potrebi, navedena mogućnost i pripadajući uvjeti predviđeni su odlukom kojom se utvrđuje operacija ZSOP-a. Klasificirani podaci EU-a objavljeni u takvim okolnostima ograničeni su na podatke izrađene za potrebe operacije ZSOP-a i imaju stupanj tajnosti ne viši od RESTREINT UE/EU RESTRICTED osim ako je u odluci kojom se utvrđuje operacija ZSOP-a utvrđen viši stupanj tajnosti. U okviru takvog administrativnog dogovora predmetna treća država ili međunarodna organizacija obvezuju se zaštititi klasificirane podatke EU-a u skladu s minimalnim standardima koji nisu ništa manje strogi od standarda utvrđenih ovom Odlukom.

31. Prije provedbe odredaba o objavi klasificiranih podataka EU-a u smislu stavaka 22., 23. i 24. nije potrebna organizacija provedbe ili posjet za procjenu stanja.

VI. IZNIMNO *AD HOC* OBJAVLJIVANJE KLASIFICIRANIH PODATAKA EU-a

32. Ako nije uspostavljen okvir u skladu s odjeljcima od III. do V. i ako Vijeće ili jedno od njegovih pripremnih tijela utvrdi iznimnu potrebu za objavljivanjem klasificiranih podataka EU-a trećoj državi ili međunarodnoj organizaciji, GSC:

(a) provjerava, u mjeri u kojoj je to moguće, pri sigurnosnim tijelima predmetne treće države ili međunarodne organizacije jesu li njezini sigurnosni propisi, strukture i postupci takvi da će objavljeni klasificirani podaci EU-a biti zaštićeni u skladu sa standardima koji nisu ništa manje strogi od standarda utvrđenih ovom Odlukom; i

(b) poziva Sigurnosni odbor da na temelju raspoloživih podataka izda preporuku u pogledu povjerenja u sigurnosne propise, strukture i postupke u trećoj državi ili međunarodnoj organizaciji kojoj se objavljuju klasificirani podaci EU-a;

33. Ako Sigurnosni odbor izda preporuku u korist objavljivanja klasificiranih podataka EU-a, pitanje se upućuje Odboru stalnih predstavnika (Coreperu) koji donosi odluku o objavi.

34. Ako preporuka Sigurnosnog odbora nije u korist objavljivanja klasificiranih podataka EU-a:

(a) za pitanja povezana sa ZVSP-om/ZSOP-om, Politički i sigurnosni odbor raspravlja o pitanju i sastavlja preporuku za odluku Corepera;

(b) za sva ostala pitanja, Coreper raspravlja o pitanju i donosi odluku.

35. Ako se smatra primjerenim i uz uvjet da vlasnik podataka da prethodnu pisanu suglasnost, Coreper može odlučiti da se klasificirani podaci mogu objaviti samo djelomično ili samo ako se prije toga smanji njihov stupanj tajnosti ili ako se deklasificiraju ili ako se podaci za objavu pripreme bez upućivanja na izvor ili izvorni stupanj tajnosti EU-a.

36. Nakon odluke o objavljivanju klasificiranih podataka EU-a, GSC prosljeđuje predmetni dokument s oznakom mogućnosti objavljivanja na kojoj je navedena treća država ili međunarodna organizacija kojoj je dokument objavljen. Prije ili nakon stvarnog objavljivanja predmetna treća stranka obvezuje se u pisanom obliku da će štititi primljene klasificirane podatke EU-a u skladu s osnovnim načelima i minimalnim standardima navedenima u ovoj Odluci.

VII. OVLAŠTENJE ZA OBJAVLJIVANJE KLASIFICIRANIH PODATAKA EU-a TREĆIM DRŽAVAMA ILI MEĐUNARODNIM ORGANIZACIJAMA

37. Ako postoji okvir u skladu sa stavkom 2. za razmjenu klasificiranih podataka s trećom državom ili međunarodnom organizacijom, Vijeće donosi odluku kojom ovlašćuje glavnog tajnika za objavljivanje klasificiranih podataka EU-a, u skladu s načelom suglasnosti onoga od kojeg podaci potječu, predmetnoj trećoj državi ili međunarodnoj organizaciji. Glavni tajnik može delegirati takva ovlaštenja na više dužnosnike GSC-a.

38. Ako postoji sporazum o sigurnosti podataka u skladu sa stavkom 2. prvom alinejom, Vijeće može donijeti odluku kojom ovlašćuje visokog predstavnika za objavljivanje klasificiranih podataka EU-a u području zajedničke vanjske i sigurnosne politike koji potječu od Vijeća, nakon dobivene suglasnosti onog od kojeg potječu bilo kakvi izvorni materijali tamo sadržani, predmetnoj trećoj državi ili međunarodnoj organizaciji. Visoki predstavnik može delegirati takva ovlaštenja na više dužnosnike EEAS-a ili na PPEU-e.

39. Ako postoji okvir u skladu sa stavkom 2. ili sa stavkom 3. za razmjenu klasificiranih podataka s trećom državom ili međunarodnom organizacijom, Visoki se predstavnik ovlašćuje za objavljivanje klasificiranih podataka EU-a, u skladu s Odlukom kojom se utvrđuje operacija ZSOP-a i načelom suglasnosti onog od kojeg podaci potječu. Visoki predstavnik može delegirati takva ovlaštenja na više dužnosnike EEAS-a, zapovjednike operacija, snaga ili misija EU-a- ili na voditelje misija EU-a.

*Dodaci*

*Dodatak A*

Definicije

*Dodatak B*

Ekvivalentnost stupnjeva tajnosti

*Dodatak C*

Popis nacionalnih sigurnosnih tijela (NSA)

*Dodatak D*

Popis kratica

*Dodatak A*

DEFINICIJE

Za potrebe ove Odluke primjenjuju se sljedeće definicije:

„akreditacija” znači proces koji rezultira službenom izjavom tijela za sigurnosnu akreditaciju (SAA-a) o odobrenju sustava za rad s određenim stupnjem tajnosti, u posebno sigurnom načinu rada u svojem radnom okruženju i uz prihvatljiv stupanj rizika, uz pretpostavku da je proveden odobreni skup tehničkih, fizičkih, organizacijskih i postupovnih sigurnosnih mjera;

„sredstvo” znači sve što je od vrijednosti organizaciji, njezine poslovne aktivnosti i njihova neprekidnost, uključujući informacijske resurse koji podupiru misiju organizacije;

„ovlaštenje za pristup klasificiranim podacima EU-a” znači odluka koju je tijelo za imenovanja GSC-a donijelo na temelju potvrde nadležnog tijela države članice da se dužnosniku GSC-a, drugom službeniku ili upućenom nacionalnom stručnjaku, pod uvjetom da je za njega utvrđena nužnost pristupa podacima i da je adekvatno informiran o svojim odgovornostima, može odobriti pristup klasificiranim podacima EU-a do navedenog stupnja tajnosti (CONFIDENTIEL UE/EU CONFIDENTIAL ili višeg) do određenog datuma;

„životni ciklus CIS-a” znači cjelokupno trajanje postojanja CIS-a, što uključuje pokretanje, koncept, planiranje, analizu zahtjeva, projektiranje, razvoj, ispitivanje, provedbu, rad, održavanje i stavljanje izvan pogona;

„klasificirani ugovor” znači ugovor sklopljen između GSC-a i ugovaratelja za isporuku robe, izvođenje radova ili pružanje usluga, a čije izvršenje zahtijeva ili uključuje pristup klasificiranim podacima EU-a ili njihovo stvaranje;

„klasificirani podugovor” znači ugovor sklopljen između ugovaratelja GSC-a i drugog ugovaratelja (tj. podugovaratelja) za isporuku robe, izvođenje radova ili pružanje usluga, a čije izvršenje zahtijeva ili uključuje pristup klasificiranim podacima EU-a ili njihovo stvaranje;

„komunikacijski i informacijski sustav” (CIS) – vidjeti članak 10. stavak 2.;

„ugovaratelj” znači pojedinac ili pravni subjekt koji ima pravnu sposobnost za sklapanje ugovora;

„kriptografski materijal (kriptomaterijal)” znači kriptografski algoritmi, kriptografski hardverski i softverski moduli i proizvodi, uključujući detalje o provedbi te povezanu dokumentaciju i materijale u vezi s ključevima;

„kriptografski proizvod” znači proizvod čija je primarna i glavna funkcija pružanje sigurnosnih usluga (povjerljivosti, cjelovitosti, dostupnosti, nepobitnosti i autentičnosti) pomoću jednog ili više kriptografskih mehanizama;

„operacija ZSOP-a” znači vojna ili civilna operacija upravljanja u kriznim situacijama uspostavljena na temelju glave V. poglavlja 2. UEU-a;

„deklasifikacija” znači uklanjanje svakog stupnja tajnosti;

„dubinska obrana” znači primjena niza sigurnosnih mjera organiziranih kao višestruki slojevi obrane;

„zaduženo sigurnosno tijelo” (DSA) znači tijelo odgovorno nacionalnom sigurnosnom tijelu (NSA-u) države članice koje je odgovorno za obavješćivanje gospodarskih i drugih subjekata o nacionalnoj politici u pogledu svih pitanja gospodarske sigurnosti te za usmjeravanje i pružanje pomoći u njezinoj provedbi. Funkciju DSA-a može obavljati NSA ili bilo koje drugo nadležno tijelo;

„dokument” znači svi zabilježeni podaci bez obzira na njihov fizički oblik ili značajke;

„smanjenje stupnja tajnosti” znači smanjenje razine stupnja tajnosti;

„klasificirani podaci EU-a” – vidjeti članak 2. stavak 1.;

„uvjerenje o sigurnosnoj provjeri pravne osobe” (FSC) znači potvrda od strane NSA-a ili DSA-a da, sa stajališta sigurnosti, pravna osoba može pružiti odgovarajuću razinu zaštite klasificiranim podacima EU-a određenog stupnja tajnosti;

„postupanje” s klasificiranim podacima EU-a znači sve moguće radnje kojima klasificirani podaci EU-a mogu biti izloženi tijekom svojeg životnog ciklusa. Ono obuhvaća njihovo stvaranje, obradu, prijenos, smanjenje stupnja tajnosti, deklasificiranje i uništavanje. U pogledu CIS-a ono također obuhvaća njihovo prikupljanje, prikaz, slanje i čuvanje;

„imatelj” znači propisno ovlašteni pojedinac s utvrđenom nužnošću pristupa podacima koji je u posjedu klasificiranog podatka EU-a te je, prema tome, odgovoran za njegovu zaštitu;

„gospodarski ili drugi subjekt” znači subjekt uključen u isporuku robe, izvođenje radova ili pružanje usluga; to može biti gospodarski, komercijalni, uslužni, znanstveni, istraživački, obrazovni ili razvojni subjekt ili samozaposlena osoba;

„gospodarska sigurnost” – vidjeti članak 11. stavak 1.;

„informacijska sigurnost” – vidjeti članak 10. stavak 1.;

„međusobno povezivanje” – vidjeti Prilog IV. stavak 32.;

„upravljanje klasificiranim podacima” – vidjeti članak 9. stavak 1.;

„materijal” znači svaki dokument, nosač podataka ili dio stroja ili opreme, bilo da je proizveden ili u procesu proizvodnje;

„onaj od kojeg podaci potječu” znači institucija, tijelo ili agencija Unije, država članica, treća država ili međunarodna organizacija pod čijom su nadležnošću stvoreni i/ili u strukture Unije uvedeni klasificirani podaci;

„sigurnost osoba” – vidjeti članak 7. stavak 1.;

„uvjerenje o sigurnosnoj provjeri osobe” (PSC) znači izjava nadležnog tijela države članice koja je sastavljena nakon završetka sigurnosne istrage koju provode nadležna tijela države članice i kojom se potvrđuje da se pojedincu može odobriti pristup klasificiranim podacima EU-a do određenog stupnja tajnosti (CONFIDENTIEL UE/EU CONFIDENTIAL ili višeg) do određenog datuma;

„certifikat o sigurnosnoj provjeri osobe” (PSCC) znači certifikat koji izdaje nadležno tijelo i kojim se utvrđuje da je pojedinac prošao sigurnosnu provjeru i da ima valjani certifikat o sigurnosnoj provjeri ili ovlaštenje tijela za imenovanja za pristup klasificiranim podacima EU-a 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 odgovarajućeg PSC-a i datum isteka samog certifikata;

„fizička sigurnost” – vidjeti članak 8. stavak 1.;

„sigurnosni naputak za program/projekt” (PSI) znači popis sigurnosnih postupaka koji se primjenjuju na određeni program/projekt s ciljem standardizacije sigurnosnih postupaka. Može se izmijeniti tijekom programa/projekta;

„upis” – vidjeti Prilog III. stavak 18.;

„preostali rizik” znači rizik koji ostaje nakon provedbe sigurnosnih mjera, uz uvjet da se ne mogu suzbiti sve prijetnje i ukloniti sve osjetljivosti;

„rizik” znači mogućnost da će određena prijetnja iskoristiti unutarnje i vanjske osjetljivosti organizacije ili bilo kojeg od sustava koje organizacija koristi i pri tome uzrokovati štetu organizaciji i njezinoj materijalnoj i nematerijalnoj imovini. Mjeri se kao kombinacija vjerojatnosti pojave prijetnje i njezina učinka:

— „prihvaćanje rizika” jest odluka o tome da je preostali rizik i nadalje prisutan nakon postupanja s rizikom,

— „procjena rizika” sastoji se od prepoznavanja prijetnji i osjetljivosti te provedbe povezane analize rizika, tj. analize vjerojatnosti i učinka,

— „obavješćivanje o rizicima” sastoji se od razvijanja svijesti o rizicima u zajednicama korisnika CIS-a, informiranja tijela za odobrenja o takvim rizicima i izvješćivanja operativnih tijela o njima,

— „postupanje s rizicima” sastoji se od ublažavanja, uklanjanja, smanjivanja (odgovarajućom kombinacijom tehničkih, fizičkih, organizacijskih ili postupovnih mjera), prijenosa ili praćenja rizika;

„pismo o sigurnosnim aspektima” (SAL) znači skup posebnih ugovornih uvjeta koji izdaje tijelo za ugovaranje, a koji čini sastavni dio klasificiranog ugovora koji uključuje pristup klasificiranim podacima EU-a ili njihovo stvaranje i kojim se utvrđuju sigurnosni zahtjevi ili oni elementi ugovora za koje je potrebna sigurnosna zaštita;

„vodič za stupnjeve tajnosti” (SCG) znači dokument u kojem su opisani klasificirani elementi programa ili ugovora te navedeni primjenljivi stupnjevi tajnosti. SCG se može proširivati tijekom trajanja programa ili ugovora, a elementi podataka mogu se ponovno klasificirati ili se može smanjiti njihov stupanj tajnosti; ako postoji SCG, on čini dio SAL-a;

„sigurnosna istraga” znači istražni postupci koje provodi nadležno tijelo države članice u skladu s nacionalnim zakonima i propisima s ciljem dobivanja jamstva da ne postoji ništa štetno zbog čega se pojedincu ne bi odobrio PSC ili ovlaštenje za pristup klasificiranim podacima EU-a do određenog stupnja tajnosti (CONFIDENTIEL UE/EU CONFIDENTIAL ili višeg);

„sigurnosni način rada” znači definiranje uvjeta pod kojima CIS radi na temelju klasifikacije podataka s kojima se u njemu postupa i razina provjere, službenih odobrenja pristupa i nužnosti pristupa korisnika podacima. Postoje četiri načina rada za postupanje s klasificiranim podacima ili njihovo slanje: namjenski način rada, način rada u sustavu visoke sigurnosti, segmentirani način rada i višerazinski način rada:

— „namjenski način rada” znači način rada u kojem su svi pojedinci s pristupom CIS-u prošli sigurnosnu provjeru za najviši stupanj tajnosti podataka s kojima se postupa u CIS-u i s općom nužnošću pristupa podacima za sve podatke koji se obrađuju u CIS-u,

— „način rada u sustavu visoke sigurnosti” znači način rada u kojem su svi pojedinci s pristupom CIS-u prošli sigurnosnu provjeru za najviši stupanj tajnosti podataka s kojima se postupa u CIS-u, ali svi pojedinci s pristupom CIS-u nemaju opću nužnost pristupa podacima za podatke koji se obrađuju u CIS-u; odobrenje za pristup podacima može dati pojedinac,

— „segmentirani način rada” znači način rada u kojem su svi pojedinci s pristupom CIS-u prošli sigurnosnu provjeru za najviši stupanj tajnosti podataka s kojima se postupa u CIS-u, ali svi pojedinci s pristupom CIS-u nemaju službeno ovlaštenje za pristup svim podacima s kojima se postupa u CIS-u; službeno ovlaštenje podrazumijeva službeno središnje upravljanje nadzorom pristupa za razliku od diskrecijske odluke pojedinca o odobrenju pristupa,

— „višerazinski način rada” znači način rada u kojem nisu svi pojedinci s pristupom CIS-u prošli sigurnosnu provjeru za najviši stupanj tajnosti podataka s kojima se postupa u CIS-u niti svi pojedinci s pristupom CIS-u imaju nužnost pristupa podacima za podatke s kojima se postupa u CIS-u;

„proces upravljanja sigurnosnim rizicima” znači cjelokupni proces prepoznavanja, nadzora i smanjenja nesigurnih događaja koji mogu utjecati na sigurnost organizacije ili nekog od sustava koje organizacija rabi. On obuhvaća sve aktivnosti povezane s rizicima, uključujući procjenu, postupanje, prihvaćanje i obavješćivanje;

„TEMPEST” znači istraživanje, proučavanje i nadzor štetnog elektromagnetnog zračenja i mjere za njegovo suzbijanje;

„prijetnja” znači mogući uzrok neželjenog incidenta koji može rezultirati štetom za organizaciju ili neki od sustava koje organizacija koristi; takve prijetnje mogu bili slučajne ili namjerne (zlonamjerne), a karakteriziraju ih prijeteći elementi, mogući ciljevi i načini napada;

„osjetljivost” znači slabost bilo koje vrste koju može iskoristiti jedna ili više prijetnji. Osjetljivost može biti propust ili se može odnositi na slabost u kontrolama u smislu njihove snage, cjelovitosti ili dosljednosti i može biti tehničke, postupovne, fizičke, organizacijske ili operativne naravi.

*Dodatak B*

EKVIVALENTNOST STUPNJEVA TAJNOSTI

| EU | TRÈS SECRET UE/EU TOP SECRET | SECRET UE/EU SECRET | CONFIDENTIEL UE/EU CONFIDENTIAL | RESTREINT UE/EU RESTRICTED |
|---|---|---|---|---|
| Belgija | Très Secret (Loi 11.12.1998.)<br>Zeer Geheim (Wet 11.12.1998.) | Secret (Loi 11.12.1998.)<br>Geheim (Wet 11.12.1998.) | Confidentiel (Loi 11.12.1998.)<br>Vertrouwelijk (Wet 11.12.1998.) | napomena (1) dolje |
| Bugarska | Строго секретно | Секретно | Поверително | За служебно ползване |
| Češka | Přísně tajné | Tajné | Důvěrné | Vyhrazené |
| Danska | YDERST HEMMELIGT | HEMMELIGT | FORTROLIGT | TIL TJENESTEBRUG |
| Njemačka | STRENG GEHEIM | GEHEIM | VS (2)— VERTRAULICH | VS — NUR FÜR DEN DIENSTGEBRAUCH |
| Estonija | Täiesti salajane | Salajane | Konfidentsiaalne | Piiratud |
| Irska | Top Secret | Secret | Confidential | Restricted |
| Grčka | Άκρως Απόρρητο<br>Abr: ΑΑΠ | Απόρρητο<br>Abr: (ΑΠ) | Εμπιστευτικό<br>Abr: (ΕΜ) | Περιορισμένης Χρήσης<br>Abr: (ΠΧ) |
| Španjolska | SECRETO | RESERVADO | CONFIDENCIAL | DIFUSIÓN LIMITADA |
| Francuska | Très Secret Défense | Secret Défense | Confidentiel Défense | napomena (3) dolje |
| Hrvatska | VRLO TAJNO | TAJNO | POVJERLJIVO | OGRANIČENO |
| Italija | Segretissimo | Segreto | Riservatissimo | Riservato |
| Cipar | Άκρως Απόρρητο<br>Abr: (ΑΑΠ) | Απόρρητο<br>Abr: (ΑΠ) | Εμπιστευτικό<br>Abr: (ΕΜ) | Περιορισμένης Χρήσης<br>Abr: (ΠΧ) |
| Latvija | Sevišķi slepeni | Slepeni | Konfidenciāli | Dienesta vajadzībām |
| Litva | Visiškai slaptai | Slaptai | Konfidencialiai | Riboto naudojimo |
| Luksemburg | Très Secret Lux | Secret Lux | Confidentiel Lux | Restreint Lux |
| Mađarska | Szigorúan titkos! | Titkos! | Bizalmas! | Korlátozott terjesztésű! |
| Malta | L-Ogħla Segretezza<br>Top Secret | Sigriet<br>Secret | Kunfidenzjali<br>Confidential | Ristrett<br>Restricted (4) |
| Nizozemska | Stg. ZEER GEHEIM | Stg. GEHEIM | Stg. CONFIDENTIEEL | Dep. VERTROUWELIJK |
| Austrija | Streng Geheim | Geheim | Vertraulich | Eingeschränkt |
| Poljska | Ściśle Tajne | Tajne | Poufne | Zastrzeżone |
| Portugal | Muito Secreto | Secreto | Confidencial | Reservado |

| EU | TRÈS SECRET UE/EU TOP SECRET | SECRET UE/EU SECRET | CONFIDENTIEL UE/EU CONFIDENTIAL | RESTREINT UE/EU RESTRICTED |
|---|---|---|---|---|
| Rumunjska | Strict secret de importanță deosebită | Strict secret | Secret | Secret de serviciu |
| Slovenija | STROGO TAJNO | TAJNO | ZAUPNO | INTERNO |
| Slovačka | Prísne tajné | Tajné | Dôverné | Vyhradené |
| Finska | ERITTÄIN SALAINEN<br>YTTERST HEMLIG | SALAINEN<br>HEMLIG | LUOTTAMUKSELLINEN<br>KONFIDENTIELL | KÄYTTÖ RAJOITETTU<br>BEGRÄNSAD TILLGÅNG |
| Švedska ([5]) | HEMLIG/TOP SECRET<br>HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET | HEMLIG/SECRET<br>HEMLIG | HEMLIG/CONFIDENTIAL<br>HEMLIG | HEMLIG/RESTRICTED<br>HEMLIG |
| Ujedinjena Kraljevina | UK TOP SECRET | UK SECRET | UK CONFIDENTIAL | UK RESTRICTED |

([1]) Diffusion Restreinte/Beperkte Verspreiding nije stupanj tajnosti u Belgiji. Belgija postupa s podacima klasificiranima kao „RESTREINT UE/EU RESTRICTED" te ih štiti na način koji nije ništa manje strog od standarda i postupaka opisanih u sigurnosnim propisima Vijeća Europske unije.
([2]) Njemačka: VS = Verschlusssache.
([3]) Francuska u svojem nacionalnom sustavu ne rabi stupanj tajnosti „RESTREINT". Francuska postupa s podacima klasificiranima kao „RESTREINT UE/EU RESTRICTED" te ih štiti na način koji nije ništa manje strog od standarda i postupaka opisanih u sigurnosnim propisima Vijeća Europske unije.
([4]) U slučaju Malte mogu se rabiti oznake i na malteškom i na engleskom jeziku.
([5]) Švedska: oznake stupnjeva tajnosti u gornjem redu koriste obrambena tijela, dok oznake u donjem redu rabe druga tijela.

*Dodatak C*

POPIS NACIONALNIH SIGURNOSNIH TIJELA (NSA)

**BELGIJA**
Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles

Tel. tajništva: +32 25014542
Telefaks: +32 25014596
E-pošta: nvo-ans@diplobel.fed.be

**BUGARSKA**
State Commission on Information Security
90 Cherkovna Str.
1505 Sofia

Tel.: +359 29333600
Telefaks: +359 29873750
E-pošta: dksi@government.bg
Web stranica: www.dksi.bg

**ČEŠKA**
Národní bezpečnostní úřad
(National Security Authority) P.O.
Na Popelce 2/16
150 06 Praha 56

Tel.: +420 257283335
Telefaks: +420 257283110
E-pošta: czech.nsa@nbu.cz
Internetska stranica: www.nbu.cz

**DANSKA**
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg

Tel.: +45 33148888
Telefaks: +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø

Tel.: +45 33325566
Telefaks: +45 33931320

**NJEMAČKA**
Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin

Tel.: +49 30186810
Telefaks: +49 30186811441
E-pošta: oesIII3@bmi.bund.de

**ESTONIJA**
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn

Tel.: +372 717 0019, +372 7170117
Telefaks: +372 7170213
E-pošta: nsa@mod.gov.ee

**IRSKA**
National Security Authority
Department of Foreign Affairs
76 - 78 Harcourt Street
Dublin 2

Tel.: +353 14780822
Telefaks: +353 14082959

**GRČKA**
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα

Τηλ.: +30 2106572045 (ώρες γραφείου)
+30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279
+30 2106577612

Hellenic National Defence General Staff (HNDGS)
Counter Intelligence and Security Directorate (NSA)
227-231 HOLARGOS
STG 1020 ATHENS

Tel.: +30 2106572045
+30 2106572009
Telefaks: +30 2106536279
+30 2106577612

**ŠPANJOLSKA**
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid

Tel.: +34 913725000
Telefaks: +34 913725808
E-pošta: nsa-sp@areatec.com

**FRANCUSKA**
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Pariz 07 SP

Tel.: +33 171758177
Telefaks: +33 171758200

**HRVATSKA**
Ured Vijeća za nacionalnu sigurnost
Croatian NSA
Jurjevska 34
10000 Zagreb
Hrvatska

Tel.: +385 14681222
Telefaks: + 385 14686049
www.uvns.hr

**ITALIJA**
Presidenza del Consiglio dei Ministri
D.I.S. - U.C.Se.
Via di Santa Susanna, 15
00187 Roma

Tel.: +39 0661174266
Telefaks: +39 064885273

**CIPAR**
ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος

Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia

Tel.: +357 22807569, +357 22807643, +357 22807764
Telefaks: +357 22302351
E-pošta: cynsa@mod.gov.cy

**LATVIJA**
National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV-1001 Riga

Tel.: +371 67025418
Telefaks: +371 67025454
E-pošta: ndi@sab.gov.lv

**LITVA**
Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania
National Security Authority)
Gedimino 40/1
LT-01110 Vilnius

Tel.: +370 706 66701, +370 706 66702
Telefaks: +370 706 66700
E-pošta: nsa@vsd.lt

**LUKSEMBURG**
Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg

Tel.: +352 24782210 centrala
+352 24782253 izravno biranje
Telefaks: +352 24782243

**MAĐARSKA**
Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B

Tel.: +36 (1) 7952303
Telefaks: +36 (1) 7950344
Poštanska adresa:
H-1357 Budapest, PO Box 2
E-pošta: nbf@nbf.hu
Internetska stranica: www.nbf.hu

**MALTA**
Ministry for Home Affairs and National Security
Box 146
MT-Valletta

Tel.: +356 21249844
Telefaks: +356 25695321

**NIZOZEMSKA**
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag

Tel.: +31 703204400
Telefaks: +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag

Tel.: +31 703187060
Telefaks: +31 703187522

**AUSTRIJA**
Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien

Tel.: +43 1531152594
Telefaks: +43 1531152615
E-pošta: ISK@bka.gv.at

| | |
|---|---|
| **POLJSKA**<br>Agencja Bezpieczeństwa Wewnętrznego – ABW<br>(Internal Security Agency)<br>2A Rakowiecka St.<br>00-993 Warszawa<br><br>Tel.: +48 225857360<br>Telefaks: +48 225858509<br>E-pošta: nsa@abw.gov.pl<br>Internetska stranica: www.abw.gov.pl | **SLOVAČKA**<br>Národný bezpečnostný úrad<br>(National Security Authority) P.O.<br>Budatínska 30<br>P.O. Box 16<br>850 07 Bratislava<br><br>Tel.: +421 268692314<br>Telefaks: +421 263824005<br>Internetska stranica: www.nbusr.sk |
| **PORTUGAL**<br>Presidência do Conselho de Ministros<br>Autoridade Nacional de Segurança<br>Rua da Junqueira, 69<br>1300-342 Lisboa<br><br>Tel.: +351 213031710<br>Telefaks: +351 213031711 | **FINSKA**<br>National Security Authority<br>Ministry for Foreign Affairs<br>P.O. Box 453<br>FI-00023 Government<br><br>Tel.: +358 16055890<br>Telefaks: +358 916055140<br>E-pošta: NSA@formin.fi |
| **RUMUNJSKA**<br>Oficiul Registrului Național al Informațiilor Secrete de Stat<br>(Romanian NSA – ORNISS<br>National Registry Office for Classified Information)<br>Str. Mureș nr. 4, sector 1<br>012275 București<br><br>Tel.: +40 212245830<br>Telefaks: +40 212240714<br>E-pošta: nsa.romania@nsa.ro<br>Internetska stranica: www.orniss.ro | **ŠVEDSKA**<br>Utrikesdepartementet<br>(Ministry for Foreign Affairs)<br>UD-RS<br>S-103 39 Stockholm<br><br>Tel.: +46 84051000<br>Telefaks: +46 87231176<br>E-pošta: ud-nsa@foreign.ministry.se |
| **SLOVENIJA**<br>Urad Vlade RS za varovanje tajnih podatkov<br>Gregorčičeva 27<br>1000 Ljubljana<br><br>Tel.: +386 14781390<br>Telefaks: +386 14781399<br>E-pošta: gp.uvtp@gov.si | **UJEDINJENA KRALJEVINA**<br>UK National Security Authority<br>Room 335, 3rd Floor<br>70 Whitehall<br>London<br>SW1A 2AS<br><br>Tel. 1: +44 2072765645<br>Tel. 2: +44 2072765497<br>Telefaks: +44 2072765651<br>E-pošta: UK-NSA@cabinet-office.x.gsi.gov.uk |

*Dodatak D*

POPIS KRATICA

| Kratica | značenje |
|---|---|
| AQUA | odgovarajuće kvalificirano tijelo |
| BPS | usluge zaštite granice |
| CAA | tijelo za odobravanje kriptomaterijala |
| CCTV | televizija zatvorenog kruga |
| CDA | tijelo za distribuciju kriptomaterijala |
| ZVSP | zajednička vanjska i sigurnosna politika |
| CIS | komunikacijski i informacijski sustavi za postupanje s klasificiranim podacima EU-a |
| Coreper | Odbor stalnih predstavnika |
| ZSOP | zajednička sigurnosna i obrambena politika |
| DSA | zaduženo sigurnosno tijelo |
| ECSD | Uprava za sigurnost Europske unije |
| EUCI | klasificirani podaci EU-a |
| PPEU | posebni predstavnik EU-a |
| FSC | uvjerenje o sigurnosnoj provjeri pravne osobe |
| GSC | Glavno tajništvo Vijeća |
| IA | informacijska sigurnost |
| IAA | tijelo za informacijsku sigurnost |
| IDS | sustav za otkrivanje neovlaštenog ulaska |
| IT | informacijska tehnologija |
| NSA | tijelo nacionalne sigurnosti |
| PSC | uvjerenje o sigurnosnoj provjeri osobe |
| PSCC | certifikat o sigurnosnoj provjeri osobe |
| PSI | sigurnosni naputak za program/projekt |
| SAA | tijelo za akreditaciju u vezi sa sigurnosti |
| OSA | Odbor za sigurnosnu akreditaciju |
| SAL | pismo o sigurnosnim aspektima |
| SecOPs | sigurnosni postupci rada |
| SCG | vodič za stupnjeve tajnosti |
| SSRS | izjava o sigurnosnim zahtjevima za specifični sustav |
| TA | tijelo TEMPEST-a |

**EUR-Lex (http://new.eur-lex.europa.eu) omogućuje izravan i besplatan pristup zakonodavstvu Europske unije. Ta stranica omogućuje pregled *Službenog lista Europske unije,* kao i Ugovora, zakonodavstva, sudske prakse i pripremnih akata.**

**Više obavijesti o Europskoj uniji može se pronaći na stranici: http://europa.eu**

Ured za publikacije Europske unije
2985 Luxembourg
LUKSEMBURG

HR