ODLUKA KOMISIJE (EU, Euratom) 2015/444

od 13. ožujka 2015.

o sigurnosnim propisima za zaštitu klasificiranih podataka EU-a

EUROPSKA KOMISIJA,

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

uzimajući u obzir Ugovor o Europskoj zajednici za atomsku energiju, a posebno njegov članak 106.,

uzimajući u obzir Protokol br. 7 o povlasticama i imunitetima Europske unije, koji je priložen Ugovorima, a posebno njegov članak 18.,

budući da:

(1) Komisijine sigurnosne odredbe koje se odnose na zaštitu klasificiranih podataka Europske unije moraju se pregledati i ažurirati uzimajući u obzir institucijski, organizacijski, operativni i tehnološki razvoj.

(2) Europska komisija sklopila je s vladama Belgije, Luksemburga i Italije ([1]) sporazume o sigurnosnim pitanjima koja se odnose na njezine glavne zgrade.

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

(4) Važno je da se načelima, standardima i pravilima za zaštitu klasificiranih podataka nužnih za zaštitu interesa Unije i njezinih država članica, prema potrebi, pridruže Europski parlament i druge institucije, agencije, tijela ili uredi Unije.

(5) 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 iz ove Odluke te primjena navedenih mjera u skladu s konceptom dubinske obrane. Djelotvornost tih mjera kontinuirano se ocjenjuje.

(6) Fizička sigurnost, čiji je cilj zaštita klasificiranih podataka, u okviru Komisije znači primjenu fizičkih i tehničkih zaštitnih mjera za sprečavanje neovlaštenog pristupa klasificiranim podacima EU-a.

(7) Upravljanje klasificiranim podacima EU-a primjena je administrativnih mjera za kontrolu klasificiranih podataka EU-a tijekom njihova životnog ciklusa kojima se dopunjuju mjere iz poglavlja 2., 3. i 5. ove Odluke i pri tome pomaže pri odvraćanju od namjerne ili slučajne ugroze ili gubitka takvih podataka, te otkrivanju takvih događaja i oporavku od njih. Te se mjere odnose posebice na stvaranje, čuvanje, registraciju, umnožavanje, prevođenje, smanjenje stupnja tajnosti, deklasifikaciju, prijenos i uništavanje klasificiranih podataka EU-a te se njima nadopunjuju opća pravila o upravljanju dokumentima Komisije (odluke 2002/47/EZ ([2]), EZUČ, Euratom i 2004/563/EZ, Euratom ([3])).

([1]) Usp. „Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité" od 31. prosinca 2004., „Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois" od 20. siječnja 2007. i „Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale" od 22. srpnja 1959.

([2]) Odluka Komisije 2002/47/EZ, EZUČ, Euratom od 23. siječnja 2002. o izmjeni njezinog Poslovnika (SL L 21, 24.1.2002., str. 23.).

([3]) Odluka Komisije 2004/563/EZ, Euratom od 7. srpnja 2004. o izmjeni njezina Poslovnika (SL L 251, 27.7.2004., str. 9.).

(8) Odredbe ove Odluke ne dovode u pitanje:

(a) Uredbu (Euratom) br. 3 ([1]);

(b) Uredbu (EZ) br. 1049/2001 Europskog parlamenta i Vijeća ([2]);

(c) Uredbu (EZ) br. 45/2001 Europskog parlamenta i Vijeća ([3]);

(d) Uredbu Vijeća (EEZ, Euratom) br. 354/83 ([4]),

DONIJELA JE OVU ODLUKU:

POGLAVLJE 1.

OSNOVNA NAČELA I MINIMALNI STANDARDI

Članak 1.

Definicije

Za potrebe ove Odluke primjenjuju se sljedeće definicije:

1. „služba Komisije” znači glavna uprava ili služba Komisije ili kabinet člana Komisije;

2. „kriptografski materijal (kriptomaterijal)” znači kriptografski algoritmi, kriptografski hardverski i softverski moduli i proizvodi, uključujući detalje o provedbi te povezanu dokumentaciju i kriptografske ključeve;

3. „deklasifikacija” znači uklanjanje svakog stupnja tajnosti;

4. „dubinska obrana” znači primjena niza sigurnosnih mjera koje su organizirane kao višestruki slojevi obrane;

5. „dokument” znači svaki zapis podataka bez obzira na njegov fizički oblik ili značajke;

6. „smanjenje stupnja tajnosti” znači smanjenje razine stupnja tajnosti;

7. „postupanje” s klasificiranim podacima EU-a znači sve radnje kojima klasificirani podaci EU-a mogu biti izloženi tijekom svojeg životnog ciklusa. Obuhvaća njihovo stvaranje, registraciju, obradu, prijenos, smanjenje stupnja tajnosti, deklasifikaciju i uništavanje. Kada je riječ o komunikacijskim i informacijskim sustavima (CIS), ono obuhvaća i njihovo prikupljanje, prikaz, slanje i čuvanje;

8. „imatelj” znači propisno ovlaštena osoba s utvrđenom nužnošću pristupa podacima koja je u posjedu klasificiranog podatka EU-a te je, prema tome, odgovorna za njegovu zaštitu;

9. „provedbena pravila” znači svaki skup pravila ili sigurnosnih obavijesti donesenih u skladu s Poglavljem 5. Odluke Komisije (EU, Euratom) 2015/443 ([5]);

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

11. „autor podatka” znači institucija, agencija ili tijelo Unije, država članica, treća država ili međunarodna organizacija pod čijom su nadležnošću stvoreni i/ili u strukture Unije uvedeni klasificirani podaci;

12. „prostori” znači sva nepokretna i slična imovina u vlasništvu ili posjedu Komisije;

([1]) Uredba (Euratom) br. 3 od 31. srpnja 1958. o provedbi članka 24. Ugovora o Europskoj zajednici za atomsku energiju (SL 17, 6.10.1958., str. 406/58.).
([2]) Uredba (EZ) br. 1049/2001 Europskog parlamenta i Vijeća od 30. svibnja 2001. o javnom pristupu dokumentima Europskog parlamenta, Vijeća i Komisije (SL L 145, 31.5.2001., str. 43.).
([3]) Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti osoba u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka (SL L 8, 12.1.2001., str. 1.).
([4]) Uredba Vijeća (EEZ, Euratom) br. 354/83 od 1. veljače 1983. o otvaranju za javnost povijesnih arhiva Europske ekonomske zajednice i Europske zajednice za atomsku energiju (SL L 43, 15.2.1983., str. 1.).
([5]) Odluka Komisije (EU, Euratom) 2015/443 od 13. ožujka 2015. o sigurnosti u Komisiji (vidjeti stranicu 41. ovog Službenog lista).

13. „proces upravljanja sigurnosnim rizicima” znači cjelokupni proces prepoznavanja, kontrole i smanjivanja pojave sigurnosnih događaja koji mogu utjecati na sigurnost organizacije ili bilo kojeg sustava kojima se organizacija koristi. Obuhvaća sve aktivnosti povezane s rizicima, uključujući procjenu, obradu, prihvaćanje i obavješćivanje;

14. „Pravilnik o osoblju” znači Pravilnik o osoblju za dužnosnike Europske unije i Uvjeti zaposlenja ostalih službenika Europske unije koji su utvrđeni Uredbom Vijeća (EEZ, Euratom, EZUČ) br. 259/68 ([1]);

15. „prijetnja” znači mogući uzrok neželjenog događaja koji može rezultirati štetom za organizaciju ili bilo koji od sustava kojima se organizacija koristi. Takve prijetnje mogu biti slučajne ili namjerne (zlonamjerne), a karakteriziraju ih prijeteći elementi, mogući ciljevi i načini napada;

16. „slaba točka” znači slabost bilo koje vrste koju može iskoristiti jedna ili više prijetnji. Slaba točka može značiti propust ili se može odnositi na slabost kontrola u smislu njihove snage, cjelovitosti ili dosljednosti i može biti tehničke, postupovne, fizičke, organizacijske ili operativne naravi.

Članak 2.

Predmet i područje primjene

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

2. Primjenjuje se na sve službe i prostore Komisije.

3. Bez obzira na posebne napomene koje se odnose na određene skupine osoblja, ova se Odluka primjenjuje na članove Komisije, na osoblje Komisije na koje se primjenjuje Pravilnik o osoblju i Uvjeti zaposlenja ostalih službenika Europskih zajednica, na nacionalne stručnjake upućene na rad u Komisiji, na pružatelje usluga i njihovo osoblje, na pripravnike i sve osobe koje imaju pristup zgradama ili drugoj imovini Komisije ili pak podacima kojima raspolaže Komisija.

4. Odredbama ove Odluke ne dovode se u pitanje Odluka 2002/47/EZ, EZUČ, Euratom i Odluka 2004/563/EZ, Euratom.

Članak 3.

Definicija klasificiranih podataka EU-a, stupnjeva i oznaka tajnosti

1. „Klasificirani podatak EU-a” znači svaki podatak ili materijal koji je označen stupnjem tajnosti EU-a i čije neovlašteno otkrivanje može prouzročiti različite stupnjeve ugroze interesa Europske unije ili jedne ili više država članica.

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

(a) TRES SECRET UE/EU TOP SECRET: podaci i materijali čije neovlašteno otkrivanje može izuzetno ozbiljno ugroziti bitne interese Europske unije ili jedne ili više država članica;

(b) SECRET UE/EU SECRET: podaci i materijali čije neovlašteno otkrivanje može nanijeti ozbiljnu štetu 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, koje nisu oznake stupnja tajnosti, ali kojima se utvrđuje djelokrug na koji se tajnost odnosi, određuje autor podatka, ograničavaju distribucija i uporaba ili navodi mogućnost objavljivanja.

([1]) Uredba (EEZ, Euratom, EZUČ) br. 259/68 Vijeća od 29. veljače 1968. kojom se utvrđuje Pravilnik o osoblju za dužnosnike i Uvjeti zaposlenja ostalih službenika Europskih zajednica i kojom se uvode posebne mjere koje se privremeno primjenjuju na dužnosnike Komisije (Uvjeti zaposlenja ostalih službenika) (SL L 56, 4.3.1968., str. 1.).

Članak 4.

Upravljanje klasifikacijom

1. Svaki član ili služba Komisije osigurava da su klasificirani podaci EU-a koje stvara klasificirani na odgovarajući način, da su jasno označeni kao klasificirani podaci EU-a te da zadrže svoj stupanj tajnosti samo koliko je potrebno.

2. Ne dovodeći u pitanje članak 26. u nastavku, stupanj tajnosti klasificiranih podataka EU-a ne smije se smanjiti, klasificirani podaci EU-a ne smiju se deklasificirati niti se smije promijeniti ili ukloniti ijedna oznaka stupnja tajnosti iz članka 3. stavka 2. bez prethodne pisane suglasnosti autora.

3. Kada je potrebno, provedbena pravila o postupanju s klasificiranim podacima EU-a, uključujući praktični vodič za klasifikaciju, donose se u skladu s člankom 60. u nastavku.

Članak 5.

Zaštita klasificiranih podataka

1. Klasificirani podaci EU-a štite se u skladu s ovom Odlukom i njezinim provedbenim pravilima.

2. Imatelj bilo kojeg klasificiranog podatka EU-a odgovoran je za njegovu zaštitu, u skladu s ovom Odlukom i njezinim provedbenim pravilima, a prema pravilima iz poglavlja 4. u nastavku.

3. Ako države članice uvedu klasificirane podatke s oznakom nacionalnog stupnja tajnosti u strukture ili mreže Komisije, Komisija štiti navedene podatke u skladu sa zahtjevima primjenljivima na klasificirane podatke EU-a na jednakoj razini prema tablici ekvivalentnosti stupnjeva tajnosti sadržanoj u Prilogu I.

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

Članak 6.

Upravljanje sigurnosnim rizicima

1. Sigurnosne mjere za zaštitu klasificiranih podataka EU-a moraju tijekom cijelog životnog ciklusa podataka biti razmjerne posebice njihovu stupnju tajnosti, obliku i količini podataka ili materijala, mjestu i konstrukciji objekata u kojima su smješteni ti podaci i lokalno procijenjenoj prijetnji koju predstavljaju zlonamjerne i/ili kriminalne aktivnosti, uključujući špijunažu, sabotažu i terorizam.

2. U kriznim se planovima mora uzeti u obzir potreba zaštite klasificiranih podataka EU-a u izvanrednim situacijama kako bi se spriječio neovlašteni pristup, njihovo otkrivanje ili gubitak cjelovitosti ili dostupnosti.

3. Planovi neprekidnosti poslovanja svih službi moraju sadržavati preventivne mjere i mjere oporavka kako bi veliki propusti ili nepredviđeni događaji što manje utjecali na postupanje s klasificiranim podacima EU-a i njihovo čuvanje.

Članak 7.

Provedba ove Odluke

1. Kada je potrebno, provedbena pravila kojima se nadopunjuje ili potkrepljuje ova Odluka donose se u skladu s člankom 60. u nastavku.

2. Službe Komisije poduzimaju sve potrebne mjere u svojoj nadležnosti kako bi osigurale da se pri postupanju s klasificiranim podacima EU-a ili drugim klasificiranim podacima i pri njihovu čuvanju primjenjuje ova Odluka i relevantna provedbena pravila.

3. Sigurnosne mjere poduzete u okviru provedbe ove Odluke sukladne su s načelima za sigurnost u Komisiji iz članka 3. Odluke (EU, Euratom) 2015/443.

4. Glavni direktor za ljudske resurse i sigurnost uspostavlja sigurnosno tijelo Komisije u okviru Glavne uprave za ljudske resurse i sigurnost. Sigurnosno tijelo Komisije ima odgovornosti koje mu se dodjeljuju ovom Odlukom i njezinim provedbenim pravilima.

5. U svakoj službi Komisije lokalnom službeniku za sigurnost (LSS), kako je utvrđeno člankom 20. Odluke (EU, Euratom) 2015/443, povjerene su sljedeće opće odgovornosti za zaštitu klasificiranih podataka EU-a u skladu s ovom Odlukom, u uskoj suradnji s Glavnom upravom za ljudske resurse i sigurnost:

(a) upravljanje zahtjevima za sigurnosna ovlaštenja osoblja;

(b) sudjelovanje u sigurnosnom osposobljavanju i organizaciji informativnih sastanaka za podizanje svijesti;

(c) nadzor rada nadzornog službenika registarskog ureda (RCO) svoje službe;

(d) izvješćivanje o povredama sigurnosti i ugrozama klasificiranih podataka EU-a;

(e) čuvanje rezervnih ključeva i zapisnika sa svim kombinacijama;

(f) obavljanje ostalih zadataka povezanih sa zaštitom klasificiranih podataka EU-a ili definiranih provedbenim pravilima.

Članak 8.

Povrede sigurnosti i ugroza klasificiranih podataka EU-a

1. Povreda sigurnosti posljedica je radnje ili propusta koji su u suprotnosti sa sigurnosnim propisima utvrđenima ovom Odlukom i njezinim provedbenim pravilima.

2. Ugroza klasificiranih podataka EU-a nastaje kada su ti podaci, kao rezultat povrede sigurnosti, djelomično ili u cijelosti otkriveni neovlaštenim osobama.

3. Svaka povreda ili sumnja na povredu sigurnosti odmah se prijavljuje sigurnosnom tijelu Komisije.

4. Ako je poznato ili postoje opravdani razlozi na temelju kojih se može pretpostaviti da su klasificirani podaci EU-a ugroženi ili izgubljeni, provodi se sigurnosna provjera u skladu s člankom 13. Odluke (EU, Euratom) 2015/443.

5. Poduzimaju se sve potrebne mjere kako bi se:

(a) obavijestilo autora;

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

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

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

(e) obavijestilo nadležna tijela o poduzetim mjerama.

6. Protiv svake osobe odgovorne za povredu sigurnosnih propisa utvrđenih ovom Odlukom može se pokrenuti disciplinski postupak u skladu s Pravilnikom o osoblju. Protiv svake osobe odgovorne za ugrozu ili gubitak klasificiranih podataka EU-a pokreće se disciplinski i/ili pravni postupak u skladu s primjenjivim zakonima, pravilima i propisima.

POGLAVLJE 2.

SIGURNOST OSOBLJA

Članak 9.

Definicije

Za potrebe ovog poglavlja primjenjuju se sljedeće definicije:

1. „ovlaštenje za pristup klasificiranim podacima EU-a” znači odluka koju je sigurnosno tijelo Komisije donijelo na temelju potvrde nadležnog tijela države članice da se dužnosniku ili drugom službeniku Komisije ili pak upućenom nacionalnom stručnjaku može odobriti pristup klasificiranim podacima EU-a do određenog stupnja tajnosti (CONFIDENTIEL UE/EU CONFIDENTIAL ili višeg) do određenog datuma pod uvjetom da je za njih utvrđena nužnost pristupa podacima i da su adekvatno upoznati sa svojim odgovornostima. Za tako opisanu osobu kaže se da je „sigurnosno ovlaštena”;

2. „sigurnosno ovlaštenje osoblja” primjena je mjera kojima se osigurava da je pristup klasificiranim podacima EU-a odobren samo osobama:

(a) kojima je nužno osigurati pristup podacima;

(b) koje su, ako je potrebno, sigurnosno ovlaštene za odgovarajući stupanj; i

(c) koje su upoznate sa svojim odgovornostima;

3. „uvjerenje o sigurnosnoj provjeri osobe” (USP) znači izjava koju nadležno tijelo države članice izdaje nakon završetka sigurnosne istrage koju provode za to nadležna tijela države članice i kojom se potvrđuje da se osobi može odobriti pristup klasificiranim podacima EU-a do određenog stupnja tajnosti (CONFIDENTIEL UE/EU CONFIDENTIAL ili višeg) do određenog datuma pod uvjetom da je za nju utvrđena nužnost pristupa podacima i da je adekvatno upoznata sa svojim odgovornostima;

4. „certifikat o sigurnosnoj provjeri osobe” (CSP) znači certifikat koji izdaje nadležno tijelo i kojim se utvrđuje da osoba ima valjano uvjerenje o sigurnosnoj provjeri ili sigurnosno ovlaštenje sigurnosnog tijela te u kojem je naveden stupanj tajnosti klasificiranih podataka EU-a do kojeg se pojedincu može odobriti pristup (CONFIDENTIEL UE/EU CONFIDENTIAL ili viši), datum valjanosti relevantnog uvjerenja o sigurnosnoj provjeri (USP) ili sigurnosnog ovlaštenja te datum isteka samog certifikata;

5. „sigurnosna istraga” znači istražni postupci koje provodi nadležno tijelo države članice u skladu s nacionalnim zakonima i propisima s ciljem dobivanja uvjerenja o nepostojanju zapreka tome da se osobi odobri uvjerenje o sigurnosnoj provjeri do određenog stupnja tajnosti (CONFIDENTIEL UE/EU CONFIDENTIAL ili višeg).

Članak 10.

Osnovna načela

1. Pristup klasificiranim podacima EU-a odobrava se samo osobama:

1. za koje je utvrđena nužnost pristupa podacima;

2. koje su upoznate sa sigurnosnim pravilima za zaštitu klasificiranih podataka EU-a i pripadajućim sigurnosnim standardima i smjernicama, i koje su dale izjavu o preuzimanju odgovornosti povezane sa zaštitom takvih podataka;

3. koje, za podatke klasificirane do stupnja CONFIDENTIEL UE/EU CONFIDENTIAL ili višeg, imaju sigurnosno ovlaštenje do odgovarajuće razine ili su na drugi način propisno ovlaštene na temelju svojih funkcija u skladu s nacionalnim zakonima i propisima.

2. Osobe, kojima zbog njihovih dužnosti može zatrebati pristup podacima EU-a klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim, moraju biti sigurnosno ovlaštene za odgovarajuću razinu prije nego što im se odobri pristup tim podacima. Dotične osobe moraju dati suglasnost u pisanom obliku da se nad njima provede postupak sigurnosne provjere. Osoba koja to ne učini ne može biti imenovana na određeno radno mjesto ili funkciju niti joj može biti dodijeljen zadatak koji zahtijeva pristup klasificiranim podacima stupnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višeg.

3. Postupcima za sigurnosnu provjeru osoba utvrđuje se može li se određenu osobu, na temelju njezine lojalnosti, vjerodostojnosti i pouzdanosti, ovlastiti za pristup klasificiranim podacima EU-a.

4. U svrhu izdavanja uvjerenja o sigurnosnoj provjeri za pristup podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim, lojalnost, vjerodostojnost i pouzdanost osobe utvrđuju se sigurnosnom istragom koju provode nadležna tijela države članice u skladu s nacionalnim zakonima i propisima.

5. Sigurnosno tijelo Komisije jedino je nadležno za kontakte s nacionalnim sigurnosnim tijelima (NST) ili drugim nacionalnim nadležnim tijelima u vezi sa svim pitanjima sigurnosne provjere. Svi kontakti između Komisijinih službi i njihova osoblja te nacionalnih sigurnosnih tijela i ostalih nadležnih tijela odvijaju se preko sigurnosnog tijela Komisije.

Članak 11.

Postupak za dobivanje sigurnosnog ovlaštenja

1. Svaki glavni direktor ili voditelj službe u Komisiji mora odrediti ona radna mjesta u svojoj službi za koja zaposlenici, da bi mogli obavljati svoje dužnosti, moraju imati pristup podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim, pa u skladu s time moraju biti sigurnosno ovlašteni.

2. Čim dobije informaciju o imenovanju određene osobe na radno mjesto za koje potreban pristup podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim, lokalni službenik za sigurnost predmetne službe Komisije mora o tome obavijestiti sigurnosno tijelo Komisije, koje dotičnoj osobi prosljeđuje upitnik za sigurnosnu provjeru koji izdaje NST države članice čije je državljanstvo osoba prijavila u trenutku imenovanja članom osoblja europskih institucija. Osoba mora dati suglasnost u pisanom obliku da se nad njom provede postupak sigurnosne provjere i ispunjeni obrazac u najkraćem roku poslati sigurnosnom tijelu Komisije.

3. Sigurnosno tijelo Komisije prosljeđuje ispunjeni upitnik za sigurnosnu provjeru NST-u države članice čije je državljanstvo osoba prijavila u trenutku imenovanja članom osoblja europskih institucija, sa zahtjevom da se provede sigurnosna istraga u skladu sa stupnjem tajnosti klasificiranih podataka EU-a za koji će se dotičnoj osobi morati osigurati pristup.

4. Ako su podaci relevantni za sigurnosnu istragu o osobi koja je podnijela zahtjev za sigurnosnu provjeru poznati sigurnosnom tijelu Komisije, ono o tome obavješćuje nadležni NST djelujući u skladu s mjerodavnim pravilima i propisima.

5. Nakon obavljene sigurnosne istrage te što je prije moguće nakon što ga predmetni NST obavijesti o svojoj ukupnoj ocjeni nalaza sigurnosne provjere, sigurnosno tijelo Komisije:

(a) može dotičnoj osobi dati ovlaštenje za pristup klasificiranim podacima EU-a i odobriti pristup tim podacima do primjerenog stupnja tajnosti do datuma koje određuje sigurnosno tijelo Komisije, a koji ne smije biti kasnije od 5 godina, ako se sigurnosnom istragom utvrdi da ne postoji ništa što bi dovodilo u pitanje lojalnost, vjerodostojnost i pouzdanost osobe;

(b) ako se sigurnosnom istragom ne utvrdi prethodno navedeno, u skladu s mjerodavnim pravilima i propisima, o tome obavješćuje dotičnu osobu, koja od sigurnosnog tijela Komisije može zatražiti saslušanje, a sigurnosno tijelo Komisije pak može od nadležnog NST-a tražiti dodatna pojašnjenja, koja mu NST može dostaviti u skladu s nacionalnim zakonima i propisima. Bude li ishod sigurnosne istrage potvrđen, osobi se ne izdaje ovlaštenje za pristup klasificiranim podacima EU-a.

6. 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 sigurnosnog tijela Komisije podliježu žalbama u skladu s Pravilnikom o osoblju.

7. Komisija prihvaća ovlaštenje za pristup klasificiranim podacima EU-a izdano od druge institucije, tijela ili agencije Unije pod uvjetom da je valjano. Ovlaštenje se odnosi na sva zaduženja dotične osobe u Komisiji. Institucija, tijelo ili agencija Unije u kojoj se osoba zapošljava obavješćuje nadležni NST o promjeni poslodavca.

8. Ako osoba ne započne službu u roku od 12 mjeseci od obavijesti o ishodu sigurnosne istrage upućene sigurnosnom tijelu Komisije ili u slučaju prekida službe u trajanju od 12 mjeseci, tijekom kojih osoba nije bila zaposlena u Komisiji ili drugoj instituciji, tijelu ili agenciji Unije, ili na radnom mjestu u nacionalnoj administraciji države članice, sigurnosno tijelo Komisije prosljeđuje predmet nadležnom NST-u na potvrdu valjanosti i primjerenosti sigurnosne provjere.

9. Ako sigurnosno tijelo Komisije sazna da osoba s valjanim sigurnosnim ovlaštenjem predstavlja sigurnosni rizik, ono o tome obavješćuje nadležni NST djelujući u skladu s relevantnim pravilima i propisima.

10. Ako NST obavijesti sigurnosno tijelo Komisije o povlačenju uvjerenja izdanog u skladu sa stavkom 5. točkom (a) osobi koja ima valjano ovlaštenje za pristup klasificiranim podacima EU-a, sigurnosno tijelo Komisije može od NST-a tražiti dodatna pojašnjenja koja mu potonji može dostaviti u skladu s nacionalnim zakonima i propisima. Ako relevantni NST potvrdi negativne informacije, osobi se oduzima sigurnosno ovlaštenje i onemogućuje pristup klasificiranim podacima EU-a i rad na radnom mjestu na kojem je takav pristup moguć ili na kojem bi mogla ugroziti sigurnost.

11. Svaka osoba koja podliježe primjeni ove Odluke obavješćuje se o svakoj odluci kojom joj se ukida ili suspendira ovlaštenje za pristup klasificiranim podacima EU-a i, prema potrebi, o razlozima za takav postupak, te može zatražiti saslušanje pred sigurnosnim tijelom Komisije. Informacije koje je dostavio NST podliježu relevantnim zakonima i propisima koji su na snazi u dotičnoj državi članici. Odluke koje u ovom kontekstu donosi sigurnosno tijelo Komisije podliježu žalbama u skladu s Pravilnikom o osoblju.

12. Službe Komisije osiguravaju da upućeni nacionalni stručnjaci, prije nego što počnu obavljati svoj posao na radnim mjestima za koja je potrebno sigurnosno ovlaštenje za pristup klasificiranim podacima EU-a, sigurnosnom tijelu Komisije predoče, u skladu s nacionalnim zakonima i propisima, valjano uvjerenje (USP) ili certifikat o sigurnosnoj provjeri osobe (CSP), na temelju kojega sigurnosno tijelo Komisije izdaje sigurnosno ovlaštenje za pristup podacima EU-a klasificiranim do stupnja tajnosti jednakog onom koji je naveden u nacionalnom uvjerenju o sigurnosnoj provjeri, čija valjanost ne može biti duža od trajanja radnog ugovora s Komisijom.

Pristup klasificiranim podacima EU-a za osobe koje su propisno ovlaštene na temelju funkcije koju obavljaju

13. Članovi Komisije, koji, u skladu s Ugovorom, po prirodi svojih funkcija imaju pristup klasificiranim podacima EU-a, moraju biti upoznati sa svojim sigurnosnim obvezama u smislu zaštite klasificiranih podataka EU-a.

Evidencija uvjerenja o sigurnosnoj provjeri i sigurnosnih ovlaštenja

14. Za evidenciju uvjerenja o sigurnosnoj provjeri i sigurnosnih ovlaštenja koja se izdaju za pristup klasificiranim podacima EU-a zaduženo je sigurnosno tijelo Komisije u skladu s ovom Odlukom. Ta evidencija mora sadržavati barem stupanj tajnosti klasificiranih podataka EU-a do kojeg se osobi može odobriti pristup, datum izdavanja uvjerenja o sigurnosnoj provjeri i njegov rok valjanosti.

15. Sigurnosno tijelo Komisije može izdati CSP u kojemu je naveden stupanj tajnosti klasificiranih podataka EU-a do kojeg se osobi može odobriti pristup (CONFIDENTIEL UE/EU CONFIDENTIAL ili viši), datum valjanosti odgovarajućeg ovlaštenja za pristup klasificiranim podacima EU-a i datum isteka samog certifikata.

Obnavljanje sigurnosnog ovlaštenja

16. Nakon prvog izdavanja sigurnosnog ovlaštenja i pod uvjetom da je osoba bez prekida obavljala službu u Europskoj komisiji ili drugoj instituciji, tijelu ili agenciji Unije te da joj je potreban kontinuirani pristup klasificiranim podacima EU-a, obnavljanje sigurnosnog ovlaštenja razmatra se u pravilu svakih pet godina od datuma obavijesti o ishodu zadnje sigurnosne istrage na kojoj se ovlaštenje temelji.

17. Sigurnosno tijelo Komisije može produžiti trajanje postojećeg sigurnosnog ovlaštenja na razdoblje do 12 mjeseci, pod uvjetom da relevantni NST ili drugo nacionalno nadležno tijelo nije dostavilo negativne informacije u roku od dva mjeseca od datuma slanja zahtjeva za obnavljanje ovlaštenja i odgovarajućeg upitnika za sigurnosnu provjeru. Ako po isteku 12-mjesečnog razdoblja relevantni NST ili drugo nacionalno nadležno tijelo ne dostavi svoje mišljenje sigurnosnom tijelu Komisije, osoba se imenuje na dužnost za koju nije potrebno sigurnosno ovlaštenje.

Članak 12.

Informativni sastanci o sigurnosnim ovlaštenjima

1. Nakon prisustvovanja informativnom sastanku o sigurnosnim ovlaštenjima u organizaciji sigurnosnog tijela Komisije, osobe koje su dobile sigurnosno ovlaštenje podnose pisanu izjavu o tome da razumiju koje su njihove obveze s obzirom na zaštitu klasificiranih podataka EU-a i koje su moguće posljedice ako bi klasificirani podaci EU-a bili ugroženi. Sigurnosno tijelo Komisije vodi evidenciju o takvim pisanim izjavama.

2. Osobe koje imaju ovlaštenje za pristup klasificiranim podacima EU-a ili od kojih se zahtijeva postupanje s klasificiranim podacima EU-a već se na početku upozorava, a potom redovito informira o sigurnosnim prijetnjama, te su dužne sigurnosnom tijelu Komisije odmah prijaviti svaki pokušaj pristupa ili aktivnost koju smatraju sumnjivom ili neuobičajenom.

3. Osobe koje prestanu obavljati dužnosti za koje je potreban pristup klasificiranim podacima EU-a upoznaje se s njihovim obvezama u pogledu daljnje zaštite klasificiranih podataka EU-a, a ako je potrebno, dužne su podnijeti i pisanu izjavu u tom smislu.

Članak 13.

Privremena sigurnosna ovlaštenja

1. U iznimnim okolnostima, ako je to propisno opravdano interesima službe, a prije završetka potpune sigurnosne istrage, sigurnosno tijelo Komisije može, nakon savjetovanja s NST-om države članice čiji je osoba državljanin i ovisno o ishodu preliminarnih provjera kojima se potvrđuje da ne postoje relevantne negativne informacije, osobi izdati privremeno ovlaštenje za pristup klasificiranim podacima EU-a za određenu funkciju, pri čemu se ne dovode u pitanje odredbe o obnavljanju sigurnosnih ovlaštenja. Takva privremena ovlaštenja za pristup klasificiranim podacima EU-a valjana su tijekom samo jednog razdoblja od najviše 6 mjeseci i na temelju njih nije moguć pristup podacima klasificiranima stupnjem tajnosti TRES SECRET UE/EU TOP SECRET.

2. Nakon što dobiju potrebne informacije u skladu s člankom 12. stavkom 1., osobe koje su dobile privremeno ovlaštenje podnose pisanu izjavu o tome da razumiju koje su njihove obveze s obzirom na zaštitu klasificiranih podataka EU-a i koje su moguće posljedice ako bi klasificirani podaci EU-a bili ugroženi. Sigurnosno tijelo Komisije vodi evidenciju o takvim pisanim izjavama.

Članak 14.

Prisustvovanje na povjerljivim sastancima koje organizira Komisija

1. Službe Komisije zadužene za organizaciju sastanaka na kojima se raspravlja o podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim obavješćuju Sigurnosno tijelo Komisije dovoljno unaprijed o datumu, vremenu, mjestu i sudionicima tih sastanaka putem svojeg LSS-a ili putem organizatora sastanka.

2. U skladu s odredbama članka 11. stavka 13. na sastancima u organizaciji Komisije na kojima se raspravlja o podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim mogu sudjelovati samo osobe koje imaju uvjerenje o sigurnosnoj provjeri ili sigurnosno ovlaštenje. Pristup takvim povjerljivim sastancima uskraćuje se osobama čiji CSP ili drugi dokaz da su prošle sigurnosnu provjeru nije dostavljen sigurnosnom tijelu Komisije te sudionicima iz Komisije koji nemaju sigurnosno ovlaštenje.

3. Prije organiziranja povjerljivog sastanka, osoba zadužena za organizaciju ili LSS Komisijine službe koja organizira sastanak vanjskim sudionicima šalje zahtjev za dostavljanje CSP-a ili drugog dokaza o sigurnosnoj provjeri sigurnosnom tijelu Komisije. Sigurnosno tijelo Komisije obavješćuje lokalnog službenika za sigurnost ili organizatora sastanka o zaprimljenom CSP-u ili drugom dokazu o sigurnosnoj provjeri. Prema potrebi, može se koristiti konsolidirani popis imena s odgovarajućim dokazom o sigurnosnoj provjeri.

4. Ako nadležna tijela obavijeste sigurnosno tijelo Komisije o tome da je osobi čije dužnosti uključuju sudjelovanje na Komisijinim sastancima oduzet CSP, sigurnosno tijelo Komisije o tome obavješćuje LSS-a Komisijine službe koja organizira sastanak.

Članak 15.

Mogući pristup klasificiranim podacima EU-a

Kuriri, zaštitari i pratnja moraju dobiti sigurnosno ovlaštenje za odgovarajući stupanj tajnosti ili se nad njima mora provesti drugačija primjerena sigurnosna istraga u skladu s nacionalnim zakonima ili propisima, te ih se mora informirati o sigurnosnim postupcima za zaštitu klasificiranih podataka EU-a i uputiti u njihove dužnosti povezane sa zaštitom podataka koji su im povjereni.

POGLAVLJE 3.

FIZIČKA SIGURNOST U CILJU ZAŠTITE KLASIFICIRANIH PODATAKA

Članak 16.

Osnovna načela

1. Svrha je mjera fizičke sigurnosti sprečavanje tajnog ili nasilnog ulaska neovlaštenih osoba, odvraćanje od neovlaštenih radnji, njihovo sprečavanje ili otkrivanje te omogućavanje razvrstavanja osoblja s obzirom na pristup klasificiranim podacima EU-a prema nužnosti pristupa. Te se mjere utvrđuju na temelju procesa upravljanja rizikom u skladu s ovom Odlukom i njezinim provedbenim pravilima.

2. Konkretno, mjere fizičke sigurnosti namijenjene su sprečavanju neovlaštenog pristupa klasificiranim podacima EU-a na sljedeće načine:

(a) njima se osigurava pravilno postupanje s klasificiranim podacima EU-a i njihovo čuvanje;

(b) omogućuje se razvrstavanje osoblja s obzirom na pristup klasificiranim podacima EU-a prema nužnosti pristupa podacima te, ako je potrebno, prema sigurnosnom ovlaštenju;

(c) služe za odvraćanje od neovlaštenih radnji, njihovo sprečavanje i otkrivanje; i

(d) njima se onemogućuju ili odgađaju tajni ili nasilni ulasci neovlaštenih osoba.

3. Mjere fizičke sigurnosti uvode se za sve prostore, zgrade, urede, prostorije i druga mjesta na kojima se klasificirani podaci EU-a koriste ili čuvaju, uključujući zone u kojima su smješteni komunikacijski i informacijski sustavi iz poglavlja 5.

4. Mjesta na kojima se čuvaju podaci EU-a klasificirani stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim definiraju se sigurnosnim zonama u skladu s ovim poglavljem, a akreditira ih Komisijino tijelo za sigurnosnu akreditaciju.

5. Za zaštitu podataka EU-a klasificiranih stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim koriste se isključivo oprema ili uređaji koje je odobrilo sigurnosno tijelo Komisije.

Članak 17.

Zahtjevi i mjere povezani s fizičkom sigurnošću

1. Odabir mjera fizičke sigurnosti ovisi o procjeni prijetnji koju izrađuje sigurnosno tijelo Komisije, konzultirajući se prema potrebi s ostalim službama Komisije, drugim institucijama, agencijama ili tijelima Unije i/ili nadležnim tijelima država članica. Za zaštitu klasificiranih podataka EU-a u svojim prostorima Komisija primjenjuje proces upravljanja rizicima kako bi osigurala da je razina fizičke zaštite razmjerna 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 količina klasificiranih podataka EU-a, imajući na umu da velike količine ili zbirka klasificiranih podataka EU-a mogu zahtijevati primjenu strožih mjera zaštite;

(c) okoliš i konstrukcija objekata ili zona u kojima su smješteni klasificirani podaci EU-a; i

(d) procijenjena prijetnja od obavještajnih službi, čija su meta Unija, njezine institucije, tijela ili agencije, ili države članice te od sabotaže, terorističkih, subverzivnih ili drugih kriminalnih aktivnosti.

2. Primjenjujući koncept dubinske obrane, sigurnosno tijelo Komisije određuje odgovarajuću kombinaciju mjera fizičke zaštite koje će provesti. U tu svrhu sigurnosno tijelo Komisije osmišljava minimalne standarde, norme i kriterije, sadržane u provedbenim pravilima.

3. Sigurnosno tijelo Komisije ovlašteno je za provođenje pretrage prilikom ulaska i izlaska s ciljem odvraćanja od neovlaštenog unosa materijala ili neovlaštenog odnošenja klasificiranih podataka EU-a iz prostora ili objekata.

4. Postoji li rizik da se klasificirani podaci EU-a previde, makar i slučajno, predmetne službe Komisije poduzimaju odgovarajuće mjere za njegovo uklanjanje, kako je to definiralo sigurnosno tijelo Komisije.

5. Za nove se objekte zahtjevi u pogledu fizičke sigurnosti i funkcionalne specifikacije definiraju u dogovoru sa sigurnosnim tijelom Komisije kao dio aktivnosti planiranja i projektiranja objekata. Za već postojeće objekte zahtjevi u pogledu fizičke sigurnosti primjenjuju se u skladu s minimalnim standardima, normama i kriterijima sadržanim u provedbenim pravilima.

Članak 18.

Oprema za fizičku zaštitu klasificiranih podataka EU-a

1. Za fizičku zaštitu klasificiranih podataka EU-a definiraju se dvije vrste fizički zaštićenih zona:

(a) administrativne zone; i

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

2. Sigurnosno tijelo Komisije određuje da određena zona ispunjava zahtjeve na temelju kojih se može definirati kao administrativna zona, sigurnosna zona ili tehnički zaštićena sigurnosna zona.

3. Za administrativne zone:

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

(b) pristup bez pratnje odobrava se samo osobama koje je propisno ovlastilo sigurnosno tijelo Komisije ili neko drugo nadležno tijelo; i

(c) ostale osobe moraju imati stalnu pratnju ili podliježu istovjetnim kontrolama.

4. Za sigurnosne zone:

(a) uspostavlja se vidljivo definiran i zaštićen perimetar unutar kojeg se nadziru svi ulasci i izlasci s pomoću propusnice ili sustava prepoznavanja osoba;

(b) pristup bez pratnje odobrava se samo osobama koje su prošle sigurnosnu provjeru i koje su posebno ovlaštene za ulazak u tu zonu na temelju nužnosti pristupa podacima;

(c) ostale osobe moraju imati stalnu pratnju ili podliježu istovjetnim kontrolama.

5. Ako se ulazak u sigurnosnu zonu može u svakom smislu smatrati izravnim pristupom u njoj sadržanim klasificiranim podacima, primjenjuju se sljedeći dodatni zahtjevi:

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

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

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

(a) takve su zone opremljene sustavom za otkrivanje neovlaštenog ulaska (IDS), zaključane su kada u njima nema nikoga i pod zaštitom kada je netko u njima. Svim se ključevima upravlja u skladu s člankom 20.;

(b) sav se materijal i osobe koji ulaze u takve zone nadziru;

(c) sigurnosno tijelo Komisije u takvim zonama redovito provodi fizičke i/ili tehničke inspekcije. Takve se inspekcije također provode nakon svakog neovlaštenog ulaska ili sumnje na 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.

7. Neovisno o stavku 6. točki (d), prije uporabe u zonama u kojima se održavaju sastanci ili obavlja posao koji uključuje podatke klasificirane stupnjem tajnosti SECRET UE/EU SECRET ili višim te u kojima je prijetnja za klasificirane podatke EU-a ocijenjena kao visoka, sve komunikacijske uređaje i električnu ili elektroničku opremu najprije ispituje sigurnosno tijelo Komisije kako bi se spriječio slučajan ili nedopušten prijenos razumljivih podataka pomoću te opreme izvan perimetra sigurnosne zone.

8. Sigurnosne zone u kojima osoblje nije prisutno 24 sata dnevno pregledavaju se, prema potrebi, na kraju redovitog radnog vremena i u nasumičnim vremenskim razmacima izvan redovitog radnog vremena, osim ako je zona opremljena IDS-om.

9. Sigurnosne zone i tehnički zaštićene sigurnosne zone mogu se privremeno uspostaviti unutar administrativne zone koja se koristi za povjerljive sastanke ili u druge slične svrhe.

10. LSS predmetne službe Komisije sastavlja sigurnosno-operativne postupke za svaku sigurnosnu zonu za koju je nadležan, a kojima se, u skladu s odredbama ove Odluke i njezinim provedbenim pravilima, definira sljedeće:

(a) stupanj tajnosti klasificiranih podataka EU-a koje se može koristiti i koji se mogu čuvati u zoni;

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

(c) osobe ovlaštene za pristup zoni bez pratnje na temelju utvrđene nužnosti pristupa podacima i sigurnosnog ovlaštenja;

(d) prema potrebi, postupci za pratitelje ili za zaštitu klasificiranih podataka EU-a ako se druge osobe ovlašćuje za pristup zoni;

(e) sve ostale odgovarajuće mjere i postupci.

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

Članak 19.

Fizičke mjere zaštite za postupanje s klasificiranim podacima EU-a i njihovo čuvanje

1. S podacima EU-a klasificiranim 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 osoba; ili

(c) izvan sigurnosne ili administrativne zone uz uvjet da imatelj prenosi klasificirane podatke EU-a u skladu s člankom 31. i da se obvezao poštovati kompenzacijske mjere utvrđene provedbenim mjerama s ciljem zaštite klasificiranih podataka EU-a od pristupa neovlaštenih osoba.

2. Podaci EU-a klasificirani stupnjem tajnosti RESTREINT UE/EU RESTRICTED čuvaju se u primjerenom uredskom namještaju pod ključem u administrativnoj ili sigurnosnoj zoni. Privremeno se mogu čuvati izvan administrativne ili sigurnosne zone uz uvjet da se imatelj obvezao poštovati kompenzacijske mjere utvrđene provedbenim pravilima.

3. S podacima EU-a klasificiranim 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 osoba; ili

(c) izvan sigurnosne ili administrativne zone uz uvjet:

i. da se imatelj obvezao poštovati kompenzacijske mjere utvrđene provedbenim pravilima s ciljem zaštite klasificiranih podataka EU-a od pristupa neovlaštenih osoba;

ii. da imatelj osobno ima stalni nadzor nad klasificiranim podacima EU-a i

iii. da je imatelj, ako su dokumenti u papirnom obliku, o tome obavijestio nadležni registar.

4. Podaci EU-a klasificirani stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET čuvaju se u sigurnosnoj zoni u sigurnosnom spremniku ili trezoru.

5. S podacima EU-a klasificiranim stupnjem tajnosti TRES SECRET UE/EU TOP SECRET postupa se u sigurnosnoj zoni koju uspostavlja i održava sigurnosno tijelo Komisije, te koju je do tog stupnja akreditiralo Komisijino tijelo za sigurnosnu akreditaciju.

6. Podaci EU-a klasificirani stupnjem tajnosti TRES SECRET UE/EU TOP SECRET čuvaju se u sigurnosnoj zoni, koju je do tog stupnja akreditiralo Komisijino tijelo za sigurnosnu akreditaciju, u jednom od sljedećih uvjeta:

(a) u sigurnosnom spremniku u skladu s odredbama članka 18. uz najmanje jednu od sljedećih dodatnih kontrola:

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

2. odobren IDS u kombinaciji s interventnim osobljem;

ili

(b) u trezoru opremljenom IDS-om u kombinaciji s interventnim osobljem.

Članak 20.

Upravljanje ključevima i kombinacijama za zaštitu klasificiranih podataka EU-a

1. Postupci za upravljanje ključevima i kombinacijama za urede, prostorije, trezore i sigurnosne spremnike utvrđuju se provedbenim pravilima u skladu s člankom 60. u nastavku. Svrha je tih postupaka zaštita od neovlaštenog pristupa.

2. Kombinacije pamti najmanji mogući broj osoba koje ih moraju znati. Kombinacije za sigurnosne spremnike i trezore u kojima se čuvaju klasificirani podaci EU-a mijenjaju se:

(a) prilikom primitka novog spremnika;

(b) pri svakoj promjeni osoblja koje zna kombinaciju;

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

(d) u slučaju održavanja ili popravka brave; i

(e) najmanje svakih 12 mjeseci.

POGLAVLJE 4.

UPRAVLJANJE KLASIFICIRANIM PODACIMA EU-a

Članak 21.

Osnovna načela

1. Svim klasificiranim dokumentima EU-a mora se upravljati u skladu s politikom Komisije o upravljanju dokumentima, te se shodno tome moraju registrirati, unositi u sustav, čuvati i konačno brisati, uzorkovati ili prenositi u povijesne arhive u skladu sa zajedničkim popisom čuvanja dokumenata Europske komisije.

2. Podaci klasificirani stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim registriraju se iz sigurnosnih razloga prije distribucije i po primitku. Podaci klasificirani stupnjem tajnosti TRES SECRET UE/EU TOP SECRET upisuju se u za to predviđene registre.

3. Sustav registriranja klasificiranih podataka EU-a u Komisiji uspostavlja se u skladu s odredbama članka 27.

4. Službe i prostorije Komisije u kojima se postupa s klasificiranim podacima EU-a ili u kojima se ti podaci čuvaju podliježu redovitim inspekcijama koje provodi sigurnosno tijelo Komisije.

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

(a) u pravilu se klasificirani podaci EU-a prenose elektroničkim sredstvima koja su zaštićena kriptografskim proizvodima odobrenima u skladu s poglavljem 5.;

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

   i. na elektroničkim medijima (npr. USB, CD, tvrdi disk) koji su zaštićeni kriptografskim proizvodima odobrenima u skladu s poglavljem 5.; ili

   ii. u svim ostalim slučajevima, u skladu s provedbenim pravilima.

Članak 22.

Klasifikacija i oznake

1. Podaci se klasificiraju ako je potrebno zaštititi njihovu tajnost, u skladu s člankom 3. stavkom 1.

2. Autor klasificiranih podataka EU-a odgovoran je za utvrđivanje stupnja tajnosti u skladu s relevantnim provedbenim pravilima, standardima i smjernicama o klasifikaciji, te za prvo širenje podataka.

3. Stupanj tajnosti klasificiranih podataka EU-a određuje se u skladu s člankom 3. stavkom 2. i s relevantnim provedbenim pravilima.

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

5. Pojedinačni dijelovi određenog dokumenta (npr. stranice, odlomci, odjeljci, prilozi, dodaci i privici) mogu zahtijevati različite stupnjeve tajnosti te stoga moraju biti označeni na odgovarajući način, uključujući dijelove pohranjene u elektroničkom obliku.

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

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

8. Stupanj tajnosti popratnog pisma ili note koji se šalju uz privitke mora biti jednak najvišem stupnju tajnosti privitaka. Autor podatka odgovarajućim oznakama jasno navodi stupanj tajnosti popratnog pisma ili note kada se odvoje od svojih privitaka, npr.:

CONFIDENTIEL UE/EU CONFIDENTIAL

Bez privitaka RESTREINT UE/EU RESTRICTED

Članak 23.

Oznake

Uz jednu od oznaka stupnja tajnosti navedenih u članku 3. stavku 2., klasificirani podaci EU-a mogu nositi dodatne oznake kao što su:

(a) oznaka kojom se određuje autor podatka;

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

(c) oznake o mogućnosti otkrivanja podataka;

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

Članak 24.

Skraćene oznake stupnja tajnosti

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

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

TRES 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

Članak 25.

Stvaranje klasificiranih podataka EU-a

1. 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 po sebi nije klasificirani podatak, osim ako je označen kao takav;

(d) dokument mora biti označen datumom;

(e) ako se dokumenti klasificirani stupnjem tajnosti SECRET UE/EU SECRET distribuiraju u nekoliko primjeraka na svakoj stranici mora stajati broj preslike.

2. Ako se stavak 1. ne može primijeniti na klasificirane podatke EU-a, poduzimaju se druge odgovarajuće mjere u skladu s provedbenim pravilima.

Članak 26.

Smanjivanje stupnja tajnosti i deklasifikacija klasificiranih podataka EU-a

1. Kada je to moguće, u trenutku stvaranja klasificiranih podataka EU-a autor navodi može li se njihov stupanj tajnosti smanjiti, odnosno mogu li se podaci deklasificirati na određeni datum ili nakon određenog događaja.

2. Svaka služba Komisije redovito pregledava klasificirane podatke EU-a čiji je autor kako bi utvrdila primjenjuje li se još uvijek stupanj tajnosti. Provedbenim se pravilima uspostavlja sustav kojim se stupanj tajnosti registriranih klasificiranih podataka EU-a čiji je autor Komisija preispituje najmanje svakih pet godina. Takvo preispitivanje nije neophodno ako je autor na početku naveo da će se stupanj tajnosti podataka automatski smanjiti ili da će se podaci automatski deklasificirati te ako su podaci sukladno tome označeni.

3. Podaci klasificirani stupnjem tajnosti RESTREINT UE/EU RESTRICTED, a čiji je autor Komisija, smatrat će se podacima koji se automatski deklasificiraju nakon trideset godina u skladu s Uredbom (EEZ, Euratom) br. 354/83 kako je izmijenjena Uredbom Vijeća (EZ, Euratom) br. 1700/2003 ([1]).

Članak 27.

Sustav registarskih ureda klasificiranih podataka EU-a u Komisiji

1. Ne dovodeći u pitanje članak 52. stavak 5. u nastavku, u svim službama Komisije u kojima se postupa s klasificiranim podacima EU-a ili se ti podaci čuvaju na stupnju tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET određuje se se mjerodavni lokalni registarski ured klasificiranih podataka EU-a kako bi se osiguralo da se s tim podacima postupa u skladu s ovom Odlukom.

2. Komisijin središnji registarski ured za klasificirane podatke EU-a jest registarski ured klasificiranih podataka EU-a kojim upravlja Glavno tajništvo. Taj se registarski ured koristi kao:

— lokalni registarski ured klasificiranih podataka EU-a za Glavno tajništvo Komisije;

— registarski ured klasificiranih podataka EU-a za privatne kabinete članova Komisije, osim ako im je već dodijeljen lokalni registarski ured klasificiranih podataka EU-a;

— registarski ured klasificiranih podataka EU-a za glavne uprave ili službe koje nemaju lokalne registarske urede klasificiranih podataka EU-a;

— glavna točka ulaska i izlaska za sve podatke klasificirane stupnjem tajnosti RESTREINT UE/EU RESTRICTED i višima, uključujući stupanj tajnosti SECRET UE/EU SECRET, koji se razmjenjuju između Komisije i njezinih službi i trećih država članica te međunarodnih organizacija, i, ako je predviđeno posebnim aranžmanima, za druge institucije, agencije i tijela Unije.

3. Na razini Komisije sigurnosno tijelo ustrojava registarski ured koji djeluje kao središnje tijelo za primanje i slanje podataka klasificiranih stupnjem tajnosti TRES SECRET UE/EU TOP SECRET. Za postupanje s tim podacima u svrhu njihove registracije po potrebi je moguće ustrojiti registarske podurede.

4. Registarski poduredi ne smiju dokumente klasificirane stupnjem tajnosti TRES SECRET UE/EU TOP SECRET slati izravno u druge podurede istog središnjeg registarskog ureda namijenjenog podacima klasificiranima stupnjem tajnosti TRES SECRET UE/EU TOP SECRET ili van bez izričitog pisanog odobrenja potonjeg.

5. Registarski uredi klasificiranih podataka EU-a ustrojavaju se kao sigurnosne zone, kako je definirano Poglavljem 3., te podliježu akreditaciji Komisijina tijela za sigurnosnu akreditaciju.

Članak 28.

Nadzorni službenik registarskog ureda

1. Svakim registarskim uredom klasificiranih podataka EU-a upravlja nadzorni službenik registarskog ureda (RCO).

2. RCO prolazi odgovarajuću sigurnosnu provjeru.

3. Kada je riječ o primjeni odredaba koje se odnose na postupanje s klasificiranim dokumentima EU-a i poštovanju relevantnih sigurnosnih pravila, standarda i smjernica, rad RCO-a nadzire LSS predmetne službe Komisije.

4. Budući da je odgovoran za upravljanje registrom klasificiranih podataka EU-a koji mu je dodijeljen, RCO u skladu s ovom Odlukom i relevantnim provedbenim pravilima, standardima i smjernicama preuzima sljedeće opće zadaće:

— upravljanje operacijama povezanima s registracijom, čuvanjem, umnožavanjem, prevođenjem, prijenosom, slanjem i uništavanjem klasificiranih podataka EU-a ili njihovim prebacivanjem u službu povijesnih arhiva;

— periodičko preispitivanje potrebe da se podaci smatraju tajnima;

— obavljanje drugih zadataka povezanih sa zaštitom klasificiranih podataka EU-a, a koji su utvrđeni provedbenim pravilima.

Članak 29.

Registracija klasificiranih podataka EU-a u sigurnosne svrhe

1. Za potrebe ove Odluke, registracija u sigurnosne svrhe (dalje u tekstu „registracija”) znači primjena postupaka za evidentiranje životnog ciklusa klasificiranih podataka EU-a, uključujući njihovo širenje.

([1]) Uredba Vijeća (EZ, Euratom) br. 1700/2003 od 22. rujna 2003. o izmjeni Uredbe (EEZ, Euratom) br. 354/83 o otvaranju za javnost povijesnih arhiva Europske ekonomske zajednice i Europske zajednice za atomsku energiju (SL L 243, 27.9.2003., str. 1.).

2. Svi podaci ili materijali klasificirani stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i višim registriraju se u relevantnim registarskim uredima u trenutku njihova zaprimanja u organizaciju ili njihova slanja iz organizacije.

3. Pri postupanju s klasificiranim podacima EU-a ili njihovu čuvanju s pomoću komunikacijskog i informacijskog sustava (CIS), postupci registracije mogu se obavljati putem procesa u samom CIS-u.

4. Detaljnije odredbe o registraciji klasificiranih podataka EU-a u sigurnosne svrhe propisuju se u provedbenim pravilima.

Članak 30.

Umnožavanje i prevođenje klasificiranih dokumenata EU-a

1. Dokumenti klasificirani stupnjem tajnosti TRES SECRET UE/EU TOP SECRET ne smiju se umnožavati ili prevoditi bez prethodne pisane suglasnosti autora.

2. Ako autor dokumenata klasificiranih stupnjem tajnosti SECRET UE/EU SECRET ili nižim nije odredio upozorenja u pogledu umnožavanja ili prijevoda, takvi se dokumenti mogu umnožavati ili prevoditi prema uputi imatelja.

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

Članak 31.

Prijenos klasificiranih podataka EU-a

1. Klasificirani podaci EU-a tijekom prijenosa moraju biti zaštićeni od neovlaštenog otkrivanja.

2. Prijenos klasificiranih podataka EU-a podliježe zaštitnim mjerama koje su:

— razmjerne stupnju tajnosti klasificiranih podataka EU-a koji se prenose i

— prilagođene posebnim uvjetima prijenosa tih podataka, posebice ovisno o tome prenose li se klasificirani podaci EU-a:

  — unutar zgrade Komisije ili kompleksa zgrada Komisije;

  — između zgrada Komisije koje se nalaze na državnom području iste države članice;

  — unutar Unije;

  — iz Unije na državno područje treće države; i

  — prilagođene vrsti i obliku klasificiranih podataka EU-a.

3. Te su zaštitne mjere detaljno navedene u provedbenim pravilima, odnosno, u slučaju projekata i programa iz članka 42., sastavni su dio relevantnih sigurnosnih uputa za programe i projekte (SUP).

4. Provedbena pravila ili sigurnosne upute za programe i projekte uključuju odredbe razmjerne stupnju tajnosti klasificiranih podataka EU-a, koje se odnose na:

— vrstu prijenosa, kao što je ručni prijenos, prijenos diplomatskom ili vojnom poštom, prijenos poštanskom službom ili komercijalnom kurirskom službom;

— pakiranje klasificiranih podataka EU-a;

— tehničke protumjere za klasificirane podatke EU-a koji se prenose na elektroničkim medijima;

— sve ostale postupovne, fizičke ili elektroničke mjere;

— postupke registracije;

— uporabu sigurnosno ovlaštenog osoblja.

5. Ako se klasificirani podaci EU-a prenose na elektroničkim medijima i neovisno o članku 21. stavku 5., zaštitne mjere iz relevantnih provedbenih pravila mogu se dopuniti odgovarajućim tehničkim protumjerama koje je odobrilo sigurnosno tijelo Komisije kako bi se umanjio rizik od gubitka ili ugroze.

Članak 32.

Uništavanje klasificiranih podataka EU-a

1. Klasificirani podaci EU-a koji više nisu potrebni mogu se uništiti uzimajući u obzir propise o arhivima i Komisijina pravila i propise o upravljanju dokumentima i arhiviranju, a posebice u skladu sa zajedničkim popisom čuvanja dokumenata Europske komisije.

2. Podatke EU-a klasificirane stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL i višim uništava RCO relevantnog registarskog ureda klasificiranih podataka EU-a na nalog imatelja ili nadležnog tijela. U skladu s time RCO ažurira očevidnike i ostale registracijske podatke.

3. Dokumente klasificirane stupnjem tajnosti SECRET UE/EU SECRET ili TRES SECRET UE/EU TOP SECRET uništava RCO u nazočnosti svjedoka koji je prošao sigurnosnu provjeru najmanje za stupanj tajnosti dokumenta koji se uništava.

4. Registrar i svjedok, ako se zahtijeva nazočnost potonjeg, potpisuju potvrdu o uništavanju koja se pohranjuje u registarskom uredu. RCO nadležnog registrarskog ureda klasificiranih podataka EU-a čuva potvrde o uništavanju dokumenata klasificiranih stupnjem tajnosti TRES SECRET UE/EU TOP SECRET najmanje 10 godina, a dokumenata klasificiranih stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET najmanje pet godina.

5. Klasificirani dokumenti, uključujući one klasificirane stupnjem tajnosti RESTREINT UE/EU RESTRICTED, uništavaju se na način definiran provedbenim pravilima i koji ispunjuje relevantne standarde EU-a ili jednakovrijedne standarde.

6. Računalni nosači podataka korišteni za klasificirane podatke EU-a uništavaju se u skladu s postupcima propisanima provedbenim pravilima.

Članak 33.

Uništavanje klasificiranih podataka EU-a u izvanrednim situacijama

1. Službe Komisije koje imaju klasificirane podatke EU-a na temelju lokalnih uvjeta pripremaju planove za sigurno čuvanje tajnog materijala EU-a u izvanrednim situacijama, uključujući prema potrebi planove za njegovo hitno uništavanje i premještanje. One izdaju upute potrebne kako bi se spriječilo da klasificirani podaci EU-a postanu dostupni neovlaštenim osobama.

2. Mjere za čuvanje i/ili uništavanje materijala s oznakom CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET u izvanrednim situacijama ne smiju ni u kakvim okolnostima ugrožavati zaštitu ili uništavanje materijala s oznakom TRES SECRET UE/EU TOP SECRET, uključujući opremu za šifriranje čije zbrinjavanje ima prioritet nad svim ostalim zadaćama.

3. Ako u izvanrednoj situaciji postoji neposredna opasnost od neovlaštenog otkrivanja, imatelj uništava klasificirane podatke EU-a tako da se ne mogu djelomično ili u cijelosti rekonstruirati. O hitnom uništenju registriranih klasificiranih podataka EU-a mora se obavijestiti autor i izvorni registar.

4. Detaljnije odredbe o uništavanju klasificiranih podataka EU-a sadržane su u provedbenim pravilima.

POGLAVLJE 5.

ZAŠTITA KLASIFICIRANIH PODATAKA EU-A U KOMUNIKACIJSKIM I INFORMACIJSKIM SUSTAVIMA (CIS)

Članak 34.

Osnovna načela informacijske sigurnosti

1. Informacijska sigurnost u području komunikacijskih i informacijskih sustava jest povjerenje da će ti sustavi štititi podatke s kojima postupaju i da će funkcionirati onako kako trebaju i kada trebaju, pod nadzorom zakonitih korisnika.

2. Učinkovitom informacijskom sigurnošću osigurava se primjerena razina sljedećih svojstava:

autentičnost: jamstvo da je podatak istinit i da potječe iz dobronamjernih (*bona fide*) izvora;

raspoloživost: svojstvo podatka koji je ovlaštenom subjektu dostupan i iskoristiv na zahtjev;

povjerljivost: svojstvo podatka koji se ne otkriva neovlaštenim osobama, subjektima ili procesima;

integritet: svojstvo čuvanja točnosti i cjelovitosti sredstava i podataka;

nepobitnost: sposobnost dokazivanja da se dogodila određena radnja ili da je nastupio određeni događaj tako da to kasnije nije moguće zanijekati.

3. Informacijska sigurnost temelji se na procesu upravljanja rizikom.

Članak 35.

Definicije

Za potrebe ovog poglavlja primjenjuju se sljedeće definicije:

(a) „akreditacija" znači formalno ovlaštenje i odobrenje koje tijelo za sigurnosnu akreditaciju izdaje za komunikacijski i informacijski sustav koji obrađuje klasificirane podatke EU-a u svojem operativnom okruženju nakon formalne validacije sigurnosnog plana i njegove pravilne provedbe;

(b) „akreditacijski postupak" znači koraci i radnje koje je potrebno poduzeti prije dobivanja akreditacije od tijela za sigurnosnu akreditaciju. Ti se koraci i radnje definiraju u dokumentu o standardima akreditacijskog postupka;

(c) „komunikacijski i informacijski sustav" (CIS) znači svaki sustav koji omogućuje postupanje s podacima u elektroničkom obliku. Komunikacijski i informacijski sustav obuhvaća sva sredstva potrebna za njegovo funkcioniranje, uključujući infrastrukturu, organizaciju, osoblje i informacijske resurse;

(d) „preostali rizik" znači rizik koji ostaje nakon provedbe sigurnosnih mjera, s obzirom na to da se ne mogu suzbiti sve prijetnje i ukloniti sve slabe točke;

(e) „rizik" znači mogućnost da će određena prijetnja iskoristiti unutarnje i vanjske slabe točke organizacije ili bilo kojeg sustava koji organizacija koristi i na taj način naštetiti organizaciji i njezinoj materijalnoj i nematerijalnoj imovini. Mjeri se kao kombinacija vjerojatnosti pojave prijetnji i njihova učinka;

(f) „prihvaćanje rizika" jest odluka o tome da je preostali rizik i dalje prisutan nakon postupanja s rizikom;

(g) „procjena rizika" sastoji se od prepoznavanja prijetnji i slabih točaka te provedbe povezane analize rizika, tj. analize vjerojatnosti pojave i učinka;

(h) „obavješćivanje o rizicima" sastoji se od razvijanja svijesti o rizicima u zajednicama korisnika CIS-a, informiranja tijela za odobrenja o tim rizicima i izvješćivanja operativnih tijela o njima;

(i) „postupanje s rizicima" znači ublažavanje, otklanjanje, smanjivanje (odgovarajućom kombinacijom tehničkih, fizičkih, organizacijskih ili postupovnih mjera), prijenos ili praćenje rizika.

Članak 36.

CIS u postupanju s klasificiranim podacima EU-a

1. CIS postupa s klasificiranim podacima EU-a u skladu s konceptom informacijske sigurnosti.

2. Kada CIS postupa s klasificiranim podacima EU-a, sukladnost s Komisijinom politikom sigurnosti informacijskih sustava iz Odluke Komisije C(2006)3602 ([1]) podrazumijeva sljedeće:

(a) pristup „isplaniraj – provedi – provjeri – djeluj" primjenjuje se na provedbu politike sigurnosti informacijskih sustava tijekom cijelog životnog ciklusa informacijskog sustava;

(b) sigurnosne potrebe moraju se identificirati putem procjene učinka na poslovanje;

(c) informacijski sustav i podaci koje sadržava moraju se formalno klasificirati kao sredstva;

([1]) C(2006) 3602 od 16. kolovoza 2006. o sigurnosti informacijskih sustava kojima se koristi Europska komisija.

(d) moraju se provoditi sve obvezne sigurnosne mjere, u skladu s politikom sigurnosti informacijskih sustava;

(e) mora se primjenjivati proces upravljanja rizikom, koji se sastoji od sljedećih koraka: identifikacija prijetnji i slabih točaka, procjena rizika, postupanje s rizikom, prihvaćanje rizika i obavješćivanje o riziku;

(f) potrebno je definirati, provoditi, provjeravati i preispitivati sigurnosni plan, uključujući sigurnosnu politiku i sigurnosno-operativne postupke.

3. Osoblje koje radi na oblikovanju, razvoju i testiranju CIS-a za postupanje s klasificiranim podacima EU-a, koje rukuje ili upravlja tim sustavom ili se njime koristi obavješćuje tijelo za sigurnosnu akreditaciju o svim potencijalnim sigurnosnim slabostima i incidentima te povredama sigurnosti ili ugrozama koje bi mogle utjecati na zaštitu CIS-a i/ili klasificiranih podataka EU-a koje on sadržava.

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

(a) prednost se daje proizvodima koje je odobrilo Vijeće ili Glavno tajništvo Vijeća u svojstvu tijela Vijeća nadležnog za odobravanje kriptomaterijala, na preporuku Komisijine stručne skupine za sigurnost;

(b) ako je to opravdano posebnim operativnim razlozima, Komisijino tijelo za odobravanje kriptomaterijala može, na preporuku Komisijine stručne skupine za sigurnost, primijeniti izuzeće od zahtjeva iz točke a) i izdati privremeno odobrenje za određeno razdoblje.

5. Tijekom prijenosa, obrade i pohranjivanja klasificiranih podataka EU-a elektroničkim sredstvima upotrebljavaju se odobreni kriptografski proizvodi. Neovisno o tom zahtjevu, u izvanrednim se okolnostima ili u slučaju posebnih tehničkih konfiguracija uz odobrenje Komisijina tijela za odobravanje kriptomaterijala mogu primjenjivati posebni postupci.

6. Kada CIS postupa s podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili višim provode se sigurnosne mjere kojima se ti podaci štite od ugroze izazvane nenamjernim elektromagnetskim zračenjem („sigurnosne mjere TEMPEST”). Takve sigurnosne mjere razmjerne su riziku od iskorištavanja i stupnju tajnosti podataka.

7. Sigurnosno tijelo Komisije preuzima sljedeće funkcije:

— tijelo za informacijsku sigurnost (IAA);

— tijelo za sigurnosnu akreditaciju (SAA);

— tijelo za TEMPEST (TA);

— tijelo za odobravanje kriptomaterijala (CAA);

— tijelo za distribuciju kriptomaterijala (CDA).

8. Sigurnosno tijelo Komisije za svaki sustav imenuje operativno tijelo za informacijsku sigurnost.

9. Odgovornosti koje podrazumijevaju funkcije iz stavaka 7. i 8. definirat će se u provedbenim pravilima.

Članak 37.

Akreditacija CIS-a za postupanje s klasificiranim podacima EU-a

1. Svaki CIS koji postupa s klasificiranim podacima EU-a prolazi akreditacijski postupak, temeljen na načelu informacijske sigurnosti, čija podrobnost mora biti razmjerna potrebnoj razini zaštite.

2. Akreditacijski postupak uključuje formalnu validaciju sigurnosnog plana za predmetni CIS koju obavlja Komisijino tijelo za sigurnosnu akreditaciju kako bi se osiguralo da je:

(a) proces upravljanja rizikom iz članka 36. stavka 2. propisno proveden;

(b) vlasnik sustava svjesno prihvatio preostali rizik; i

(c) u skladu s ovom Odlukom postignuta dostatna razina zaštite CIS-a i klasificiranih podataka EU-a s kojima se u okviru njega postupa.

3. Komisijino tijelo za sigurnosnu akreditaciju izdaje izjavu o akreditaciji u kojoj se utvrđuje najviši stupanj tajnosti podataka EU-a s kojima CIS može postupati i odgovarajući operativni uvjeti sustava. Time se ne dovode u pitanje zadaće povjerene Odboru za sigurnosnu akreditaciju (SAB) iz članka 11. Uredbe (EU) br. 512/2014 Europskog parlamenta i Vijeća ([1]).

4. Zajednički Odbor za sigurnosnu akreditaciju nadležan je za akreditaciju Komisijina CIS-a i uključuje više strana. Sastavljen je od predstavnika tijela za sigurnosnu akreditaciju svih uključenih strana, a njime predsjeda predstavnik Komisijina tijela za sigurnosnu akreditaciju.

5. Akreditacijski postupak sastoji se od niza zadataka koje obavljaju uključene strane. Odgovornost za pripremu akreditacijskih spisa i dokumentacije u potpunosti snosi vlasnik CIS-a.

6. Za akreditaciju je nadležno Komisijino tijelo za sigurnosnu akreditaciju, koje u bilo kojem trenutku životnog ciklusa CIS-a ima pravo:

(a) zahtijevati primjenu akreditacijskog postupka;

(b) provesti reviziju ili inspekciju CIS-a;

(c) u slučaju nepoštovanja operativnih uvjeta, zahtijevati da se u jasno definiranom roku osmisli i u djelo provede plan za jačanje sigurnosti, uz moguće povlačenje odobrenja za rad s CIS-om dok se operativni uvjeti ne počnu ponovno zadovoljavati.

7. Akreditacijski postupak utvrđuje se u dokumentu o standardima akreditacijskog postupka za CIS u postupanju s klasificiranim podacima EU-a, koji se donosi u skladu s člankom 10. stavkom 3. Odluke C(2006) 3602.

Članak 38.

Izvanredne okolnosti

1. Neovisno o odredbama ovog poglavlja, u nastavku opisani posebni postupci mogu se primjenjivati u izvanrednoj situaciji, primjerice tijekom prijeteće ili stvarne krize, sukoba, rata ili u izvanrednim operativnim okolnostima.

2. Klasificirani podaci EU-a mogu se slati s 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 bi neupitno bila veća od štete uzrokovane otkrivanjem klasificiranih podataka i ako:

(a) pošiljatelj i primatelj nemaju potreban uređaj za kodiranje; i

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

3. Klasificirani podaci preneseni u okolnostima navedenima u stavku 1. nemaju nikakve oznake ili upozorenja prema kojima se razlikuju od podataka koji nisu klasificirani ili koji se mogu zaštiti raspoloživim kriptografskim proizvodom. Primatelje se bez odgode obavješćuje o stupnju tajnosti drugim sredstvima.

4. Naknadno se podnosi izvješće nadležnom tijelu i Komisijinoj stručnoj skupini za sigurnost.

POGLAVLJE 6.

GOSPODARSKA SIGURNOST

Članak 39.

Osnovna načela

1. Gospodarska sigurnost primjena je mjera kojima zaštitu klasificiranih podataka EU-a

(a) u okviru klasificiranih ugovora osiguravaju:

i. kandidati ili ponuditelji tijekom cijelog natječajnog postupka i postupka dodjele ugovora;

ii. ugovaratelji ili podugovaratelji tijekom cijelog životnog ciklusa klasificiranih ugovora;

([1]) Uredba (EU) br. 512/2014 Europskog parlamenta i Vijeća od 16. travnja 2014. o izmjeni Uredbe (EU) br. 912/2010 o osnivanju Europske agencije za GNSS (SL L 150, 20.5.2014., str. 72.).

(b) u okviru klasificiranih ugovora o bespovratnim sredstvima osiguravaju:

i. podnositelji zahtjeva tijekom postupaka dodjele bespovratnih sredstava;

ii. korisnici tijekom životnog ciklusa klasificiranih ugovora o bespovratnim sredstvima.

2. Nijedan od tih ugovora ne smije uključivati podatke koji su klasificirani stupnjem tajnosti TRES SECRET UE/EU TOP SECRET.

3. Osim ako je drukčije navedeno, odredbe koje se u ovom poglavlju odnose na klasificirane ugovore ili ugovaratelje primjenjive su i na klasificirane podugovore ili podugovaratelje.

Članak 40.

Definicije

Za potrebe ovog poglavlja primjenjuju se sljedeće definicije:

(a) „klasificirani ugovor" znači okvirni ugovor ili ugovor, kako je navedeno u Uredbi Vijeća (EZ, Euratom) br. 1605/2002 ([1]), koji Komisija ili jedna od njezinih službi sklapa s ugovarateljem za nabavu pokretne ili nepokretne imovine, izvođenje radova ili pružanje usluga, čije izvršenje zahtijeva ili uključuje stvaranje klasificiranih podataka EU-a, postupanje s njima ili njihovo čuvanje;

(b) „klasificirani podugovor" znači ugovor sklopljen između ugovaratelja Komisije ili jedne od njezinih službi i drugog ugovaratelja (tj. podugovaratelja) za nabavu pokretne ili nepokretne imovine, izvođenje radova ili pružanje usluga, čije izvršenje zahtijeva ili uključuje stvaranje klasificiranih podataka EU-a, postupanje s njima ili njihovo čuvanje;

(c) „klasificirani ugovor o bespovratnim sredstvima" znači ugovor u okviru kojeg Komisija dodjeljuje bespovratna sredstva, kako je navedeno u dijelu I., glavi VI. Uredbe (EZ, Euratom) br. 1605/2002, čije izvršenje zahtijeva ili uključuje stvaranje klasificiranih podataka EU-a, postupanje s njima ili njihovo čuvanje;

(d) „zaduženo sigurnosno tijelo" (ZST) znači tijelo koje odgovara nacionalnom sigurnosnom tijelu (NST) države članice nadležnom za obavješćivanje gospodarskih i drugih subjekata o nacionalnoj politici u pogledu svih pitanja gospodarske sigurnosti te za davanje smjernica i pružanje pomoći u njezinoj provedbi. Funkciju ZST-a može obavljati NST ili bilo koje drugo nadležno tijelo.

Članak 41.

Postupak za klasificirane ugovore i klasificirane ugovore o bespovratnim sredstvima

1. Svaka služba Komisije, u svojstvu tijela za ugovaranje, osigurava da minimalni standardi gospodarske sigurnosti iz ovog poglavlja budu navedeni u ugovoru ili ugrađeni u njega, te da ih se poštuje pri dodjeljivanju klasificiranih ugovora i klasificiranih ugovora o bespovratnim sredstvima.

2. Za potrebe stavka 1., nadležne službe u Komisiji savjetuju se s Glavnom upravom za ljudske resurse i sigurnost, a posebice njezinom Upravom za sigurnost te osiguravaju da modeli ugovora i podugovora te ugovora o bespovratnim sredstvima uključuju odredbe koje odražavaju osnovna načela i minimalne standarde za zaštitu klasificiranih podataka EU-a koje ugovaratelji i podugovaratelji te korisnici bespovratnih sredstava moraju poštovati.

3. Komisija usko surađuje s NST-om, ZST-om ili drugim nadležnim tijelom dotične države članice.

4. Kada namjerava pokrenuti postupak za sklapanje klasificiranog ugovora ili klasificiranog ugovora o bespovratnim sredstvima, tijelo za ugovaranje savjetuje se sa sigurnosnim tijelom Komisije o pitanjima koja se odnose na povjerljivu prirodu i elemente postupka u svim njegovim fazama.

5. Predlošci i modeli za klasificirane ugovore i podugovore te klasificirane ugovore o bespovratnim sredstvima, pozive na natječaj, smjernice za situacije u kojima je potrebno uvjerenje o sigurnosnoj provjeri pravne osobe (USPPO), sigurnosne upute za programe i projekte (SUP), pisma o sigurnosnim aspektima, posjeti te slanje i prijenos klasificiranih podataka EU-a u okviru klasificiranih ugovora ili klasificiranih ugovora o bespovratnim sredstvima utvrđuju se u provedbenim pravilima o gospodarskoj sigurnosti nakon savjetovanja s Komisijinom stručnom skupinom za sigurnost.

([1]) Uredba Vijeća (EZ, Euratom) br. 1605/2002 od 25. lipnja 2002. o Financijskoj uredbi koja se primjenjuje na opći proračun Europskih zajednica (SL L 248, 16.9.2002., str. 1.).

6. Komisija može sklapati klasificirane ugovore ili klasificirane ugovore o bespovratnim sredstvima na temelju kojih određene zadatke koji uključuju ili podrazumijevaju pristup klasificiranim podacima EU-a, postupanje s njima ili njihovo čuvanje povjerava gospodarskim subjektima registriranima u državi članici ili trećoj zemlji s kojom je sklopljen sporazum ili administrativni dogovor u skladu s poglavljem 7. ove Odluke.

Članak 42.

Sigurnosni elementi klasificiranog ugovora ili klasificiranog ugovora o bespovratnim sredstvima

1. Klasificirani ugovori ili klasificirani ugovori o bespovratnim sredstvima obuhvaćaju sljedeće sigurnosne elemente:

Sigurnosne upute za program ili projekt

(a) „Sigurnosne upute za program ili projekt" (SUP) znači popis sigurnosnih postupaka koji se primjenjuju na određeni program ili projekt s ciljem standardizacije sigurnosnih postupaka. Mogu se mijenjati za vrijeme trajanja programa ili projekta.

(b) Glavna uprava za ljudske resurse i sigurnost sastavlja opći SUP, dok službe Komisije zadužene za programe i projekte koji podrazumijevaju postupanje s klasificiranim podacima EU-a i njihovo čuvanje mogu, prema potrebi, razvijati posebne SUP-ove, temeljene na općem SUP-u.

(c) Poseban SUP sastavlja se posebice za programe i projekte šireg područja primjene, većih razmjera ili složenosti, ili pak one koje odlikuje veći broj ili veća raznolikost ugovaratelja, korisnika i drugih partnera i dionika, primjerice s obzirom na pravni status. Poseban SUP razvijaju službe Komisije koje upravljaju programom ili projektom u uskoj suradnji s Glavnom upravom za ljudske resurse i sigurnost.

(d) Glavna uprava za ljudske resurse i sigurnost u procesu savjetovanja podnosi i opće i posebne SUP-ove Komisijinoj stručnoj skupini za sigurnost.

Pismo o sigurnosnim aspektima

(a) „Pismo o sigurnosnim aspektima" (SAL) znači skup posebnih ugovornih uvjeta koji izdaje tijelo za ugovaranje, te je sastavni dio klasificiranog ugovora koji uključuje pristup klasificiranim podacima EU-a ili njihovo stvaranje i njime se utvrđuju sigurnosni zahtjevi ili oni elementi ugovora koji zahtijevaju sigurnosnu zaštitu.

(b) Sigurnosni zahtjevi povezani s konkretnim ugovorom opisuju se u pismu o sigurnosnim aspektima. Prema potrebi, pismo o sigurnosnim aspektima sadržava vodič za stupnjeve tajnosti i sastavni je dio klasificiranog ugovora ili podugovora ili klasificiranog ugovora o bespovratnim sredstvima.

(c) Pismo o sigurnosnim aspektima sadržava odredbe kojima se od ugovaratelja ili korisnika traži poštovanje minimalnih standarda utvrđenih ovom Odlukom. Tijelo za ugovaranje osigurava da nepoštovanje tih minimalnih standarda bude u pismu o sigurnosnim aspektima navedeno kao dovoljan razlog za mogući raskid ugovora ili ugovora o bespovratnim sredstvima.

2. I SUP-ovi i pisma o sigurnosnim aspektima uključuju vodič za stupnjeve tajnosti kao obavezni sigurnosni element:

(a) „Vodič za stupnjeve tajnosti" (SCG) znači dokument u kojem su opisani klasificirani elementi programa, projekta, ugovora ili ugovora o bespovratnim sredstvima te navedeni primjenljivi stupnjevi tajnosti. Taj se vodič tijekom trajanja programa, projekta, ugovora ili ugovora o bespovratnim sredstvima može proširiti, a pojedini elementi podatka mogu se ponovno klasificirati ili im se može smanjiti stupanj tajnosti; ako vodič za stupnjeve tajnosti već postoji, on je dio pisma o sigurnosnim aspektima.

(b) Prije otvaranja natječaja ili dodjele klasificiranog ugovora, služba Komisije u svojstvu tijela za ugovaranje određuje stupanj tajnosti svakog podatka koji će se dostaviti kandidatima, ponuditeljima ili ugovarateljima, kao i stupanj tajnosti svakog podatka koji će stvoriti ugovaratelj. U tu svrhu, služba Komisije priprema vodič za stupnjeve tajnosti koji će se koristiti za izvršenje ugovora, u skladu s ovom Odlukom i njezinim provedbenim pravilima, nakon savjetovanja sa sigurnosnim tijelom Komisije.

(c) Za određivanje stupnja tajnosti različitih elemenata klasificiranog ugovora primjenjuju se sljedeća načela:

i. prilikom pripreme vodiča za stupnjeve tajnosti služba Komisije, u svojstvu tijela za ugovaranje, uzima u obzir sve važne sigurnosne aspekte, uključujući stupanj tajnosti dodijeljen podacima kojeg je autor dostavio i odobrio za uporabu u ugovoru;

ii. cjelokupni stupanj tajnosti ugovora ne smije biti niži od najvišeg stupnja tajnosti bilo kojeg njegova dijela; i

iii. prema potrebi, u slučaju bilo kakve promjene koja se odnosi na stupanj tajnosti podataka koje su stvorili ugovaratelji ili koji su dostavljeni ugovarateljima tijekom izvršenja ugovora i prilikom naknadnih izmjena vodiča za stupnjeve tajnosti tijelo za ugovaranje se preko sigurnosnog tijela Komisije povezuje s NST-om, ZST-om ili bilo kojim drugim sigurnosnim tijelom države članice nadležnim za konkretni predmet.

Članak 43.

Pristup klasificiranim podacima EU-a za osoblje ugovaratelja i korisnika

Tijelo za ugovaranje ili dodjelu bespovratnih sredstava osigurava da klasificirani ugovor ili klasificirani ugovor o bespovratnim sredstvima uključuje odredbe prema kojima se osoblju ugovaratelja, podugovaratelja ili korisnika kojem je, za potrebe izvršenja klasificiranog ugovora, podugovora ili ugovora o bespovratnim sredstvima, potrebno osigurati pristup klasificiranim podacima EU-a, taj pristup omogućuje samo ako je dotični član osoblja:

(a) sigurnosno ovlašten do odgovarajuće razine ili je drugačije propisno ovlašten na temelju nužnosti pristupa podacima;

(b) upoznat s primjenjivim sigurnosnim pravilima za zaštitu klasificiranih podataka EU-a te je dao izjavu u preuzimanju odgovornosti povezanih sa zaštitom takvih podataka;

(c) prošao sigurnosnu provjeru odgovarajuće razine za podatke klasificirane stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET koju provodi nadležni NST, ZST ili drugo nadležno tijelo.

Članak 44.

Uvjerenje o sigurnosnoj provjeri pravne osobe

1. „Uvjerenje o sigurnosnoj provjeri pravne osobe" (USPPO) znači potvrda koju izdaje NST, ZST ili drugo nadležno sigurnosno tijelo o tome da u pogledu sigurnosti pravna osoba može pružiti odgovarajuću razinu zaštite klasificiranih podataka EU-a određenog stupnja tajnosti.

2. Uvjerenje o sigurnosnoj provjeri pravne osobe koji izdaje NST, ZST ili drugo nadležno sigurnosno tijelo države članice, a u kojem se navodi, u skladu s nacionalnim zakonima i propisima, da gospodarski subjekt može u svojem objektu zaštititi klasificirane podatke EU-a s odgovarajućim stupnjem tajnosti (CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET), mora se dostaviti sigurnosnom tijelu Komisije, koje ga onda prosljeđuje službi Komisije koja djeluje u svojstvu tijela za ugovaranje ili dodjelu bespovratnih sredstava, kako bi kandidat, ponuditelj ili ugovaratelj odnosno podnositelj zahtjeva za bespovratna sredstva ili korisnik mogli dobiti pristup klasificiranim podacima EU-a.

3. Prema potrebi, tijelo za ugovaranje preko sigurnosnog tijela Komisije obavješćuje odgovarajući NST, ZST ili drugo nadležno sigurnosno tijelo o tome da je za izvršenje ugovora potreban USPPO. USPPO ili USP potrebni su ako se podaci EU-a klasificirani stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET moraju dostaviti tijekom natječajnog postupka ili postupka dodjele bespovratnih sredstava.

4. Tijelo za ugovaranje ili dodjelu bespovratnih sredstava ne dodjeljuje klasificirani ugovor ili klasificirani ugovor o dodjeli bespovratnih sredstava najboljem ponuditelju ili sudioniku prije nego što dobije potvrdu od NST-a, ZST-a ili drugog nadležnog sigurnosnog tijela države članice u kojoj je dotični ugovaratelj ili podugovaratelj registriran da je, prema potrebi, izdan odgovarajući USPPO.

5. Nakon što NST, ZST ili drugo nadležno sigurnosno tijelo koje je izdalo USPPO obavijesti sigurnosno tijelo Komisije o promjenama koje utječu na USPPO, potonje o tome obavješćuje službu Komisije koja djeluje u svojstvu tijela za ugovaranje ili dodjelu bespovratnih sredstava. U slučaju podugovora potrebno je na odgovarajući način obavijestiti NST, ZST ili drugo nadležno sigurnosno tijelo.

6. Ako nadležni NST, ZST ili drugo nadležno sigurnosno tijelo povuče USPPO, tijelo za ugovaranje ili dodjelu bespovratnih sredstava ima dovoljan razlog za raskid klasificiranog ugovora ili isključivanje kandidata, ponuditelja ili podnositelja zahtjeva iz natječaja. U buduće modele ugovora i ugovora za dodjelu bespovratnih sredstava uključuje se odredba u tom smislu.

Članak 45.

Odredbe za klasificirane ugovore i klasificirane ugovore o bespovratnim sredstvima

1. Ako se klasificirani podaci EU-a dostave kandidatu, ponuditelju ili podnositelju zahtjeva tijekom natječajnog postupka, poziv na natječaj ili poziv na podnošenje prijedloga mora sadržavati odredbu kojom se kandidat, ponuditelj ili podnositelj zahtjeva koji ne dostavi ponudu ili prijedlog ili ne bude izabran obvezuje na vraćanje svih klasificiranih dokumenata u određenom roku.

2. Tijelo za ugovaranje ili dodjelu bespovratnih sredstava preko sigurnosnog tijela Komisije obavješćuje nadležni NST, ZST ili drugo nadležno sigurnosno tijelo o tome da je klasificirani ugovor ili klasificirani ugovor o bespovratnim sredstvima dodijeljen te o relevantnim podacima, kao što su ime ugovaratelja ili korisnika, trajanje ugovora i maksimalni stupanj tajnosti.

3. Ako se takav ugovor ili ugovor o bespovratnim sredstvima raskine, tijelo za ugovaranje ili dodjelu bespovratnih sredstava preko sigurnosnog tijela Komisije o tome hitno obavješćuje NST, ZST ili drugo nadležno sigurnosno tijelo države članice u kojoj je ugovaratelj ili korisnik bespovratnih sredstava registriran.

4. Po raskidu klasificiranog ugovora ili ugovora o bespovratnim sredstvima ili po prestanku sudjelovanja korisnika bespovratnih sredstava, u pravilu se od dotičnog ugovaratelja ili korisnika bespovratnih sredstava zahtijeva da tijelu za ugovaranje ili za dodjelu bespovratnih sredstava vrati sve klasificirane podatke EU-a u svojem posjedu.

5. Posebne odredbe za raspolaganje klasificiranim podacima EU-a tijekom izvršenja klasificiranog ugovora ili klasificiranog ugovora o bespovratnim sredstvima ili nakon njihova raskida utvrđuju se u pismu o sigurnosnim aspektima.

6. Ako je ugovaratelj ili korisnik bespovratnih sredstava po raskidu klasificiranog ugovora ili klasificiranog ugovora o bespovratnim sredstvima ovlašten da zadrži klasificirane podatke EU-a, dužan je i dalje poštovati minimalne standarde iz ove Odluke te štititi tajnost klasificiranih podataka EU-a.

Članak 46.

Posebne odredbe za klasificirane ugovore

1. Uvjeti relevantni za zaštitu klasificiranih podataka EU-a pod kojima ugovaratelj može sklopiti podugovor određuju se u pozivu na natječaj i klasificiranom ugovoru.

2. Ugovaratelj je dužan od tijela za ugovaranje pribaviti odobrenje prije podugovaranja dijela klasificiranog ugovora. Uvjet za dodjelu podugovora koji podrazumijeva pristup klasificiranim podacima EU-a podugovarateljima registriranim u trećim zemljama jest postojanje regulatornog okvira za sigurnost podataka, u skladu s odredbama iz poglavlja 7.

3. Ugovaratelj mora osigurati da su sve aktivnosti podugovaranja poduzete u skladu s minimalnim standardima utvrđenima ovom Odlukom i ne smije dostavljati klasificirane podatke EU-a podugovaratelju bez prethodne pisane suglasnosti tijela za ugovaranje.

4. Kada je riječ o klasificiranim podacima EU-a koje je stvorio ili s kojima postupa ugovaratelj, Komisija se smatra autorom podataka, a prava koja joj kao autoru pripadaju ostvaruje tijelo za ugovaranje.

Članak 47.

Posjeti povezani s klasificiranim ugovorima

1. Ako je osoblju Komisije ili osoblju ugovaratelja ili korisnika bespovratnih sredstava za potrebe izvršenja klasificiranog ugovora potreban pristup podacima klasificiranima stupnjem tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET u prostorijama jednih ili drugih, posjeti se organiziraju u dogovoru s nadležnim NST-om, ZST-om ili drugim nadležnim sigurnosnim tijelom. O tim se posjetima obavješćuje sigurnosno tijelo Komisije. Međutim, u kontekstu posebnih programa ili projekata NST, ZST ili drugo nadležno sigurnosno tijelo može dogovoriti i postupak prema kojem se takvi posjeti organiziraju neposredno.

2. Kako bi dobili pristup klasificiranim podacima EU-a povezanima s klasificiranim ugovorom, svi posjetitelji moraju imati odgovarajuće uvjerenje o sigurnosnoj provjeri te nužnost pristupa podacima.

3. Posjetitelji imaju pristup samo onim klasificiranim podacima EU-a koji su povezani sa svrhom njihova posjeta.

4. Detaljnije odredbe utvrđuju se u provedbenim pravilima.

5. Poštovanje odredaba iz ove Odluke i provedbenih pravila iz stavka 4. koje se odnose na posjete povezane s klasificiranim ugovorima obvezno je.

Članak 48.

Slanje i prijenos klasificiranih podataka EU-a povezanih s klasificiranim ugovorima ili klasificiranim ugovorima o bespovratnim sredstvima

1. U pogledu slanja klasificiranih podataka EU-a elektroničkim sredstvima primjenjuju se odgovarajuće odredbe iz poglavlja 5. ove Odluke.

2. U pogledu prijenosa klasificiranih podataka EU-a primjenjuju se odgovarajuće odredbe iz poglavlja 4. ove Odluke i njezinih provedbenih pravila, u skladu s nacionalnim zakonima i propisima.

3. Prilikom određivanja sigurnosnih mjera za prijevoz klasificiranih podataka kao tereta primjenjuju se sljedeća načela:

(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) prije prekograničnog kretanja materijala klasificiranog kao CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET pošiljatelj sastavlja plan prijevoza koji odobrava nadležni NST, ZST ili drugo nadležno sigurnosno tijelo;

(d) 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;

(e) kada god je to moguće, pravci bi trebali prolaziti samo kroz države članice. Pravce kroz države koje nisu države članice moraju prethodno odobriti NST, ZST ili drugo nadležno sigurnosno tijelo države pošiljatelja i države primatelja.

Članak 49.

Prijenos klasificiranih podataka EU-a ugovarateljima ili korisnicima bespovratnih sredstava smještenima u trećim državama

Klasificirani se podaci EU-a prenose ugovarateljima ili korisnicima bespovratnih sredstava smještenima u trećim državama u skladu sa sigurnosnim mjerama dogovorenima između sigurnosnog tijela Komisije, službe Komisije, u svojstvu tijela za ugovaranje ili dodjelu bespovratnih sredstava, i NST-a, ZST-a ili drugog nadležnog sigurnosnog tijela treće države u kojoj je ugovaratelj ili korisnik registriran.

Članak 50.

Postupanje s podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED u kontekstu klasificiranih ugovora i klasificiranih ugovora o bespovratnim sredstvima

1. Zaštita podataka klasificiranih stupnjem tajnosti RESTREINT UE/EU RESTRICTED s kojima se postupa ili koji se čuvaju u okviru klasificiranih ugovora i klasificiranih ugovora o bespovratnim sredstvima temelji se na načelima proporcionalnosti i troškovne učinkovitosti.

2. U kontekstu klasificiranih ugovora i klasificiranih ugovora o bespovratnim sredstvima koji uključuju postupanje s podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED ne zahtijevaju se USPPO ili USP.

3. Ako ugovor ili ugovor o bespovratnim sredstvima uključuje postupanje s podacima klasificiranima stupnjem tajnosti RESTREINT UE/EU RESTRICTED u CIS-u kojim upravlja ugovaratelj ili korisnik bespovratnih sredstava, tijelo za ugovaranje ili dodjelu bespovratnih sredstava nakon savjetovanja sa sigurnosnim tijelom Komisije osigurava da su nužni tehnički i administrativni zahtjevi u pogledu akreditacije ili odobrenja CIS-a navedeni u ugovoru ili ugovoru o bespovratnim sredstvima razmjerni procijenjenom riziku, uzimajući u obzir sve važne čimbenike. Sigurnosno tijelo Komisije i nadležni NST ili ZST dogovaraju opseg akreditacije ili odobrenja tog CIS-a.

POGLAVLJE 7.

RAZMJENA KLASIFICIRANIH PODATAKA S DRUGIM INSTITUCIJAMA, AGENCIJAMA, TIJELIMA I UREDIMA UNIJE, S DRŽAVAMA ČLANICAMA I TREĆIM ZEMLJAMA TE MEĐUNARODNIM ORGANIZACIJAMA

Članak 51.

Osnovna načela

1. Kada Komisija ili neka od njezinih službi utvrdi da postoji potreba za razmjenom klasificiranih podataka EU-a s drugom institucijom, agencijom, tijelom ili uredom Unije, ili s trećom zemljom ili međunarodnom organizacijom, poduzimaju se koraci potrebni za uspostavljanje odgovarajućeg pravnog ili administrativnog okvira, koji može uključivati sporazume o sigurnosti podataka ili administrativne dogovore sklopljene u skladu s mjerodavnim propisima.

2. Ne dovodeći u pitanje članak 57., klasificirani podaci EU-a razmjenjuju se s drugim institucijama, agencijama, tijelima i uredima Unije, s trećim zemljama i međunarodnim organizacijama samo uz uvjet da postoji odgovarajući pravni ili administrativni okvir, te da postoje dovoljna jamstva o tome da dotična institucija, agencija, tijelo ili ured Unije, ili dotična treća zemlja ili međunarodna organizacija primjenjuje istovjetna osnovna načela i minimalne standarde za zaštitu klasificiranih podataka.

Članak 52.

Razmjena klasificiranih podataka EU-a s drugim institucijama, agencijama, tijelima i uredima Unije

1. Prije sklapanja administrativnog dogovora za razmjenu klasificiranih podataka EU-a s drugom institucijom, agencijom, tijelom ili uredom Unije, Komisija traži uvjerenje o tome da dotična institucija, agencija, tijelo ili ured Unije:

(a) posjeduje regulatorni okvir za zaštitu klasificiranih podataka EU-a kojim su utvrđena osnovna načela i minimalni standardi istovjetni onima utvrđenim ovom Odlukom i njezinim provedbenim pravilima;

(b) primjenjuje sigurnosne standarde i smjernice koji se odnose na sigurnost osoblja, fizičku sigurnost, upravljanje klasificiranim podacima EU-a i sigurnost komunikacijskih i informacijskih sustava (CIS), te koji jamče razinu zaštite klasificiranih podataka EU-a istovjetnu Komisijinoj.

(c) označuje klasificirane podatke koje stvara kao klasificirane podatke EU-a.

2. Glavna uprava za ljudske resurse i sigurnost, u uskoj suradnji s drugim nadležnim službama Komisije, glavno je tijelo u Komisiji zaduženo za sklapanje administrativnih dogovora za razmjenu klasificiranih podataka EU-a s drugim institucijama, agencijama, tijelima ili uredima Unije.

3. Administrativni dogovori u pravilu se sklapaju razmjenom pisama koja u ime Komisije potpisuje glavni direktor za ljudske resurse i sigurnost.

4. Prije sklapanja administrativnog dogovora o razmjeni klasificiranih podataka EU-a, sigurnosno tijelo Komisije provodi posjet radi procjene regulatornog okvira za zaštitu klasificiranih podataka EU-a te provjere učinkovitosti mjera kojima se štite klasificirani podaci EU-a. Administrativni dogovor stupa na snagu, a klasificirani se podaci EU-a razmjenjuju samo ako je ishod posjeta radi procjene stanja zadovoljavajući i ako se poštuju preporuke dane nakon posjeta. Poduzimaju se i redoviti popratni posjeti radi procjene stanja kako bi se provjerilo da se administrativni dogovor poštuje te da postojeće sigurnosne mjere i dalje ispunjuju utvrđena osnovna načela i minimalne standarde.

5. Registarski ured klasificiranih podataka EU-a kojim upravlja Glavno tajništvo u pravilu je, na razini Komisije, glavna točka ulaska i izlaska za razmjenu klasificiranih podataka s drugim institucijama, agencijama, tijelima i uredima Unije. Međutim, ako je zbog sigurnosnih, organizacijskih ili operativnih razloga zaštitu klasificiranih podataka EU-a primjerenije organizirati preko lokalnih registarskih ureda uspostavljenih u službama Komisije u skladu s ovom Odlukom i njezinim provedbenim pravilima, tada ti lokalni registarski uredi klasificiranih podataka EU-a postaju točke ulaska i izlaska za klasificirane podatke povezane s pitanjima u nadležnosti dotičnih službi Komisije.

6. O procesu sklapanja administrativnih dogovora u skladu sa stavkom 2. obavješćuje se Komisijina stručna skupina za sigurnost.

Članak 53.

Razmjena klasificiranih podataka EU-a s državama članicama

1. Klasificirani podaci EU-a mogu se prenositi državama članicama ili razmjenjivati s njima uz uvjet da one štite te podatke u skladu sa zahtjevima primjenjivima na klasificirane podatke koji su na nacionalnoj razini označeni istovjetnim stupnjem tajnosti prema tablici ekvivalentnosti stupnjeva tajnosti sadržanoj u Prilogu I.

2. Ako države članice uvedu klasificirane podatke s oznakom nacionalnog stupnja tajnosti u strukture ili mreže Europske unije, Komisija štiti navedene podatke u skladu sa zahtjevima primjenljivima na klasificirane podatke EU-a na istovjetnoj razini prema tablici ekvivalentnosti stupnjeva tajnosti sadržanoj u Prilogu I.

Članak 54.

Razmjena klasificiranih podataka s trećim državama i međunarodnim organizacijama

1. Ako Komisija utvrdi da postoji dugoročna potreba za razmjenom klasificiranih podataka s trećim zemljama ili međunarodnim organizacijama, poduzimaju se koraci potrebni za uspostavljanje odgovarajućeg pravnog ili administrativnog okvira, koji može uključivati sporazume o sigurnosti podataka ili administrativne dogovore sklopljene u skladu s mjerodavnim propisima.

2. Sporazumi o sigurnosti podataka ili administrativni dogovori iz stavka 1. sadržavaju odredbe kojima se osigurava odgovarajuća zaštita podataka koje prime treće države ili međunarodne organizacije u skladu sa stupnjem tajnosti tih podataka i minimalnim standardima koji su istovjetni onima utvrđenima ovom Odlukom.

3. Komisija može sklapati administrativne dogovore u skladu s člankom 56. ako stupanj tajnosti klasificiranih podataka EU-a u pravilu nije viši od RESTREINT UE/EU RESTRICTED.

4. Administrativni dogovori o razmjeni klasificiranih podataka iz stavka 3. sadržavaju odredbe kojima se osigurava odgovarajuća zaštita podataka koje prime treće države ili međunarodne organizacije u skladu sa stupnjem tajnosti tih podataka i minimalnim standardima koji su istovjetni onima utvrđenima ovom Odlukom. U pogledu sklapanja sporazuma o sigurnosti podataka ili administrativnih dogovora potrebno je savjetovati se s Komisijinom stručnom skupinom za sigurnost.

5. Odluku o prenošenju klasificiranih podataka EU-a čiji je autor Komisija trećoj državi ili međunarodnoj organizaciji donosi služba Komisije, koja je autor tih podataka u Komisiji, za svaki slučaj posebno, ovisno o prirodi i sadržaju podatka, primateljevom nužnosti za pristupom podacima i koristi koju će imati Unija. Ako Komisija nije autor klasificiranih podataka koji se žele prenijeti ili izvornog materijala koji ti podaci sadržavaju, služba Komisije koja ima te klasificirane podatke najprije mora zatražiti autorovu pisanu suglasnost za prijenos podataka. Ako se autora ne može odrediti, služba Komisije koja ima te klasificirane podatke, nakon savjetovanja s Komisijinom stručnom skupinom za sigurnost preuzima odgovornost autora.

Članak 55.

Sporazumi o sigurnosti podataka

1. Sporazumi o sigurnosti podataka s trećim zemljama ili međunarodnim organizacijama sklapaju se u skladu s člankom 218. UFEU-a.

2. Sporazumima o sigurnosti podataka predviđeno je sljedeće:

(a) osnovna načela i minimalni standardi kojima se uređuje razmjena klasificiranih podataka između Unije i treće države ili međunarodne organizacije;

(b) tehnički provedbeni mehanizmi koje dogovaraju nadležna sigurnosna tijela mjerodavnih institucija i tijela Unije s jedne strane i nadležno sigurnosno tijelo treće države ili međunarodne organizacije s druge strane. U tim je mehanizmima uzeta u obzir razina zaštite predviđena postojećim sigurnosnim propisima, strukturama i postupcima treće države ili međunarodne organizacije.

(c) prije razmjene klasificiranih podataka u skladu sa sporazumom potvrđuje se da stranka primateljica može na odgovarajući način štititi i čuvati dostavljene joj podatke.

3. Ako se utvrdi potreba za razmjenom klasificiranih informacija u skladu s člankom 51. stavkom 1., Komisija se prema potrebi savjetuje s Europskom službom za vanjsko djelovanje, Glavnim tajništvom Vijeća i drugim institucijama i tijelima Unije kako bi odredila je li potrebno uputiti preporuku u skladu s člankom 218. stavkom 3. UFEU-a.

4. Nijedan se klasificirani podatak EU-a ne smije razmjenjivati elektroničkim sredstvima, osim ako je to izričito predviđeno sporazumom o sigurnosti podataka ili tehničkim provedbenim mehanizmima.

5. Registarski ured klasificiranih podataka EU-a kojim upravlja Glavno tajništvo u pravilu je, na razini Komisije, glavna točka ulaska i izlaska za razmjenu klasificiranih podataka s trećim zemljama i međunarodnim organizacijama. Međutim, ako je zbog sigurnosnih, organizacijskih ili operativnih razloga zaštitu klasificiranih podataka EU-a primjerenije organizirati preko lokalnih registarskih ureda uspostavljenih u službama Komisije u skladu s ovom Odlukom i njezinim provedbenim pravilima, tada ti lokalni registarski uredi klasificiranih podataka EU-a postaju točke ulaska i izlaska za klasificirane podatke povezane s pitanjima u nadležnosti dotičnih službi Komisije.

6. Kako bi se ocijenila učinkovitost sigurnosnih propisa, struktura i postupaka u trećoj zemlji ili međunarodnoj organizaciji, Komisija u suradnji s drugim institucijama, agencijama ili tijelima Unije te u dogovoru s dotičnom trećom zemljom ili međunarodnom organizacijom sudjeluje u posjetima radi procjene stanja. Tim se posjetima za procjenu stanja ocjenjuje sljedeće:

(a) mjerodavni regulatorni okvir za zaštitu klasificiranih podataka;

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

(c) postojeće sigurnosne mjere i postupci; i

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

Članak 56.

Administrativni dogovori

1. Ako u kontekstu političkog ili pravnog okvira Unije 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 sigurnosno tijelo Komisije nakon savjetovanja s Komisijinom stručnom skupinom za sigurnost utvrdilo da dotična stranka nema dovoljno razvijen sigurnosni sustav za sklapanje sporazuma o sigurnosti podataka, Komisija može s tim nadležnim tijelima treće zemlje ili međunarodne organizacije sklopiti administrativni dogovor.

2. Administrativni dogovor u pravilu ima oblik razmjene pisama.

3. Prije sklapanja dogovora provodi se posjet radi procjene stanja. O ishodu posjeta radi procjene stanja obavješćuje se Komisijinu stručnu skupinu za sigurnost. Ako postoje izvanredni razlozi za hitnu razmjenu klasificiranih podataka, klasificirani podaci EU-a mogu se otkriti uz uvjet da je učinjeno sve kako bi se takav posjet radi procjene stanja proveo što je prije moguće.

4. Nijedan klasificirani podatak EU-a ne smije se razmjenjivati elektroničkim sredstvima, osim ako je tako izričito navedeno u administrativnom dogovoru.

Članak 57.

Iznimno *ad hoc* otkrivanje klasificiranih podataka EU-a

1. U slučaju da ne postoji sporazum o sigurnosti podataka ili administrativni dogovor te ako Komisija ili neka od njezinih službi utvrdi da u kontekstu političkog ili pravnog okvira Unije postoji iznimna potreba za otkrivanjem klasificiranih podataka EU-a trećoj zemlji ili međunarodnoj organizaciji, sigurnosno tijelo Komisije u suradnji sa sigurnosnim tijelima treće zemlje ili međunarodne organizacije u mjeri u kojoj je to moguće provjerava jesu li njihovi sigurnosni propisi, strukture i postupci takvi da će klasificirani podaci EU-a koji im se otkriju biti zaštićeni prema standardima koji nisu manje strogi od onih utvrđenih ovom Odlukom.

2. Odluku o otkrivanju klasificiranih podataka EU-a trećoj zemlji ili međunarodnoj organizaciji donosi Komisija nakon savjetovanja sa svojom stručnom skupinom za sigurnost, a na temelju prijedloga člana Komisije nadležnog za sigurnosna pitanja.

3. Slijedom Komisijine odluke o otkrivanju klasificiranih podataka EU-a te uz prethodno pisano dopuštenje autora, uključujući autore izvornog materijala koji ti podaci mogu sadržavati, nadležna služba Komisije prosljeđuje predmetne podatke, koji nose oznaku o mogućnosti otkrivanja u kojoj se navodi treća zemlja ili međunarodna organizacija kojoj su podaci otkriveni. Prije ili nakon otkrivanja podataka dotična treća strana obvezuje se u pisanom obliku da će štititi primljene klasificirane podatke EU-a u skladu s osnovnim načelima i minimalnim standardima navedenima u ovoj Odluci.

POGLAVLJE 8.

ZAVRŠNE ODREDBE

Članak 58.

Zamjena prethodne odluke

Ovom se Odlukom stavlja izvan snage i zamjenjuje Odluka Komisije 2001/844/EZ, EZUČ, Euratom ([1]).

Članak 59.

Klasificirani podaci stvoreni prije stupanja na snagu ove Odluke

1. Svi podaci EU-a klasificirani u skladu s Odlukom 2001/844/EZ, EZUČ, Euratom i dalje su zaštićeni u skladu s odgovarajućim odredbama ove Odluke.

2. Na sve klasificirane podatke kojima je Komisija raspolagala na dan stupanja na snagu Odluke 2001/844/EZ, EZUČ, Euratom, uz iznimku klasificiranih podataka Euratoma, primjenjuje se sljedeće:

(a) ako ih je stvorila Komisija, i dalje se smatra da su automatski reklasificirani stupnjem tajnosti RESTREINT UE, osim ako ih je autor odlučio drugačije klasificirati do 31. siječnja 2002. te ako je o tome obavijestio sve strane kojima je dokument namijenjen;

(b) ako su ih stvorili autori izvan Komisije, ti podaci zadržavaju prvobitni stupanj tajnosti i kao takvi se smatraju klasificiranim podacima EU-a istovjetnog stupnja tajnosti, osim ako autor pristaje na ukidanje ili snižavanje stupnja tajnosti podatka.

Članak 60.

Provedbena pravila i sigurnosne obavijesti

1. Provedbena pravila za ovu Odluku donijet će se prema potrebi putem posebne odluke Komisije o ovlaštenju člana Komisije nadležnog za sigurnosna pitanja, u skladu s Poslovnikom.

2. Kada dobije ovlasti na temelju prethodno navedene odluke Komisije, član Komisije nadležan za sigurnosna pitanja može pripremiti sigurnosne obavijesti u kojima se navode sigurnosne smjernice i najbolja praksa u okviru područja primjene ove Odluke i njezinih provedbenih pravila.

3. Komisija može prenijeti zadaće navedene u prvom i drugom stavku ovog članka na glavnog direktora za ljudske resurse i sigurnost posebnom odlukom o prijenosu ovlasti, u skladu s Poslovnikom.

Članak 61.

Stupanje na snagu

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

Sastavljeno u Bruxellesu 13. ožujka 2015.

Za Komisiju

Predsjednik

Jean-Claude JUNCKER

([1]) Odluka Komisije 2001/844/EZ, EZUČ, Euratom od 29. studenoga 2001. o izmjeni njezina unutarnjeg Poslovnika (SL L 317, 3.12.2001., str. 1.).

PRILOG I.

EKVIVALENTNOST STUPNJEVA TAJNOSTI

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Euratom	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA 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.)	bilješka (1) u nastavku
Bugarska	Строго секретно	Секретно	Поверително	За служебно ползване
Češka	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danska	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Njemačka	Streng geheim	Geheim	VS (2) — Vertraulich	VS — Nur für den Dienstgebrauch
Estonija	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irska	Top Secret	Secret	Confidential	Restricted
Grčka	Άκρως Απόρρητο 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	bilješka (3) u nastavku
Hrvatska	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
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-Għola 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

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Rumunjska	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenija	Strogo tajno	Tajno	Zaupno	Interno
Slovačka	Prísne tajné	Tajné	Dôverné	Vyhradené
Finska	ERITTÄIN SALAINEN 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	UK TOP SECRET	UK SECRET	Ekvivalent ne postoji ([5])	UK OFFICIAL – SENSITIVE

([1]) Diffusion Restreinte/Beperkte Verspreiding nije stupanj tajnosti u Belgiji. Belgija s podacima klasificiranima kao „RESTREINT UE/EU RESTRICTED" postupa i štiti ih na način koji nije ništa manje strog od standarda i postupaka opisanih u sigurnosnim propisima Vijeća Europske unije.

([2]) Njemačka: VS = Verschlusssache

([3]) Francuska u svojem nacionalnom sustavu ne koristi stupanj tajnosti „RESTREINT". Francuska s podacima klasificiranima kao „RESTREINT UE/EU RESTRICTED" postupa i štiti ih 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.

([5]) Ujedinjena Kraljevina s podacima EU-a klasificiranima kao „CONFIDENTIEL UE/EU CONFIDENTIAL" postupa i štiti ih u skladu sa zaštitnim sigurnosnim zahtjevima za stupanj tajnosti „UK SECRET".

PRILOG II.

POPIS KRATICA

Akronim	Značenje
CA	Služba Crypto
CAA	Tijelo za odobravanje kriptomaterijala
CCTV	Televizija zatvorenog kruga
CDA	Tijelo za distribuciju kriptomaterijala
CIS	Komunikacijski i informacijski sustavi za postupanje s klasificiranim podacima EU-a
ZST	Zaduženo sigurnosno tijelo (Designated Security Authority, DSA)
EUCI	Klasificirani podaci EU-a
USPPO	Uvjerenje o sigurnosnoj provjeri pravne osobe (Facility Security Clearance, FSC)
IA	Informacijska sigurnost
IAA	Tijelo za informacijsku sigurnost
IDS	Sustav za otkrivanje neovlaštenog ulaska
IT	Informacijska tehnologija
LSS	Lokalni službenik sigurnosti (Local Security Officer, LSO)
NST	Nacionalno sigurnosno tijelo (National Security Authority, NSA)
USP	Uvjerenje o sigurnosnoj provjeri osobe (Personnel Security Clearance, PSC)
CSP	Certifikat o sigurnosnoj provjeri osobe (Personnel Security Clearance Certificate, PSCC)
SUP	Sigurnosne upute za program ili projekt (Programme/Project Security Instructions, PSI)
RCO	Nadzorni službenik registarskog ureda
SAA	Tijelo za sigurnosnu akreditaciju
SAL	Pismo o sigurnosnim aspektima
SCG	Vodič za stupnjeve tajnosti
SecOPs	Sigurnosni operativni postupci
TA	Tijelo za TEMPEST
UFEU	Ugovor o funkcioniranju EU-a

PRILOG III.

POPIS NACIONALNIH SIGURNOSNIH TIJELA

BELGIJA

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement;
15, rue des Petits Carmes
B-1000 Bruxelles
Tel. tajništva: +32 25014542
Faks: +32 25014596
E-pošta: nvo-ans@diplobel.fed.be

BUGARSKA

State Commission on Information Security
90 Cherkovna Str.
1505 Sofia
Telefon: +359 29333600
Faks: +359 29873750
E-pošta: dksi@government.bg
Web-mjesto: www.dksi.bg

ČEŠKA

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Telefon: +420 257283335
Faks: +420 257283110
E-pošta: czech.nsa@nbu.cz
Web-mjesto: www.nbu.cz

DANSKA

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Telefon: +45 33148888
Faks: +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Telefon: +45 33325566
Faks: +45 33931320

NJEMAČKA

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin
Telefon: +49 30186810
Faks: +49 30186811441
E-pošta: oesIII3@bmi.bund.de

ESTONIJA

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn
Telefon: +372 7170113 0019, +372 7170117
Faks: +372 7170213
E-pošta: nsa@mod.gov.ee

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
Telefon: +30 2106572045
+ 30 2106572009
Faks: +30 2106536279, +30 2106577612

ŠPANJOLSKA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid
Telefon: +34 913725000
Faks: +34 913725808
E-pošta: nsa-sp@areatec.com

FRANCUSKA

Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Pariz 07 SP
Telefon: +33 171758177
Faks: + 33 171758200

HRVATSKA

Ured Vijeća za nacionalnu sigurnost
Croatian NSA
Jurjevska 34
10000 Zagreb
Hrvatska
Telefon: +385 14681222
Faks: + 385 14686049
Web-mjesto: www.uvns.hr

IRSKA

National Security Authority
Department of Foreign Affairs
76 – 78 Harcourt Street
Dublin 2
Telefon: +353 14780822
Faks: +353 14082959

ITALIJA

Presidenza del Consiglio dei Ministri
D.I.S. – U.C.Se.
Via di Santa Susanna, 15
00187 Roma
Telefon: +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

Ministarstvo obrane
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia
Telefon: +357 22807569, +357 22807643,
+357 22807764
Faks: +357 22302351
E-pošta: cynsa@mod.gov.cy

LATVIJA

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV-1001 Riga
Telefon: +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
Telefon: +370 706 66701, +370 706 66702
Faks: +370 706 66700
E-pošta: nsa@vsd.lt

LUKSEMBURG

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luksemburg
Telefon: +352 24782210 centrala
+ 352 24782253 izravno biranje
Faks: +352 24782243

MAĐARSKA

Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Telefon: +36 (1) 7952303
Faks: +36 (1) 7950344

Poštanska adresa:
H-1357 Budapest, PO Box 2
E-pošta: nbf@nbf.hu
Web-mjesto: www.nbf.hu

MALTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Telefon: +356 21249844
Faks: +356 25695321

NIZOZEMSKA

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Telefon: +31 703204400
Faks: +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag
Telefon: +31 703187060
Faks: +31 703187522

AUSTRIJA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien
Telefon: +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
Telefon: +48 22 58 57 944
Faks: +48 22 58 57 443
E-pošta: nsa@abw.gov.pl
Web-mjesto: www.abw.gov.pl

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Telefon: +351 213031710
Faks: +351 213031711

RUMUNJSKA

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA – ORNISS National Registry Office for Classified Information)
4 Mures Street
012275 București
Telefon: +40 212245830
Faks: +40 212240714
E-pošta: nsa.romania@nsa.ro
Web-mjesto: www.orniss.ro

SLOVENIJA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Telefon: +386 14781390
Faks: +386 14781399
E-pošta: gp.uvtp@gov.si

SLOVAČKA

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava
Telefon: +421 268692314
Faks: +421 263824005
Web-mjesto: www.nbusr.sk

FINSKA

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Telefon: 16055890
Faks: +358 916055140
E-pošta: NSA@formin.fi

ŠVEDSKA

Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
S-103 39 Stockholm
Telefon: +46 84051000
Faks: +46 87231176
E-pošta: ud-nsa@foreign.ministry.se

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