32011D0292

27.5.2011. SLUŽBENI LIST EUROPSKE UNIJE L 141/17

ODLUKA VIJEĆA

od 31. ožujka 2011.

o sigurnosnim propisima za zaštitu klasificiranih podataka EU

(2011/292/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 (GTV) postupaju s klasificiranim podacima EU-a.

(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 i Komisija ustraju u primjenjivanju jednakih sigurnosnih standarda za zaštitu klasificiranih podataka EU-a.

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

(6) Agencije i tijela EU-a uspostavljene na temelju glave V. poglavlja 2. Ugovora o Europskoj uniji, Europol i Eurojust primjenjuju, u sklopu svoje unutarnje organizacije, osnovna načela i minimalne standarde utvrđene ovom Odlukom za zaštitu klasificiranih podataka EU-a, kako je predviđeno njihovim odgovarajućim aktima o osnivanju.

(7) U operacijama upravljanja u kriznim situacijama uspostavljene na temelju glave V. poglavlja 2. UEU-a primjenjuju se sigurnosni propisi koje je donijelo Vijeće radi zaštite klasificiranih podataka EU-a, a njih primjenjuje i osoblje koje sudjeluje u tim operacijama.

(8) Posebni predstavnici EU-a i članovi njihovih timova primjenjuju sigurnosne propise koje je donijelo Vijeće za zaštitu klasificiranih podataka EU-a.

(9) Ovom se Odlukom ne dovode u pitanje članci 15. i 16. Ugovora o funkcioniranju Europske unije (UFEU) kao ni instrumenti za njihovo provođenje.

(10) Ovom se Odlukom ne dovode u pitanje postojeće prakse u državama članicama u pogledu informiranja nacionalnih parlamenata o aktivnostima Unije,

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.

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

2. Navedeni minimalni standardi i osnovna načela primjenjuju se na Vijeće i GTV, a države članice moraju ih poštovati u skladu s odgovarajućim 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" znače 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 izuzetno 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 nijedna oznaka iz članka 2. stavka 3.

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

Članak 4.

Zaštita klasificiranih podataka

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

2. Imatelj bilo kojeg 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 Europske unije, Vijeće i GTV štite navedene podatke u skladu sa zahtjevima primjenljivim na klasificirane podatke EU-a na jednakoj razini kako je utvrđeno u tablici ekvivalentnosti stupnjeva tajnosti sadržanoj u Dodatku B.

4. Kod velikih količina ili zbirke klasificiranih podataka EU-a može biti opravdana razina zaštite koja odgovara višem stupnju tajnosti.

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 voditi računa o potrebi 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 osoba

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 GTV-u koji zbog svojih dužnosti mogu zatrebati pristup klasificiranim podacima EU-a sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili više, moraju proći sigurnosnu provjeru za odgovarajuću razinu prije nego što im se omogući pristup takvim klasificiranim podacima EU-a. Postupak za sigurnosnu provjeru osoba za dužnosnike GTV-a i druge službenike naveden je u Prilogu I.

4. Osoblje država članica iz članka 14. stavka 3. koje zbog svojih dužnosti može zatrebati pristup klasificiranim podacima EU-a sa stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili više, mora proći sigurnosnu provjeru za odgovarajuću razinu 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 ih se čuva, 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, otkrivanju i oporavku od namjerne ili slučajne ugroze ili gubitka takvih podataka. Takve se mjere posebno odnose na stvaranje, upis, umnožavanje, prevođenje, prijevoz 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 GTV-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 ih se čuva 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 koriste 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 Prilogu III.

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

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

4. Svaki KIS 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 KIS-a u skladu s ovom Odlukom. U izjavi o akreditaciji određuju se najviši stupanj tajnosti podataka s kojima se može postupati u KIS-u i odgovarajući uvjeti.

5. KIS u kojem se postupa s podacima klasificiranim kao CONFIDENTIEL UE/EU CONFIDENTIAL i više zaštićen je tako da podaci ne mogu biti ugroženi nenamjernim elektromagnetskim zračenjem (sigurnosne mjere TEMPEST).

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 (dalje u tekstu „glavni tajnik") u ulozi CAA-a na preporuku Sigurnosnog odbora.

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

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

8. Nadležna tijela GTV-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 GTV-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. GTV može na temelju ugovora povjeriti zadatke 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 zemlji koja je sklopila sporazum ili administrativni dogovor u skladu s člankom 12. stavkom 2. točkom (a) ili (b).

3. GTV, 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 navedenoj državi članici i koji sudjeluju u klasificiranim ugovorima ili podugovorima koji zahtijevaju pristup podacima klasificiranim 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 poduzeća (FSC) za odgovarajući stupanj tajnosti.

6. Osoblju ugovaratelja ili podugovaratelja kojem za izvršenje klasificiranog ugovora treba pristup podacima klasificiranim 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 s trećim zemljama i međunarodnim organizacijama

1. Ako Vijeće utvrdi da postoji potreba za razmjenom klasificiranih podataka EU-a s trećim zemljama 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) Vijeće sklapa sporazume o sigurnosnim postupcima za razmjenu i zaštitu klasificiranih podataka (dalje u tekstu „sporazumi o sigurnosti podataka"); ili

(b) glavni tajnik može sklapati administrativne dogovore 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 zemlje 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 zemlji 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 EU. Ako onaj od kojeg potječu klasificirani podaci koji se žele objaviti nije Vijeće, GTV najprije mora zatražiti pisanu suglasnost za objavljivanje od onog od kojeg podaci potječu. Ako se isti 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 zemlji ili međunarodnoj organizaciji za zaštitu dostavljenih ili razmijenjenih klasificiranih podataka EU-a.

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

Članak 13.

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, nadležno sigurnosno 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 EU-a ili država članica;

(d) poduzelo odgovarajuće mjere za sprečavanje ponovne povrede;

(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 14.

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 njihova čuvanja, dužnosnici GTV-a i drugi službenici, osoblje dodijeljeno GTV-u i ugovaratelji GTV-a primjenjuju ovu Odluku u prostorijama koje koristi Vijeće i unutar GTV-a, uključujući njegove urede za vezu u trećim zemljama.

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 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 15.

Organizacija sigurnosti u Vijeću

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

(a) sporazume iz članka 12. stavka 2. točke (a);

(b) odluke kojima se odobrava objava klasificiranih podataka EU-a trećim zemljama i međunarodnim organizacijama;

(c) godišnji program inspekcija na prijedloga glavnog tajnika i na preporuku Sigurnosnog odbora za inspekcije službi i prostorija država članica, agencija i tijela EU-a uspostavljenih na temelju glave V. poglavlja 2. UEU-a kao i Europola i Eurojusta te posjete radi procjene stanja trećim zemljama 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 GTV-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) odobrava EU PSC-e dužnosnicima GTV-a i drugim službenicima u skladu s člankom 7. stavkom 3., prije nego što im se odobri pristup podacima klasificiranim kao CONFIDENTIEL UE/EU CONFIDENTIAL ili više;

(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 GTV-a;

(f) poduzima periodične inspekcije sigurnosnih mjera za zaštitu klasificiranih podataka EU-a u agencijama i tijelima EU-a uspostavljenima na temelju glave V. poglavlja 2. UEU-a, Europolu, Eurojustu, kao i u operacijama upravljanja u kriznim situacijama uspostavljenima na temelju glave V. poglavlja 2. UEU-a te sigurnosnih mjera posebnih predstavnika EU-a (EUSR) i članova njihovih timova;

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

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

(i) sklapa administrativne dogovore iz članka 12. stavka 2. točke (b); i

(j) poduzima početne i periodične posjete radi procjene stanja trećim zemljama ili međunarodnim organizacijama, kako bi potvrdio učinkovitost provedenih mjera za zaštitu dostavljenih ili razmijenjenih klasificiranih podataka EU-a.

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

3. Za potrebe provedbe članka 14. stavka 3. države članice trebaju:

(a) odrediti NSA 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;

iii. svi pojedinci zaposleni u nacionalnoj administraciji ili kod ugovaratelja 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 s ciljem 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 koje su podnijele agencije i tijela EU-a uspostavljene na temelju glave V. poglavlja 2. UEU-a, Europol, Eurojust kao i operacije upravljanja u kriznim situacijama uspostavljene na temelju glave V. poglavlja 2. UEU-a te EUSR-i i njihovi timovi.

NSA-i su navedeni u Dodatku C;

(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 16.

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 Europske službe za vanjsko djelovanje. Njime predsjeda glavni tajnik ili njegov imenovani izaslanik. Sastaje se po uputi Vijeća ili na zahtjev glavnog tajnika ili NSA-a.

Predstavnici agencija i tijela EU-a uspostavljenih na temelju glave V. poglavlja 2. UEU-a te Europola i Eurojusta mogu biti pozvani i sudjelovati 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 17.

Zamjena prethodne odluke

1. Ovom se Odlukom stavlja izvan snage i zamjenjuje Odluka Vijeća 2001/264/EZ od 19. ožujka 2001. o donošenju sigurnosnih propisa Vijeća [1].

2. Svi klasificirani podaci EU-a klasificirani u skladu s Odlukom 2001/264/EZ i dalje su zaštićeni u skladu s odgovarajućim odredbama ove Odluke.

Članak 18.

Stupanje na snagu

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

Sastavljeno u Bruxellesu 31. ožujka 2011.

Za Vijeće
Predsjednik
VÖLNER P.

[1] 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 KIS-u

PRILOG V.

Gospodarska sigurnost

PRILOG VI.

Razmjena klasificiranih podataka s trećim zemljama i međunarodnim organizacijama

PRILOG I.

SIGURNOST OSOBA

I. UVOD

1. U ovom se Prilogu određuju odredbe za provedbu članka 7. U njemu se posebno 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 pridržavati.

2. U cijelom ovom Prilogu, osim ako je razlikovanje bitno, pojam „uvjerenje o sigurnosnoj provjeri osobe" odnosi se na nacionalno uvjerenje o sigurnosnoj provjeri osobe (nacionalni PSC) i/ili uvjerenje EU-a o sigurnosnoj provjeri osobe (EU PSC) kako je određeno u Dodatku A.

II. ODOBRAVANJE PRISTUPA KLASIFICIRANIM PODACIMA EU-a

3. Pojedinac je ovlašten pristupiti podacima klasificiranim kao CONFIDENTIEL UE/EU CONFIDENTIAL ili više samo nakon što:

(a) je za njega utvrđena nužnost pristupa podacima;

(b) mu je odobren PSC za odgovarajuću razinu ili je na neki drugi način propisno ovlašten na temelju svojih funkcija u skladu s nacionalnim zakonima i propisima; i

(c) je upoznat sa sigurnosnim propisima i postupcima za zaštitu klasificiranih podataka EU-a te je potvrdio svoje odgovornosti povezane sa zaštitom takvih podataka.

4. Svaka država članica i GTV utvrđuju položaje u svojim strukturama za koje je potreban pristup podacima klasificiranim kao CONFIDENTIEL UE/EU CONFIDENTIAL ili više i stoga zahtijevaju PSC za odgovarajuću razinu.

III. ZAHTJEVI POVEZANI S UVJERENJEM O SIGURNOSNOJ PROVJERI OSOBA

5. 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 klasificiranim kao CONFIDENTIEL UE/EU CONFIDENTIAL ili više. Standardi istrage moraju biti u skladu s nacionalnim zakonima i propisima.

6. Ako dotični pojedinac prebiva na području druge države članice ili treće zemlje, 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.

7. Ako je to dopušteno prema nacionalnim zakonima i propisima, NSA-i ili druga nadležna nacionalna tijela mogu provoditi istrage stranaca koji traže pristup podacima klasificiranim kao CONFIDENTIEL UE/EU CONFIDENTIAL ili više. Standardi istrage moraju biti u skladu s nacionalnim zakonima i propisima.

Kriteriji sigurnosne istrage

8. Lojalnost, vjerodostojnost i pouzdanost pojedinca utvrđuje se, u svrhu izdavanja PSC-a za pristup podacima klasificiranim kao CONFIDENTIEL UE/EU CONFIDENTIAL ili više, sredstvima sigurnosne istrage. Nadležno nacionalno tijelo izrađuje opću procjenu na temelju nalaza takve sigurnosne istrage. Ni jedan pojedinačni negativni nalaz ne predstavlja nužno razlog za odbijanje PSC-a. Temeljni kriteriji koji se u tu svrhu koriste trebaju uključivati, u mjeri u kojoj je to moguće prema nacionalnim zakonima i propisima, ispitivanje je li pojedinac:

(a) počinio ili namjeravao počiniti bilo koje 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 EU-a i/ili država članica, osim ako je takva suradnja bila ovlaštena u okviru službene dužnosti;

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

(d) podržava ili je podržavao bilo koju organizaciju opisanu pod točkom (c), odnosno usko 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 kaznena djela ili prekršaje;

(g) bio ovisan o alkoholu, koristio 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;

(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 EU-a i/ili država članica).

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

10. Ako je potrebno i u skladu s nacionalnim zakonima i propisima, karakter, 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

Izdavanje prvog PSC-a

11. Prvi PSC za pristup podacima klasificiranim kao 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.

12. Prvi PSC za pristup podacima klasificiranim kao 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 8. 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.

13. 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 PSC-a

14. Nakon izdavanja prvog PSC-a i uz uvjet da pojedinac ima neprekinuti radni staž u nacionalnoj administraciji ili GTV-u te stalnu potrebu za pristupom klasificiranim podacima EU-a, PSC 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 PSC-a obuhvaćaju razdoblje od prethodne takve istrage.

15. Za obnovu PSC-a istražuju se elementi opisani u stavcima 11. i 12.

16. Zahtjevi za obnovu podnose se pravovremeno vodeći računa o vremenu potrebnom 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 PSC-a i ako potrebne sigurnosne istrage još nisu završene, nadležno nacionalno tijelo može, ako je to dopušteno prema nacionalnim zakonima i propisima, produljiti valjanost postojećeg PSC-a za najviše 12 mjeseci. Ako na kraju razdoblja od 12 mjeseci sigurnosna istraga još nije završena, pojedincu se dodjeljuju dužnosti za koje nije potreban PSC.

Postupci povezani s PSC-om u GTV-u

17. Za dužnosnike i druge službenike GTV-a, sigurnosno tijelo GTV-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.

18. Ako GTV-u postanu poznati podaci važni za sigurnosnu istragu povezani s pojedincem koji se prijavio za EU PSC, GTV djelujući u skladu s mjerodavnim pravilima i propisima, o tome obavješćuje nadležni NSA.

19. Po završetku sigurnosne istrage, nadležni NSA obavješćuje sigurnosno tijelo GTV-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 GTV-a može izdati EU PSC predmetnom pojedincu i ovlastiti ga za pristup klasificiranim podacima EU-a do odgovarajućeg stupnja tajnosti do određenog datuma;

(b) Ako sigurnosna istraga ne rezultira takvom potvrdom, tijelo za imenovanja GTV-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 odobrava se EU PSC.

20. 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 GTV-a podliježu žalbama u skladu s Pravilnikom o osoblju za dužnosnike Europske unije i Uvjetima zaposlenja ostalih službenika Europske unije utvrđenih Uredbom (EEZ, Euratom, ECSC) br. 259/68 ([1]) (dalje u tekstu „Pravilnik o osoblju i Uvjeti zaposlenja").

21. Potvrdom na kojoj se temelji EU PSC, uz uvjet da ostane valjana, obuhvaćena su sva zaduženja predmetnog pojedinca u GTV-u ili Komisiji.

22. Ako pojedinac ne započne službu u roku od 12 mjeseci od obavijesti o ishodu sigurnosne istrage upućene tijelu za imenovanja GTV-a ili ako prekid radnog staža pojedinca traje 12 mjeseci tijekom kojih nije zaposlen u GTV-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.

23. Ako GTV-u postanu poznati podaci o sigurnosnom riziku povezanom s pojedincem koji posjeduje valjani EU PSC, GTV, djelujući u skladu s mjerodavnim pravilima i propisima, obavješćuje nadležni NSA o tome. Ako NSA obavijesti GTV o povlačenju potvrde izdane u skladu sa stavkom 19.a za pojedinca koji posjeduje valjani EU PSC, tijelo za imenovanja GTV-a može zatražiti svako objašnjenje koje NSA može dati u skladu sa svojim nacionalnim zakonima i propisima. Ako se štetni podaci potvrde, EU PSC se oduzima, a pojedincu se onemogućuje pristup klasificiranim podacima EU-a i uklanja ga se s položaja na kojem je takav pristup moguć ili na kojem bi mogao ugroziti sigurnost.

24. Obavijest o svakoj odluci o oduzimanju EU PSC-a dužnosniku GTV-a ili drugom službeniku 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 GTV-a podliježu žalbama u skladu s Pravilnikom o osoblju i Uvjetima zapošljavanja.

25. Nacionalni stručnjaci dodijeljeni GTV-u za položaj za koji je potreban EU PSC moraju prije no što preuzmu svoja zaduženja sigurnosnom tijelu GTV-a predočiti valjani nacionalni PSC za pristup klasificiranim podacima EU-a.

Evidencija PSC-a

26. Svaka država članica i GTV vodi evidenciju o nacionalnim PSC-ima i EU PSC-ima odobrenim za pristup klasificiranim podacima EU-a. Navedena evidencija mora sadržavati barem stupanj tajnosti klasificiranih podataka EU-a do kojeg se pojedincu odobrava pristup (CONFIDENTIEL UE/EU CONFIDENTIAL ili više), datum odobrenja PSC-a i njegov rok valjanosti.

27. Nadležno sigurnosno tijelo može izdati certifikat o sigurnosnoj provjeri osobe (PSCC) koji pokazuje stupanj tajnosti klasificiranih podataka EU-a do kojeg se pojedincu može odobriti pristup (CONFIDENTIEL UE/EU CONFIDENTIAL ili više), datum valjanosti odgovarajućeg nacionalnog PSC-a za pristup klasificiranim podacima EU-a ili EU PSC-a i datum isteka samog certifikata.

Izuzeci 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 odobren PSC 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 GTV, čuva evidenciju o takvoj pisanoj potvrdi prema potrebi.

30. Sve pojedince kojima je ovlašten 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.

([1]) SL L 56, 4.3.1968., str. 1.

V. IZNIMNE OKOLNOSTI

32. Ako je dopušteno prema nacionalnim zakonima i propisima, na temelju uvjerenja o sigurnosnoj provjeri osobe koje odobrava nadležno nacionalno tijelo države članice za pristup nacionalnim klasificiranim podacima nacionalnim se dužnosnicima, u ograničenom razdoblju do izdavanja nacionalnog PSC-a za pristup klasificiranim podacima EU-a, može omogućiti pristup klasificiranim podacima EU-a do jednakog stupnja tajnosti navedenog u tablici ekvivalentnosti u Dodatku B ako je takav privremeni pristup u interesu EU-a. 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 GTV-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 GTV-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 klasificiranim 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. GTV čuva evidenciju o takvim pisanim potvrdama.

34. Ako se pojedinac upućuje na položaj za koji je potreban PSC 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 zadatak;

(c) pojedinac posjeduje valjani nacionalni PSC ili EU PSC;

(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;

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

35. Gore opisani postupak koristi se za jednokratni pristup klasificiranim podacima EU-a sa stupnjem tajnosti za jedan višim od onog za koji je pojedinac prošao sigurnosnu provjeru. Ovaj 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 u svrhu spašavanja života, države članice i glavni tajnik mogu odobriti, ako je moguće u pisanom obliku, pristup podacima klasificiranim kao CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET pojedincima koji ne posjeduju potrebni PSC, 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 državljane EU-a kojima je odobren pristup nacionalnom ekvivalentu podataka sa stupnjem tajnosti TRÈS SECRET UE/EU TOP SECRET ili podacima klasificiranim 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 klasificiranim kao CONFIDENTIEL UE/EU CONFIDENTIAL ili više, mogu sudjelovati samo nakon potvrde PSC statusa pojedinca. Za izaslanike nadležna tijela prosljeđuju PSCC ili drugi dokaz o PSC-u Uredu za sigurnost GTV-a ili ga iznimno može predočiti predmetni izaslanik. Ako je to primjenljivo, može se koristiti konsolidirani popis imena s odgovarajućim dokazom o PSC-u.

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 GTV.

VII. MOGUĆI PRISTUP KLASIFICIRNIM PODACIMA EU-a

43. Kada se zapošljavaju pojedinci u okolnostima u kojima mogu imati pristup podacima klasificiranim kao CONFIDENTIEL UE/EU CONFIDENTIAL ili više, moraju proći odgovarajuću sigurnosnu provjeru i stalno imati pratnju.

44. Kuriri, zaštitari i pratnja moraju proći sigurnosnu provjeru za odgovarajuću razinu ili drugu vrstu odgovarajuće istrage u skladu s nacionalnim zakonima ili propisima, mora ih 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 KIS.

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. GTV 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 može 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 EU 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 uključivati 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 koristiti, kako bi se poboljšala razina 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, između ostalog, odvratilo pojedince koji planiraju tajni neovlašteni ulazak;

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

(f) sigurnosna rasvjeta: sigurnosna se rasvjeta može koristiti 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 PODATAK 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 se koristi 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 Odluci svako upućivanje na administrativne zone i sigurnosne zone, uključujući tehnički zaštićene sigurnosne zone, smatra se 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 kontroliraju 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;

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

16. Ako ulazak u sigurnosnu zonu praktički predstavlja izravan pristup klasificiranim podacima sadržanim u toj zoni, primjenjuju se sljedeći 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 kontroliraju u skladu s odjeljkom VI.;

(b) kontroliraju 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 uključuje 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 redovnog radnog vremena i u nasumičnim vremenskim razmacima izvan redovnog 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;

(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, a 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 prevozi klasificirane podatke EU-a u skladu sa stavcima od 28. do 40. 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. prevozi klasificirane podatke EU-a u skladu sa stavcima od 28. do 40. 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 papirnatom 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 u sigurnosnom spremniku ili 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 jednu ili više 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;

ili

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

29. Pravila kojima se uređuje prijevoz 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) pri svakoj promjeni osoblja koje zna kombinaciju;

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

(c) u slučaju popravka ili održavanja brave; i

(d) 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, kako bi se pružila pomoć u odvraćanju, otkrivanju i oporavku od 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 barem 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, budući da mu se može odrediti viši stupanj tajnosti od onog koji imaju njegovi sastavni dijelovi.

8. Ako je to moguće, dokumenti koji sadrže 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 koja uključuje privitke mora biti jednak najvišem stupnju tajnosti njezinih 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/privitaka 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;

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

Skraćene oznake stupnja tajnosti

11. Mogu se koristiti 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;

(e) dokumenti klasificirani kao SECRET UE/EU SECRET ili više moraju imati broj preslike 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. GTV redovito pregledava klasificirane podatke EU-a u svom posjedu, kako bi utvrdio primjenjuje li se još uvijek stupanj tajnosti. GTV uspostavlja sustav za pregled stupnja tajnosti upisanih klasificiranih podataka EU-a koji potječu od njega najmanje svakih 5 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 GTV-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 (dalje u tekstu „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 GTV-a čuva evidenciju o svim klasificiranim podacima koje su Vijeće i GTV objavili trećim zemljama i međunarodnim organizacijama, te o svim klasificiranim podacima primljenim od trećih zemalja ili međunarodnih organizacija.

21. U slučaju KIS-a, postupak upisa provodi se kroz procese unutar samog KIS-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 GTV-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, takve se dokumente može umnožavati ili prevoditi prema uputi imatelja.

27. Sigurnosne mjere primjenljive 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 40. 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 GTV-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 EU-a

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 klasificirani kao SECRET UE/EU SECRET prenose se unutar EU-a na jedan od sljedećih načina:

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

(b) ručno, uz sljedeće uvjete:

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

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

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

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;

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 do stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL.

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

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

Iz EU-a na državno područje treće zemlje

36. Klasificirani podaci koji se iz EU-a prenose na državno područje treće zemlje zapakirani su tako da su zaštićeni od neovlaštenog otkrivanja.

37. Podaci klasificirani kao CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET prenose se iz EU-a na državno područje treće zemlje 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.

38. Prijenos podataka klasificiranih kao CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET koje je EU objavio trećoj zemlji ili međunarodnoj organizaciji udovoljava odgovarajućim odredbama sporazuma o sigurnosti podataka ili administrativnog dogovora u skladu s člankom 12. stavkom 2. točkom (a) ili (b).

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

40. Podaci klasificirani kao TRÈS SECRET UE/EU TOP SECRET prenose se iz EU-a na državno područje treće zemlje po vojnom ili diplomatskom kuriru.

VI. UNIŠTAVANJE KLASIFICIRANIH PODATAKA EU-a

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

42. 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.

43. 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.

44. 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 5 godina.

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

46. Računalni nosači podataka koji su se koristili za klasificirane podatke EU-a uništavaju se u skladu sa stavkom 36. Priloga IV.

VII. INSPEKCIJE I POSJETI ZA PROCJENU STANJA

47. Pojam „inspekcija" koristi se dalje u tekstu za označivanje:

(a) svake inspekcije u skladu s člankom 9. stavkom 3. i člankom 15. stavkom 2. točkama (e), (f) i (g); ili

(b) svakog posjeta radi procjene stanja u skladu s člankom 12. stavkom 5.

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

48. Inspekcije se provode kako bi se, između ostalog:

(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.

49. Prije završetka svake kalendarske godine Vijeće za sljedeću godinu donosi program inspekcija predviđen u točki (c) članka 15. stavka 1. Stvarni datumi svake inspekcije određuju se u dogovoru s predmetnom agencijom ili tijelom EU-a, državom članicom, trećom zemljom ili međunarodnom organizacijom.

Provođenje inspekcija

50. Inspekcije se provode s ciljem provjere mjerodavnih pravila, propisa i postupaka u subjektu koji se pregledava te kako bi se provjerilo jesu li prakse subjekta u skladu s osnovnim načelima i minimalnim standardima utvrđenim ovom Odlukom i odredbama kojima se uređuje razmjena klasificiranih podataka s tim subjektom.

51. Inspekcije se provode u dvije faze. Prije same inspekcije organizira se, prema potrebi, pripremni sastanak s predmetnim subjektom. Nakon pripremnog sastanka inspekcijski tim, u dogovoru s navedenim subjektom, utvrđuje detaljan program inspekcije kojim su obuhvaćena sva područja sigurnosti. Inspekcijski tim ima pristup svim lokacijama na kojima se postupa s klasificiranim podacima EU-a, a posebno registrima i točkama pristupa KIS-u.

52. Inspekcije u nacionalnim administracijama država članica provode se u nadležnosti zajedničkog inspekcijskog tima GTV-a/Komisije u potpunoj suradnji s dužnosnicima subjekta koji se pregledava.

53. Inspekcije trećih zemalja i međunarodnih organizacija provode se u nadležnosti zajedničkog inspekcijskog tima GTV-a/Komisije u potpunoj suradnji s dužnosnicima treće zemlje ili međunarodne organizacije koja se pregledava.

54. Inspekcije agencija i tijela EU-a uspostavljenih na temelju glave V. poglavlja 2. UEU-a, kao i Europola i Eurojusta, provodi Ured za sigurnost GTV-a uz pomoć stručnjaka NSA-a na čijem se državnom području agencija ili tijelo nalazi. Može se uključiti Uprava za sigurnost Europske komisije (ECSD) ako redovito razmjenjuje klasificirane podatke EU-a s predmetnom agencijom ili tijelom.

55. Za inspekcije agencija i tijela EU-a uspostavljenih na temelju glave V. poglavlja 2. UEU-a, kao i Europola i Eurojusta te trećih zemalja i međunarodnih organizacija, traži se pomoć i doprinos stručnjaka NSA-a u skladu s detaljnim rješenjima koje je dogovorio Sigurnosni odbor.

Izvješća o inspekcijama

56. Na kraju inspekcije pregledanom se subjektu predstavljaju glavni zaključci i preporuke. Nakon toga sigurnosno tijelo GTV-a (Ured za sigurnost) odgovorno je za sastavljanje izvješća o inspekciji. Ako su predložene korektivne mjere i preporuke, doneseni se zaključci moraju dovoljno detaljno potkrijepiti u izvješću. Izvješće se prosljeđuje odgovarajućem tijelu pregledanog subjekta.

57. Za inspekcije provedene u nacionalnim administracijama država članica:

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

(b) osim ako predmetni NSA države članice na zabrani opću distribuciju, izvješće o inspekciji prosljeđuje se članovima Sigurnosnog odbora i ECSD-u; izvješće je klasificirano kao RESTREINT UE/EU RESTRICTED;

Sigurnosno tijelo GTV-a (Ured za sigurnost) odgovorno je za pripremu redovitog izvješća u kojem se ističu lekcije naučene iz inspekcija provedenih u državama članicama u određenom razdoblju i koje pregledava Sigurnosni odbor.

58. Izvješće o posjetima trećim zemljama i međunarodnim organizacijama za procjenu stanja distribuira se Sigurnosnom odboru i ECSD-u. Izvješće je klasificirano najmanje kao RESTREINT UE/EU RESTRICTED. Sve korektivne radnje provjeravaju se tijekom sljedećeg posjeta te se o njima izvješćuje Sigurnosni odbor.

59. Izvješća o inspekcijama agencija i tijela EU-a uspostavljenih na temelju glave V. poglavlja 2. UEU-a, kao i Europola i Eurojusta, distribuiraju se članovim Sigurnosnog odbora i ECSD-u. Nacrt izvješća o inspekcijama 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.

60. Sigurnosno tijelo GTV-a provodi redovite inspekcije organizacijskih subjekata GTV-a u svrhe utvrđene u stavku 48.

Inspekcijska kontrolna lista

61. Sigurnosno tijelo GTV-a (Ured za sigurnost) sastavlja i ažurira sigurnosnu inspekcijsku kontrolnu listu stavki koje se provjeravaju tijekom inspekcije. Kontrolna se lista prosljeđuje Sigurnosnom odboru.

62. Podaci za popunjavanje kontrolnih lista dobivaju se tijekom inspekcije posebno od rukovodstva za sigurnost pregledanog subjekta. Nakon što je popunjena detaljnim 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 KIS-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 KIS-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 kasnije nije moguće zanijekati.

II. NAČELA INFORMACIJSKE SIGURNOSTI

3. Odredbe navedene u nastavku čine osnovu sigurnosti svakog KIS-a u kojem se postupa s klasificiranim podacima EU-a. Detaljni 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 KIS-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 KIS-a i njegovih sastavnih dijelova mora biti jasno određeno od samog početka procesa procjene rizika.

5. Nadležna tijela pregledavaju moguće prijetnje KIS-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 detalja koje je odredio nadležni SAA za akreditaciju KIS-a razmjerni su procijenjenom riziku, uzimajući u obzir važne čimbenike, uključujući stupanj tajnosti klasificiranih podataka EU-a s kojima se postupa u KIS-u. Akreditacija uključuje službenu izjavu o preostalom riziku koju daje odgovorno tijelo i time prihvaća preostali rizik.

Sigurnost tijekom životnog ciklusa KIS-a

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

9. Uloga i međudjelovanje svakog činioca uključenog u KIS u pogledu njegove sigurnosti određuju se za svaku fazu životnog ciklusa.

10. Svaki KIS, 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 KIS-a i ako nastupe izvanredne okolnosti.

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

Najbolja praksa

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

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

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

Dubinska obrana

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

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

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

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

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

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

Stupanj strogoće takvih sigurnosnih mjera određuje se nakon procjene rizika.

17. Nadležna tijela osiguravaju mogućnost odgovaranja na incidente koji mogu prelaziti organizacijske i državne granice s ciljem koordinacije odgovora i razmjene podataka o navedenim incidentima i povezanim rizicima (sposobnost odgovora na izvanredne situacije u području računarstva).

Načelo minimalnosti i najmanjih povlastica

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

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

20. Postupci upisa koje provodi KIS 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 KIS-a. Cjelokupno osoblje uključeno u životni ciklus KIS-a, uključujući imatelje, mora posebno razumjeti:

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

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

(c) svoju osobnu obveznost i odgovornost za sigurnost KIS-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 KIS-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 priznatih ili nacionalno odobrenih procesa i metodologija. Navedeno prvenstveno uključuje ocjenjivanje, kontrole i reviziju.

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

26. Prije no što ih se preporuči 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. i dati privremeno odobrenje za određeno razdoblje u skladu s postupkom utvrđenim u članku 10. stavku 6.

28. 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.

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

Slanje unutar sigurnosnih zona

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

Sigurno međusobno povezivanje KIS-a

31. 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.

32. KIS sa svim međusobno povezanim IT sustavima postupa kao da su nepouzdani i provodi mjere zaštite s ciljem kontrole razmjene klasificiranih podataka.

33. Za svako međusobno povezivanje KIS-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 KIS-a provode se usluge zaštite granice (BPS).

34. Nema međusobnog povezivanja između akreditiranog KIS-a i nezaštićene ili javne mreže, osim ako KIS ima odobreni BPS instaliran u tu svrhu između KIS-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 koristi isključivo za prijenos i ako su podaci kodirani pomoću kriptografskog proizvoda odobrenog u skladu s člankom 10., takvo se povezivanje ne smatra međusobnim povezivanjem.

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

Mediji za pohranu podataka

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

37. Mediji za pohranu podataka ponovno se koriste, njihov se stupanj tajnosti smanjuje ili se deklasificiraju u skladu sa sigurnosnom politikom koja se utvrđuje u skladu s člankom 6. stavkom 1.

Izvanredne okolnosti

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

39. 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.

40. Klasificirani podaci preneseni u okolnostima navedenim u stavku 38. 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.

41. Ako se primjenjuje stavak 38., nadležnom se tijelu i Sigurnosnom odboru podnosi naknadno izvješće.

III. FUNKCIJE I NADLEŽNA TIJELA ZA INFORMACIJSKU SIGURNOST

42. U državama članicama i GTV-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.

Tijelo za informacijsku sigurnost

43. 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.

Tijelo za TEMPEST

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

Tijelo za odobravanje kriptomaterijala

45. 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.

Tijelo za distribuciju kriptomaterijala

46. 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;

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

Tijelo za sigurnosnu akreditaciju

47. Za svaki je sustav SAA odgovoran za:

(a) osiguravanje usklađenosti KIS-a s mjerodavnim sigurnosnim politikama i sigurnosnim smjernicama, davanje izjave o odobrenju za KIS 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 KIS 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 (dalje u tekstu „SSRS”), dokumentaciju o provjeri provedbe sigurnosti i sigurnosno-operativne postupke (dalje u tekstu „SecOP”), i osiguravanje njegove usklađenosti sa sigurnosnim propisima i politikama Vijeća;

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

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

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

(h) odobravanje, ili prema potrebi, sudjelovanje u zajedničkom odobravanju međusobnog povezivanja KIS-a s drugim KIS-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.

48. SAA GTV-a odgovoran je za akreditaciju svih KIS-a koji rade u nadležnosti GTV-a.

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

50. Zajednički odbor za sigurnosnu akreditaciju (SAB) odgovoran je za akreditaciju KIS-a u nadležnosti tijela za sigurnosnu akreditaciju GTV-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 KIS-u pozivaju se na sudjelovanje kada se raspravlja o navedenom sustavu.

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

Operativno tijelo za informacijsku sigurnost

51. 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 i plan kriptomaterijala u okviru procesa akreditacije KIS-a;

(b) sudjelovanje u odabiru i ispitivanju tehničkih sigurnosnih mjera za specifični sustav, uređaja i softvera s ciljem nadziranja 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 je potrebno 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 KIS;

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

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 GTV.

2. Vijeće odobrava politiku o gospodarskoj sigurnosti kojom se posebno detaljno opisuju zahtjevi povezani s FSC-ima, pismima o sigurnosnim aspektima (SAL), 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, GTV 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 GTV 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 GTV 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) prema potrebi, GTV 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 predstavljati dovoljan razlog za prekid ugovora.

Sigurnosni naputak 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 sigurnosni naputak za program/projekt (PSI). PSI zahtijeva odobrenje NSA-a/DSA-a države članice ili bilo kojeg drugog nadležnog sigurnosnog tijela koje sudjeluje u programu/projektu 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 GTV-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 utvrđenim 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;

(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. Prema potrebi, GTV, kao tijelo za ugovaranje, obavješćuje odgovarajući NSA/DSA ili bilo koje 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 bilo kojeg 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 bilo koje drugo nadležno sigurnosno tijelo koje je izdalo FSC obavješćuje GTV 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 bilo koje drugo nadležno sigurnosno tijelo ukine FSC, GTV kao tijelo za ugovaranje ima dovoljan razlog za prekid 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, GTV, kao tijelo za ugovaranje, obavješćuje NSA/DSA ili bilo koje drugo nadležno sigurnosno tijelo ugovaratelja ili podugovaratelja o sigurnosnim odredbama klasificiranog ugovora.

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

17. U pravilu se od ugovaratelja ili podugovaratelja zahtijeva da po prestanku klasificiranog ugovora ili podugovora tijelu za ugovaranje vrati sve klasificirane podatke EU-a u njegovu 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 GTV-a, kao tijela za ugovaranje, pribaviti dopuštenje prije podugovaranja bilo kojeg dijela klasificiranog ugovora. Ne može se sklopiti podugovor s gospodarskim ili drugim subjektima registriranim u državi koja nije članica EU-a i koja nije sklopila sporazum o sigurnosti podataka s EU-om.

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 GTV, ugovaratelji ili podugovaratelji trebaju pristup podacima klasificiranim 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 bilo kojim 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 GTV-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;

(f) kadgod je to moguće, rute trebaju prolaziti samo kroz države članice. Rute mogu 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 ZEMLJAMA

30. Klasificirani se podaci EU-a prenose ugovarateljima i podugovarateljima smještenim u trećim zemljama u skladu sa sigurnosnim mjerama dogovorenim između GTV-a, kao tijela za ugovaranje, i NSA-a/DSA-a predmetne treće zemlje u kojoj je ugovaratelj registriran.

VIII. POSTUPANJE S PODACIMA KLASIFICIRANIM KAO RESTREINT UE/EU RESTRICTED I NJIHOVO ČUVANJE

31. GTV kao tijelo za ugovaranje prema potrebi ima pravo, u suradnji s NSA-om/DSA-om države članice, obavljati posjete objektima 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, GTV, kao tijelo za ugovaranje, obavješćuje NSA/DSA 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 GTV-om koji sadrže podatke klasificirane kao RESTREINT UE/EU RESTRICTED.

34. GTV, kao tijelo za ugovaranje, ispituje odgovore na poziv za sudjelovanje u natječaju za ugovore koji zahtijevaju pristup podacima klasificiranim 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 klasificiranim kao RESTREINT UE/EU RESTRICTED u KIS-u kojim upravlja ugovaratelj, GTV, kao tijelo za ugovaranje, osigurava da su u ugovoru ili svakom podugovoru navedeni neophodni tehnički i upravni zahtjevi u pogledu akreditacije KIS-a razmjerni procijenjenom riziku, uzimajući u obzir sve važne čimbenike. Tijelo za ugovaranje i nadležni NSA/DSA dogovaraju područje primjene akreditacije takvog KIS-a.

PRILOG VI.

RAZMJENA KLASIFICIRANIH PODATAKA S TREĆIM ZEMLJAMA I MEĐUNARODNIM ORGANIZACIJAMA

I. UVOD

1. U ovom se Prilogu određuju odredbe za provedbu članka 12.

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 12. stavkom 2. i odjeljcima III. i IV. na temelju preporuke Sigurnosnog odbora.

3. Ako se klasificirani podaci EU-a izrađeni za potrebe operacije ZSOP-a dostavljaju trećim zemljama 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 zemlji ili međunarodnoj organizaciji iznimno i *ad hoc* u skladu s odjeljkom VI., od predmetne se treće zemlje ili međunarodne organizacije traže pisana jamstva kojima se osigurava zaštita svih klasificiranih podataka EU-a objavljenih trećoj zemlji 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 EU-a i treće zemlje ili međunarodne organizacije.

6. Sporazumima o sigurnosti podataka predviđena je tehnička organizacija provedbe koju dogovaraju Ured za sigurnost GTV-a, ECSD i nadležno sigurnosno tijelo predmetne treće zemlje ili međunarodne organizacije. Pri takvoj se organizaciji uzima u obzir razina zaštite predviđena sigurnosnim propisima, strukturama i postupcima uspostavljenim u predmetnoj trećoj zemlji ili međunarodnoj organizaciji. Organizaciju provedbe odobrava Sigurnosni odbor.

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

8. Sporazumima o sigurnosti podataka predviđeno je da se prije razmjene klasificiranih podataka prema sporazumu Ured za sigurnost GTV-a i ECSD suglase da stranka primateljica može na odgovarajući način zaštititi i čuvati dostavljene joj podatke.

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

10. Kako bi se ocijenila učinkovitost sigurnosnih propisa, struktura i postupaka u predmetnoj trećoj zemlji ili međunarodnoj organizaciji, Ured za sigurnost GTV-a zajedno s ECSD-om i u međusobnom dogovoru s predmetnom državom članicom ili međunarodnom organizacijom organizira posjete za procjenu stanja. Takvi posjeti za procjenu 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 načina na koji je sigurnost organizirana u trećoj zemlji 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.

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

12. 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.

13. Mora se učiniti sve kako bi se organizirao posjet predmetnoj trećoj zemlji 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 GTV-a na temelju raspoloživih podataka, kojim se Sigurnosni odbor obavješćuje o primjenljivim sigurnosnim propisima i načinu na koji je sigurnost organizirana u predmetnoj trećoj zemlji ili međunarodnoj organizaciji.

14. Sigurnosni odbor može odlučiti da se do ispitivanja ishoda posjeta za procjenu stanja ne objavljuju nikakvi klasificirani podaci EU-a ili da se mogu objavljivati podaci do određenog stupnja tajnosti ili može utvrditi druge posebne uvjete kojima se uređuje objavljivanje klasificiranih podataka EU-a predmetnoj trećoj zemlji ili međunarodnoj organizaciji. Ured za sigurnost GTV-a o tome obavješćuje predmetnu treću zemlju ili međunarodnu organizaciju.

15. U međusobnom dogovoru s predmetnom trećom zemljom ili međunarodnom organizacijom, Ured za sigurnost GTV-a u pravilnim vremenski razmacima provodi prateći posjet radi procjene stanja, kako bi provjerio ispunjavaju li uspostavljene mjere i dalje dogovorene minimalne standarde.

16. Nakon stupanja sporazuma o sigurnosti podataka na snagu i nakon razmjene podataka s predmetnom trećom zemljom 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 zemljom 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, sklopiti administrativni dogovor s nadležnim tijelima predmetne treće zemlje 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 predmetnoj trećoj zemlji ili međunarodnoj organizaciji provodi se posjet za procjenu stanja iz stavka 10. i prosljeđuje se izvješće Sigurnosnom odboru za koje on mora utvrditi da je zadovoljavajuće. Međutim, ako postoje iznimni razlozi za hitnu razmjenu klasificiranih podataka te ako je Vijeću skrenuta pozornost na njih, klasificirani se podaci EU-a mogu objaviti uz uvjet da je učinjeno sve kako bi se takav posjet radi procjene stanja proveo što je prije moguće.

21. Nijedan klasificirani podatak EU-a ne smije se razmjenjivati elektroničkim sredstvima, osim ako je tako izričito navedeno u administrativnom 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 zemljama 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 misije 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 uključuju odredbe o objavi klasificiranih podataka EU-a izrađenih za potrebe navedene operacije trećoj zemlji 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. *Ad hoc* administrativni dogovori o sudjelovanju treće zemlje ili međunarodne organizacije u određenoj operaciji ZSOP-a mogu obuhvaćati, između ostalog, objavu klasificiranih podataka EU-a izrađenih za potrebe operacije navedenoj trećoj zemlji ili međunarodnoj organizaciji. Takvi se *ad hoc* administrativni dogovori sklapaju u skladu s postupcima navedenim u stavcima 17. i 18. odjeljka IV. 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. 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.

26. Ako država domaćin na čijem se državnom području provodi operacija ZSOP-a nema na snazi sporazum o sigurnosti podataka ili administrativni dogovor s EU-om za razmjenu klasificiranih podataka, u slučaju posebne ili neodgodive operativne potrebe može se uspostaviti *ad hoc* administrativni dogovor. 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. U okviru takvog *ad hoc* administrativnog dogovora država domaćin obvezuje se zaštiti klasificirane podatke EU-a u skladu s minimalnim standardima koji nisu ništa manje strogi od standarda utvrđenih ovom Odlukom.

27. 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 zemlja ili međunarodna organizacija osigurava da će njezino osoblje dodijeljeno 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.

28. Ako EU i sudjelujuća treća zemlja ili međunarodna organizacija naknadno sklope sporazum o sigurnosti podataka, sporazum o sigurnosti podataka zamjenjuje svaki okvirni sporazum o sudjelovanju, *ad hoc* sporazum o sudjelovanju ili *ad hoc* administrativni dogovor u pogledu razmjene klasificiranih podataka EU-a i postupanja s njima.

29. 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 zemljom ili međunarodnom organizacijom, osim ako je izričito navedeno u predmetnom sporazumu ili dogovoru.

30. Klasificirani podaci EU-a izrađeni za potrebe operacije ZSOP-a mogu se otkriti osoblju koje je treća zemlja ili međunarodna organizacija dodijelila predmetnoj operaciji u skladu sa stavcima od 22. do 29. Kada se takvo osoblje ovlašćuje za pristup klasificiranim podacima EU-a u prostorijama ili KIS-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.

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

31. 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 zemlji ili međunarodnoj organizaciji, GTV:

(a) provjerava, u mjeri u kojoj je to moguće, kod sigurnosnih tijela predmetne treće zemlje 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;

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

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

33. 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 COREPER-a;

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

34. 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.

35. Nakon odluke o objavljivanju klasificiranih podataka EU-a, GTV prosljeđuje predmetni dokument s oznakom mogućnosti objavljivanja na kojoj je navedena treća zemlja 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 navedenim u ovoj Odluci.

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

36. Ako postoji okvir u skladu sa stavkom 2. za razmjenu klasificiranih podataka s trećom zemljom ili međunarodnom organizacijom, Vijeće donosi odluku kojom ovlašćuje glavnog tajnika za objavljivanje klasificiranih podataka EU-a, u skladu s načelom suglasnosti onog od kojeg podaci potječu, predmetnoj trećoj zemlji ili međunarodnoj organizaciji.

37. Ako postoji okvir u skladu sa stavkom 3. za razmjenu klasificiranih podataka s trećom zemljom ili međunarodnom organizacijom, glavni se tajnik 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.

38. Glavni tajnik može delegirati takva ovlaštenja na više dužnosnike GTV-a ili druge osobe pod njegovom nadležnošću.

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 svom 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,

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

„klasificirani ugovor” znači ugovor sklopljen između GTV-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 GTV-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” (KIS) – vidjeti članak 10. stavak 2.,

„ugovaratelj” znači pojedinac ili pravni subjekt koji ima pravnu sposobnost za ugovorno obvezivanje,

„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,

„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) 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 karakteristike,

„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 administrativno utvrđivanje koje provodi NSA ili DSA da, sa stajališta sigurnosti, pravna osoba može pružiti odgovarajuću razinu zaštite klasificiranim podacima EU-a određenog stupnja tajnosti te da je njezino osoblje koje traži pristup klasificiranim podacima EU-a prošlo odgovarajuću sigurnosnu provjeru i da je upućeno u odgovarajuće sigurnosne zahtjeve potrebne za pristup klasificiranim podacima EU-a i njihovu zaštitu,

„postupanje” s klasificiranim podacima EU-a znači sve moguće radnje kojima klasificirani podaci EU-a mogu biti izloženi tijekom svog životnog ciklusa. Ono obuhvaća njihovo stvaranje, obradu, prijenos, smanjenje stupnja tajnosti, deklasificiranje i uništavanje. U pogledu KIS-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 31.,

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

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

„onaj od kojeg podaci potječu” znači institucija, agencija ili tijelo EU-a, država članica, treća zemlja ili međunarodna organizacija u čijoj su nadležnosti stvoreni i/ili u strukture EU-a uvedeni klasificirani podaci,

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

„uvjerenje o sigurnosnoj provjeri osobe” (PSC) znači jedno ili oboje od sljedećeg:

— „uvjerenje EU-a o sigurnosnoj provjeri osobe” (EU PSC) za pristup klasificiranim podacima EU-a znači ovlaštenje tijela za imenovanja GTV-a koje je doneseno u skladu s ovom Odlukom nakon završetka sigurnosne istrage koju provode nadležna tijela države članice i kojim se potvrđuje da se pojedincu može, uz uvjet da je za njega utvrđena nužnost pristupa podacima, odobriti pristup klasificiranim podacima EU-a do određenog stupnja tajnosti (CONFIDENTIEL UE/EU CONFIDENTIAL ili više) do određenog datuma; za tako opisanog pojedinca kaže se da je „prošao sigurnosnu provjeru”,

— „nacionalno uvjerenje o sigurnosnoj provjeri osobe” (nacionalni PSC) za pristup klasificiranim podacima EU-a znači izjavu nadležnog tijela države članice koja je sačinjena nakon završetka sigurnosne istrage koju provode nadležna tijela države članice i kojom se potvrđuje da se pojedincu može, uz uvjet da je za njega utvrđena nužnost pristupa podacima, odobriti pristup klasificiranim podacima EU-a do određenog stupnja tajnosti (CONFIDENTIEL UE/EU CONFIDENTIAL ili više) do određenog datuma; za tako opisanog pojedinca kaže se da je „prošao sigurnosnu provjeru”,

„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 nacionalni ili EU PSC te koji pokazuje stupanj tajnosti klasificiranih podataka EU-a do kojeg se pojedincu može odobriti pristup (CONFIDENTIEL UE/EU CONFIDENTIAL ili više), 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” je 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 KIS-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 nacionalni ili EU PSC za pristup klasificiranim podacima EU-a do određenog stupnja tajnosti (CONFIDENTIEL UE/EU CONFIDENTIAL ili više),

„sigurnosni način rada” znači definiranje uvjeta pod kojima KIS 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 KIS-u prošli sigurnosnu provjeru za najviši stupanj tajnosti podataka s kojima se postupa u KIS-u i s općom nužnošću pristupa podacima za sve podatke koji se obrađuju u KIS-u,

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

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

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

„proces upravljanja sigurnosnim rizicima” znači cjelokupni proces prepoznavanja, kontrole i smanjenja nesigurnih događaja koji mogu utjecati na sigurnost organizacije ili bilo kojeg od sustava koje organizacija koristi. Njime su obuhvaćene sve aktivnosti povezane s rizicima, uključujući procjenu, postupanje, prihvaćanje i obavješćivanje,

„TEMPEST” znači istraživanje, proučavanje i kontrola štetnog elektromagnetskog zračenja i mjere za njegovo suzbijanje,

„prijetnja” znači mogući uzrok neželjenog incidenta koji može rezultirati štetom za organizaciju ili bilo koji 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 prirode.

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) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	Napomena [1] dolje
Bugarska	Строго секретно	Секретно	Поверително	За служебно ползване
Češka Republika	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 Kratica: ΑΑΠ	Απόρρητο Kratica: (ΑΠ)	Εμπιστευτικό Kratica: (ΕΜ)	Περιορισμένης Χρήσης Kratica: (ΠΧ)
Španjolska	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Francuska	Très Secret Défense	Secret Défense	Confidentiel Défense	Napomena [3] dolje
Italija	Segretissimo	Segreto	Riservatissimo	Riservato
Cipar	Άκρως Απόρρητο Kratica: (ΑΑΠ)	Απόρρητο Kratica: (ΑΠ)	Εμπιστευτικό Kratica: (ΕΜ)	Περιορισμένης Χρήσης Kratica: (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	Sigriet	Kunfidenzjali	Ristrett
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
Rumunjska	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu

EU	TRÈS SECRET UE/ EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Slovenija	Strogo tajno	Tajno	Zaupno	Interno
Slovačka	Prísne tajné	Tajné	Dôverné	Vyhradené
Finska	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Švedska ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Ujedinjena Kraljevina	Top Secret	Secret	Confidential	Restricted

([1]) Diffusion Restreinte/Beperkte Verspreiding nije stupanj tajnosti u Belgiji. Belgija postupa s podacima klasificiranim 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 svom nacionalnom sustavu ne koristi stupanj tajnosti „RESTREINT". Francuska postupa s podacima klasificiranim 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]) Švedska: oznake stupnjeva tajnosti u gornjem redu koriste obrambena tijela, dok oznake u donjem redu koriste 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
Faks: +32 25014596
E-pošta: nvo-ans@diplobel.fed.be

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

Tel.: +45 33148888
Faks: +45 33430190

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

Tel.: +45 33325566
Faks: +45 33931320

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

Tel.: +359 29215911
Faks: +359 29873750
E-pošta: dksi@government.bg
Web stranica: www.dksi.bg

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

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

ČEŠKA REPUBLIKA
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56

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

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

Tel.: +372 7170113, +372 7170117
Faks: +372 7170213
E-pošta: nsa@kmin.ee

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

Tel.: +353 14780822
Faks: +353 14082959

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

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

GRČKA
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
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)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos – Athens

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

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 Paris 07 SP

Tel.: +33 171758177
Faks: + 33 171758200

ITALIJA
Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
D.I.S. - U.C.Se.
Via di Santa Susanna, 15
00187 Roma

Tel.: +39 0661174266
Faks: +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
Faks: +357 22302351
E-pošta: cynsa@mod.gov.cy

LUKSEMBURG
Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg

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

MAĐARSKA
Nemzeti Biztonsági Felügyelet
(National Security Authority)
P.O. Box 2
1357 Budapest

Tel.: +361 3469652
Faks: +361 3469658
E-pošta: nbf@nbf.hu
Web stranica: www.nbf.hu

MALTA
Ministry of Justice and Home Affairs
P.O. Box 146
MT-Valletta

Tel.: +356 21249844
Faks: +356 25695321

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

Tel.: +371 67025418
Faks: +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 52663201, +370 52663202
Faks: +370 52663200
E-pošta: nsa@vsd.lt

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

Tel.: +31 703204400
Faks: +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag

Tel.: +31 703187060
Faks: +31 703187522

AUSTRIJA
Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien

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

POLJSKA
Agencja Bezpieczeństwa Wewnętrznego – ABW
(Internal Security Agency)
2A Rakowiecka St.
00-993 Warszawa

Tel.: +48 225857360
Faks: +48 225858509
E-pošta: nsa@abw.gov.pl
Web stranica: www.abw.gov.pl

Służba Kontrwywiadu Wojskowego
(Military Counter-Intelligence Service)
Classified Information Protection Bureau
Oczki 1
02-007 Warszawa

Tel.: +48 226841247
Faks: +48 226841076
E-pošta: skw@skw.gov.pl

RUMUNJSKA
Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA – ORNISS
National Registry Office for Classified Information)
4 Mures Street
012275 Bucharest

Tel.: +40 212245830
Faks: +40 212240714
E-pošta: nsa.romania@nsa.ro
Web stranica: www.orniss.ro

PORTUGAL
Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa

Tel.: +351 213031710
Faks: +351 213031711

SLOVENIJA
Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana

Tel.: +386 14781390
Faks: +386 14781399

SLOVAČKA

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava

Tel.: +421 268692314
Faks: +421 263824005
Web stranica: www.nbusr.sk

ŠVEDSKA
Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
S-103 39 Stockholm

Tel.: +46 84051000
Faks: +46 87231176
E-pošta: ud-nsa@foreign.ministry.se

FINSKA
National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government

Tel. 1: +358 916056487
Tel. 2: +358 916056484
Faks: +358 916055140
E-pošta: NSA@formin.fi

UJEDINJENA KRALJEVINA
UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS

Tel. 1: +44 2072765649
Tel. 2: +44 2072765497
Faks: +44 2072765651
E-pošta: UK-NSA@cabinet-office.x.gsi.gov.uk

Dodatak D

POPIS KRATICA

Akronim	Značenje
AQUA	Appropriately Qualified Authority (odgovarajuće kvalificirano tijelo)
BPS	Boundary Protection Services (usluge zaštite granice)
CAA	Crypto Approval Authority (tijelo za odobravanje kriptomaterijala)
CCTV	Closed Circuit Television (televizija zatvorenog kruga)
CDA	Crypto Distribution Authority (tijelo za distribuciju kriptomaterijala)
CFSP	Common Foreign and Security Policy (zajednička vanjska i sigurnosna politika (ZVSP))
CIS	Communication and Information Systems handling EUCI (komunikacijski i informacijski sustavi za postupanje s klasificiranim podacima EU-a (KIS))
COREPER	Committee of Permanent Representatives (Odbor stalnih predstavnika)
CSDP	Common Security and Defence Policy (zajednička sigurnosna i obrambena politika (ZSOP))
DSA	Designated Security Authority (zaduženo sigurnosno tijelo)
ECSD	European Commission Security Directorate (Uprava za sigurnost Europske unije)
EUCI	EU Classified Information (klasificirani podaci EU-a)
EUSR	EU Special Representative (posebni predstavnik EU-a)
FSC	Facility Security Clearance (uvjerenje o sigurnosnoj provjeri pravne osobe)
GSC	General Secretariat of the Council (Glavno tajništvo Vijeća (GTV))
IA	Information Assurance (informacijska sigurnost)
IAA	Information Assurance Authority (tijelo za informacijsku sigurnosti)
IDS	Intrusion Detection System (sustav za otkrivanje neovlaštenog ulaska)
IT	Information Technology (informacijske tehnologije)
NSA	National Security Authority (nacionalno sigurnosno tijelo)
PSC	Personnel Security Clearance (uvjerenje o sigurnosnoj provjeri osobe)
PSCC	Personnel Security Clearance Certificate (certifikat o sigurnosnoj provjeri osobe)
PSI	Programme/Project Security Instructions (sigurnosni naputak za program/ projekt)
SAA	Security Accreditation Authority (tijelo za sigurnosnu akreditaciju)
SAB	Security Accreditation Board (odbor za sigurnosnu akreditaciju)
SAL	Security Aspects Letter (pismo o sigurnosnim aspektima)
SecOPs	Security Operating Procedures (sigurnosno-operativni postupci)
SCG	Security Classification Guide (vodič za stupnjeve tajnosti)
SSRS	System-Specific Security Requirement Statement (izjava o sigurnosnim zahtjevima za specifični sustav)
TA	TEMPEST Authority (tijelo za TEMPEST)