32001D0844

3.12.2001. *SLUŽBENI LIST EUROPSKIH ZAJEDNICA* L 317/1

ODLUKA KOMISIJE

od 29. studenoga 2001.

o izmjeni njezina unutarnjeg Poslovnika

(priopćena pod brojem dokumenta C(2001) 3031)

(2001/844/EZ, EZUČ, Euratom)

KOMISIJA EUROPSKIH ZAJEDNICA,

uzimajući u obzir Ugovor o osnivanju Europske zajednice, a posebno njegov članak 218. stavak 2.,

uzimajući u obzir Ugovor o osnivanju Europske zajednice za ugljen i čelik, a posebno njegov članak 16.,

uzimajući u obzir Ugovor o osnivanju Europske zajednice za atomsku energiju, a posebno njegov članak 131.,

uzimajući u obzir Ugovor o Europskoj uniji, a posebno njegov članak 28. stavak 1. i članak 41. stavak 1.,

ODLUČILA JE:

Članak 1.

Pravilnik Komisije o sigurnosti, čiji je tekst priložen ovoj Odluci, dodaje se Poslovniku Komisije kao prilog.

Članak 2.

Ova Odluka stupa na snagu na dan objave u *Službenom listu Europskih zajednica.*

Primjenjuje se od 1. prosinca 2001.

Sastavljeno u Bruxellesu 29. studenoga 2001.

Za Komisiju
Predsjednik
Romano PRODI

PRILOG

PRAVILNIK KOMISIJE O SIGURNOSTI

budući da:

(1) Razvijanje djelatnosti Komisije na područjima koja zahtijevaju određeni stupanj klasifikacije zahtijeva uspostavu cjelovitog sigurnosnog sustava koji će se primjenjivati za Komisiju, ostale institucije, tijela, urede i agencije osnovane na temelju Ugovora o EZ-u ili Ugovora o Europskoj uniji, države članice kao i sve druge primatelje klasificiranih podataka Europske unije, u daljnjem tekstu „klasificirani podaci EU-a".

(2) Kako bi se osigurala učinkovitost tako uspostavljenog sigurnosnog sustava, klasificirane podatke EU-a Komisija stavlja na raspolaganje samo onim vanjskim tijelima koja jamče da su poduzela sve potrebne mjere za primjenu propisa jednakovrijednih ovom pravilniku.

(3) Pravilnik se donosi ne dovodeći u pitanje Uredbu br. 3 od 31. srpnja 1958. o provedbi članka 24. Ugovora o osnivanju Europske zajednice za atomsku energiju [1], Uredbu vijeća (EZ) br. 1588/90 od 11. lipnja 1990. o prijenosu povjerljivih statističkih podataka Statističkom uredu Europskih zajednica [2] i Odluku Komisije C (95) 1510 završno s 23. studenoga 1995. o zaštiti informatičkih sustava.

(4) Sigurnosni sustav Komisije temelji se na načelima određenima u Odluci Vijeća 2001/264/EZ od 19. ožujka 2001. o usvajanju propisa Vijeća o sigurnosti [3], s namjerom osiguravanja neometanog funkcioniranja postupka odlučivanja Unije.

(5) Komisija naglašava važnost povezivanja, ako je potrebno, drugih institucija propisima i standardima osiguranja povjerljivosti koji su nužni za zaštitu interesa Unije i njezinih država članica.

(6) Komisija potvrđuje potrebu izrade vlastitog koncepta sigurnosti, uzimajući u obzir sve elemente sigurnosti i posebne značajke Komisije kao institucije.

(7) Ovaj se pravilnik donosi ne dovodeći u pitanje članak 255. Ugovora i Uredbu (EZ) br. 1049/2001 Europskog parlamenta i Vijeća od 30. svibnja 2001. o javnom pristupu dokumentima Europskog parlamenta, Vijeća i Komisije [4],

Članak 1.

Pravilnik Komisije o sigurnosti nalazi se u Prilogu.

Članak 2.

1. Član Komisije odgovoran za sigurnosna pitanja poduzima odgovarajuće mjere kako bi se osiguralo da, pri rukovanju klasificiranim podacima EU-a, dužnosnici i ostali službenici Komisije kao i osoblje privremeno dodijeljeno Komisiji poštuju propise iz članka 1.; isto se odnosi na rad u svim prostorima Komisije, uključujući predstavništva i urede u Uniji i njezinim delegacijama u trećim zemljama kao i na vanjske suradnike Komisije.

2. Državama članicama, drugim institucijama, tijelima, uredima i agencijama osnovanima na temelju Ugovora, dopušteno je primati klasificirane podatke EU-a pod uvjetom da se pri rukovanju klasificiranim podacima, u okviru njihovih službi i prostora, osigura poštovanje propisa, jednakovrijednih onima iz članka 1., posebno od:

(a) članova stalnih predstavništava država članica u Europskoj uniji kao i članova državnih delegacija koje prisustvuju sastancima Komisije ili njezinih tijela, ili sudjeluju u ostalim aktivnostima Komisije,

(b) ostalih članova nacionalnih administracija država članica koji rade s klasificiranim podacima EU-a, bilo da djeluju na državnom području države članice ili izvan njega,

(c) vanjskih suradnika i privremeno dodijeljenog osoblja koji rade s klasificiranim podacima EU-a.

[1] SL L 17/58, 6.10.1958., str. 406/58.
[2] SL L 151, 15.6.1990., str. 1.
[3] SL L 101, 11.4.2001., str. 1.
[4] SL L 145, 31.5.2001., str. 43.

Članak 3.

Trećim zemljama, međunarodnim organizacijama i drugim tijelima dopušteno je primanje klasificiranih podataka EU-a, pod uvjetom da se pri rukovanju takvim podacima osigura poštivanje pravila jednakovrijednih onima iz članka 1.

Članak 4.

Pridržavajući se temeljnih načela i minimalnih standarda sigurnosti sadržanih u dijelu I. Priloga, član Komisije odgovoran za sigurnosna pitanja može poduzeti mjere u skladu s dijelom II. Priloga.

Članak 5.

Od dana početka primjene ovaj pravilnik zamjenjuje:

(a) Odluku Komisije C (94) 3282 od 30. studenoga 1994. o sigurnosnim mjerama koje se primjenjuju na klasificirane podatke koji nastaju ili se prenose u vezi s djelatnostima Europske unije;

(b) Odluku Komisije C (99) 423 od 25. veljače 1999. koja se odnosi na postupke kojima se dužnosnicima i ostalim zaposlenicima Europske Komisije može omogućiti pristup klasificiranim podacima koje drži Komisija.

Članak 6.

Od dana početka primjene ovog pravilnika svi klasificirani podaci koje je do tog datuma držala Komisija, izuzev klasificiranih podataka Euratoma:

(a) ako ih je izradila Komisija, u pravilu se smatraju ponovno klasificiranima kao „RESTREINT UE", osim ako im do 31. siječnja 2002. njihov autor dodijeli drugačiji stupanj klasifikacije. U tom slučaju autor obavještava sve adresate dotičnog dokumenta;

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

PRILOG

PRAVILNIK O SIGURNOSTI

Sadržaj

DIO I.: TEMELJNA NAČELA I MINIMALNI STANDARDI SIGURNOSTI

1. UVOD

Ovim pravilnikom se utvrđuju temeljna načela i minimalni standardi sigurnosti koje Komisija, kao i svi primatelji klasificiranih podataka EU-a, moraju na odgovarajući način poštivati na svim svojim zaposleničkim mjestima, tako da je sigurnost zajamčena i svatko može biti uvjeren da je uspostavljen zajednički standard zaštite.

2. OPĆA NAČELA

Sigurnosna politika Zajednice čini sastavni dio njezine opće unutarnje politike upravljanja pa se tako zasniva na načelima kojima se rukovodi i njezina opća politika.

Ova načela uključuju poštivanje propisa, transparentnost, odgovornost i supsidijarnost (razmjernost).

Načelo poštovanja propisa znači da se pri izvršavanju sigurnosnih dužnosti djeluje strogo u okviru pravnog sustava. Ono također znači da se nadležnosti na području sigurnosti temelje na odgovarajućim propisima. U potpunosti se primjenjuju odredbe Pravilnika o osoblju, posebno njegov članak 17. o obavezi diskrecionog ponašanja osoblja u vezi s podacima Komisije te glava VI. o disciplinskim mjerama. To u konačnici znači da se kršenje propisa o sigurnosti u nadležnosti Komisije rješava u skladu s politikom Komisije o disciplinskim mjerama i njezinom politikom suradnje s državama članicama na području kaznenog prava.

Načelo transparentnosti znači jasnoću svih sigurnosnih propisa i odredaba o ravnoteži između različitih službi i različitih područja (fizičko osiguranje zaštita podataka itd.) i potrebu za dosljednom i organiziranom, osviještenom politikom sigurnosti. Ono određuje i potrebu za jasnim pisanim smjernicama za provođenje sigurnosnih mjera.

Načelo odgovornosti znači da su nadležnosti na području sigurnosti jasno određene. Osim tog, ono znači i potrebu redovitih provjera pravilnog izvršavanja tih nadležnosti.

Supsidijarnost ili razmjernost znači da je sigurnost organizirana na najnižoj mogućoj razini i što je bliže moguće glavnim direkcijama i službama Komisije. Ona također znači da se sigurnosne radnje ograničavaju samo na stvarno potrebne elemente. Također, ona znači da su mjere sigurnosti razmjerne interesima koje je potrebno zaštititi i stvarnoj ili mogućoj opasnosti od ugrožavanja tih interesa, uz pružanje zaštite koja će za posljedicu imati najmanje moguće poremećaje.

3. TEMELJI SIGURNOSTI

Temelji učinkovite sigurnosti su:

(a) organizacija nacionalne sigurnosti u svakoj državi članici odgovorna za:

1. prikupljanje i bilježenje obavještajnih podataka o špijunskim, sabotažnim, terorističkim i drugim subverzivnim djelovanjima, i

2. pružanje podataka i savjeta o prijetnjama sigurnosti, njihovoj naravi i načinima zaštite od njih svojim vladama i posredstvom njih Komisiji;

(b) tehničko tijelo INFOSEC (*INFOSEC Authority, IA*) u svakoj državi članici i u okviru Komisije nadležno je za rad s određenim tijelom sigurnosti radi pružanja informacija i savjeta o prijetnjama sigurnosti s tehničkog stajališta i načinima zaštite od njih;

(c) redovna suradnja među vladinim službama i odgovarajućim službama europskih institucija kako bi se, prema potrebi, utvrdilo i donijelo preporuke u vezi s:

1. osobama, podacima i izvorima kojima je potrebna zaštita, i

2. zajedničkim standardima zaštite.

d) uska suradnja Sigurnosnog ureda Komisije sa službama sigurnosti drugih europskih institucija te sa Službom sigurnosti NATO-a (*NOS, NATO Office of Security*).

4. NAČELA SIGURNOSTI PODATAKA

4.1. **Ciljevi**

Ciljevi osiguranja klasificiranih podataka su:

(a) zaštititi klasificirane podatke EU-a (*EUCI, EU classified information*) od špijunaže, ugrožavanja njihove tajnosti ili neovlaštenog razotkrivanja;

(b) zaštititi podatke EU-a u komunikacijskim i informacijskim sustavima i mrežama od ugrožavanja njihove povjerljivosti, cjelovitosti i raspoloživosti;

(c) zaštititi prostore Komisije u kojima se nalaze podaci EU-a od sabotaže i zlonamjernog štetnog djelovanja;

(d) u slučaju greške, procijeniti nastalu štetu, ograničiti njezine posljedice i donijeti nužne popravne mjere.

4.2. **Definicije**

Za potrebe ovog Pravilnika:

(a) izraz „klasificirani podaci EU-a" znači sve podatke i materijale čije bi neovlašteno razotkrivanje u različitoj mjeri moglo štetiti interesu EU-a ili jedne ili više njezinih država članica, bilo da takvi podaci nastaju u EU-u ili su primljeni od država članica, trećih zemalja ili međunarodnih organizacija;

(b) izraz „dokument" znači svako pismo, bilješku, zapisnik, izvještaj, memorandum, signal/poruku, skicu, fotografiju, dijapozitiv, film, zemljovid, grafikon, nacrt, bilježnicu, matricu, kopirni papir, traku pisaćeg stroja ili pisača, magnetnu traku, kasetu, računalni disk, CD-ROM ili drugi fizički medij na kojem su podaci pohranjeni;

(c) izraz „materijal" znači „dokument" kako je utvrđeno pod (b) kao i svaki dio opreme, bilo da je proizveden ili je u procesu proizvodnje;

(d) izraz „potreba poznavanja" znači potrebu pojedinog zaposlenika za pristupom klasificiranim podacima EU-a radi provođenja određene radnje ili zadatka;

(e) „ovlaštenje" znači odluku Predsjednika Komisije da pojedincu dodijeli pravo na pristup klasificiranim podacima EU-a do točno određene razine, na temelju pozitivnog ishoda sigurnosnog pregleda (vetiranja) koje, prema nacionalnome zakonodavstvu, provodi tijelo nacionalne sigurnosti;

(f) izraz „stupanj klasifikacije" znači dodjelu odgovarajuće razine sigurnosti podacima čije bi neovlašteno razotkrivanje moglo prouzročiti određeni stupanj narušavanja interesa Komisije ili države članice;

(g) izraz „snižavanje stupnja klasifikacije" (deklasiranje) znači svrstavanje u niži stupanj klasifikacije;

(h) izraz „ukidanje tajnosti" (deklasifikacija) znači ukidanje svih stupnjeva klasifikacije;

(i) izraz „izvor od kojeg podaci potječu" znači propisno ovlaštenog autora tajnog dokumenta. Voditelji službi mogu, u okviru Komisije, ovlastiti svoje osoblje za stvaranje klasificiranih podataka EU-a;

(j) izraz „službe Komisije" znači odjele i službe Komisije, uključujući kabinete, na svim mjestima zapošljavanja, uključujući Zajednički istraživački centar, predstavništva i urede u Uniji i delegacije u trećim zemljama.

4.3. **Klasifikacija**

(a) Kada se radi o povjerljivosti podataka, potrebno je brižljivo postupanje i iskustvo u odabiru podataka i materijala koje treba zaštititi kao i procjeni potrebnog stupnja zaštite. Od temeljnog je značaja da stupanj zaštite odgovara kritičnome stupnju sigurnosti svakog pojedinog podatka i materijala kojeg treba zaštititi;

(b) sustav klasifikacije je sredstvo koje omogućuje učinkovitost ovih načela; sličan sustav treba slijediti pri planiranju i organiziranju načina suprotstavljanja špijunaži, sabotažama, terorizmu i drugim oblicima prijetnji tako da se najveće mjere zaštite pružaju najznačajnijim prostorima u kojima se nalaze klasificirani podaci i njihovim najosjetljivijim točkama;

(c) za klasifikaciju podataka odgovoran je isključivo izvor od kojeg podaci potječu;

(d) razina stupnja klasifikacije temelji se isključivo na sadržaju podataka;

(e) kada se nekoliko različitih podataka poveže u cjelinu, razina tajnosti koja se primjenjuje na cjelinu mora odgovarati najvišem stupnju klasifikacije pojedinačnih podataka. Skupini podataka može se, međutim, dodijeliti i viši stupanj klasifikacije nego što ga imaju njezini sastavni dijelovi;

(f) stupnjevi klasifikacije dodjeljuju se samo kada je to nužno i na onoliko dugo koliko je potrebno.

4.4. **Ciljevi sigurnosnih mjera**

Sigurnosne mjere:

(a) vrijede za sve osobe koje imaju pristup klasificiranim podacima, za medije-nositelje klasificiranih podataka, sve prostore u kojima se nalaze takvi podaci i značajni objekti;

(b) su predviđene tako da otkrivaju osobe koje bi s svojim položajem mogle ugroziti sigurnost klasificiranih podataka i značajnih objekata u kojima se takvi podaci nalaze te da omoguće njihovo isključivanje ili uklanjanje;

(c) svim neovlaštenim osobama onemogućavaju pristup do klasificiranih podataka ili objekata koji sadrže te podatke;

(d) osiguravaju da se klasificirani podaci daju na korištenje isključivo na osnovi poznavanja temeljnog načela „potrebno je znati" a koje je temeljno načelo svih gledišta u vezi sa sigurnosti;

(e) osiguravaju cjelovitost (tj. sprečavaju iskrivljavanje ili neovlašteno mijenjanje ili neovlašteno brisanje) i dostupnost (tj. ne brani se pristup onima kojima je potreban i koji su za njega ovlašteni) svih podataka, bilo da su klasificirani ili ne i posebno pohranjenih, obrađenih ili prenesenih u elektromagnetskom obliku.

5. ORGANIZACIJA SIGURNOSTI

5.1. **Zajednički minimalni standardi**

Komisija osigurava da svi primatelji klasificiranih podataka EU-a poštuju zajedničke minimalne standarde sigurnosti unutar institucije i na temelju njezine nadležnosti, tj. sve službe i vanjski suradnici kako bi se klasificirani podaci EU-a pouzdano prosljeđivali s uvjerenjem da će se s njima postupati s jednakom pažnjom. Takvi minimalni standardi uključuju kriterije za sigurnosnu provjeru osoblja i postupke zaštite klasificiranih podataka EU-a.

Komisija omogućuje vanjskim tijelima pristup klasificiranim podacima EU-a samo pod uvjetom da se pri rukovanju klasificiranim podacima EU-a osigura poštivanje odredbi koje su jednakovrijedne ili strože od ovih minimalnih standarda.

5.2. **Organizacija**

Sigurnost u okviru Komisije je organizirana na dvije razine:

(a) na razini Komisije kao cjeline je Sigurnosni ured Komisije pri kojem djeluje tijelo za akreditaciju u vezi sa sigurnosti - SAA (*Security Accreditation Authority*) koje djeluje i kao tijelo Crypto (*CrA, Crypto Authority*) i kao tijelo TEMPEST (*TEMPEST Authority, TA*), te tijelo INFOSEC i jedan ili više središnjih registara klasificiranih podataka EU-a, svaki s jednim ili više nadzornih službenika registra (*RCO, Registry Control Officer*);

(b) na razini pojedinih tijela Komisije sigurnost je u nadležnosti jednog ili više lokalnih službenika sigurnosti - LSO (*Local Security Officer*), jednog ili više službenika za informacijsku sigurnost na središnjoj razini - CISO (*Central Informatics Security Officer*), službenika za informacijsku sigurnost na lokalnoj razini - LISO (*Local Informatics Security Officer*) te lokalnih registarskih ureda klasificiranih podataka EU-a s jednim ili više nadzornih službenika;

(c) središnje službe sigurnosti pružaju operativne smjernice lokalnim službama sigurnosti.

6. SIGURNOST OSOBLJA

6.1. **Sigurnosna provjera osoblja**

Sve osobe koje traže pristup podacima stupnja klasifikacije CONFIDENTIEL UE ili većeg na odgovarajući se način provjeravaju prije nego im se takav pristup dopusti. Slična provjera traži se i za osobe kojima radni zadaci uključuju tehničko djelovanje ili održavanje komunikacijskih i informacijskih sustava koji sadrže klasificirane podatke. Ovakvom se provjerom utvrđuje jesu li spomenute osobe:

(a) neupitno lojalne;

(b) takvih osobina i diskretnog ponašanja da ne postoji sumnja u vezi s njihovom čestitošću pri rukovanju klasificiranim podacima; ili

(c) podložne utjecaju vanjskih ili drugih izvora.

U postupcima sigurnosne provjere posebno detaljnom promatranju podvrgavaju se osobe:

(d) kojima se daje pristup podacima TRÈS SECRET UE;

(e) koje imaju položaje s redovnim pristupom znatnoj količini podataka SECRET UE;

(f) koje imaju radi radnih dužnosti poseban pristup sigurnosnim komunikacijskim ili informacijskim sustavima te im daju priliku za neovlašteno pristupanje velikoj količini klasificiranih podataka EU-a ili za nanošenje ozbiljne štete tehničkim sabotažnim radnjama, izvršavanju određenog naloga.

U okolnostima navedenim u podstavcima (d), (e) i (f) u najvećoj mogućoj mjeri provodi se metoda pozadinske istrage.

Kada se osobe za koje nije utvrđena „potreba poznavanja" namjeravaju zaposliti u okolnostima pri kojima bi mogle imati pristup klasificiranim podacima EU-a (npr. kuriri, zaštitari, osoblje zaduženo za održavanje i čišćenje, itd.), te osobe najprije prolaze odgovarajuću sigurnosnu provjeru.

6.2. **Evidencije sigurnosnih provjera osoblja**

Sve službe Komisije u kojima se rukuje klasificiranim podacima EU-a ili pri kojima se nalaze sigurnosni komunikacijski ili informacijski sustavi vode evidenciju sigurnosnih provjera osoba koje su im dodijeljene. Svaka se sigurnosna provjera, ovisno o prilikama, verificira kako bi se utvrdila njezina primjerenost s obzirom na trenutna zaduženja osobe; uvijek kada se pojave novi podaci koji ukazuju da nastavak izvršavanja zadataka na klasificiranim poslovima nije više u skladu s interesima sigurnosti postupak sigurnosne provjere odmah se ponavlja. Lokalni službenik sigurnosti pojedine službe Komisije vodi evidenciju sigurnosnih provjera na svom području.

6.3. **Sigurnosne upute za osoblje**

Osoblju na radnim mjestima na kojima bi moglo imati pristup klasificiranim podacima daju se, pri preuzimanju zadatka i u redovnim razmacima, temeljite upute o potrebi sigurnosti i postupcima za njezino postizanje. Od osoblja se zahtijeva pismena potvrda da je važeće sigurnosne odredbe pročitalo i u potpunosti razumjelo.

6.4. **Odgovornosti upravljačkog osoblja**

Uprava mora znati koji su od njezinih zaposlenika uključeni u klasificirane poslove ili imaju pristup sigurnosnim komunikacijskim ili informacijskim sustavima te bilježiti i izvještavati o svakom incidentu ili očitim slabostima koje bi lako mogle imati utjecaja na sigurnost.

6.5. **Sigurnosni status osoblja**

Utvrđuju se postupci kako bi se osiguralo da se, u slučaju nepovoljnih saznanja u vezi s nekom osobom, utvrdi je li ta osoba zaposlena na klasificiranom poslu ili ima pristup sigurnosnim komunikacijskim ili informacijskim sustavima te da se o tim saznanjima obavijesti Sigurnosni ured Komisije. Ukoliko se utvrdi da takva osoba predstavlja rizik za sigurnost, uklanja se sa zadataka na kojima bi on ili ona ugrozili sigurnost.

7. FIZIČKA SIGURNOST

7.1. **Potreba za zaštitom**

Stupanj mjera fizičke sigurnosti koje se primjenjuju kako bi se osigurala zaštita klasificiranih podataka EU-a razmjeran je dodijeljenom stupnju klasifikacije, obimu i ugroženosti čuvanih podataka i materijala. Svi koji posjeduju klasificirane podatke EU-a slijede jedinstvene postupke vezane za stupanj klasifikacije tih podataka i zadovoljavaju zajedničke standarde zaštite u vezi sa sigurnim čuvanjem, prijenosom i uništavanjem podataka i materijala kojima je zaštita potrebna.

7.2. **Provjera**

Prije napuštanja i ostavljanja bez nadzora područja na kojima se nalaze klasificirani podaci EU-a, osobe kojima je povjerena briga o tim podacima osiguravaju da su podaci sigurno pohranjeni i da su svi sigurnosni uređaji aktivirani (brave, alarmi i dr.). Dodatne nezavisne provjere provode se nakon radnog vremena.

7.3. **Sigurnost zgrada**

Zgrade u kojima se nalaze klasificirani podaci EU-a ili sigurnosni komunikacijski ili informacijski sustavi zaštićuju se od nedozvoljenog pristupa. Vrsta zaštite klasificiranih podataka EU-a, npr. sigurnosne šipke na prozorima, sigurnosne brave na vratima, straže na ulazima, automatizirani sustavi nadzora pristupa, sigurnosni pregledi i ophodnje, alarmni sustavi, sustavi otkrivanja provala i psi čuvari ovisit će o:

(a) stupnju klasifikacije, obimu i položaju zaštićenih podataka i materijala unutar zgrade;

(b) kakvoći sigurnosnih spremnika tih podataka i materijala, i

(c) fizičkim osobinama i položaju zgrade.

Na sličan način, priroda zaštite koja se daje komunikacijskim i informacijskim sustavima, ovisi o njihovoj procijenjenoj vrijednosti i mogućoj šteti u slučaju ugrožavanja sigurnosti, o fizičkim osobinama i položaju zgrade u kojoj se sustav nalazi i o položaju sustava unutar zgrade.

7.4. **Planovi postupanja u izvanrednim situacijama**

Unaprijed se pripremaju detaljni planovi za zaštitu klasificiranih podataka u slučaju izvanrednih situacija na lokalnoj ili državnoj razini.

8. SIGURNOST PODATAKA

Sigurnost podataka (INFOSEC) odnosi se na utvrđivanje i primjenu mjera sigurnosti za zaštitu klasificiranih podataka EU-a koji se obrađuju, pohranjuju ili prenose komunikacijskim, informacijskim ili drugim elektroničkim sustavima od slučajnog ili namjernoga gubitka njihove tajnosti, cjelovitosti i raspoloživosti. Odgovarajuće protumjere poduzimaju se da bi se neovlaštenim korisnicima spriječio pristup klasificiranim podacima EU-a, da bi se spriječilo onemogućivanje pristupa klasificiranim podacima EU-a ovlaštenim korisnicima i da bi se spriječilo iskrivljavanje ili neovlašteno mijenjanje ili brisanje klasificiranih podataka EU-a.

9. MJERE PROTUSABOTAŽE I NADZOR OSTALIH OBLIKA ZLONAMJERNIH ŠTETNIH DJELOVANJA

Fizičke mjere predostrožnosti za zaštitu važnih objekata u kojima se nalaze klasificirani podaci predstavljanju najbolju sigurnosnu zaštitu od sabotaže i zlonamjernog nanošenja štete te ih sigurnosne provjere osoblja same za sebe ne mogu učinkovito nadomjestiti. Od nadležnog državnog tijela traže se informacije o špijunskim, sabotažnim, terorističkim i drugim subverzivnim aktivnostima.

10. DAVANJE KLASIFICIRANIH PODATAKA TREĆIM ZEMLJAMA ILI MEĐUNARODNIM ORGANIZACIJAMA

Odluku o davanju klasificiranih podataka EU-a, koji nastaju pri Komisiji, trećoj zemlji ili međunarodnoj organizaciji donosi Komisija kao kolegij. Ako Komisija nije izvor od kojeg podaci koji se žele otkriti potječu, ona prvo traži pristanak onog od koga podaci potječu. Ako izvor od kojeg podaci potječu nije moguće utvrditi Komisija preuzima nadležnosti istog.

Ako Komisija primi klasificirane podatke od trećih zemalja, međunarodnih organizacija ili drugih trećih stranaka, tim se podacima daje zaštita u skladu s njihovim stupnjem klasifikacije, istovjetna utvrđenim standardima u ovom pravilniku za klasificirane podatke EU-a ili višim standardima koje može zahtijevati treća strana koja podatke daje. Dogovorno se mogu provoditi i uzajamne provjere.

Navedena načela primjenjuju se u skladu s detaljnim odredbama navedenim u dijelu II., odjeljku 26. i Dodacima 3., 4. i 5.

DIO II.: ORGANIZACIJA SIGURNOSTI U KOMISIJI

11. ČLAN KOMISIJE ODGOVORAN ZA SIGURNOSNA PITANJA

Član Komisije odgovoran za sigurnosna pitanja:

(a) provodi sigurnosnu politiku Komisije;

(b) razmatra sigurnosna pitanja koje mu predloži Komisija ili njezina nadležna tijela;

(c) u uskoj vezi s tijelima nacionalne sigurnosti država članica (*NSA, National Security Authorities*) (ili odgovarajućim) razmatra pitanja u vezi s izmjenama sigurnosne politike Komisije.

Član Komisije, odgovoran za sigurnosna pitanja, brine se posebno za:

(a) usklađivanje svih sigurnosnih pitanja u vezi s djelatnostima Komisije;

(b) upućivanje zahtjeva zaduženim tijelima nacionalne sigurnosti država članica za provođenje sigurnosne provjere osoblja zaposlenog u Komisiji u skladu s odjeljkom 20.;

(c) istraživanje ili podnošenje zahtjeva za istragu o svakom otkrivanju klasificiranih podataka EU-a za koje se pretpostavlja da se pojavilo unutar Komisije;

(d) predlaganje zahtjeva odgovarajućim tijelima sigurnosti da pokrenu istražne postupke kada se čini da je došlo do otkrivanja klasificiranih podataka EU-a izvan Komisije i usklađivanje istražnih radnji kada je uključeno više sigurnosnih tijela;

(e) provođenje redovnog nadzora sigurnosnih rješenja zaštite klasificiranih podataka EU-a;

(f) održavanje uske povezanosti sa svim sigurnosnim tijelima na koje se to odnosi kako bi se postigla sveukupna usklađenost sigurnosti;

(g) održavanje sigurnosne politike i postupaka Komisije pod stalnim nadzorom i, prema potrebi, pripremanje odgovarajućih preporuka. S tim u vezi, član Komisije odgovoran za sigurnosna pitanja predočava Komisiji godišnji plan inspekcijskih pregleda koji priprema Sigurnosna služba Komisije.

12. SAVJETODAVNA SKUPINA ZA SIGURNOSNU POLITIKU KOMISIJE

Osniva se savjetodavna skupina za sigurnosnu politiku Komisije. Nju čine član Komisije odgovoran za sigurnosna pitanja ili njegov/njezin izaslanik koji predsjedava skupini te predstavnici tijela nacionalne sigurnosti svake države članice. Predstavnici drugih europskih institucija također mogu biti pozvani. Predstavnici relevantnih decentraliziranih agencija EZ-a i EU-a mogu također biti pozvani da prisustvuju raspravama o pitanjima koja se na njih odnose.

Savjetodavna skupina za sigurnosnu politiku Komisije sastaje se na zahtjev predsjedavajućeg ili nekog od članova. Zadaća skupine je ispitati i procijeniti sva bitna sigurnosna pitanja te iznijeti Komisiji odgovarajuće prijedloge.

13. SIGURNOSNI ODBOR KOMISIJE

Osniva se Sigurnosni odbor Komisije. Njega sačinjavaju glavni tajnik koji predsjedava odborom, ravnatelji Pravne službe, Službe za kadrovske i administrativne poslove, Službe za vanjske odnose, pravosuđe i unutrašnja pitanja i Zajedničkog istraživačkog centra te voditelji Službe za unutrašnju reviziju i Sigurnosnog ureda Komisije. I drugi dužnosnici Komisije također mogu biti pozvani. Zadatak Odbora je procijeniti sigurnosne mjere unutar Komisije te dati preporuke iz ovog područja članu Komisije odgovornom za sigurnosna pitanja.

14. SIGURNOSNI URED KOMISIJE

Članu Komisije odgovornom za sigurnosna pitanja pri ispunjavanju svojih dužnosti iz odjeljka 11. na poslovima usklađivanja, nadgledanja i provedbe sigurnosnih mjera pomaže Sigurnosni ured Komisije.

Čelnik Sigurnosnog ureda Komisije je glavni savjetnik člana Komisije odgovornog za sigurnosna pitanja i djeluje kao tajnik Savjetodavne skupine za sigurnosnu politiku. S tim u vezi čelnik je nadležan za pripremu potrebnih izmjena sigurnosnih propisa i usklađivanje sigurnosnih mjera s nadležnim tijelima država članica te, prema potrebi, međunarodnim organizacijama koje su s Komisijom zaključile sigurnosne sporazume. U te svrhe čelnik obavlja dužnosti službenika za vezu.

Čelnik Sigurnosnog ureda Komisije odgovoran je za akreditaciju sustava i mreža informacijske tehnologije - IT (*Information Technology*) unutar Komisije. U dogovoru s odgovarajućim tijelima nacionalne sigurnosti čelnik Sigurnosnog ureda Komisije odlučuje o akreditaciji sustava i mreža IT koji uključuju Komisiju s jedne te svakog primatelja klasificiranih podataka EU-a s druge strane.

15. SIGURNOSNI INSPEKCIJSKI PREGLEDI

Sigurnosni ured Komisije provodi redovne inspekcijske preglede sigurnosnih mjera za zaštitu klasificiranih podataka EU-a.

Sigurnosnom uredu Komisije pri obavljanju ovih zadaća mogu pomagati sigurnosne službe drugih institucija EU-a koje imaju klasificirane podatke EU-a ili tijela nacionalne sigurnosti država članica [1].

Na zahtjev države članice inspekcijski pregled klasificiranih podataka EU-a može provesti njezino tijelo nacionalne sigurnosti u okviru Komisije, zajednički i na temelju međusobnog dogovora sa Sigurnosnom službom Komisije.

[1] Ne dovodeći u pitanje Bečku Konvenciju iz 1961. o diplomatskim odnosima i Protokol o povlasticama i imunitetima Europskih zajednica od 8. travnja 1965.

16. STUPNJEVI KLASIFIKACIJE, SIGURNOSNA OBILJEŽJA I OZNAKE

16.1. **Stupnjevi klasifikacije** [1]

Podaci se klasificiraju prema sljedećim stupnjevima klasifikacije (vidjeti također Dodatak 2.):

TRÈS SECRET UE: ovaj stupanj klasifikacije dodjeljuje se samo onim podacima i materijalu čije bi neovlašteno otkrivanje moglo prouzročiti izuzetno ozbiljne posljedice za temeljne interese Europske unije ili jedne ili više njezinih država članica.

SECRET UE: ovaj stupanj klasifikacije dodjeljuje se samo onim podacima i materijalu čije bi neovlašteno otkrivanje moglo ozbiljno štetiti temeljnim interesima Europske unije ili jedne ili više njezinih država članica.

CONFIDENTIEL UE: ovaj stupanj klasifikacije dodjeljuje se onim podacima i materijalu čije bi neovlašteno otkrivanje moglo štetiti temeljnim interesima Europske unije ili jedne ili više njezinih država članica.

RESTREINT UE: ovaj stupanj klasifikacije dodjeljuje se onim podacima i materijalu čije bi neovlašteno otkrivanje moglo nepovoljno djelovati na interese Europske unije ili jedne ili više njezinih država članica.

Drugi stupnjevi klasifikacije nisu dozvoljeni.

16.2. **Sigurnosna obilježja**

Kako bi se vremenski ograničila valjanost klasifikacije (za klasificirane podatke, označavanje trenutka automatskog snižavanja ili ukidanja stupnja klasifikacije) koristi se dogovoreno sigurnosno obilježje. Ovo obilježje treba biti u obliku „DO… (vrijeme/datum)" ili „DO… (događaj)".

Dodatna sigurnosna obilježja kao što je CRYPTO ili bilo koje drugo od EU-a priznato sigurnosno obilježje upotrebljavaju se kada se nalaže potreba ograničene distribucije i posebnog načina rukovanja podacima, pored onog koje je označeno sigurnosnom stupnju klasifikacije.

Sigurnosna obilježja upotrebljavaju se zajedno sa stupnjem klasifikacije.

16.3. **Oznake**

Označivanje se može upotrebljavati za određivanje područja koje pokriva dokument ili posebnog načina distribucije na temelju načela potrebe poznavanja ili (za podatke koji nisu klasificirani) za označavanje kraja embarga.

Oznaka nije stupanj klasifikacije i ne smije se upotrebljavati u zamjenu za njega.

Oznaka ESDP (*European Security and Defence Policy*) se upotrebljava za dokumente i njihove preslike vezane za sigurnost i obranu Unije ili jedne ili više njezinih država članica, ili vezane za upravljanje vojnim ili nevojnim kriznim situacijama.

16.4. **Postavljanje stupnja klasifikacije**

Stupanj klasifikacije se označava:

(a) na dokumentima RESTREINT UE mehaničkim ili elektroničkim sredstvom;

(b) na dokumentima CONFIDENTIEL UE mehaničkim sredstvom, ručno ili tiskanjem na prethodno žigosanom, registriranom papiru;

(c) na dokumente SECRET UE ili TRÈS SECRET UE mehaničkim sredstvom ili ručno.

16.5. **Postavljanje sigurnosnih obilježja**

Sigurnosna obilježja postavljaju se neposredno ispod stupnja klasifikacije, na isti način na koji se postavljaju stupnjevi klasifikacije.

[1] Vidjeti usporednu tablicu sigurnosnih klasifikacija EU-a, NATO-a, ZEU-a i država članica u Dodatku 1.

17. MJERILA ZA ODREĐIVANJE STUPNJA KLASIFIKACIJE

17.1. **Općenito**

Podacima se dodjeljuje stupanj klasifikacije samo kada je to nužno. Stupanj klasifikacije se jasno i ispravno označuje i zadržava samo onoliko dugo koliko je to potrebno radi zaštite podataka.

Odgovornost za razvrstavanje podataka prema tajnosti i za svako sljedeće snižavanje ili ukidanje stupnja klasifikacije ostaje isključivo na izvoru od kojeg podaci potječu.

Dužnosnici i ostali zaposlenici Komisije rade na razvrstavanju, snižavanju ili ukidanju stupnja klasifikacije podataka prema uputama ili u dogovoru s voditeljem službe.

Detaljni postupci za postupanje s klasificiranim dokumentima osmišljeni su tako da osiguravaju njihovu odgovarajuću zaštitu u skladu s podacima koje dokumenti sadrže.

Broj osoba ovlaštenih za pripremu dokumenata TRÈS SECRET UE ograničava se na minimum, a njihova se imena čuvaju na popisu koji se vodi u Sigurnosnom uredu Komisije.

17.2. **Primjena stupnjeva klasifikacije**

Stupanj klasifikacije dokumenta određuje se ovisno o stupnju osjetljivosti njegovog sadržaja u skladu s određenjem iz odjeljka 16. Važno je da se razvrstavanje prema tajnosti provodi pažljivo i na pravilan način. To se posebno odnosi na stupanj klasifikacije TRÈS SECRET UE.

Izvor od kojeg potječe dokument kojem se dodjeljuje stupanj klasifikacije pridržava se gore navedenih pravila i odupire se svakom nastojanju da se stupanj klasifikacije precijeni ili podcijeni.

Praktične upute za razvrstavanje prema tajnosti su u Dodatku 2.

Za pojedine stranice, stavke, odjeljke, priloge, dodatke, dodane i priložene dijelove određenog dokumenta može se zahtijevati drugačiji stupanj klasifikacije pa ih se prema tome i razvrstava. Stupanj klasifikacije dokumenta kao cjeline je onaj koji pripada njegovom najviše razvrstanome dijelu.

Stupanj klasifikacije pisma ili bilješke s prilozima je jednak najvišem stupanju tajnosti njegovih priloženih dijelova. Izvor od kojeg podaci potječu jasno naznačuje koji stupanj klasifikacije treba dodijeliti kada se pismo ili bilješka nalaze odvojeno od priloga.

Pristup javnosti i dalje se uređuje Uredbom (EZ) br. 1049/2001.

17.3. **Snižavanje i ukidanje stupnja klasifikacije**

Klasificiranim dokumentima EU-a može se sniziti ili ukinuti stupanj klasifikacije samo uz dozvolu izvora od kojeg ti podaci potječu te, prema potrebi, nakon rasprave s ostalim zainteresiranim stranama. Snižavanje ili ukidanje stupnja klasifikacije potvrđuje se pismeno. Izvor od kojeg podaci potječu dužan je o promjeni obavijestiti svoje naslovnike, a oni su nadalje zaduženi za obavještavanje o promjeni svih sljedećih naslovnika kojima su dokument proslijedili ili ga preslikali.

Ako je moguće izvor od kojeg podaci potječu na klasificiranim dokumentima navodi datum, razdoblje ili događaj nakon kojeg se sadržaju dokumenta može sniziti ili ukinuti stupanj klasifikacije. U protivnom, dokumente ponovno pregledavaju, najmanje svakih pet godina, kako bi se potvrdila potreba prvobitnog stupnja klasifikacije.

18. FIZIČKA SIGURNOST

18.1. **Općenito**

Glavni ciljevi mjera fizičke sigurnosti su spriječiti neovlaštenim osobama pristup do klasificiranih podataka i/ili materijala EU-a, spriječiti krađu ili oštećenje opreme i druge svojine te spriječiti uznemiravanje ili bilo koju vrstu pritiska na osoblje, zaposlenike i posjetitelje.

18.2. **Sigurnosni zahtjevi**

Svi prostori, zgrade, prostorije, komunikacijski i informacijski sustavi itd. u kojima se čuvaju odnosno obrađuju klasificirani podaci i materijali EU-a, zaštićuju se odgovarajućim mjerama fizičke zaštite.

Prilikom odlučivanja o potrebnom stupnju fizičke zaštite vodi se računa o svim relevantnim čimbenicima kao što su:

(a) stupanj klasifikacije podataka ili materijala;

(b) količina i oblik čuvanih podatka (npr. preslika na papiru, računalni medij za pohranjivanje);

(c) lokalno procijenjena prijetnja koju, za države članice i/ili druge institucije ili treće stranke koje posjeduju klasificirane podatke EU-a, predstavljaju obavještajne službe čija su djelovanja kao sabotaže, teroristička ili druge subverzivne i/ili kriminalne aktivnosti, usmjerena protiv EU-a.

Fizičke mjere sigurnosti primjenjuju se radi:

(a) onemogućavanja potajnih ili nasilnih upada nepoželjnih osoba;

(b) odvraćanja, ometanja i otkrivanja djelovanja nelojalnog osoblja;

(c) sprečavanja pristupa klasificiranim podacima EU-a za osobe koje nemaju potrebu poznavanja.

18.3. **Mjere fizičke sigurnosti**

18.3.1. *Sigurnosna područja*

Područja obrade ili pohrane klasificiranih podataka stupnja CONFIDENTIEL UE ili višeg organizirana su i ustrojena tako da odgovaraju jednom od sljedećih razreda:

(a) sigurnosno područje I. razreda: područje na kojem se s podacima CONFIDENTIEL UE ili višim postupa i pohranjuje ih se tako da ulaz na to područje u svakom slučaju predstavlja ujedno i pristup klasificiranim podacima. Za takvo se područje zahtijeva:

   i. jasno određen i zaštićen prostor preko kojeg se nadziru svi ulasci i izlasci;

   ii. sustav nadzora ulazaka koji propušta samo one osobe koje su propisno provjerene i posebno ovlaštene za ulazak na to područje;

   iii. detaljan popis stupnjeva klasifikacije podataka koji se obično čuvaju na tom području, tj. podataka koji ulaskom na područje postaju dostupni.

(b) sigurnosno područje II. razreda: područje na kojem se s podacima CONFIDENTIEL UE ili višim postupa i pohranjuje ih se tako da su pomoću uspostavljenih unutrašnjih načina nadzora zaštićeni od pristupa neovlaštenih osoba, npr. prostori na kojima se nalaze službe koje redovno čuvaju ili rukuju podacima CONFIDENTIEL UE ili višim. Za takvo se područje zahtijeva:

   i. jasno određen i zaštićen prostor kroz koji se nadziru svi ulasci i izlasci;

   ii. sustav nadzora ulazaka koji na područje bez nadzora propušta samo one osobe koje su propisno provjerene i posebno ovlaštene za ulazak na to područje. Za sve ostale osobe treba predvidjeti nadgledanje ili odgovarajuće načine nadzora radi sprečavanja neovlaštenog pristupa klasificiranim podacima EU-a i nekontroliranog ulaska na područja koja su podložna tehničkim inspekcijskim pregledima sigurnosti.

   Područja na kojima službeno osoblje nije prisutno 24 sata na dan pregledavaju se odmah po završetku uobičajenog radnog vremena kako bi se potvrdilo da su klasificirani podaci EU-a ispravno osigurani.

18.3.2. *Administrativno područje*

Na područjima koja okružuju ili vode do sigurnosnih područja I. i II. razreda može se uspostaviti upravno područje nižeg stupnja sigurnosti. Na takvom se području zahtijeva vidljivo označen prostor na kojem je moguća provjera osoblja i vozila. Na takvim područjima čuvaju se i obrađuju samo podaci RESTREINT UE ili oni koji nisu označeni stupnjem klasifikacije.

18.3.3. *Nadzor ulazaka i izlazaka*

Nadzor ulazaka na sigurnosna područja I. i II. razreda te izlazaka iz njih provodi se putem propusnica ili sustava za prepoznavanje osoba koji se primjenjuje na cijelo osoblje koje uobičajeno radi na tim područjima. Također treba uspostaviti sustav provjere posjetitelja, osmišljen tako da onemogući neovlašteni pristup klasificiranim podacima EU-a. Sustav propusnica može se dodatno pojačati sustavom automatskog utvrđivanja identiteta koji se smatra dopunom, ali ne i potpunom zamjenom za stražarsko osoblje. Promjena u vezi s procjenom prijetnje može imati za posljedicu pojačanje mjera nadzora ulazaka i izlazaka, na primjer, za vrijeme posjeta uglednih osoba.

18.3.4. *Stražarske ophodnje*

Izvan uobičajenog radnog vremena organiziraju se stražarske ophodnje sigurnosnih područja I. i II. razreda kako bi se imovina EU-a zaštitila od ugrožavanja, oštećenja ili gubitka. Učestalost ophodnji određuje se prema lokalnim okolnostima, no preporuka je da se provode svaka dva sata.

18.3.5. *Sigurnosni spremnici i zaštićene prostorije*

Za pohranjivanje klasificiranih podataka EU-a koriste se spremnici razvrstani u tri razreda:

— razred A: spremnici odobreni na državnoj razini za pohranjivanje klasificiranih podataka TRÈS SECRET UE, unutar sigurnosnih područja I. ili II. razreda

— razred B: spremnici odobreni na državnoj razini za pohranjivanje klasificiranih podataka SECRET UE i CONFIDENTIEL UE, unutar sigurnosnih područja I. ili II. razreda

— razred C: namjensko pokućstvo prikladno samo za pohranjivanje klasificiranih podataka RESTREINT UE.

U zaštićenim prostorijama trezorskog tipa unutar sigurnosnih područja I. ili II. razreda i u svim sigurnosnim područjima I. razreda u kojima se na otvorenim policama ili izloženo na grafikonima, zemljovidima, planovima i sl. čuvaju podaci sa stupnjem klasifikacije CONFIDENTIEL UE i višim, sve zidne stijene, podovi i stropovi te vrata s bravama moraju biti odobreni od SAA kao oprema koja nudi zaštitu istovjetnog stupnja kao sigurnosni spremnik odgovarajućeg razreda odobren za pohranjivanje podataka istovrsnog stupnja klasifikacije.

18.3.6. *Brave*

Brave koje se koriste na sigurnosnim spremnicima i trezorima za čuvanje klasificiranih podataka EU-a moraju zadovoljavati sljedeće standarde:

— Skupina A: odobrene na državnoj razini za spremnike razreda A

— Skupina B: odobrene na državnoj razini za spremnike razreda B

— Skupina C: prikladne samo za namjensko pokućstvo razreda C.

18.3.7. *Nadzor ključeva i kombinacija*

Ključevi sigurnosnih spremnika ne smiju se iznositi izvan zgrada Komisije. Postavke kombinacija sigurnosnih spremnika povjeravaju se na pamćenje osobama koje ih trebaju poznavati. U slučaju nužde koriste se rezervni ključevi i pismene bilješke o svim postavkama kombinacija za koje je odgovoran lokalni službenik sigurnosti nadležnog ureda Komisije; pismene se bilješke kombinacija čuvaju u zasebnim, zapečaćenim neprozirnim omotnicama. Radni ključevi, rezervni sigurnosni ključevi i postavke kombinacija drže se u zasebnim sigurnosnim spremnicima. Ovim ključevima i postavkama kombinacija daje se sigurnosna zaštita istog ili višeg stupnja nego što je ima materijal do kojeg se pomoću njih pristupa.

Poznavanje postavki kombinacija sigurnosnih spremnika ograničava se na što je manje moguće ljudi. Kombinacije se mijenjaju:

(a) prilikom primitka novog spremnika;

(b) uvijek kada dođe do promjene osoblja;

(c) uvijek prilikom pojave ili sumnje na ugrožavanje;

(d) po mogućnosti u razmacima od 6 mjeseci, a najmanje svakih 12 mjeseci.

18.3.8. *Uređaji za otkrivanje nedozvoljenih upada*

Kada se za zaštitu klasificiranih podataka EU-a upotrebljavaju alarmni sustavi, televizija zatvorenog kruga (videonadzor) i druge električne naprave mora postojati električno napajanje u nuždi, kako bi se osigurao neprekidan rad sustava ukoliko dođe do kvara glavnog napajanja. Drugi osnovni zahtjev je da se u slučaju kvara ili neovlaštenog upada u takve sustave aktivira alarm ili drugi pouzdani način upozorenja osoblju zaduženom za nadgledanje.

18.3.9. *Odobrena oprema*

Sigurnosni ured Komisije vodi i održava ažurirane popise prema vrsti i modelu sigurnosne opreme odobrene za zaštitu klasificiranih podataka u različitim specifičnim okolnostima i uvjetima. Sigurnosni ured Komisije, između ostalog, zasniva ove popise na podacima koje dostavljaju tijela nacionalne sigurnosti.

18.3.10. *Fizička zaštita kopirnih strojeva i telefaks uređaja*

Kopirni strojevi i telefaks uređaji fizički se zaštićuju u potrebnoj mjeri da ih za rad s klasificiranim podacima mogu upotrebljavati samo ovlaštene osobe i da su svi klasificirani dokumenti nastali njihovom upotrebom pod odgovarajućim nadzorom.

18.4. **Zaštita od neželjenih pogleda i prisluškivanja**

18.4.1. *Neželjeni pogledi*

I noću i danju potrebno je poduzeti sve odgovarajuće mjere osiguranja kako neovlaštene osobe niti slučajno ne bi stekle uvid u klasificirane podatke EU-a.

18.4.2. *Prisluškivanje*

Radne prostorije i područja u kojima se redovno raspravlja o klasificiranim podacima SECRET UE ili višim, kada to nalaže stupanj rizika, zaštićuju se od pasivnih i aktivnih pokušaja prisluškivanja. Procjena rizika od takvih pokušaja u nadležnosti je Sigurnosnog ureda Komisije koji se prema potrebi savjetuje s tijelima nacionalne sigurnosti.

18.4.3. *Unos elektroničke opreme i uređaja za snimanje*

Na sigurnosna ili tehnički sigurna područja nije dozvoljeno unositi mobilne telefone, privatna računala, naprave za snimanje, kamere i drugu elektroničku opremu ili uređaje za snimanje bez prethodnog odobrenja čelnika Sigurnosnog ureda Komisije.

Sigurnosni ured Komisije može, pri određivanju zaštitnih mjera za prostore osjetljive na pasivno prisluškivanje (npr. izolacija zidnih stijena, vrata, podova i stropova, mjerenje opasnog izlaza zvuka) i na aktivno prisluškivanje (npr. traženje mikrofona), zatražiti pomoć stručnjaka iz tijela nacionalne sigurnosti.

Isto tako, kada to okolnosti zahtijevaju, telekomunikacijsku opremu i električnu ili elektroničku uredsku opremu bilo koje vrste koja se koristi tijekom sastanaka na razini SECRET UE ili višoj, mogu na zahtjev čelnika Sigurnosnog ureda Komisije provjeriti specijalisti za tehničku sigurnost pri tijelima nacionalne sigurnosti.

18.5. **Tehnički sigurna područja**

Određena područja mogu se obilježiti kao tehnički sigurna područja. Na ulazu u takva područja provode se posebni postupci provjere. Kada nisu zauzeta ta se područja prema odobrenom postupku zaključavaju i svi se ključevi tretiraju kao sigurnosni ključevi. Takva su područja predmet redovnih inspekcijskih pregleda koji se također obavljaju i nakon svakog neovlaštenog ulaska ili sumnje da je do njega došlo.

Vodi se detaljan popis opreme i namještaja radi nadzora i promjene njihove lokacije. Na takvo područje ne smije se unositi niti jedan komad namještaja ili opreme prije nego što specijalno obučeno sigurnosno osoblje provede pažljivi pregled s namjerom otkrivanja bilo kakvog uređaja za prisluškivanje. Opće pravilo je da postavljanje komunikacijskih vodova u tehnički sigurnim područjima nije dozvoljeno bez prethodnog ovlaštenja nadležnog tijela.

19. OPĆA PRAVILA O NAČELU POTREBE POZNAVANJA I O SIGURNOSNIM PROVJERAMA OSOBLJA EU-a

19.1. **Općenito**

Pristup klasificiranim podacima EU-a odobrava se samo onim osobama koje radi izvršavanja svojih dužnosti imaju „potrebu poznavanja". Pristup podacima TRÈS SECRET UE, SECRET UE i CONFIDENTIEL UE, odobrava se samo osobama koje su prošle odgovarajuće sigurnosne provjere.

Za određivanje osoba za koje vrijedi „potreba poznavanja" je nadležna služba u kojoj se dotična osoba namjerava zaposliti.

Sigurnosne provjere osoblja zahtijeva nadležna služba.

Na kraju postupka izdaje se „sigurnosna potvrda EU-a za osoblje" koja određuje stupanj klasifikacije podataka do kojih provjerena osoba može imati pristup, kao i datum prestanka važenja potvrde.

Sigurnosna potvrda EU-a za osoblje može posjedniku omogućiti pristup podacima nižeg stupnja klasifikacije od dodijeljenog.

Osobe koje nisu dužnosnici niti drugi zaposlenici EU-a, kao što su vanjski suradnici, stručnjaci ili savjetnici s kojima treba raspravljati o klasificiranim podacima EU-a ili im te podatke treba prikazati, moraju imati sigurnosnu potvrdu u vezi s klasificiranim podacima EU-a i biti jasno upoznate sa svojom odgovornosti za sigurnost.

Pristup javnosti i dalje uređuje Uredba (EZ) br. 1049/2001.

19.2. **Posebna pravila za pristup podacima sa stupnjem klasifikacije TRÈS SECRET UE**

Sve osobe za koje se traži pristup podacima TRÈS SECRET UE prvo prolaze postupak provjere za pristup takvim podacima.

Sve osobe za koje se traži pristup podacima TRÈS SECRET UE određuje član Komisije odgovoran za sigurnosna pitanja i njihova se imena čuvaju u odgovarajućem registru TRÈS SECRET UE. Sigurnosni ured Komisije uspostavlja i vodi taj registar.

Prije nego im se omogući pristup podacima TRÈS SECRET UE sve osobe potpisuju potvrdu kojom se dokazuje da su upoznate sa sigurnosnim postupcima Komisije i da u potpunosti razumiju posebnu odgovornost za sigurno čuvanje podataka TRÈS SECRET UE, kao i posljedice koje propisi EU-a i nacionalnog zakonodavstva predviđaju u slučaju da klasificirani podaci dospiju u ruke neovlaštenih osoba, bilo namjernim djelovanjem ili iz nemara.

Za osobe koje imaju na sastancima itd., pristup podacima TRÈS SECRET UE nadležni će nadzorni službenik službe ili tijela u kojem je ta osoba zaposlena, obavijestiti tijelo koje sastanak organizira o tome da dotične osobe imaju takvo odobrenje.

Imena svih osoba kojima prestaje zaposlenje na dužnostima koje zahtijevaju pristup podacima TRÈS SECRET UE skidaju se s popisa TRÈS SECRET UE. Dodatno, svim takvim osobama treba ponovno skrenuti pažnju na naročitu odgovornost koju nose u vezi s čuvanjem podataka TRÈS SECRET UE. Te osobe potpisuju izjavu da neće upotrebljavati niti dalje prosljeđivati podatke TRÈS SECRET UE s kojima su upoznati.

19.3. **Posebna pravila za pristup podacima sa stupnjem klasifikacije SECRET UE i CONFIDENTIEL UE**

Sve osobe za koje se traži pristup podacima sa stupnjem klasifikacije SECRET UE ili CONFIDENTIEL UE najprije prolaze postupak provjere za dobivanje pristupa do odgovarajućeg stupnja klasifikacije podataka.

Sve osobe za koje se traži pristup podacima SECRET UE ili CONFIDENTIEL UE upoznaju se s odgovarajućim sigurnosnim odredbama i posljedicama zanemarivanja tih odredaba.

Za osobe koje imaju na sastancima itd., pristup podacima SECRET UE ili CONFIDENTIEL UE službenik sigurnosti tijela u kojem je ta osoba zaposlena obavještava tijelo koje sastanak organizira o tome da dotične osobe imaju takvo odobrenje.

19.4. **Posebna pravila za pristup podacima sa stupnjem klasifikacije RESTREINT UE**

Osobe koje imaju pristup podacima RESTREINT UE upoznaju se s ovim pravilnikom kao i s posljedicama njegovog zanemarivanja.

19.5. **Premještaji**

Kada se član osoblja premješta s mjesta koje uključuje rukovanje klasificiranim materijalom EU-a, registarski ured nadgleda pravilan prijenos tog materijala od dužnosnika koji odlazi dužnosniku u dolasku.

Kada se član osoblja premješta na drugo mjesto koje uključuje rukovanje klasificiranim materijalom EU-a, lokalni službenik sigurnosti ga odgovarajuće poučava.

19.6. **Posebne upute**

Osobe od kojih se zahtijeva rukovanje klasificiranim podacima EU-a, pri prvom preuzimanju dužnosti kao i redovno nakon tog, upoznaju se s:

(a) opasnostima za sigurnost koje proizlaze iz nesmotrenih razgovora;

(b) mjerama predostrožnosti koje treba poduzeti u odnosima s tiskom i predstavnicima posebnih interesnih skupina;

(c) prijetnjom koju predstavljaju djelovanja obavještajnih službi usmjerena protiv EU-a i država članica u vezi s klasificiranim podacima i djelatnosti EU-a;

(d) obavezom trenutačnog obavještavanja odgovarajućih sigurnosnih tijela o svakom pristupanju ili radnji koja izaziva sumnju da je riječ o špijunskom djelovanju ili o svim neobičnim okolnostima u vezi sa sigurnosti.

Sve osobe koje su uobičajeno izložene čestom kontaktu s predstavnicima zemalja čije obavještajne službe djeluju protiv EU-a i država članica u vezi s klasificiranim podacima i djelatnostima EU-a moraju biti jasno upoznate s tehnikama za koje se zna da ih primjenjuju različite obavještajne službe.

Ne postoje sigurnosne odredbe Komisije u vezi s privatnim putovanjima na bilo koju destinaciju osoba koje su prošle sigurnosnu provjeru za pristup klasificiranim podacima EU-a. Sigurnosni ured Komisije, međutim, upoznaje dužnosnike i druge djelatnike koji su u njegovoj nadležnosti s pravilima putovanja koja moraju poštivati.

20. POSTUPAK SIGURNOSNE PROVJERE ZA DUŽNOSNIKE KOMISIJE I OSTALE ZAPOSLENIKE

(a) Samo dužnosnici i drugi zaposlenici Komisije ili osobe koje rade u okviru Komisije i zbog svojih dužnosti i zahtjeva službe moraju poznavati ili upotrebljavati klasificirane podatke koje čuva Komisija, imaju pravo pristupa tim podacima.

(b) Kako bi im se odobrio pristup do podataka TRÈS SECRET UE, SECRET UE i CONFIDENTIEL UE osobe navedene u stavku (a) moraju imati ovlaštenje u skladu s postupcima iz stavaka (c) i (d) ovog odjeljka.

(c) Ovlaštenje se daje samo osobama koje su sigurnosno provjerene kod nadležnih državnih tijela država članica (tijela nacionalne sigurnosti) u skladu s postupkom iz stavaka (i) do (n).

(d) Čelnik Sigurnosnog ureda Komisije odgovoran je za dodjelu ovlaštenja iz stavaka (a), (b) i (c).

(e) Čelnik izdaje ovlaštenje nakon prikupljanja mišljenja nadležnih državnih tijela država članica na temelju sigurnosne provjere provedene u skladu sa stavcima (i) do (n).

(f) Sigurnosni ured Komisije vodi i održava popis svih osjetljivih radnih mjesta pri odgovarajućim službama Komisije i svih osoba s privremeno dodijeljenim ovlaštenjem.

(g) Ovlaštenje se izdaje za razdoblje od pet godina, ali njegova valjanost ne smije premašiti vremensko trajanje zadaća za koje je dodijeljeno. U skladu s postupkom navedenim u stavku (e) može ga se obnoviti.

(h) Čelnik Sigurnosnog ureda Komisije oduzima ovlaštenje kada smatra da za to postoje opravdani razlozi. Svaka odluka kojom se ovlaštenje povlači dostavlja se dotičnoj osobi; ona može zatražiti saslušanje kod čelnika Sigurnosnog ureda Komisije i nadležnog državnog tijela.

(i) Sigurnosna provjera provodi se uz pomoć zainteresiranih osoba i na zahtjev čelnika Sigurnosnog ureda Komisije. Nadležno državno tijelo za postupak provjere je tijelo države članice čiji je državljanin osoba za koju se ovlaštenje traži. Kada dotična osoba nije državljanin države članice EU-a, čelnik Sigurnosnog ureda Komisije zatražit će sigurnosnu provjeru od države članice EU-a u kojoj osoba ima stalno prebivalište ili stalno boravište.

(j) Kao dio postupka provjere od dotične osobe se traži ispunjavanje upitnika s osobnim podacima.

(k) Čelnik Sigurnosnog ureda Komisije u svojem zahtjevu navodi vrstu i razinu tajnosti podataka koji će biti na raspolaganju dotičnoj osobi.

(l) Cjelokupni postupak sigurnosne provjere, zajedno s dobivenim rezultatima, podliježe odgovarajućim pravilima i propisima koji su na snazi u dotičnoj državi članici, uključujući one koji se odnose na pravna sredstva.

(m) Kada nadležna državna tijela država članica daju pozitivno mišljenje, čelnik Sigurnosnog ureda Komisije može dotičnoj osobi dodijeliti ovlaštenje.

(n) O negativnom mišljenju nadležnih državnih tijela obavještava se dotična osoba; ona može tražiti saslušanje kod čelnika Sigurnosnog ureda Komisije. Ako smatra da je potrebno, čelnik Sigurnosnog ureda Komisije može od nadležnih državnih tijela zatražiti daljnja pojašnjenja. Ako se negativno mišljenje potvrdi, ovlaštenje se ne izdaje.

(o) Sve osobe s dodijeljenim ovlaštenjem u smislu stavaka (d) i (e) primaju, u tom trenutku, kao i kasnije u redovitim vremenskim razmacima, potrebne upute u vezi sa zaštitom klasificiranih podataka i načina postizanja te zaštite. Takve osobe potpisuju izjavu kojom potvrđuju primitak uputa i obvezuju se da će ih poštivati.

(p) Čelnik Sigurnosnog ureda Komisije poduzima sve potrebne mjere kako bi se provele odredbe ovog odjeljka, posebno u vezi s pravilima o uređenju pristupa popisu ovlaštenih osoba.

(q) Ako tako zahtijeva služba, čelnik Sigurnosnog ureda Komisije iznimno može, nakon što o tome obavijesti nadležna državna tijela i pod uvjetom da u roku jednog mjeseca nije bilo njihovog odaziva, dodijeliti privremeno ovlaštenje za razdoblje od najviše šest mjeseci do objave rezultata provjere iz stavka (i).

(r) Tako izdana uvjetna i privremena ovlaštenja ne omogućavaju pristup podacima TRÈS SECRET UE; takav se pristup ograničava na dužnosnike koji su uspješno prošli postupak provjere s pozitivnim rezultatima, u skladu sa stavkom (i). Do objave rezultata postupka provjere, dužnosnici za koje se zahtijeva provjeravanje na razini TRÈS SECRET UE mogu privremeno i uvjetno dobiti ovlaštenje za pristup razvrstanim podacima do stupnja SECRET UE, uključujući i njega.

21. PRIPREMA, DISTRIBUCIJA, PRIJENOS, SIGURNOST KURIRSKOG OSOBLJA I DODATNE PRESLIKE ILI PRIJEVODI TE IZVADCI KLASIFICIRANIH DOKUMENATA EU-a

21.1. **Priprema**

1. Stupnjevi klasifikacije EU-a primjenjuju se kako je utvrđeno u odjeljku 16.; za CONFIDENTIEL UE i više stupnjeve označava se na vrhu i na dnu svake stranice, smješteno u sredini; svaka se stranica numerira. Svaki klasificirani dokument EU-a ima svoj referentni broj i datum. U slučaju dokumenata TRÈS SECRET UE i SECRET UE ovaj se referentni broj pojavljuje na svakoj stranici. Ako se ti dokumenti šalju u nekoliko preslika, svaki od njih nosi broj preslike postavljen na prvoj stranici, zajedno s ukupnim brojem stranica. Na prvoj stranici dokumenta CONFIDENTIEL UE ili višim navode se svi dodaci i prilozi.

2. Dokumente sa stupnjem klasifikacije CONFIDENTIEL UE ili višim tipkaju, prevode, pohranjuju, preslikavaju, umnožavaju na magnetskom mediju ili mikrofilmiraju samo osobe koje su prošle sigurnosnu provjeru za pristup klasificiranim podacima EU-a, najmanje do stupnja sigurnosti odgovarajućeg stupnja klasifikacije dotičnog dokumenta.

3. Računalna priprema klasificiranih dokumenata uređuje se u odjeljku 25.

21.2. **Distribucija**

1. Klasificirani podaci EU-a šalju se samo osobama za koje vrijedi „potreba poznavanja" i koje su odgovarajuće sigurnosno provjerene. Prvi prijenos određuje izvor od kojeg podaci potječu.

2. Dokumenti TRÈS SECRET UE dostavljaju se preko registara TRÈS SECRET UE (vidjeti odjeljak 22.2.). U slučaju poruka označenih kao TRÈS SECRET UE nadležni registar može ovlastiti voditelja komunikacijskog centra za izradu broja preslika navedenog u popisu naslovnika.

3. Dokumente sa stupnjem klasifikacije SECRET UE i nižim, početni naslovnik može dalje slati drugim naslovnicima vodeći se načelom „potrebe poznavanja". Izvor od kojeg podaci potječu, međutim, jasno navodi sva ograničenja koja želi postaviti. Kad god postoje takva ograničenja naslovnici mogu ponovno slati dokumente samo uz ovlaštenje izvora od kojeg podaci potječu.

4. Svaki se dokument sa stupnjem klasifikacije CONFIDENTIEL UE i višim, na dolasku ili odlasku od ravnatelja ili iz službe bilježi se u lokalnom registru klasificiranih podataka EU-a određene službe. Pojedinosti koje se navode (reference, datum i, ako je potrebno, broj preslike) moraju biti takve da se prema njima dokumenti mogu prepoznati i unose se u knjigu bilježaka ili na posebno zaštićen računalni medij (odjeljak 22.1).

21.3. **Prijenos klasificiranih dokumenata EU-a**

21.3.1. *Pakiranje, potvrde primitka*

1. Dokumenti sa stupnjem klasifikacije CONFIDENTIEL UE i višim šalju se u čvrstim, neprozirnim dvostrukim omotnicama. Unutarnja omotnica označava se odgovarajućim stupnjem klasifikacije EU-a i na njoj se, po mogućnosti, navode sve pojedinosti u vezi s nazivom radnog mjesta i adrese primatelja.

2. Samo nadzorni službenik registarskog ureda (vidjeti odjeljak 22.1.) ili njegov zamjenik smiju otvoriti unutarnju omotnicu i potvrditi primitak umetnutih dokumenata, osim u slučaju da je omotnica naslovljena na pojedinca. Tada odgovarajući registarski ured (vidjeti odjeljak 22.1) u knjigu bilježaka upisuje primitak omotnice, a samo osoba na koju je ista naslovljena smije otvoriti unutarnju omotnicu i potvrditi primitak sadržanih dokumenata.

3. Obrazac potvrde primitka stavlja se u unutarnju omotnicu. Na potvrdi primitka, koja se ne smatra klasificiranom, navodi se referentni broj, datum i broj preslike dokumenta, ali nikada predmet dokumenta.

4. Unutarnja omotnica ulaže se u vanjsku omotnicu koja nosi otpremni broj za potrebe prijema. Ni u kakvim okolnostima oznaka stupnja klasifikacije ne smije biti vidljiva na vanjskoj omotnici.

5. Za dokumente sa stupnjem klasifikacije CONFIDENTIEL UE i višim, kuriri i nosioci poruka dobivaju potvrde primitka koje moraju odgovarati brojevima s pakiranja.

21.3.2. *Prijenos unutar zgrade ili skupine zgrada*

Unutar određene zgrade ili skupine zgrada, klasificirani se dokumenti šalju u zapečaćenoj omotnici na kojoj se navodi samo naziv naslovnika, pod uvjetom da ju prenosi osoba provjerena sukladno stupnju klasifikacije dokumenata.

21.3.3. *Prijenos unutar zemlje*

1. Unutar države dokumenti TRÈS SECRET UE šalju se samo putem kurirske službe ili osobe ovlaštene za pristup podacima TRÈS SECRET UE.

2. Uvijek kada se kurirska služba koristi za prijenos dokumenata TRÈS SECRET UE izvan zgrade ili skupine zgrada, poštuju se odredbe o pakiranju i primitku sadržane u ovom poglavlju. Službe za dostavu moraju biti tako opremljene da su pošiljke koje sadrže dokumente TRÈS SECRET UE uvijek pod izravnim nadzorom odgovore osobe.

3. Iznimno se dokumenti TRÈS SECRET UE mogu iznositi izvan kruga zgrade ili skupine zgrada u svrhu lokalne upotrebe na sastancima i raspravama, pod uvjetom:

(a) da je prenositelj ovlašten za pristup tim dokumentima;

(b) da je način prijenosa u skladu s pravilima o prijenosu dokumenata TRÈS SECRET UE;

(c) da ni u kojem slučaju prenositelj ne ostavlja dokumente TRÈS SECRET UE bez nadzora;

(d) da se popis ovako prenošenih dokumenata čuva u registru TRÈS SECRET UE u kojem se dokumenti čuvaju i zapisuju u kontrolnu knjigu te se prema tom zapisu provjeravaju na povratku.

4. Unutar pojedine države dokumenti TRÈS SECRET UE i CONFIDENTIEL UE mogu se slati poštom, ako je to prema nacionalnim propisima dozvoljeno i u skladu s odredbama ovog pravilnika, ili putem kurirske službe ili osoba provjerenih za pristup klasificiranim dokumentima EU-a.

5. Sigurnosni ured Komisije na temelju ovih propisa priprema upute o osobnom prenošenju klasificiranih dokumenata EU-a. Te upute nositelj je dužan pročitati i potpisati. Posebno se u uputama jasno naglašava da se, ni u kakvim okolnostima, dokumenti:

(a) ne smiju ispustiti iz ruku nositelja sve dok nisu pod sigurnom nadzorom u skladu s odredbama iz odjeljka 18.;

(b) ne smiju ostavljati bez nadzora u sredstvima javnog prometa ili privatnim vozilima ili na mjestima kao što su restorani ili hoteli. Ne smiju se pohranjivati u hotelskim sefovima ili ostavljati bez nadzora u hotelskim sobama;

(c) ne smiju čitati na javnim mjestima kao što su zrakoplovi ili vlakovi.

21.3.4. *Prijenos iz jedne države u drugu*

1. Materijale sa stupnjem CONFIDENTIEL UE i višim prenose diplomatske ili vojne kurirske službe EU-a.

2. Međutim, osobno prenošenje materijala sa stupnjem SECRET UE i CONFIDENTIEL UE može se dozvoliti ako su uvjeti prenošenja takvi da materijal ne može dospjeti u ruke niti jedne neovlaštene osobe.

3. Član Komisije odgovoran za sigurnosna pitanja može odobriti osobni prijenos kada diplomatski i vojni kuriri nisu na raspolaganju ili bi korištenje njihovih usluga rezultiralo kašnjenjem koje bi štetilo operacijama EU-a, a primatelju je materijal hitno potreban. Sigurnosni ured Komisije priprema upute za osobno međunarodno prenošenje materijala razvrstanih do stupnja SECRET UE i uključivo njega, od strane osoba koje nisu diplomatski ili vojni kuriri. U uputama se zahtijeva da:

(a) nositelj ima odgovarajuću sigurnosnu potvrdu;

(b) se u nadležnoj službi ili registarskom uredu vodi evidencija o svim prenošenim materijalima;

(c) je na paketima ili vrećama s materijalom EU-a stavljena službena plomba radi sprečavanja carinskih pregleda, kao i identifikacijske naljepnice s uputama nalazniku;

(d) nositelj posjeduje kurirsku potvrdu i/ili nalog za izvršavanje zadatka koji priznaju sve države članice EU s kojim je nositelj ovlašten za prijenos označenog paketa;

(e) se pri putovanju kopnom ne smije prelaziti granice niti jedne države koja nije članica EU-a, osim ako država pošiljatelj ima posebno jamstvo te države;

(f) su detalji putovanja nositelja u vezi s odredištem, smjerovima putovanja i korištenih načina prijevoza u skladu s propisima EU-a ili u skladu s nacionalnim propisima o ovim pitanjima, ako su ovi stroži;

(g) nositelj ne smije ispuštati materijal iz ruku sve dok nije sigurno pohranjen u skladu s odredbama iz odjeljka 18.;

(h) materijal ne smije ostati bez nadzora u javnim ili osobnim vozilima ili na mjestima kao što su restorani ili hoteli. Ne smije se pohranjivati u hotelskim sefovima ili ostavljati bez nadzora u hotelskim sobama;

(i) ukoliko prenošeni materijal sadrži dokumente, ti se dokumenti ne smiju čitati na javnim mjestima (npr. u zrakoplovima, vlakovima itd.).

4. Osoba koja je određena za prenošenje tajnog materijala dužna je pročitati i potpisati sigurnosne upute koje sadrže minimalno gore spomenute upute i postupke koje treba slijediti u slučaju nužde ili u slučaju da carinski ili aerodromski službenici zahtijevaju pregled paketa s klasificiranim materijalom.

21.3.5. *Prijenos dokumenata RESTREINT UE*

Za prijenos dokumenata RESTREINT UE ne postoje posebne odredbe, osim što treba osigurati da takvi dokumenti ne padnu u ruke neovlaštenim osobama.

21.4. **Sigurnost kurirskog osoblja**

Svi kuriri zaposleni na prenošenju dokumenata sa stupnjem klasifikacije SECRET UE i CONFIDENTIEL UE moraju biti sigurnosno provjereni.

21.5. **Elektronička i druga sredstva tehničkog prijenosa**

1. Sigurnosne mjere u području komunikacija uvode se radi osiguranja sigurnog prijenosa klasificiranih podataka EU-a. Detaljna pravila koja se primjenjuju na prijenos takvih klasificiranih podataka EU-a određena su u odjeljku 25.

2. Samo akreditirani komunikacijski centri i mreže i/ili terminali i sustavi smiju prenositi podatke sa stupnjem klasifikacije CONFIDENTIEL UE i SECRET UE.

21.6. **Dodatne preslike i prijevodi te izvadci iz klasificiranih dokumenata EU-a**

1. Kopiranje ili prijevod dokumenata TRÈS SECRET UE može odobriti samo izvor od kojeg podaci potječu.

2. Ako osobe bez sigurnosne provjere stupnja TRÈS SECRET UE zahtijevaju podatke koji iako sadržani u dokumentu razvrstanom kao TRÈS SECRET UE nemaju taj status, čelniku registra TRÈS SECRET UE (vidjeti odjeljak 22.2) može se dozvoliti da izradi potreban broj izvadaka iz tog dokumenta. U isto vrijeme čelnik poduzima potrebne korake za dodjelu odgovarajućeg stupnja klasifikacije tim izvadcima.

3. Dokumente stupnja klasifikacije SECRET UE i nižim može, u skladu s ovim pravilnikom, umnožavati i prevoditi naslovnik pod uvjetom da se strogo poštuje načelo potrebe poznavanja. Sigurnosne mjere koje se primjenjuju na izvorni dokument važeće su i za njegove preslike i/ili prijevode.

22. EU REGISTRI, INVENTURNI POPISI, PROVJERE, ARHIVA KLASIFICIRANIH PODATAKA I UNIŠTAVANJE KLASIFICIRANIH PODATAKA

22.1. **Lokalni registri klasificiranih podataka EU-a**

1. Unutar Komisije, prema potrebi, u svakoj službi postoji jedan ili više lokalnih registara klasificiranih podataka EU-a za registriranje, umnožavanje, pošiljanje, pohranjivanje i uništavanje dokumenata sa stupnjem SECRET UE i CONFIDENTIEL UE.

2. Kada služba nema lokalni registar klasificiranih podataka EU-a, tu ulogu preuzima lokalni registar klasificiranih podataka EU-a glavnog tajništva.

3. Lokalni registar klasificiranih podataka EU-a podnosi izvješća voditelju službe od koje primaju upute. Čelnik ovih registarskih ureda je nadzorni službenik registarskog ureda (RCO).

4. Lokalni registri klasificiranih podataka EU-a su pod nadzorom lokalnog službenika sigurnosti u vezi s provedbom propisa o rukovanju klasificiranim dokumentima EU-a i poštivanje odgovarajućih sigurnosnih mjera.

5. Dužnosnicima koji su dodijeljeni lokalnim registarskim uredima klasificiranih podataka EU-a dozvoljen je pristup klasificiranim podacima EU-a u skladu s odjeljkom 20.

6. Pod vodstvom nadležnog voditelja službe lokalni registri klasificiranih podataka EU-a:

   (a) vode postupke u vezi s registracijom, umnožavanjem, prevođenjem, prijenosom, pošiljanjem i uništavanjem takvih podataka;

   (b) ažuriraju registar o klasificiranim podacima;

   (c) redovito provjeravaju potrebu zadržavanja stupnja klasifikacije podataka.

7. Lokalni registri za klasificirane podatke EU-a vode evidenciju o sljedećim podacima:

   (a) datumu nastanka klasificiranih podataka;

   (b) stupnju tajnosti;

   (c) datumu prestanka važenja stupnja klasifikacije podatka;

   (d) nazivu i službi izvora od kojeg podaci potječu;

   (e) primatelju ili primateljima sa serijskim brojem;

   (f) predmetu;

   (g) broju;

   (h) broju preslika u opticaju;

   (i) pripremi popisa klasificiranih podataka koji su poslani službi;

   (j) registru ukidanja ili snižavanja stupnja klasifikacije podataka.

8. Opća pravila navedena u odjeljku 21. primjenjuju se na lokalne registre klasificiranih podataka EU-a pri Komisiji, osim ako ta pravila mijenjaju posebna pravila ovog odjeljka.

22.2. **Središnji registar TRÈS SECRET UE**

22.2.1. *Općenito*

1. Središnji registar TRÈS SECRET UE osigurava evidentiranje, obradu i distribuciju dokumenata TRÈS SECRET UE u skladu s ovim pravilnikom. Čelnik registra TRÈS SECRET UE je nadzorni službenik registra TRÈS SECRET UE.

2. Središnji registar TRÈS SECRET UE djeluje kao glavno tijelo Komisije za primanje i pošiljanje zajedno s drugim institucijama EU-a, državama članicama, međunarodnim organizacijama i trećim zemljama s kojima Komisija ima sporazume o sigurnosnim postupcima za razmjenu klasificiranih podataka.

3. Ako je potrebno osnivaju se podregistri koji su odgovorni za unutrašnje upravljanje dokumentima TRÈS SECRET UE; oni vode ažurirane evidencije o kruženju svakog dokumenta za kojeg je podregistarski ured zadužen.

4. Podregistri TRÈS SECRET UE osnivaju se zbog dugoročnih potreba kako je navedeno u odjeljku 22.2.3. i pridružuju su središnjem registru TRÈS SECRET UE. Ako postoji privremena ili povremena potreba za proučavanjem dokumenata TRÈS SECRET UE, ovi se dokumenti mogu dostavljati bez uspostavljanja podregistra TRÈS SECRET UE, pod uvjetom da su utvrđena pravila prema kojima dokumenti ostaju pod nadzorom odgovarajućeg registra TRÈS SECRET UE i da su uzete u obzir sve sigurnosne mjere za fizičku zaštitu i zaštitu osoblja.

5. Podregistri ne smiju slati dokumente TRÈS SECRET UE izravno drugim podregistrima istog središnjeg registra TRÈS SECRET UE bez izričitog pismenog odobrenja središnjeg registra.

6. Sve razmjene dokumenata TRÈS SECRET UE između podregistara koji nisu pridruženi istom središnjem registru odvijaju se preko središnjih registara TRÈS SECRET UE.

22.2.2 *Središnji registar TRÈS SECRET UE*

Kao nadzorni službenik, čelnik središnjeg registra TRÈS SECRET UE odgovoran je za:

(a) prijenos dokumenata TRÈS SECRET UE u skladu s odredbama iz odjeljka 21.3.;

(b) vođenje popisa svih pripadajućih podregistarskih ureda TRÈS SECRET UE, zajedno s imenima i potpisima imenovanih nadzornih službenika i njihovih ovlaštenih namještenika;

(c) čuvanje potvrda primitaka registarskih ureda za sve dokumente TRÈS SECRET UE koje šalje središnji registar;

(d) vođenje evidencije o pohranjenim i poslanim dokumentima TRÈS SECRET UE;

(e) vođenje ažuriranog popisa svih središnjih registara TRÈS SECRET UE s kojima se uobičajeno izmjenjuje korespondencija, zajedno s imenima i potpisima imenovanih nadzornih službenika i njihovih ovlaštenih namještenika;

(f) fizičku zaštitu svih dokumenata TRÈS SECRET UE čuvanih u registru, sukladno pravilima navedenim u odjeljku 18.

22.2.3. *Podregistri TRÈS SECRET UE*

Kao nadzorni službenik, čelnik pojedinog podregistra TRÈS SECRET UE odgovoran je za:

(a) prijenos dokumenata TRÈS SECRET UE u skladu s odredbama utvrđenim odjeljkom 21.3.;

(b) vođenje ažuriranog popisa svih osoba ovlaštenih za pristup podacima TRÈS SECRET UE pod njegovim nadzorom;

(c) distribuciju dokumenata TRÈS SECRET UE u skladu s uputama izvora od kojeg podaci potječu ili na temelju „potrebe poznavanja”, uz prethodnu provjeru ima li naslovnik traženu sigurnosnu provjeru;

(d) vođenje ažurirane evidencije svih dokumenata TRÈS SECRET UE koji se čuvaju ili kruže pod njegovim nadzorom, ili koji su predani drugom registru TRÈS SECRET UE, kao i za čuvanje svih odgovarajućih potvrda primitaka;

(e) vođenje ažuriranog popisa središnjih registara TRÈS SECRET UE s kojima je ovlašten razmjenjivati dokumente TRÈS SECRET UE, zajedno s imenima i potpisima njihovih nadzornih službenika i ovlaštenih zamjenika;

(f) fizičku zaštitu svih dokumenata TRÈS SECRET UE koji se čuvaju u podregistru, sukladno odredbama odjeljka 18.

22.3. **Popisi, inventurni popisi i provjere klasificiranih dokumenata EU-a**

1. Svaki registar TRÈS SECRET UE, kako se navodi u ovome odjeljku, svake godine provodi detaljan popis dokumenata TRÈS SECRET UE. Smatra se da je dokument evidentiran ako registar njime raspolaže u fizičkom smislu ili posjeduje potvrdu o primitku registra TRÈS SECRET UE kojemu je dokument dostavljen, potvrdu o uništenju dokumenta ili uputu o snižavanju ili ukidanju stupnja klasifikacije dokumenta. Rezultati godišnjeg popisa prosljeđuju se članu Komisije odgovornom za sigurnosna pitanja najkasnije do 1. travnja svake godine.

2. Podregistri TRÈS SECRET UE prosljeđuju rezultate svojih godišnjih popisa središnjem registru kojem odgovaraju, s datumom kojeg ovaj odredi.

3. Klasificirani dokumenti EU-a s nižim stupnjem klasifikacije od TRÈS SECRET UE podliježu internim pregledima u skladu s uputama člana Komisije odgovornog za sigurnosna pitanja.

4. U tim postupcima posjednik dokumenta može izraziti mišljenje u vezi:

   (a) mogućnosti snižavanja ili ukidanja stupnja klasifikacije određenih dokumenata;

   (b) dokumenata koje treba uništiti.

22.4 **Pohranjivanje klasificiranih podataka EU-a**

1. Klasificirani podaci EU-a pohranjuju se u uvjetima koji su u skladu s uvjetima navedenim u odjeljku 18.

2. Kako bi se problemi skladištenja sveli na najmanju moguću mjeru, nadzorni službenici svih registara ovlašćuju se za mikrofilmiranje ili drugačije spremanje na magnetskim ili optičkim medijima za arhiviranje dokumenata TRÈS SECRET UE, SECRET UE i CONFIDENTIEL UE, pod uvjetom da:

   (a) mikrofilmiranje/postupak spremanja provodi osoba s važećom sigurnosnom provjerom za odgovarajući stupanj klasifikacije;

   (b) se mikrofilmu/mediju za pohranu dodijeli jednak sigurnosni stupanj kao izvornom dokumentu;

   (c) se mikrofilmiranje/spremanje bilo kojeg dokumenta TRÈS SECRET UE prijavi izvoru od kojeg podaci potječu;

   (d) koluti filma ili druge vrste nosača, sadrže samo dokumente istog stupnja klasifikacije: TRÈS SECRET UE, SECRET UE ili CONFIDENTIEL UE;

   (e) je mikrofilmiranje/spremanje dokumenta TRÈS SECRET UE ili SECRET UE jasno naznačeno u evidenciji koja se koristi za godišnji popis;

   (f) se originalni dokumenti koji su mikrofilmirani ili na drugi način spremljeni unište u skladu s pravilima iz odjeljka 22.5.

3. Ova se pravila primjenjuju i na svaki drugi oblik ovlaštenog spremanja, kao što su elektromagnetski medij i optički disk.

22.5. **Uništavanje klasificiranih dokumenata EU-a**

1. Kako bi se spriječilo nepotrebno nakupljanje klasificiranih dokumenata EU-a, dokumenti koje čelnik službe koja ih čuva smatra nevažećim i prekobrojnim uništavaju se što je ranije moguće, na sljedeći način:

   (a) dokumente TRÈS SECRET UE uništava jedino središnji registarski ured koji je za njih odgovoran. Svaki uništeni dokument navodi se u potvrdi uništenja koju potpisuju službenik zadužen za nadzor za stupanj TRÈS SECRET UE i službenik koji je svjedočio uništenju i koji mora imati sigurnosnu provjeru za stupanj TRÈS SECRET UE. U tu svrhu se u upisnik unosi odgovarajuća bilješka.

   (b) registarski ured čuva potvrde o uništenju zajedno s dokumentacijom o prijenosu deset godina;

   (c) dokumenti TRÈS SECRET UE, uključujući i sav otpad tajnog materijala nastao prilikom pripremanja dokumenata TRÈS SECRET UE kao što su: oštećene preslike, radni prijedlozi, tipkane bilješke, diskete, nadgledano od nadzornog službenika registarskog ureda TRÈS SECRET UE uništavaju se spaljivanjem, mljevenjem, trganjem ili drugim postupkom pretvaranja u neraspoznatljiv i neobnovljiv oblik.

2. Dokumente SECRET UE uništava registarski ured koji je za njih odgovoran pod nadzorom osobe sa sigurnosnom provjerom, koristeći se nekim od postupaka navedenih u stavku 1. c). Uništeni dokumenti SECRET UE navode se na potpisanoj potvrdi o uništenju koju, zajedno s dokumentacijom o prijenosu, registarski ured čuva najmanje tri godine.

3. Dokumente CONFIDENTIEL UE uništava registarski ured koji je za te dokumente odgovoran pod nadzorom osobe sa sigurnosnom provjerom, nekim od postupaka navedenih u stavku 1.(c). Njihovo se uništenje evidentira u skladu s uputama člana Komisije odgovornog za sigurnosna pitanja.

4. Dokumente RESTREINT UE uništava registarski ured koji je za te dokumente odgovoran ili korisnik, u skladu s uputama člana Komisije odgovornog za sigurnosna pitanja.

22.6. **Uništavanje u slučaju nužde**

1. Službe Komisije uz poštivanje lokalnih uvjeta pripremaju planove za sigurno čuvanje tajnog materijala EU-a u kriznim situacijama, uključujući prema potrebi planove o uništavanju i premještanju u nuždi. Objavljuju upute koje smatraju prijeko potrebnima da klasificirani podaci EU-a ne bi došli u ruke neovlaštenim osobama.

2. Mjere u vezi s čuvanjem i/ili uništavanjem materijala SECRET UE i CONFIDENTIEL UE u kriznim situacijama ne smiju, ni u kakvim okolnostima, utjecati na sigurno čuvanje ili uništavanje materijala TRÈS SECRET UE, uključujući opremu za šifriranje čije zbrinjavanje ima prioritet nad svim ostalim zadaćama.

3. Mjere koje se donose za sigurno čuvanje i uništavanje opreme za šifriranje u nuždi, određene su u posebnim uputama.

4. Upute moraju biti raspoložive na licu mjesta u zapečaćenoj omotnici. Na raspolaganju moraju biti i sredstva/alati za uništenje.

23. SIGURNOSNE MJERE ZA POSEBNE SASTANKE KOJI SE ODRŽAVAJU IZVAN PROSTORA KOMISIJE I UKLJUČUJU KLASIFICIRANE PODATKE EU-a

23.1. **Općenito**

Kada se sastanci Komisije ili drugi važni sastanci održavaju izvan prostora Komisije i kada je to opravdano posebnim sigurnosnim zahtjevima vezanim za visoku osjetljivost pitanja ili podataka koji su predmet sastanka, poduzimaju se dolje opisane sigurnosne mjere. Ove mjere odnose se samo na zaštitu klasificiranih podataka EU-a, a mogu se predvidjeti i druge sigurnosne mjere.

23.2. **Odgovornosti**

23.2.1. *Sigurnosni ured Komisije*

Sigurnosni ured Komisije surađuje s nadležnim tijelima država članica na čijem se teritoriju sastanak održava (država članica domaćin), kako bi se osigurala sigurnost sastanaka Komisije ili drugih važnih sastanaka te delegata i osoblja. U vezi s očuvanjem sigurnosti naročito treba osigurati da:

(a) se razrade planovi u vezi s ugrožavanjem sigurnosti i incidenata u vezi sa sigurnosti, pri čemu dotične mjere obuhvaćaju prije svega sigurnu skrb nad klasificiranim dokumentima EU-a u službenim prostorijama;

(b) se poduzmu mjere koje omogućavaju pristup komunikacijskom sustavu Komisije za prijem i slanje klasificiranih poruka EU-a. Od države članice domaćina zahtijeva se, ako je potrebno, pristup sigurnim telefonskim sustavima.

Sigurnosni ured Komisije djeluje kao savjetodavno tijelo za pitanja sigurnosti u vezi s pripremom sastanka; na sastanku ima svog predstavnika radi pružanja pomoći i savjeta službeniku za sigurnost sastanka i delegacijama, ako je to potrebno.

Svaka delegacija na sastanku određuje službenika sigurnosti koji će biti odgovoran za rješavanje sigurnosnih pitanja svoje delegacije i za održavanje veze sa službenikom za sigurnost sastanka, kao i s predstavnikom Sigurnosnog ureda Komisije, ako je potrebno.

23.2.2. *Službenik za sigurnost sastanka (MSO)*

Imenuje se službenik za sigurnost sastanka koji je odgovoran za opće pripreme i nadzor općih unutrašnjih mjera sigurnosti, kao i za usklađivanje s drugim dotičnim nadležnim tijelima. Mjere koje poduzima službenik za sigurnost sastanka uglavnom se odnose na:

(a) zaštitne mjere mjesta sastanka kako bi se osiguralo održavanje sastanka bez incidenata koji bi mogli ugroziti sigurnost bilo kojeg korištenog tajnog podatka EU-a na sastanku;

(b) pregledavanje osoblja s dozvolom pristupa mjestu održavanja sastanka, prostorima delegacija i konferencijskim dvoranama, kao i pregledavanje cjelokupne opreme;

(c) stalnu koordinaciju s nadležnim tijelima države članice domaćina i Sigurnosnim uredom Komisije;

(d) uključivanje sigurnosnih uputa u materijal za sastanak, uz poštivanje odredbi ovog pravilnika kao i svih drugih sigurnosnih uputa koje se pokažu potrebnima.

23.3. **Sigurnosne mjere**

23.3.1. *Sigurnosna područja*

Uspostavljaju se sljedeća sigurnosna područja:

(a) sigurnosno područje razreda II. koje se sastoji od prostorije za pripremanje klasificiranih dokumenata, službenih prostorija Komisije i grafičke opreme za umnožavanje, kao i službenih prostorija za delegacije, ako je to prikladno;

(b) sigurnosno područje razreda I. koje se sastoji od konferencijske dvorane i kabina za tumače i tonske tehničare;

(c) upravna područja koja se sastoje od područja za novinare i onih dijelova mjesta sastanka za potrebe uprave, ugostiteljstva i smještaja, kao i područja u neposrednoj blizini novinarskog centra i mjesta sastanka.

23.3.2 *Propusnice*

Službenik za sigurnost sastanka izdaje odgovarajuće značke kada to traže delegacije u skladu sa svojim potrebama. Pri tome može, ako je potrebno, uvesti razliku u pristupu različitim sigurnosnim područjima.

Sigurnosne upute za sastanak od svih osoba na koje se to odnosi zahtijevaju da nose svoje značke na vidnome mjestu čitavo vrijeme sastanka, u okviru mjesta održavanja sastanka, kako bi ih sigurnosno osoblje prema potrebi moglo provjeriti.

Osim sudionika sastanka koji nose značke, pristup na mjesto sastanka dozvoljava se što manjem broju osoba. Službenik za sigurnost sastanka dozvoljava primanje posjetitelja za vrijeme sastanka jedino državnim delegacijama na temelju njihovog zahtjeva. Posjetiteljima se daje značka za posjetitelje. Na propusnicu posjetitelja unosi se njegovo ime i ime osobe koju posjećuje. Posjetitelji moraju čitavo vrijeme biti u pratnji redara za sigurnost ili osobe koju posjećuju. Propusnicu posjetitelja nosi osoba u pratnji, koja ju zajedno sa značkom posjetitelja vraća sigurnosnom osoblju nakon što posjetitelj napusti mjesto sastanka.

23.3.3. *Nadzor fotografske i audio opreme*

Na sigurnosno područje I. razreda ne smiju se unositi kamere ili oprema za snimanje, osim opreme fotografa i tonskih tehničara s propisnim ovlaštenjem službenika za sigurnost sastanka.

23.3.4. *Pregledavanje službenih torbi, prijenosnih računala i pošiljki*

Osobe s propusnicom i dozvolom pristupa na sigurnosno područje mogu uobičajeno, bez provjere, unijeti svoje službene torbe i prijenosna računala (samo s vlastitim izvorom napajanja). U slučaju pošiljki upućenih delegacijama, delegacije mogu preuzeti dostavljene pošiljke koje će pregledati sigurnosni službenik delegacije, provjeravajući ih posebnom opremom ili otvorene od strane sigurnosnog osoblja radi pregleda. Ako službenik za sigurnost sastanka smatra da je potrebno, mogu se odrediti strože mjere za pregled službenih torbi i pošiljki.

23.3.5. *Tehnička sigurnost*

Dvoranu za sastanke može, u tehničkom smislu, osigurati tehnička ekipa za sigurnost koja može uvesti i elektronski nadzor za vrijeme sastanka.

23.3.6. *Dokumenti delegacija*

Delegacije su odgovorne za donošenje klasificiranih dokumenata EU-a na sastanak, kao i njihovo odnošenje sa sastanka. Također su odgovorne za ovjeru i sigurnost tih dokumenata za vrijeme njihove upotrebe u dodijeljenim prostorima. Od države članice domaćina može se zatražiti pomoć za prenošenje klasificiranih dokumenata na mjesto sastanka i s njega.

23.3.7. *Sigurno čuvanje dokumenata*

Ako Komisija ili delegacije nisu u mogućnosti pohraniti svoje klasificirane dokumente u skladu s važećim standardima mogu ih, uz potvrdu primitka, u zapečaćenoj omotnici predati na čuvanje službeniku za sigurnost sastanka koji dokumente pohranjuje u skladu s važećim standardima.

23.3.8. *Pregled službenih prostorija*

Službenik za sigurnost sastanka organizira pregled prostora pisarnice Komisije i delegacija na kraju svakog radnog dana, kako bi se osiguralo da svi klasificirani dokumenti EU-a budu pohranjeni na sigurno. U suprotnome, poduzima odgovarajuće mjere.

23.3.9. *Odlaganje otpadnog materijala klasificiranih sadržaja EU-a*

Za sav materijal u vezi s klasificiranim podacima EU-a koji se smatra otpadom, predstavnicima Komisije i delegacijama daju se koševi i vreće za odlaganje. Prije napuštanja prostorija koje su im dodijeljene predstavnici Komisije i delegacije predaju svoj otpadni materijal službeniku za sigurnost sastanka koji će se pobrinuti za njegovo uništenje u skladu s pravilima.

Na kraju sastanka svi dokumenti predstavnika Komisije i delegacija koji im više nisu potrebni smatraju se otpadnim materijalom. Temeljito pretraživanje prostorija Komisije i delegacija obavlja se prije ukidanja sigurnosnih mjera koje su donijete u vezi sa sastancima. Dokumenti za koje je potpisan primitak uništavaju se, koliko je to moguće, kako je propisano u odjeljku 22.5.

24. KRŠENJA SIGURNOSTI I RAZOTKRIVANJE KLASIFICIRANIH PODATAKA EU-a

24.1. **Definicije**

Kršenje sigurnosti nastaje kao posljedica djelovanja ili izostanka djelovanja koje bi protivno sigurnosnim odredbama Komisije moglo prouzročiti ugrožavanje ili razotkrivanje klasificiranih podataka EU-a.

Do razotkrivanja klasificiranih podataka EU-a dolazi kada u potpunosti ili djelomično dospiju u ruke neovlaštenih osoba, tj. osoba koje nisu prošle odgovarajuću sigurnosnu provjeru ili nemaju nužnu potrebu poznavanja, ili postoji velika vjerojatnost da do tog dođe.

Do ugrožavanja klasificiranih podataka EU-a može doći uslijed nebrige, zanemarivanja ili nesmotrenog ponašanja, kao i uslijed djelovanja službi usmjerenih protiv EU-a ili njezinih država članica u vezi s klasificiranim podacima i aktivnosti EU-a ili uslijed djelovanja subverzivnih organizacija.

24.2. **Prijavljivanje kršenja sigurnosti**

Sve osobe od kojih se zahtijeva rukovanje klasificiranim podacima EU-a detaljno se upoznaju sa svojim dužnostima u vezi s tim. O svim kršenjima sigurnosti koje zamijete te osobe odmah podnose izvješće.

Kada lokalni službenik sigurnosti ili službenik za sigurnost sastanka otkrije ili dobije informaciju o kršenju sigurnosti koje se odnosi na klasificirane podatke EU-a ili o gubitku ili nestanku tajnog materijala EU-a, poduzima pravovremene mjere kako bi se:

(a) sačuvali dokazi;

(b) utvrdile činjenice;

(c) procijenila i na minimum svela počinjena šteta;

(d) spriječilo ponovno kršenje;

(e) obavijestila nadležna tijela o posljedicama kršenja sigurnosti.

S tim u vezi, dostavljaju se sljedeći podaci:

i. opis predmetnih podataka, uključujući njihov stupanj klasifikacije, referentni broj i broj preslike, datum, izvor iz kojeg podaci potječu, predmet i područje primjene;

ii. sažet opis okolnosti kršenja sigurnosti, uključujući datum i razdoblje u kojem su podaci bili ugroženi;

iii. izjavu da je izvor od kojeg podaci potječu upoznat s razotkrivanjem.

Dužnost svakog tijela za sigurnost je da čim primi obavijest o mogućem kršenju sigurnosti, o tome odmah izvijesti Sigurnosni ured Komisije.

O slučajevima koji se odnose na podatke sa stupnjem klasifikacije RESTREINT UE prijavljuju se ako su neuobičajeni.

Nakon primitka obavijesti o nastalom kršenju sigurnosti član Komisije odgovoran za sigurnosna pitanja:

(a) obavještava izvor od kojeg potječu predmetni klasificirani podaci;

(b) zahtijeva od odgovarajućih sigurnosnih tijela da započnu istragu;

(c) usklađuje upite kada se tiču više sigurnosnih tijela;

(d) prikuplja izvještaje o okolnostima kršenja, datumu ili razdoblju tijekom kojeg je ono nastupilo i bilo otkriveno, s detaljnim opisom sadržaja i stupnjem klasifikacije uključenog materijala. Šteta počinjena interesima EU-a ili jedne ili više njezinih država članica, kao i radnje poduzete za sprečavanje ponovnog kršenja također se prijavljuju.

Izvor od kojeg potječu podaci obavještava naslovnike i daje odgovarajuće upute.

24.3. **Pravna sredstva**

Svaka osoba koja je odgovorna za razotkrivanje klasificiranih podataka EU-a disciplinski je odgovorna u skladu s odgovarajućim pravilima i propisima, posebno glavom VI. Propisa o osoblju. Te mjere ne dovode u pitanje bilo koje daljnje pravne mjere.

Član Komisije odgovoran za sigurnosna pitanja u primjerenim slučajevima, na temelju izvještaja spomenutog u odjeljku 24.2., poduzima sve potrebne mjere kako bi omogućio nadležnim državnim tijelima da započnu s kaznenim postupcima.

25. ZAŠTITA KLASIFICIRANIH PODATAKA EU-a U SUSTAVIMA INFORMACIJSKE TEHNOLOGIJE I KOMUNIKACIJSKIM SUSTAVIMA

25.1. **Uvod**

25.1.1. *Općenito*

Sigurnosna politika i sigurnosni zahtjevi primjenjuju se na sve komunikacijske i informacijske sustave i mreže (nadalje sustave) koji obrađuju podatke sa stupnjem klasifikacije CONFIDENTIEL UE i višim. Primjenjuju se kao dopuna Odluci Komisije C (95) 1510 od 23. studenoga 1995. o zaštiti informacijskih sustava.

Sustavi koji obrađuju podatke RESTREINT UE također zahtijevaju sigurnosne mjere za zaštitu povjerljivosti tih podataka. Pri svim sustavima potrebne su sigurnosne mjere za zaštitu cjelovitosti i raspoloživosti navedenih sustava i podataka koje sadrže.

Sigurnosna politika informacijske tehnologije koju primjenjuje Komisija sadrži sljedeće elemente:

— sastavni je dio opće sigurnosti i dopunjuje sve elemente informacijske sigurnosti, sigurnosti osoblja i fizičke sigurnosti;

— raspodjela odgovornosti između imatelja tehničkih sustava, imatelja klasificiranih podataka EU-a pohranjenih i obrađenih u tehničkim sustavima, stručnjaka za sigurnost informacijske tehnologije i korisnika;

— sigurnosna načela i zahtjevi svakog IT sustava;

— odobrenje ovih načela i zahtjeva od tijela koje je za to određeno;

— uzimanje u obzir posebnih vrsta ugroženosti i ranjivosti u području informacijske tehnologije.

25.1.2. *Ugroženost i ranjivost sustava*

Ugroženost se može odrediti kao mogućnost namjernog ili slučajnog ugrožavanja sigurnosti. U sustavima, takva ugroženost obuhvaća gubitak jednog ili više svojstava kao što su tajnost, cjelovitost i raspoloživost. Ranjivost se može odrediti kao nedostatnost ili pomanjkanje nadzora koje može pospješiti ili omogućiti nastanak prijetnje za specifično sredstvo ili cilj.

Klasificirani podaci EU-a i podaci koji nisu klasificirani, obrađeni u sustavima u koncentriranom obliku, osmišljeni za brzo preuzimanje, prenošenje i upotrebu izloženi su mnogim oblicima ugroženosti. To uključuju pristup neovlaštenih korisnika podacima, ali i obratno, sprečavanje pristupa ovlaštenim korisnicima. Također postoje i rizici neovlaštenog razotkrivanja, iskrivljavanja, mijenjanja ili brisanja podataka. Nadalje, složena i ponekad osjetljiva oprema je skupa te se ponekad teško popravlja ili brzo zamjenjuje.

25.1.3. *Glavna namjena mjera sigurnosti*

Glavna je namjena mjera sigurnosti navedenih u ovome odjeljku pružiti zaštitu od neovlaštenog razotkrivanja klasificiranih podataka EU-a (gubitka tajnosti) i gubitka njihove cjelovitosti i raspoloživosti. Da bi se postigla odgovarajuća sigurnosna zaštita sustava koji obrađuje klasificirane podatke EU-a, Sigurnosni ured Komisije utvrđuje odgovarajuće standarde uobičajene sigurnosti, zajedno s odgovarajućim posebnim sigurnosnim postupcima i tehnikama posebno osmišljenim za svaki sustav.

25.1.4. *Određenje sigurnosnih zahtjeva koji su specifični za sustav (SSRS)*

Za sve sustave koji rukuju podacima stupnja klasifikacije CONFIDENTIEL UE i višim zahtijeva se Određenje sigurnosnih zahtjeva koji su specifični za sustav – SSRS (*Specific Security Requirement Statement*) koju sastavlja imatelj tehničkog sustava – TSO (*Technical System Owner*, vidjeti odjeljak 25.3.4.) i imatelj podataka – IO (*Information Owner*) (vidjeti odjeljak 25.3.5.) uz dopunu i pomoć, ako je potrebno, projektnog osoblja i Ureda komisije za sigurnost (kao tijelo INFOSEC, vidjeti odjeljak 25.3.3.), odobrena od tijela za akreditaciju u vezi sa sigurnosti (SAA, vidjeti odjeljak 25.3.2.).

SSRS se traži i kada se raspoloživost i cjelovitost podataka RESTREINT UE ili podataka koji nisu klasificirani, prema procjeni Tijela za akreditaciju u vezi sa sigurnosti (SAA), čine kritični.

SSRS se oblikuje u najranijoj fazi uvođenja projekta te se razvija i raste kako se razvija i projekt, ispunjavajući različite uloge u različitim projektnim fazama u cijelom razdoblju djelovanja sustava.

25.1.5. *Sigurnosni načini rada*

Svi sustavi u kojima se obrađuju podaci sa stupnjem klasifikacije CONFIDENTIEL UE i višim smiju djelovati samo na jedan način ili, kada je to odobreno zahtjevima u različitim vremenskim razdobljima, više sljedećih sigurnosnih načina rada ili na njima istovjetan način prema zahtjevima pojedine države:

(a) namjenski

(b) visoke razine sustava

(c) na više razina.

25.2. **Definicije**

„Akreditacija” znači: ovlaštenje i odobrenje koje se daje sustavu za obradu klasificiranih podataka EU-a u svom operativnom okruženju.

Napomena:

Takva se akreditacija daje nakon provedbe svih odgovarajućih sigurnosnih mjera i kada je postignuta dovoljna razina zaštite resursa sustava. Akreditacija se obično daje na temelju SSRS, uključujući sljedeće:

(a) utvrđivanje cilja akreditacije sustava; posebno razine tajnosti podataka koji se obrađuju i predloženi sigurnosni način rada sustava ili mreže;

(b) izrada pregleda upravljanja rizikom radi utvrđivanja vrsta ugroženosti i ranjivosti te odgovarajućih protumjera;

(c) sigurnosni postupci rada, SecOPs (*Security Operating Procedures*) s detaljnim opisom predloženih radnji (npr. načini, službe koje treba predvidjeti) uključujući opis sigurnosnih značajki sustava koje predstavljaju osnovu za akreditaciju;

(d) plan uvođenja i održavanja sigurnosnih značajki;

(e) plan početnog i daljnjih ispitivanja, procjene i ovjeravanja sigurnosti sustava ili mreže; i

(f) ovjeravanje, ako se traži, zajedno s drugim elementima akreditacije.

„Službenik za informacijsku sigurnost na središnjoj razini” (CISO) je službenik u središnjoj IT službi koji radi na usklađivanju i nadgledanju sigurnosnih mjera u centralno organiziranim sustavima.

„Ovjeravanje” znači: izdavanje službene potvrde koja se temelji na neovisnom pregledu izvođenja i rezultata procjene i koja ukazuje do koje mjere sustav zadovoljava sigurnosne zahtjeve ili do koje mjere proizvod za sigurnost računala ispunjava unaprijed određene sigurnosne zahtjeve.

„Sigurnost komunikacija, COMSEC” (*Communication Security*) znači: primjena sigurnosnih mjera na telekomunikacije radi sprečavanja pristupa neovlaštenim osobama do vrijednih podataka koji bi mogli nastati posjedovanjem i proučavanjem takvih telekomunikacija ili radi osiguravanja vjerodostojnosti takvih telekomunikacija.

Napomena:

Te mjere uključuju kriptografsku sigurnost, sigurnost prijenosa i emisije; uključuju i sigurnost postupaka, fizičku sigurnost, sigurnost osoblja te sigurnost dokumenata i računala.

„Sigurnost računala, COMPUSEC” (*Computer Security*) znači: primjena sigurnosnih značajki strojne opreme, sustava programa i programske opreme u računalnom sustavu radi sprečavanja ili zaštite od neovlaštenog razotkrivanja, manipulacije, promjene/brisanja podataka ili odbijanja pružanja usluge.

„Proizvod za sigurnost računala” znači: generički proizvod za sigurnost računala namijenjen uključivanju u IT sustav radi poboljšavanja ili osiguravanja tajnosti, cjelovitosti ili raspoloživosti obrađenih podataka.

„Namjenski sigurnosni način rada” znači: način rada pri kojemu svi pojedinci s pristupom sustavu prolaze provjeru do najvišeg stupnja klasifikacije podataka koji se obrađuju u sustavu i s općom potrebom poznavanja svih podatka unutar sustava.

Napomene:

(1) Opća potreba poznavanja ukazuje da ne postoji obavezan zahtjev za sigurnosne značajke računala koje omogućavaju odvajanje podataka unutar sustava.

(2) Ostale sigurnosne značajke (na primjer fizička sigurnost, sigurnost osoblja i postupaka) moraju zadovoljavati zahtjeve za najviši stupanj klasifikacije i sve kategorije podataka koji se obrađuju unutar sustava.

„Procjena” znači: detaljan tehnički pregled, koji provodi nadležno tijelo, sigurnosnih aspekata sustava ili kriptografskog proizvoda ili proizvoda za sigurnost računala.

Napomene:

(1) Procjenom se provjerava prisutnost tražene sigurnosne učinkovitosti i odsustvo ugrožavajućih popratnih učinaka takve učinkovitosti te se procjenjuje mogućnost utjecanja na tu učinkovitost.

(2) Procjenom se utvrđuje do koje su mjere ispunjeni sigurnosni zahtjevi sustava ili proizvoda za sigurnost računala i određuje razina zaštite sustava ili pouzdanosti kriptografskog proizvoda ili proizvoda za sigurnost računala.

„Imatelj podatka” (IO) je tijelo (voditelj službe) koje je nadležno za stvaranje, obradu i upotrebu podataka, uključujući i odlučivanje o tome kome će se dozvoliti pristup tim podacima.

„Sigurnost podataka” INFOSEC (*Information Security*) znači: primjenu sigurnosnih mjera za zaštitu podataka koji se obrađuju, pohranjuju ili prenose komunikacijskim, informacijskim ili drugim elektroničkim sustavima od namjernog ili slučajnoga gubitka tajnosti, cjelovitosti ili raspoloživosti i za sprečavanje gubitka tajnosti, cjelovitosti ili raspoloživosti samih sustava.

„Mjere INFOSEC” uključuju mjere sigurnosti računala, prijenosa, emisije i kriptografske sigurnosti te otkrivanje, dokumentiranje i otklanjanje opasnosti za podatke i sustave.

„IT područje” znači: područje koje sadrži jedno ili više računala, njihove lokalne ili periferne jedinice za pohranjivanje, kontrolne jedinice i namjensku mrežnu i komunikacijsku opremu.

Napomena:

Ovo ne uključuje zasebno područje u kojemu su smješteni udaljeni periferni uređaji ili terminali/radne stanice, iako su ti uređaji povezani s opremom u IT području.

„IT mreža” znači: geografski raširena organizacija IT sustava, međusobno povezanih za razmjenu podataka, koja sadrži dijelove međusobno povezanih IT sustava i njihovog sučelja s podržavajućim komunikacijskim mrežama ili mrežama podataka.

Napomene:

(1) IT mreža može koristiti usluge jedne ili nekoliko komunikacijskih međusobno povezanih mreža za razmjenu podataka; više IT mreža može koristiti usluge zajedničke komunikacijske mreže.

(2) IT mreža naziva se lokalna ako povezuje nekoliko računala na istome mjestu.

„Sigurnosne značajke IT mreže” uključuju sigurnosne značajke pojedinih IT sustava koji čine mrežu zajedno s onim dodatnim komponentama i značajkama koje su pridružene mreži kao takvoj (na primjer mrežne komunikacije, mehanizmi i postupci sigurnosnog prepoznavanja i označivanja, nadziranje pristupa, programi i kontrola knjiženja), potrebnim radi pružanja prihvatljive razine zaštite klasificiranih podataka.

„IT sustav” znači: skup opreme, metoda i postupaka te, prema potrebi, osoblja organiziranog radi ostvarivanja zadaća u vezi s obradom podataka.

Napomene:

(1) To znači cjelinu uređaja sastavljenih za obradu podataka unutar sustava.

(2) Takvi sustavi mogu služiti kao podrška savjetovanju, vođenju, nadzoru, komunikacijama, znanstvenim ili administrativnim aplikacijama uključujući i one za obradu teksta;

(3) Granice sustava općenito su određene kao dijelovi pod nadzorom jednog imatelja tehničkog sustava.

(4) IT sustav može sadržavati podsustave od kojih su neki i sami IT sustavi.

„Sigurnosne značajke IT sustava" obuhvaćaju sve funkcije, značajke i svojstva strojne opreme/sustava programa/programske opreme; operativne postupke, postupke odgovornosti i kontrole pristupa, IT područje, područje udaljenog terminala/radne stanice i upravljačka ograničenja, fizičku strukturu i uređaje, nadzor osoblja i komunikacija potrebnog radi pružanja prihvatljive razine zaštite klasificiranih podataka koji se obrađuju unutar IT sustava.

„Službenik za informacijsku sigurnost na lokalnoj razini" (LISO) je službenik službe Komisije koji je odgovoran za usklađivanje i nadgledanje sigurnosnih mjera u okviru svog djelokruga rada.

„Sigurnosni način rada na više stupnjeva" znači: način rada kod kojeg svi pojedinci s pristupom sustavu nisu provjereni do najvišeg stupnja klasifikacije podataka koji se u sustavu obrađuju, niti svi pojedinci s pristupom sustavu imaju opću potrebu poznavanja podataka koji se u sustavu obrađuju.

Napomene:

(1) Ovaj način rada trenutačno dopušta rukovanje podacima različitih stupnjeva klasifikacije i obilježja kategorije podatka.

(2) Činjenica da sve osobe nisu prošle provjeru do najvišeg stupnja te nemaju opću potrebu poznavanja ukazuje da postoji zahtjev za sigurnosne značajke računala koje omogućavaju selektivan pristup i razdvajanje podataka unutar sustava.

„Udaljeni terminal/radna stanica" znači: područje koje sadrži računalnu opremu, njezine periferne uređaje ili terminale/radne stanice i svu pripadnu komunikacijsku opremu, odvojenu od IT područja.

„Sigurnosni postupci rada" su postupci koje sastavlja imatelj tehničkih sustava određujući načela koja treba donijeti u vezi sa sigurnosnim mjerama, operativnih postupaka kojih se treba pridržavati i u vezi s odgovornošću osoblja.

„Sigurnosni način rada SYSTEM-HIGH" je način rada kod kojeg su SVI pojedinci s pristupom sustavu provjereni do najvišeg stupnja klasifikacije podataka koji se u sustavu obrađuju, ali opća potreba poznavanja podataka ne vrijedi za SVE pojedince s pristupom sustavu.

Napomene:

(1) Nedostatak opće potrebe poznavanja ukazuje da postoji zahtjev za sigurnosne značajke računala koje pružaju mogućnost selektivnog pristupa podacima unutar sustava te njihovo razdvajanje.

(2) Ostale sigurnosne značajke (na primjer fizička sigurnost, sigurnost osoblja i postupaka) usklađuju se sa zahtjevima najvišeg stupnja klasifikacije i svih obilježja kategorija podataka obrađenih unutar sustava.

(3) Svi podaci koji se obrađuju ili su dostupni u sustavu u tom načinu rada, kao i izlazni podaci koji u njemu nastaju, zaštićuju se kao da pripadaju obilježju kategorije i najvišem stupnju klasifikacije podataka u sustavu, sve dok se ne utvrdi drugačije, osim ako za svaku postojeću vrstu obilježavanja ne postoji prihvatljiva razina pouzdanosti.

„Određenje sigurnosnih zahtjeva koji su specifični za sustav" (SSRS) je potpuna i izričita izjava o sigurnosnim načelima koja se moraju uzeti u obzir i detaljnim sigurnosnim zahtjevima koje treba ispuniti. Zasniva se na sigurnosnoj politici Komisije i procjeni rizika ili, ako to nalažu parametri radnog okruženja, na najnižem stupnju sigurnosne provjere osoblja, najvišem stupnju klasifikacije obrađenih podataka, sigurnosnom načinu rada ili zahtjevima korisnika. SSRS je sastavni dio dokumentacije projekta dostavljene odgovarajućim tijelima u svrhu tehničkog, proračunskog i sigurnosnog odobrenja. U konačnom obliku, SSRS predstavlja potpuno određenje sigurnog sustava.

„Imatelj tehničkih sustava" (TSO) je služba koja je nadležna za stvaranje, održavanje, rad i prestanak rada sustava.

Protumjere „Tempest" su: sigurnosne mjere namijenjene zaštiti opreme i komunikacijske infrastrukture od ugrožavanja klasificiranih podataka uslijed slučajnih elektromagnetskih emisija i provodljivosti.

25.3. **Nadležnosti u području sigurnosti**

25.3.1. *Općenito*

U nadležnosti savjetodavne skupine za sigurnosnu politiku Komisije, određene u odjeljku 12., su i pitanja INFOSEC-a. Ova skupina organizira svoje djelovanje tako da može pružiti savjet stručnjaka o gore navedenim pitanjima.

Sigurnosni ured Komisije nadležan je za donošenje detaljnih propisa o INFOSEC-u na temelju odredaba ovog poglavlja.

U slučaju problema u vezi sa sigurnosti (incidenti, kršenja, itd.) Sigurnosni ured Komisije poduzima mjere.

Sigurnosni ured Komisije u svom sastavu ima jedinicu INFOSEC.

25.3.2. *Tijelo za akreditaciju sigurnosti (SAA)*

Čelnik Sigurnosnog ureda Komisije vodi Tijelo za akreditaciju sigurnosti (SAA) za Komisiju. SAA je nadležna za područje opće sigurnosti kao i za specijalizirana područja INFOSEC-a, sigurnosti komunikacija, crypto sigurnosti i Tempest sigurnosti.

Služba za akreditaciju sigurnosti je nadležna za osiguravanje usklađenosti sustava sa sigurnosnom politikom Komisije. Jedna od njezinih zadaća je izdavanje odobrenja sustavu za obradu klasificiranih podataka EU-a do određenog stupnja klasifikacije, u svojem operativnom okružju.

U nadležnosti SAA Komisije su svi radni sustavi u okviru prostora Komisije. Kada različiti dijelovi sustava dolaze pod nadležnost SAA-a Komisije i drugih tijela SAA-a, sve zainteresirane stranke imenuju zajednički odbor za akreditaciju pod vodstvom SAA-a Komisije.

25.3.3. *Tijelo INFOSEC (IA)*

Voditelj jedinice INFOSEC pri Sigurnosnom uredu Komisije vodi tijelo INFOSEC za Komisiju. Tijelo INFOSEC je nadležno za:

— tehničko savjetovanje i pomoć tijelima za akreditaciju sigurnosti (SAA);

— pomoć u razvijanju SSRS;

— pregled SSRS radi osiguravanja usklađenosti s ovim sigurnosnim propisima i dokumentima o politici i strukturi INFOSEC-a.

— sudjelovanje, kako se traži, u komisijama/odborima za akreditaciju i pribavljanje INFOSEC preporuke za akreditaciju SAA-u;

— pružanje podrške aktivnostima osposobljavanja i obrazovanja INFOSEC;

— tehničko savjetovanje pri istragama incidenata u vezi s INFOSEC-om;

— pripremu tehničko-strateških smjernica kako bi se osigurala upotreba isključivo odobrene programske opreme.

25.3.4. *Imatelj tehničkih sustava (TSO)*

Za primjenu i djelovanje nadzora i posebnih sigurnosnih značajki sustava je nadležan imatelj dotičnog sustava koji se naziva imatelj tehničkih sustava (TSO). Za centralne sustave imenuje se službenik za informacijsku sigurnost na središnjoj razini, CISO. Svaka služba, prema potrebi, imenuje službenika za informacijsku sigurnost na lokalnoj razini (LISO). U nadležnosti TSO je izrada sigurnosnih postupaka rada (SecOPs); što vrijedi kroz čitav životni vijek sustava, od faze idejnog projekta do konačnog prestanka rada sustava.

TSO određuje sigurnosne standarde i postupke koje dobavljač sustava treba poštivati.

TSO može, ako je potrebno, prenijeti dio svojih nadležnosti na službenika za informacijsku sigurnost na lokalnoj razini. Jedna osoba može obavljati različite funkcije INFOSEC-a.

25.3.5. *Imatelj podataka (IO)*

Imatelj podataka (IO) je odgovoran za klasificirane podatke EU-a (i ostale podatke) koje treba unijeti, obraditi i izraditi u tehničkim sustavima. On utvrđuje zahtjeve za pristup ovim podacima u sustavima. Svoju odgovornost imatelj podataka može dijelom prenijeti na upravitelja podataka ili upravitelja baze podataka, unutar svog djelokruga.

25.3.6. *Korisnici*

Svi korisnici su odgovorni za svoje postupke koji ne smiju nepovoljno utjecati na sigurnost sustava kojeg koriste.

25.3.7. *Osposobljavanje INFOSEC*

Izobrazba i osposobljavanje INFOSEC su na raspolaganju cjelokupnom osoblju koje ga treba.

25.4. **Netehničke mjere sigurnosti**

25.4.1. *Sigurnost osoblja*

Korisnici sustava obavljaju sigurnosnu provjeru i moraju imati „potrebu poznavanja" odgovarajućeg stupnja klasifikacije i sadržaja podataka koji se obrađuju unutar pojedinog sustava. Za pristup određenoj opremi ili podacima specifičnim za sigurnost sustava potrebna je posebna potvrda o sigurnosnoj provjeri izdana u skladu s propisanim postupkom Komisije.

SAA određuje sva osjetljiva mjesta i utvrđuje stupanj provjere i nadzora koji se zahtijeva za sve osoblje na tim mjestima.

Sustavi se određuju i projektiraju tako da se olakša raspodjela dužnosti i odgovornosti između osoblja, kako bi se spriječilo da samo jedna osoba bude u potpunosti upoznata s temeljnim sigurnosnim točkama sustava i ima potpuni nadzor nad njima.

IT područja i područja udaljenih terminala/radnih stanica na kojima je moguće izmijeniti sigurnost sustava ne smije zauzimati samo jedan ovlašteni dužnosnik ili drugi zaposlenik.

Sigurnosne postavke sustava mijenjaju najmanje dvije ovlaštene osobe koje u tome zajednički sudjeluju.

25.4.2. *Fizička sigurnost*

IT područja i područja udaljenih terminala/radnih stanica (kako je određeno u odjeljku 25.2.) na kojima se uz pomoć sredstava informacijske tehnologije obrađuju podaci stupnja klasifikacije CONFIDENTIEL UE i viši, ili na kojima postoji mogućnost pristupa takvim podacima, uspostavljaju se kao sigurnosna područja EU-a I. i II. razreda, ovisno o potrebama.

25.4.3. *Nadzor pristupa sustavu*

Svi podaci i materijali koji omogućavaju nadzor pristupanja sustavu zaštićuju se na način koji odgovara najvišem stupnju klasifikacije i obilježju kategorije podataka do kojih se može pristupiti.

Kada se više ne koriste u ove svrhe, podaci i materijali za nadzor pristupanja uništavaju se u skladu s odredbama iz odjeljka 25.5.4.

25.5. **Tehničke mjere sigurnosti**

25.5.1. *Sigurnost podataka*

Dužnost je izvora od kojeg podaci potječu prepoznati i razvrstati po tajnosti sve dokumente u kojima se nalaze podaci, bilo da su u obliku papirnate preslike ili računalnog medija za pohranjivanje. Svaka stranica papirnate preslike označava se, na vrhu i na dnu, oznakom tajnosti. Izlazni podaci, bilo da su preslike u papirnatom obliku ili u obliku računalnog medija za pohranjivanje, imaju isti stupanj klasifikacije kao i najviši stupanj klasifikacije ulaznih podataka. Način rada sustava također može utjecati na razvrstavanje po tajnosti izlaznih podataka tog sustava.

Dužnost službi Komisije i njihovih posjednika podataka je razmotriti probleme koji se javljaju grupiranjem pojedinačnih elemenata podataka i međudjelovanje koje može nastati među srodnim elementima te odrediti je li potreban viši stupanj klasifikacije podataka kao cjeline.

Činjenica da podaci mogu biti u obliku skraćenog koda, koda prijenosa ili u bilo kojem obliku binarnog prikaza ne predstavlja nikakvu sigurnosnu zaštitu i kao takva ne smije utjecati na razvrstavanje stupnja klasifikacije podataka.

Kada se podaci prenose iz jednog sustava u drugi zaštićuju se tijekom prijenosa i u prijemnom sustavu sukladno originalnom stupnju klasifikacije i kategoriji podataka.

Svi računalni mediji za pohranjivanje podataka moraju biti u skladu s najvišim stupnjem klasifikacije pohranjenih podataka ili oznakom medija; ti mediji moraju u svakom trenutku biti na odgovarajući način zaštićeni.

Računalni mediji za pohranjivanje namijenjeni višekratnoj upotrebi koji se koriste za spremanje klasificiranih podataka EU-a zadržavaju najviši stupanj klasifikacije za koji su ikada bili upotrijebljeni, sve dok se tim podacima na odgovarajući način ne snizi ili ne ukine stupanj klasifikacije i medij se ponovno razvrsta po tajnosti ili se njegov stupanj klasifikacije ukine, ili se medij uništi u skladu s postupkom odobrenim od SAA (vidjeti 25.5.4.)

25.5.2. *Nadzor i uknjižba podataka*

Evidencija pristupa klasificiranim podacima sa stupnjem SECRET UE i višim vodi se automatski ili ručno upisom u upisnik. Ti se zapisi čuvaju u skladu s ovim pravilnikom.

Izlazni ispisi klasificiranih podataka EU-a koji se čuvaju unutar IT područja mogu se smatrati kao zaseban klasificirani materijal i ne moraju se upisati u upisnik pod uvjetom da se materijal na primjereni način razvrsta, označi pripadnim stupnjem klasifikacije i drži pod nadzorom.

Kada izlazni ispisi dolaze iz sustava u kojem se obrađuju klasificirani podaci EU-a i prenose se iz IT područja na područje udaljenog terminala/radnih stanica treba, u dogovoru sa SAA, utvrditi postupke za kontrolu i registraciju izdanih podataka. Za podatke sa stupnjem SECRET UE i višim ti postupci uključuju posebne upute za uknjižívanje podataka.

25.5.3. *Postupanje i nadzor nad pokretnim računalnim medijima za pohranjivanje*

Sa svim računalnim medijima za pohranu podataka sa stupnjem klasifikacije CONFIDENTIEL UE i višim postupa se kao s klasificiranim materijalom i primjenjuju se opća pravila. Identifikacijske oznake i oznake razvrstavanja po tajnosti prilagođavaju se specifičnom fizičkom izgledu medija, kako bi se omogućila njihova jasna prepoznatljivost.

Korisnici su dužni osigurati da su klasificirani podaci EU-a pohranjeni na mediju s odgovarajućom zaštitom i oznakom stupnja klasifikacije. Treba utvrditi postupke za spremanje podataka EU-a svih razina na računalnim medijima za pohranjivanje, u skladu s ovim pravilnikom.

25.5.4. *Ukidanje stupnja klasifikacije i uništavanje računalnih medija za pohranjivanje*

Računalnim medijima za pohranjivanje koji se koriste za bilježenje klasificiranih podataka EU-a može se sniziti ili ukinuti stupanj klasifikacije u skladu s postupkom koji odobrava SAA.

Računalnim medijima za pohranjivanje na kojima su se čuvali podaci TRÈS SECRET UE ili podaci posebne kategorije ne može se ukinuti stupanj klasifikacije niti ih se može ponovno upotrebljavati.

Ako se računalnim medijima za pohranjivanje ne može ukinuti stupanj klasifikacije ili se ne mogu ponovno upotrebljavati u skladu s gore spomenutim postupkom, uništava ih se.

25.5.5. *Sigurnost komunikacija*

Čelnik Ureda Komisije je nadležan za Crypto.

Kada se klasificirani podaci EU-a prenose elektromagnetskim putem, primjenjuju se posebne mjere za zaštitu tajnosti, cjelovitosti i raspoloživosti takvih prijenosa. SAA određuje zahtjeve za zaštitu prijenosa od otkrivanja i prekida. Podaci koji se prenose u komunikacijskom sustavu zaštićuju se na temelju zahtjeva za povjerljivost, cjelovitost i raspoloživost.

Kada se, radi omogućavanja tajnosti, cjelovitosti i raspoloživosti, zahtijevaju kriptografske metode te metode i s njima povezane proizvode, posebno za tu namjenu, odobrava SAA u ulozi službe Crypto.

Tijekom prijenosa podataka SECRET UE i višim, njihova se tajnost štiti kriptografskim metodama ili proizvodima koje odobrava član Komisije odgovoran za sigurnosna pitanja, nakon savjetovanja sa savjetodavnom skupinom Komisije za sigurnosnu politiku. Tijekom prijenosa klasificiranih podataka sa stupnjem CONFIDENTIEL UE ili RESTREINT UE, njihova se tajnost štiti kriptografskim metodama ili proizvodima odobrenim od tijela Crypto pri Komisiji, nakon savjetovanja sa savjetodavnom skupinom Komisije za sigurnosnu politiku.

Detaljna pravila prijenosa klasificiranih podataka EU-a određuju se u posebnim sigurnosnim uputama koje odobrava Sigurnosni ured Komisije, nakon savjetovanja sa savjetodavnom skupinom Komisije za sigurnosnu politiku.

Pod izuzetnim radnim okolnostima, podaci sa stupnjem klasifikacije RESTREINT UE, CONFIDENTIEL UE i SECRET UE mogu se prenositi kao čitljivi tekst, pod uvjetom da svaki od takvih slučajeva izričito odobri i propisno registrira imatelj podataka. Takve izuzetne okolnosti su sljedeće:

(a) za vrijeme prijetećih ili stvarnih kriznih situacija, sukoba ili rata, i

(b) kada je brzina isporuke od iznimne važnosti, a sredstva za kodiranje nisu na raspolaganju i procijenjeno je da prenošenje podataka nije moguće pravovremeno iskoristiti za negativan utjecaj na tijek operacija.

Sustav mora biti sposoban onemogućiti pristup do klasificiranih podataka EU-a u bilo kojoj ili u svim dislociranim radnim stanicama ili terminalima, koji se, ako je potrebno, isključuju na fizički način ili uz pomoć posebnih rješenja programske opreme odobrenih od SAA.

25.5.6. *Sigurnosne mjere u vezi s postavljanjem i zračenjem*

Početno postavljanje sustava i svaka njihova značajna izmjena izvodi se tako da postavljanje provode radnici sa sigurnosnom provjerom, pod stalnim nadzorom tehnički kvalificiranog osoblja sa sigurnosnom provjerom za pristup klasificiranim podacima EU-a do stupnja koji odgovara najvišem stupnju klasifikacije podataka što će se, prema očekivanju, u sustavu pohranjivati i obrađivati.

Sustavi u kojima se obrađuju podaci s stupnjem klasifikacije CONFIDENTIEL UE i višim, zaštićuju se tako da njihovu sigurnost ne može ugroziti nepoželjno zračenje i/ili provodljivost; proučavanje i nadzor ovih pojava naziva se „Tempest".

Protumjere Tempest pregledava i odobrava tijelo Tempest (vidjeti 25.3.2.).

25.6. **Sigurnost pri rukovanju**

25.6.1. *Sigurnosni postupci rada (SecOPs)*

Sigurnosni postupci rada (SecOPs) određuju načela koja treba donijeti o sigurnosnim pitanjima, operativne postupke koje treba poštivati kao i odgovornosti osoblja. Pripremanje sigurnosnih postupaka rada u nadležnosti je imatelja tehničkih sustava (TSO).

25.6.2. *Zaštita programske opreme/upravljanje konfiguracijama*

Sigurnosna zaštita programskih aplikacija određuje se na temelju procjene stupnja sigurnosti samog programa, a ne na temelju tajnosti podataka koji će se obrađivati. Korištene programske verzije redovno se provjeravaju kako bi se osigurala njihova cjelovitost i ispravno funkcioniranje.

Nove ili izmijenjene verzije programske opreme ne koriste se za rukovanje klasificiranim podacima EU-a dok ih ne provjeri TSO.

25.6.3. *Provjeravanje prisutnosti štetne programske opreme/računalnih virusa*

Provjeravanje prisutnosti štetne programske opreme/računalnih virusa provodi se redovito u skladu sa zahtjevima SAA.

Prije njihova uvođenja u bilo koji sustav, svi se računalni mediji za pohranjivanje koji pristižu u Komisiju provjeravaju radi otkrivanja eventualne prisutnosti bilo koje štetne programske opreme ili računalnog virusa.

25.6.4. *Održavanje*

Ugovori i postupci za redovno održavanje sustava, kao i održavanje prema pozivu, za koji postoji SSRS, određuju zahtjeve i rješenja s osobljem zaduženim za održavanje i njima pripadajuće opreme koji ulaze na područje IT.

Zahtjevi se jasno navode u SSRS, a postupci u SecOPs. Ugovorno održavanje koje zahtijeva dijagnostičke postupke s udaljenim pristupom, dozvoljava se samo u iznimnim okolnostima, pod strogim sigurnosnim nadzorom, i samo uz odobrenje SAA.

25.7. **Nabava**

25.7.1. *Općenito*

Svaki sigurnosni proizvod koji se nabavlja za upotrebu u sustavu mora biti procijenjen i ovjeren ili mora biti u postupku procjene i ovjeravanja kod odgovarajućeg tijela za procjenu ili ovjeravanje jedne od država članica EU-a, prema međunarodno priznatim mjerilima (kao što su Zajednička mjerila za procjenu sigurnosti informacijske tehnologije, vidjeti ISO 15408). U posebnom postupku treba dobiti odobrenje od Savjetodavnog odbora za nabavu i ugovaranje (*ACPC, Advisory Committee on Procurement and Contracts*).

Kod odlučivanja o tome treba li opremu unajmiti ili kupiti, posebno računalne medije za pohranjivanje, treba imati na umu da takva oprema nakon što se upotrebljavala za obradu klasificiranih podataka EU-a ne može biti odnijeta izvan prikladno osiguranog područja bez prethodnog ukidanja stupnja klasifikacije uz odobrenje SAA, imajući u vidu da to odobrenje nije uvijek moguće.

25.7.2. *Akreditacija*

Sve sustave za koje, prije rukovanja klasificiranim podacima EU-a, treba sastaviti SSRS, akreditira SAA na temelju podataka danih u SSRS, SecOPs i drugim odgovarajućim dokumentima. Podsustavi i udaljeni terminali/radne stanice akreditiraju se kao dijelovi svih sustava s kojima su povezani. Kada sustav služi i Komisiji i drugim organizacijama, akreditaciju zajednički dogovaraju Komisija i odgovarajuća sigurnosna tijela.

Postupak akreditacije može se provoditi sukladno strategiji akreditiranja, primjerenoj pojedinom sustavu, koju određuje SAA.

25.7.3. *Procjena i ovjeravanje*

Prije akreditiranja se, u nekim slučajevima, sigurnosne značajke strojne opreme, sustavnih programa i programske opreme procjenjuju i ovjeravaju vezano za sposobnost sigurnog čuvanja podataka željenog stupnja klasifikacije.

Zahtjevi za procjenu i ovjeravanje uključuju se u planiranje sustava i jasno navode u SSRS.

Postupak procjene i ovjeravanja, sukladno odobrenim smjernicama, provodi tehnički kvalificirano i na odgovarajući način provjereno osoblje koje djeluje u ime TSO.

Stručni timovi se mogu sastaviti iz imenovanog tijela države članice za procjenu i ovjeravanje ili po njemu imenovanih predstavnika, kao što je na primjer ovlašteni i provjereni ugovorni partner.

Postupci procjene i ovjeravanja mogu se skratiti (na primjer tako da uključuje samo vidike integracije) kada se sustavi temelje na postojećim, na nacionalnoj razini procijenjenim i ovjerenim proizvodima za sigurnost računala.

25.7.4. *Rutinske provjere sigurnosnih značajki za produženje akreditacije*

TSO uspostavlja rutinske postupke nadzora kojima se provjerava valjanost svih sigurnosnih značajki sustava.

Izmjene koje bi dovele do ponovne akreditacije ili koje zahtijevaju prethodno odobrenje od SAA, jasno se utvrđuju i navode u SSRS. Nakon svake promjene, popravka ili kvara koji su mogli utjecati na sigurnosne značajke sustava, TSO mora osigurati provjeru ispravnosti rada sigurnosnih značajki. Produženje akreditacije sustava obično ovisi o pozitivnoj procjeni pregleda.

Sve sustave koji imaju sigurnosne značajke redovito pregledava i provjerava SAA. Pregledi sustava u kojima se rukuje podacima TRÈS SECRET UE izvode se najmanje jednom godišnje.

25.8. **Privremena ili povremena upotreba**

25.8.1. *Sigurnost mikroračunala/osobnih računala*

Mikroračunala/osobna računala PC (*PCs, Personal Computers*) s ugrađenim diskovima (ili drugim oblikom medija za trajno pohranjivanje) koja rade samostalno ili u mrežnoj konfiguraciji i prijenosni računalni uređaji (na primjer prijenosni PC i elektronički „*notebook*") s ugrađenim čvrstim diskovima, smatraju se medijima za pohranjivanje jednako kao i diskete ili druge vrste pokretnih računalnih medija za pohranjivanje.

Toj se opremi dodjeljuje stupanj zaštite u smislu pristupa, rukovanja, pohranjivanja i prijenosa koji odgovara najvišem stupnju klasifikacije podataka ikad pohranjenih ili obrađivanih (do snižavanja ili ukidanja stupnja klasifikacije u skladu s odobrenim postupcima).

25.8.2. *Upotreba privatne IT opreme u službene svrhe za poslove Komisije*

Upotreba privatnih pokretnih računalnih medija za pohranjivanje, programske i strojne opreme IT (na primjer PC i pokretni računalni uređaji) s mogućnošću pohranjivanja, nije dozvoljena za obradu klasificiranih podataka EU-a.

Strojna oprema, programska oprema i mediji za pohranjivanje u privatnom vlasništvu ne smiju se, bez pismenog ovlaštenja čelnika Sigurnosnog ureda Komisije, unositi na područje I. ili II. razreda na kojem se rukuje klasificiranim podacima EU-a. To se ovlaštenje može izdati samo iz tehničkih razloga i u izvanrednim slučajevima.

25.8.3. *Upotreba unajmljene IT opreme ili one koju dobavljaju države u službene svrhe za poslove Komisije*

Upotrebu unajmljene IT opreme i programske opreme, u organizacijama podrške službenim poslovima Komisije, može dozvoliti čelnik Sigurnosnog ureda Komisije. Također, može se dozvoliti upotreba IT opreme i programske opreme koju dobavljaju države; u tom se slučaju IT oprema uvrštava pod nadzor odgovarajućeg inventarskog popisa Komisije. U oba se slučaja, ako se IT oprema koristi za obradu klasificiranih podataka EU-a, treba savjetovati sa SAA kako bi se elementi INFOSEC-a, primjenjivi za tu vrstu opreme pravilno razmotrili i proveli.

26. DAVANJE KLASIFICIRANIH PODATAKA EU-a TREĆIM ZEMLJAMA ILI MEĐUNARODNIM ORGANIZACIJAMA

26.1.1. *Načela u vezi s davanjima klasificiranih podataka EU-a*

Komisija kao kolegij odlučuje o davanju klasificiranih podataka EU-a trećim zemljama ili međunarodnim organizacijama na temelju:

— prirode i sadržaja takvih podataka;

— primateljeve potrebe poznavanja;

— prednosti za EU.

Od izvora od kojeg potječu klasificirani podaci EU-a koji se namjeravaju dati zatražit će se suglasnost.

Ovakve odluke donose se od slučaja do slučaja, ovisno o:

— željenom stupnju suradnje s trećim zemljama ili određenim međunarodnim organizacijama;

— povjerenju koje im se može pripisati, što proizlazi iz razine sigurnosti koju bi za povjerene im klasificirane podatke EU-a primijenile te države ili organizacije, kao i o usklađenosti sigurnosnih propisa koji se u njima primjenjuju s onima EU-a. Savjetodavna skupina za sigurnosnu politiku Komisije iznosi svoje mišljenje o ovom pitanju Komisiji.

Prihvaćanje klasificiranih podataka EU-a u trećim zemljama ili međunarodnim organizacijama podrazumijeva da se podaci neće koristiti ni u koje druge svrhe osim onih zbog kojih je do davanja ili razmjene podataka došlo te da će im se pružiti zaštita kakvu zahtijeva Komisija.

26.1.2. *Razine*

Jednom kada se donese odluka za davanje ili razmjenu klasificiranih podataka s određenom državom ili međunarodnom organizacijom, Komisija određuje moguću razinu suradnje. To naročito ovisi o sigurnosnoj politici i važećim propisima u toj državi ili organizaciji.

Postoje tri razine suradnje:

Razina 1

Suradnja s trećim zemljama ili međunarodnim organizacijama čija su sigurnosna politika i propisi vrlo bliski onima EU-a.

Razina 2

Suradnja s trećim zemljama ili međunarodnim organizacijama čija se sigurnosna politika i propisi znatno razlikuju od onih u EU.

Razina 3

Povremena suradnja s trećim zemljama ili međunarodnim organizacijama čiju politiku i propise nije moguće procijeniti.

Za svaku od razina suradnje određeni su postupci i sigurnosne odredbe, detaljno navedeni u Dodacima 3., 4. i 5.

26.1.3. *Sigurnosni sporazumi*

Kad Komisija odluči da postoji trajna ili dugoročna potreba za razmjenom klasificiranih podataka između Komisije i trećih zemalja ili drugih međunarodnih organizacija, izrađuju se „sporazumi o sigurnosnim postupcima razmjene klasificiranih podataka" u kojima se utvrđuje svrha suradnje kao i uzajamna pravila o zaštiti razmijenjenih podataka.

U slučaju povremene suradnje razine 3, koja je po određenju ograničena vremenom i svrhom, može se umjesto „sporazuma o sigurnosnim postupcima razmjene klasificiranih podataka" izraditi jednostavni memorandum o suglasnosti kojim se utvrđuje priroda klasificiranih podataka koji se razmjenjuju i uzajamne obaveze u vezi s tim podacima, pod uvjetom da njihov stupanj klasifikacije nije viši od RESTREINT UE.

Savjetodavna skupina za sigurnosnu politiku Komisije razmatra nacrte sporazuma o sigurnosnim postupcima ili memoranduma razumijevanja prije njihovog predstavljanja Komisiji radi odlučivanja.

Član Komisije odgovoran za sigurnosna pitanja zahtijeva svu potrebnu pomoć od tijela nacionalne sigurnosti države članice kako bi se osigurala upotreba i zaštita podataka koji se daju u skladu s odredbama sporazuma o sigurnosnim postupcima ili memoranduma o razumijevanju.

Dodatak 1.

USPOREDBA STUPNJEVA KLASIFIKACIJE NACIONALNE SIGURNOSTI

Stupanj tajnosti EU-a	EU TOP SECRET	EU SECRET	EU CONFIDENTIAL	EU RESTRICTED
Stupanj klasifikacije NATO-a (1)				
Stupnjevi klasifikacije WEU-a	Focal Top Secret	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Stupnjevi klasifikacije EURATOMA (2)	EURATOM Top Secret	EURATOM SECRET	EURATOM Confidential	EURATOM Restricted
Belgija	Tres Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Danska	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Njemačka	STRENG GEHEIM	GEHEIM	VS (3) -VERTRAULICH	VS-NUR FUR DEN DIENSTGEBRAUCH
Grčka	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Španjolska	Secreto	Reservado	Confidencial	Difusion limitada
Francuska	Tres Secret Defense (4)	Secret Defense	Confidentiel Defense	Diffusion restreinte
Irska	Top Secret	Secret	Confidential	Restricted
Italija	Segretissimo	Segreto	Riservatissimo	Riservato
Luksemburg	Tres Secret	Secret	Confidentiel	Diffusion restreinte
Nizozemska	Stg. Zeer Geheim	Stg. Geheim	Stg. Confidentieel	
Austrija	Streng Geheim	Geheim	Vertraulich	Eingeschrankt
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Finska	Erittain salainen	Erittain salainen	Salainen	Luottamuksellinen
Švedska	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Ujedinjena Kraljevina	Top secret	Secret	Confidential	Restricted

(1) NATO – usklađenost sa stupnjevima tajnosti NATO-a utvrdit će se kad se bude pregovaralo o sigurnosnom sporazumu između Komisije i NATO-a.
(2) Uredba Euratoma br. 3 od 31. srpnja 1958. o zaštiti tajnih podataka Euratoma.
(3) Njemačka: VS = Verschlusssache.
(3) Francuska: stupanj tajnosti „Tres Secret Defense", koji pokriva prioritetna pitanja vlade, može se mijenjati samo uz ovlaštenje predsjednika vlade.

Dodatak 2.

PRAKTIČNE UPUTE ZA STUPNJEVE KLASIFIKACIJE

Ove upute su opisne i ne može ih se tumačiti kao mijenjanje osnovnih odredaba utvrđenih u odjeljcima 16., 17., 20. i 21.

Stupanj klasifikacije	Kada	Tko	Postavljanje	Snižavanje/ukidanje/uništavanje	
				Tko	Kada
TRÈS SECRET UE Ovaj se stupanj klasifikacije dodjeljuje samo podacima i materijalima čije bi neovlašteno razotkrivanje moglo prouzročiti iznimno štetne posljedice za temeljne interese Europske unije ili jedne ili više njezinih država članica (16.1.).	Ugrožavanje materi-jala TRÈS SECRET UE moglo bi: — izravno ugroziti unutarnju stabilnost EU-a ili jedne od njezinih država članica ili prijateljskih država — prouzročiti iznimno veliku štetu odnosima s prijateljskim vladama — izravno dovesti do gubitka velikog broja života — nanijeti iznimno veliku štetu operativnoj učinkovitosti ili sigurnosti oružanih snaga država članica ili drugih sudionika, ili trajnoj učinkovitosti izuzetno vrijednih sigurnosnih ili obavještajnih operacija — prouzročiti ozbiljnu dugoročnu štetu gospodarstvu Europske unije ili država članica.	Propisno ovlaštene osobe (izvor od kojeg podaci potječu), ravnatelji, voditelji službi (17.1.) Izvor od kojeg podaci potječu navodi datum, razdoblje ili događaj nakon kojega se sadržaju može sniziti ili ukinuti stupanj klasifikacije. (16.2.) U suprotnom, dokumenti se pregledavaju najmanje svakih pet godina kako bi se potvrdila potreba izvornog stupnja klasifikacije (17.3.).	Stupanj klasifikacije TRÈS SECRET UE i, ako se primjenjuje, sigurnosno obilježje i/ili obrambena oznaka – ESDP, postavlja se na dokumente sa stupnjem klasifikacije TRÈS SECRET UE mehaničkim sredstvima ili ručno (16.4., 16.5., 16.3.). Stupnjevi klasifikacije EU-a i sigurnosna obilježja pojavljuju se na vrhu i dnu svake stranice, na sredini, i svaka je stranica numerirana. Svaki dokument nosi referentni broj i datum; ovaj se referentni broj javlja na svakoj stranici. Ako se materijal šalje u više preslika, svaka preslika dobiva svoj broj koji se pojavljuje na prvoj stranici, zajedno s ukupnim brojem stranica. Svi se dodaci i prilozi nabrajaju na prvoj stranici (21.1.).	Odluka o snižavanju ili ukidanju stupnja klasifikacije isključivo je na izvoru od kojeg podaci potječu koji o promjeni obavještava sve daljnje naslovnike kojima je dokument dostavio, odnosno preslikao (17.3.). Dokumente sa stupnjem klasifikacije TRÈS SECRET UE uništava središnji registarski ured ili podregistarski ured odgovoran za njih. Svaki uništeni dokument navodi se u potvrdi o uništenju koju potpisuje nadzorni službenik TRÈS SECRET UE i službenik koji je svjedočio uništenju i provjeren je prema kriteriju TRÈS SECRET UE. O ovome se u knjigu bilježaka unosi napomena. Registar u razdoblju od deset godina čuva potvrde o uništenju, zajedno s distribucijskim listama (22.5.).	Prekobrojne preslike kao i dokumenti koji više nisu potrebni uništavaju se (22.5.). Dokumenti sa stupnjem klasifikacije TRÈS SECRET UE uključujući sav otpadni materijal koji je nastao tijekom njihovog pripremanja kao što su oštećene preslike, radne preslike, tipkane bilješke i preslike na papiru uništavaju se uz prisutnost nadzornog službenika TRÈS SECRET UE spaljivanjem, mljevenjem, trganjem ili na drugi način usitnjavanjem u neraspoznatljiv i neobnovljiv oblik (22.5.).

Stupanj klasifikacije	Kada	Tko	Postavljanje	Snižavanje/ukidanje/uništavanje	
				Tko	Kada
SECRET UE: Ovaj se stupanj klasifikacije dodjeljuje samo podacima i materijalima čije bi neovlašteno razotkrivanje moglo ozbiljno štetiti temeljnim interesima Europske unije ili jedne ili više njezinih država članica (16.1.).	Ugrožavanje materijala sa stupnjem klasifikacije SECRET UE moglo bi: — podići napetost u međunarodnim odnosima — ozbiljno naškoditi odnosima s prijateljskim vladama — neposredno ugroziti živote ili ozbiljno zaprijetiti javnom redu ili osobnoj sigurnosti i slobodi pojedinaca — nanijeti iznimno veliku štetu operativnoj učinkovitosti ili sigurnosti oružanih snaga država članica ili drugih sudionika, ili trajnoj učinkovitosti izuzetno vrijednih sigurnosnih ili obavještajnih operacija — prouzročiti ozbiljnu materijalnu štetu financijskim, monetarnim, gospodarskim i komercijalnim interesima Europske unije ili neke od njezinih država članica.	Ovlaštene osobe (izvor od kojeg podaci potječu), ravnatelji, voditelji službi (17.1.) Izvori od kojih podaci potječu navode datum nakon kojega se sadržajima može sniziti ili ukinuti stupanj klasifikacije. (16.2.) U suprotnom, dokumenti se pregledavaju najmanje svakih pet godina kako bi se potvrdila potreba izvornog stupnja klasifikacije (17.3.).	Stupanj klasifikacije SECRET UE i, ako se primjenjuju, sigurnosno obilježje i/ili obrambena oznaka – ESDP postavlja se na dokumente SECRET UE mehaničkim sredstvima ili ručno (16.4., 16.5., 16.3.). Stupnjevi klasifikacije EU-a i sigurnosna obilježja pojavljuju se na vrhu i dnu svake stranice, na sredini i svaka je stranica numerirana. Svaki dokument nosi referentni broj i datum; ovaj se referentni broj javlja na svakoj stranici. Ako se materijal šalje u više preslika, svaka preslika dobiva svoj broj koji se pojavljuje na prvoj stranici, zajedno s ukupnim brojem stranica. Svi se dodaci i prilozi nabrajaju na prvoj stranici (21.1.).	Odluka o snižavanju ili ukidanju stupnja klasifikacije isključivo je na onome od koga podaci potječu, koji o promjeni obavještava sve sljedeće naslovnike kojima je dokument dostavio, odnosno preslikao (17.3.). Dokumente sa stupnjem klasifikacije SECRET UE uništava registar odgovoran za njih, pod nadzorom osobe sa sigurnosnom provjerom. Uništeni dokumenti SECRET UE navode se u potpisanoj potvrdi o uništenju koja se u registru čuva u razdoblju od najmanje tri godine, zajedno s obrascem uništenja (22.5.).	Prekobrojne preslike kao i dokumenti koji više nisu potrebni uništavaju se (22.5.). Dokumenti sa sta-tusom SECRET UE uključujući sav otpadni materijal koji je nastao tijekom njihovog pripremanja kao što su oštećene preslike, radne preslike, tipkane bilješke i papire preslika uništavaju se spaljivanjem, mljevenjem, trganjem ili na drugi način usitnjavanjem u neraspoznatljiv i neobnovljiv oblik (22.5.).

Stupanj klasifikacije	Kada	Tko	Postavljanje	Snižavanje/ukidanje/uništavanje	
				Tko	Kada
CONFIDENTIEL UE: Ovaj se stupanj klasifikacije dodjeljuje podacima i materijalima čije bi neovlašteno razotkrivanje moglo štetiti temeljnim interesima Europske unije ili jedne ili više njezinih država članica (16.1.).	Ugrožavanje materijala CONFIDENTIEL UE moglo bi: — u materijalnom smislu štetiti diplomatskim odnosima, odnosno prouzročiti formalni protest ili druge sankcije; — dovesti u pitanje osobnu sigurnost ili slobodu pojedinca; — iznimno štetiti operativnoj učinkovitosti ili sigurnosti oružanih snaga država članica ili drugih sudionika, ili učinkovitosti vrijednih sigurnosnih ili obavještajnih operacija; — znatno oslabiti financijsku isplativost glavnih organizacija; — omesti istragu ili omogućiti izvođenje ozbiljnog kaznenog djela; — bitno naškoditi financijskim, monetarnim, gospodarskim i komercijalnim interesima Europske unije ili neke od njezinih država članica; — ozbiljno ometati razvoj ili provođenje u djelo glavnih politika EU-a; — ugasiti ili na drugi način prekinuti važne aktivnosti EU-a.	Ovlaštene osobe (izvor od kojeg podaci potječu), ravnatelji, voditelji službi (17.1.) Izvori od kojih podaci potječu navode datum ili razdoblje nakon kojega se sadržajima može smanjiti ili ukinuti stupanj klasifikacije. U suprotnom, dokumenti se pregledavaju najmanje svakih pet godina kako bi se potvrdila potreba izvornog stupnja klasifikacije (17.3.).	Stupanj klasifikacije CONFIDENTIEL UE i, ako se primjenjuju, sigurnosno obilježje i/ili obrambena oznaka – ESDP postavljaju se na dokumente CONFIDENTIEL UE mehaničkim sredstvima i ručno ili tiskanjem na prethodno žigosanom, registriranom papiru (16.4., 16.5., 16.3.). Stupnjevi klasifikacije EU-a i sigurnosna obilježja pojavljuju se na vrhu i dnu svake stranice, na sredini i svaka je stranica numerirana. Svaki dokument nosi referentni broj i datum. Svi se dodaci i prilozi nabrajaju na prvoj stranici (21.1.).	Odluka o snižavanju ili ukidanju stupnja klasifikacije isključivo je na izvoru od kojeg podaci potječu, koji o promjeni obavještava sve sljedeće naslovnike kojima je dokument dostavio, odnosno preslikao (17.3.). Dokumente sa stupnjem CONFIDENTIEL UE uništava registar odgovoran za njih, pod nadzorom osobe sa sigurnosnom provjerom. Njihovo se uništenje bilježi sukladno nacionalnim propisima i, u slučaju decentralizirane agencije Komisije ili EU-a, u skladu s uputama predsjednika (22.5.).	Prekobrojne preslike kao i dokumenti koji više nisu potrebni uništavaju se (22.5.). Dokumenti sa stupnjem klasifikacije CONFIDENTIEL UE uključujući sav otpadni materijal koji je nastao tijekom njihovog pripremanja kao što su oštećene preslike, radne preslike, tipkane bilješke i papiri preslika uništavaju se spaljivanjem, mljevenjem, trganjem ili na drugi način usitnjavanjem u neraspoznatljiv i neobnovljiv oblik (22.5.).

Stupanj klasifikacije	Kada	Tko	Postavljanje	Snižavanje/ukidanje/uništavanje	
				Tko	Kada
RESTREINT UE: Ovaj se stupanj klasifikacije dodjeljuje podacima i materijalima čije bi neovlašteno razotkrivanje moglo predstavljati nedostatak interesima Europske unije ili jedne ili više njezinih država članica (16.1.).	Ugrožavanje materijala RESTREINT UE moglo bi: — nepovoljno utjecati na diplomatske odnose; — prouzročiti ozbiljnu opasnost za pojedince; — dodatno otežati održavanje operativne učinkovitosti ili sigurnosti oružanih snaga država članica ili drugih sudionika; — prouzročiti financijski gubitak ili omogućiti nepropisno stjecanje dobitka ili prednosti pojedincima ili poduzećima; — kršiti obveze održavanja povjerljivosti podataka koje im pružaju treće stranke; — kršiti zakonska ograničenja u vezi s otkrivanjem podataka; — dovesti u pitanje istragu ili omogućiti izvođenje kaznenog djela; — predstavljati nedostatak za EU ili države članice u komercijalnim ili političkim pregovorima s drugima; — ometati učinkovit razvoj ili provođenje u djelo politika EU-a; — oslabiti pravilno upravljanje EU-om i njezinim operacijama.	Ovlaštene osobe (izvor od kojeg podaci potječu), ravnatelji, voditelji službi (17.1.) Izvori od kojih podaci potječu navode datum, razdoblje ili događaj nakon kojega se sadržajima može sniziti ili ukinuti stupanj klasifikacije (16.2.). U suprotnom, dokumenti se pregledavaju najmanje svakih pet godina kako bi se potvrdila potreba izvornog stupnja klasifikacije (17.3.).	Stupanj klasifikacije RESTREINT UE i, ako se primjenjuju, sigurnosno obilježje i/ili obrambena oznaka – ESDP postavljaju se na dokumente RESTREINT UE mehaničkim ili elektroničkim sredstvima (16.4., 16.5., 16.3.). Stupnjevi klasifikacije EU-a i sigurnosna obilježja pojavljuju se na vrhu prve stranice i svaka je stranica numerirana. Svaki dokument nosi referentni broj i datum (21.1.).	Odluka o snižavanju ili ukidanju stupnja klasifikacije isključivo je na izvoru od kojeg podaci potječu, koji o promjeni obavještava sve sljedeće naslovnike kojima je dokument dostavio, odnosno preslikao (17.3.). Dokumente sa stupnjem klasifikacije RESTREINT UE uništava registar odgovoran za njih ili korisnik, u skladu s uputama predsjednika (22.5.).	Prekobrojne preslike kao i dokumenti koji više nisu potrebni uništavaju se (22.5.).

Dodatak 3.

Smjernice za davanje klasificiranih podataka EU-a trećim zemljama ili međunarodnim organizacijama: Razina suradnje 1

POSTUPCI

1. Komisija kao kolegijalno tijelo ima ovlaštenje za davanje klasificiranih podataka EU-a zemljama koje nisu članice Europske unije ili drugim međunarodnim organizacijama čija su sigurnosna politika i propisi usporedivi s onima EU-a.

2. Do sastavljanja sigurnosnog sporazuma član Komisije odgovoran za sigurnosna pitanja nadležan je za preispitivanje zahtjeva za davanjem klasificiranih podataka EU-a.

3. Pri tome član Komisije:

   — traži mišljenja izvora od kojeg potječu klasificirani podaci EU-a koji se daju;

   — uspostavlja potrebne kontakte sa sigurnosnim tijelima ovime obuhvaćenih zemalja ili međunarodnih organizacija, da bi se provjerilo mogu li njihova sigurnosna politika i propisi osigurati zaštitu klasificiranih podataka koji se daju u skladu s ovim pravilnikom;

   — traži mišljenje savjetodavne skupine za sigurnosnu politiku Komisije u vezi s povjerenjem koje se obuhvaćenim državama ili međunarodnim tijelima može dati.

4. Član Komisije odgovoran za sigurnosna pitanja upućuje zahtjev i mišljenje savjetodavne skupine za sigurnosnu politiku Komisije na odlučivanje Komisiji.

SIGURNOSNE ODREDBE KOJE MORAJU PRIMJENJIVATI KORISNICI OVE POGODNOSTI

5. Član Komisije odgovaran za sigurnosna pitanja obavještava ovime obuhvaćene zemlje ili međunarodne organizacije o odluci Komisije da se odobri davanje klasificiranih podataka EU-a.

6. Odluka o davanju stupa na snagu tek nakon što korisnici ove pogodnosti daju pismeno uvjerenje da će:

   — podatke koristiti samo u dogovorene svrhe;

   — zaštititi podatke u skladu s ovim pravilnikom i naročito u skladu s posebnim pravilima koja se niže navode.

7. Osoblje

   (a) Broj službenika s pristupom klasificiranim dokumentima EU-a je strogo ograničen, prema načelu potrebe poznavanja, na osobe čije dužnosti zahtijevaju takav pristup;

   (b) svi službenici ili državljani s ovlaštenjem za pristup klasificiranim podacima sa stupnjem klasifikacije CONFIDENTIEL UE ili višim moraju imati sigurnosnu potvrdu odgovarajuće razine ili jednako vrijednu sigurnosnu provjeru, koju izdaje vlada njihove države.

8. Prijenos dokumenata

   a) Praktični postupci prijenosa dokumenata dogovaraju se sporazumom. Sve do sklapanja takvog sporazuma primjenjuju se odredbe odjeljka 21. U sporazumu se posebno navode registarski uredi kojima treba proslijediti klasificirane podatke EU-a;

   b) ako se među klasificiranim podacima čije je davanje odobrila Komisija nalaze oni sa stupnjem EU TOP SECRET, zemlja ili međunarodna organizacija koja ovu pogodnost uživa uspostavlja središnji registarski ured EU-a i, ako je potrebno, podregistarske urede EU-a. Ovi registarski uredi primjenjuju odredbe strogo istovjetne onima iz odjeljka 22. ovog pravilnika.

9. Registracija

   Čim registarski ured zaprimi dokument EU-a sa stupnjem klasifikacije CONFIDENTIEL UE ili višim, upisuje dokument u poseban registar organizacije, sa stupcima predviđenim za: datum primitka, pojedinosti dokumenta (datum, referentni broj i broj preslike), stupanj klasifikacije, naslov, ime ili naziv primatelja, datum vraćanja potvrde primitka i datum vraćanja dokumenta izvoru EU-a od kojeg podaci potječu ili datum uništenja.

10. Uništenje

(a) Klasificirani dokumenti EU-a uništavaju se u skladu s uputama iznesenim u odjeljku 22. ovog pravilnika. Preslike potvrda o uništenju dokumenata sa stupnjem klasifikacije SECRET UE i TRÈS SECRET UE šalju se u registarski ured EU-a koji je dokumente proslijedio;

(b) klasificirani dokumenti EU-a uključuju se u planove uništavanja u nuždi za klasificirane dokumente samih korisnika ove pogodnosti.

11. Zaštita dokumenata

Poduzimaju se sve mjere kako bi se neovlaštenim osobama onemogućio pristup do klasificiranih podataka EU-a.

12. Preslike, prijevodi i izvadci

Dokumenti sa stupnjem klasifikacije CONFIDENTIEL UE ili SECRET UE ne smiju se preslikavati ili prevoditi bez ovlaštenja čelnika dotične sigurnosne organizacije koji te preslike, prijevode ili izvatke registrira i provjerava te prema potrebi pečatira.

Ovlaštenje za umnožavanje ili prevođenje dokumenata sa stupnjem klasifikacije TRÈS SECRET UE daju samo izvori od kojih podaci potječu koji određuju dozvoljeni broj preslika; ako se izvor od kojeg podaci potječu ne može odrediti upućuje se zahtjev Sigurnosnoj službi Komisije.

13. Kršenja sigurnosti

Kada dođe do kršenja sigurnosti u vezi s klasificiranim dokumentom EU-a, ili se na to sumnja, ovisno o sklopljenom sigurnosnom sporazumu poduzimaju se odmah sljedeće radnje:

(a) provodi se istraga kako bi se utvrdile okolnosti kršenja sigurnosti;

(b) obavještava se Sigurnosni ured Komisije, odgovarajuće tijelo nacionalne sigurnosti i izvor od kojeg podaci potječu ili se jasno navodi ukoliko posljednji nije obaviješten;

(c) poduzimaju se mjere za umanjivanje učinaka kršenja sigurnosti;

(d) razmatraju se i uvode mjere sprečavanja ponovnog kršenja;

(e) provode se sve mjere koje preporuča Sigurnosni ured Komisije radi sprečavanja ponovnog kršenja.

14. Pregledi

Sigurnosni ured Komisije, na temelju sporazuma s državama ili dotičnim međunarodnim organizacijama, procjenjuje učinkovitost mjera zaštite klasificiranih dokumenata EU-a koji se daju.

15. Izvještavanje

Ovisno o sklopljenom sigurnosnom sporazumu, sve dok posjeduje klasificirane podatke EU-a, država ili međunarodna organizacija podnosi godišnji izvještaj kojim se potvrđuje da se ovaj pravilnik poštuje s datumom koji se određuje pri izdavanju ovlaštenja za davanje podataka.

Dodatak 4.

Smjernice za davanje klasificiranih podataka EU-a trećim zemljama ili međunarodnim organizacijama: Razina suradnje 2

POSTUPCI

1. Ovlaštenje za davanje klasificiranih podataka EU-a trećim zemljama ili međunarodnim organizacijama čija su sigurnosna politika i propisi znatno drugačiji od onih EU-a ima izvor od kojeg podaci potječu. Ovlaštenje za davanje klasificiranih podataka EU-a nastalih unutar Komisije ima Komisija kao kolegij.

2. Načelno je to ograničeno na podatke do stupnja klasifikacije SECRET UE, uključujući i njega; ne odnosi se na klasificirane podatke zaštićene posebnim sigurnosnim obilježjima ili oznakama.

3. Do sastavljanja sigurnosnog sporazuma, član Komisije odgovoran za sigurnosna pitanja nadležan je za preispitivanje zahtjeva za davanjem klasificiranih podataka EU-a.

4. Pri tome član Komisije:

   — traži mišljenja izvora od kojeg potječu klasificirani podaci EU-a koji se daju;

   — uspostavlja potrebne kontakte sa sigurnosnim tijelima ovime obuhvaćenih država ili međunarodnih organizacija, da bi se prikupili podaci o njihovoj sigurnosnoj politici i odredbama, posebno da bi se sastavila usporedna tablica stupnjeva klasifikacije koji se primjenjuju u EU i u dotičnoj državi ili organizaciji;

   — organizira sastanak savjetodavne skupine za sigurnosnu politiku Komisije ili se, ako je potrebno, taktički raspituje kod tijela nacionalne sigurnosti država članica radi dobivanja mišljenja savjetodavne skupine za sigurnosnu politiku Komisije.

5. Mišljenje savjetodavne skupine za sigurnosnu politiku Komisije obuhvaća sljedeće:

   — povjerenje koje se obuhvaćenim državama ili međunarodnim organizacijama može dati radi procjene sigurnosnog rizika kojemu su izložene EU ili države članice;

   — ocjenu sposobnosti korisnika ove pogodnosti u zaštiti klasificiranih podataka koje daje EU;

   — prijedloge u vezi s posebnim postupcima za rukovanje klasificiranim podacima EU-a (na primjer pribavljanje pročišćene verzije teksta) i dokumenata koji se šalju (zadržavanje ili brisanje zaglavlja, posebnih oznaka i dr. u vezi sa stupnjevima klasifikacije EU-a);

   — snižavanje ili ukidanje stupnja klasifikacije podataka prije njihovog davanja ovime obuhvaćenim zemljama ili međunarodnim organizacijama.

6. Član Komisije odgovoran za sigurnosna pitanja upućuje zahtjev i mišljenje savjetodavne skupine za sigurnosnu politiku Komisije na odlučivanje Komisiji.

SIGURNOSNE ODREDBE KOJE MORAJU PRIMJENJIVATI KORISNICI OVE POGODNOSTI

7. Član Komisije odgovaran za sigurnosna pitanja obavještava ovime obuhvaćene države ili međunarodne organizacije o odluci Komisije o davanju klasificiranih podataka EU-a, kao i o njezinim ograničenjima.

8. Odluka o davanju stupa na snagu tek kada korisnici ove pogodnosti pismeno potvrde da će:

   — podatke upotrebljavati samo u dogovorene svrhe;

   — zaštititi podatke u skladu s odredbama koje utvrdi Komisija.

9. Primjenjuju se odredbe o zaštiti koje slijede, osim kada Komisija, po pribavljanju mišljenja savjetodavne skupine za sigurnosnu politiku Komisije, odluči o posebnom postupku za rukovanje klasificiranim dokumentima EU-a (brisanje navedenih stupnjeva klasifikacije EU-a, posebnih oznaka i dr.).

10. Osoblje

    (a) Broj službenika s pristupom klasificiranim dokumentima EU-a strogo je ograničen, prema načelu potrebe poznavanja, na osobe čije dužnosti zahtijevaju takav pristup;

    (b) svi službenici ili državljani s ovlaštenjem za pristup klasificiranim podacima koje daje Komisija moraju imati državnu sigurnosnu provjeru ili ovlaštenje za pristup do odgovarajuće razine istovjetne onoj EU-a, kako je utvrđeno usporednom tablicom;

    (c) ove državne sigurnosne provjere ili ovlaštenja prosljeđuju se predsjedniku za informaciju.

11. Prijenos dokumenata

Praktični postupci prijenosa dokumenata dogovaraju se sporazumom. Sve do sklapanja takvog sporazuma primjenjuju se odredbe odjeljka 21. U sporazumu se posebno navode registarski uredi i točne adrese na koje treba proslijediti klasificirane podatke EU-a, kao i kurirske ili poštanske službe koje se koriste za prijenos klasificiranih podataka EU-a.

12. Registracija o primitku

Tijelo nacionalne sigurnosti naslovljene države ili njemu istovjetno tijelo države koje u ime svoje vlade prima klasificirane podatke koje proslijedi Komisija ili ured sigurnosti međunarodne organizacije primatelja otvara poseban registar za upis klasificiranih podataka EU-a po njihovom primitku. Registar sadržava stupce za datum primitka, pojedinosti dokumenta (datum, referentni broj i broj preslike), stupanj klasifikacije, naslov, ime ili naziv naslovnika, datum vraćanja potvrde primitka i datum vraćanja dokumenta u EU ili datum njegova uništenja.

13. Vraćanje dokumenata

Kada primatelj vraća klasificirani dokument Komisiji, postupa na način kako je utvrđeno u gornjem odjeljku „Prijenos dokumenata”.

14. Zaštita

(a) Kada dokumenti nisu u upotrebi, čuvaju se u sigurnosnom spremniku odobrenom za čuvanje državnih klasificiranih materijala istovrsnog stupnja klasifikacije. Na spremniku ne smije biti nikakvih naznaka o njegovom sadržaju koji je dostupan samo ovlaštenim osobama za rukovanje klasificiranim podacima EU-a. Kada se upotrebljavaju brave s kombinacijama, kombinacije smiju znati samo oni službenici u državi ili organizaciji koji imaju ovlaštenje za pristup klasificiranim podacima EU-a pohranjenim u spremniku; kombinacije se mijenjaju svakih šest mjeseci ili ranije prilikom premještanja službenika, povlačenja sigurnosne provjere nekog od službenika koji poznaje kombinaciju ili ako postoji rizik od ugrožavanja;

(b) klasificirane dokumente EU-a iz sigurnosnog spremnika uklanjanju samo oni službenici koji su prošli provjeru za pristup klasificiranim dokumentima EU-a i imaju potrebu poznavanja. Sve dok su ti dokumenti kod njih, navedeni službenici su i dalje odgovorni za sigurnu brigu o njima i, posebno, za zaštitu dokumenata od pristupa neovlaštenih osoba. Također se brinu da se po završetku upotrebe i izvan radnog vremena dokumenti pohrane u sigurnosni spremnik;

(c) bez ovlaštenja Sigurnosnog ureda Komisije ne smiju se izrađivati preslike niti uzimati izvadci dokumenata sa stupnjem klasifikacije CONFIDENTIEL UE ili višim;

(d) postupak za brzo i potpuno uništenje dokumenata u slučaju nužde, utvrđuje se i potvrđuje u Sigurnosnom uredu Komisije.

15. Fizička sigurnost

(a) Kada nisu u upotrebi, sigurnosni spremnici za čuvanje klasificiranih dokumenata EU-a uvijek se zaključavaju;

(b) kad osoblje zaduženo za održavanje ili čišćenje ulazi ili radi u prostoriji u kojoj se nalaze sigurnosni spremnici, te osobe su uvijek u pratnji člana službe sigurnosti države ili organizacije, ili službenika posebno odgovornog za nadzor sigurnosti prostorije;

(c) izvan uobičajenog radnog vremena (noću, vikendima i blagdanima) sigurnosni spremnici koji sadrže klasificirane dokumente EU-a su pod nadzorom straže ili automatskog alarmnog sustava.

16. Kršenja sigurnosti

U slučaju kršenja sigurnosti u vezi s klasificiranim dokumentom EU-a ili kada se na to sumnja, odmah se poduzimaju sljedeće radnje:

(a) odmah se upućuje izvještaj Sigurnosnom uredu Komisije ili tijelu nacionalne sigurnosti države članice koja je preuzela inicijativu upućivanja dokumenata (uz presliku Sigurnosnom uredu Komisije);

(b) provodi se ispitivanje nakon kojega se sigurnosnom tijelu podnosi puni izvještaj (vidjeti gore pod (a). Nakon tog donose se mjere za popravak nastale situacije.

17. Inspekcijski pregledi

Sigurnosnom uredu Komisije dozvoljava se, na temelju sporazuma s državama ili dotičnim međunarodnim organizacijama, procjena učinkovitosti mjera zaštite danih klasificiranih dokumenata EU-a.

18. Izvještavanje

Ovisno o sklopljenom sigurnosnom sporazumu, sve dok posjeduje klasificirane podatke EU-a država ili međunarodna organizacija podnosi godišnji izvještaj kojim se potvrđuje da je ovaj pravilnik poštivan, s datumom koji se određuje pri izdavanju ovlaštenja za davanje podataka.

Dodatak 5.

Smjernice za davanje klasificiranih podataka EU-a trećim zemljama ili međunarodnim organizacijama: Razina suradnje 3

POSTUPCI

1. Komisija može povremeno, u nekim posebnim okolnostima, izraziti želju za suradnjom s državama ili organizacijama koje ne mogu pružiti jamstva kakva zahtijeva ovaj pravilnik, iako ta suradnja može zahtijevati davanje klasificiranih podataka EU-a.

2. Ovlaštenje za davanje klasificiranih podataka EU-a trećim zemljama ili međunarodnim organizacijama, čija je sigurnosna politika i propisi znatno drugačija od onih EU-a, ima izvor od kojeg podaci potječu. Ovlaštenje za davanje klasificiranih podataka EU-a nastalih unutar Komisije ima Komisija kao kolegijalno tijelo.

   Načelno je to ograničeno na podatke do stupnja klasifikacije SECRET UE, uključujući i njega; ne odnosi se na klasificirane podatke zaštićene posebnim sigurnosnim obilježjima ili oznakama.

3. Komisija razmatra pitanje promišljenosti davanja klasificiranih podataka, ocjenjuje potrebu poznavanja korisnika ove pogodnosti i odlučuje o prirodi klasificiranih podataka koji se mogu priopćiti.

4. Ako Komisija pristaje, član Komisije odgovoran za sigurnosna pitanja:

   — traži mišljenje izvora od kojega potječu klasificirani podaci EU-a koji se daju;

   — organizira sastanak savjetodavne skupine za sigurnosnu politiku Komisije ili se, ako je potrebno, taktički raspituje kod tijela nacionalne sigurnosti država članica radi dobivanja mišljenja savjetodavne skupine Komisije za sigurnosnu politiku.

5. Mišljenje savjetodavne skupine za sigurnosnu politiku Komisije obuhvaća sljedeće:

   (a) procjenu sigurnosnog rizika kojemu su EU ili države članice izložene;

   (b) stupanj klasifikacije podataka koji se mogu dati;

   (c) snižavanje ili ukidanje stupnja klasifikacije prije davanja podataka;

   (d) postupke rukovanja dokumentima koji se daju (vidjeti odjeljak niže);

   (e) moguće načine prijenosa (upotreba javnih poštanskih službi, javnih ili sigurnih telekomunikacijskih sustava, diplomatskih pošiljki, provjerenih kurira, itd.).

6. Dokumenti koji se predaju državama ili organizacijama na koje se ovaj Dodatak odnosi, u načelu se pripremaju bez navođenja porijekla ili stupnja klasifikacije EU-a. Savjetodavna skupina za sigurnosna politiku Komisije može preporučiti:

   — upotrebu posebnih oznaka ili kodova;

   — upotrebu posebnog sustava razvrstavanja koji povezuje osjetljivost podataka s nadzornim mjerama za prijenos dokumenata koji se traže od korisnika ove pogodnosti.

7. Predsjednik upućuje mišljenje savjetodavne skupine za sigurnosnu politiku Komisije na odlučivanje Komisiji.

8. Kada Komisija odobri davanje klasificiranih podataka EU-a i praktične provedbene postupke, Sigurnosni ured Komisije uspostavlja potreban kontakt sa sigurnosnim tijelom države ili dotične organizacije kako bi se omogućila primjena predviđenih sigurnosnih mjera.

9. Član Komisije odgovoran za sigurnosna pitanja obavještava države članice o prirodi i stupnju klasifikacije podataka, navodeći popis organizacija i zemalja kojima se, prema odluci Komisije, podaci smiju dati.

10. Sigurnosni ured Komisije poduzima sve potrebne mjere kako bi se omogućila procjena moguće štete i preispitivanje postupaka.

    Komisija ponovno razmatra to pitanje uvijek kada se mijenjaju uvjeti suradnje,.

SIGURNOSNE ODREDBE KOJE MORAJU PRIMJENJIVATI KORISNICI OVE POGODNOSTI

11. Član Komisije odgovaran za sigurnosna pitanja obavještava ovime obuhvaćene države ili međunarodne organizacije o odluci Komisije o davanju klasificiranih podataka EU-a, zajedno s detaljnim pravilima zaštite koje savjetodavna skupina za sigurnosnu politiku Komisije predloži i Komisija ih odobri.

12. Odluka stupa na snagu tek kada korisnici ove pogodnosti daju pismeno uvjerenje da će:

— podatke upotrebljavati samo za potrebe suradnje koje odluči Komisija;

— pružiti zaštitu podataka kakvu traži Komisija.

13. Prijenos dokumenata

(a) Praktične postupke za prijenos dokumenata dogovaraju Sigurnosni ured Komisije i sigurnosna tijela država ili međunarodnih organizacija primatelja. Njima se posebno navode točne adrese na koje treba proslijediti dokumente;

(b) dokumenti sa stupnjem klasifikacije CONFIDENTIEL UE ili višim šalju se u dvostrukom omotu. Unutarnja omotnica nosi poseban pečat ili dogovoreno kodno ime i napomenu o posebnom stupnju klasifikacije odobrenom za dokument. Obrazac potvrde primitka umeće se u omotnicu za svaki klasificirani dokument. Na potvrdi primitka koja sama po sebi nije tajna, navode se samo pojedinosti (datum, referentni broj i broj preslike) i jezik, ali ne i naslov dokumenta;

(c) unutarnja omotnica se zatim umeće u vanjsku, na kojoj se navodi broj paketa radi zaprimanja. Vanjska omotnica ne nosi oznaku sigurnosnog stupnja klasifikacije;

(d) kuriru se uvijek predaje potvrda primitka s brojem pakiranja.

14. Registracija o primitku

Tijelo nacionalne sigurnosti naslovljene države ili njemu istovjetno tijelo države koje u ime svoje vlade prima klasificirane podatke koje proslijedi Komisija, ili ured sigurnosti međunarodne organizacije primatelja otvara poseban registar za upis klasificiranih podataka EU-a po njihovom primitku. Registar sadržava stupce za datum primitka, pojedinosti dokumenta (datum, referentni broj i broj preslike), stupanj klasifikacije, naslov, ime ili naziv naslovnika, datum vraćanja potvrde primitka i datum vraćanja dokumenta u EU ili datum njegova uništenja.

15. Upotreba i zaštita razmijenjenih klasificiranih podataka

(a) Podacima sa stupnjem klasifikacije SECRET UE rukuju za to posebno određeni službenici s ovlaštenjem pristupa za podatke s ovim stupnjem klasifikacije. Ti se podaci čuvaju u kvalitetnim sigurnosnim ormarićima koje mogu otvarati samo osobe s ovlaštenjem za pristup podacima koji su u njima. Područja u kojima su smješteni ovakvi ormarići stalno se nadgledaju, a uspostavlja se i sustav provjeravanja koji dozvoljava ulaz samo osobama s propisnim ovlaštenjem. Podaci SECRET UE upućuju se kao diplomatska pošiljka, sigurnom poštanskom službom ili sigurnim telekomunikacijskim putem. Dokument sa stupnjem klasifikacije SECRET UE preslikava se samo uz pismeni pristanak izvora od kojeg podaci potječu. Sve se preslike registriraju i prate. Za sve postupke u vezi s dokumentima SECRET UE izdaju se potvrde;

(b) podacima sa stupnjem klasifikacije CONFIDENTIEL UE rukuju propisno imenovani službenici koji su ovlašteni za primanje podataka o predmetnome. Dokumenti se čuvaju u zaključanim sigurnosnim ormarićima u područjima pod nadzorom;

podaci CONFIDENTIEL UE upućuju se kao diplomatske pošiljke, vojnim poštanskim službama i putem sigurnih telekomunikacija. Tijelo primatelja može izrađivati preslike, njihov se broj i raspodjela bilježi u posebnim registrima;

(c) podacima CONFIDENTIEL UE rukuje se u prostorima koji su nedostupni neovlaštenom osoblju, ti se podaci čuvaju u zaključanim spremnicima. Dokumenti se mogu upućivati javnim poštanskim službama kao registrirana pošta u dvostrukoj omotnici te, u hitnim slučajevima za vrijeme operacija, putem nezaštićenog telekomunikacijskog sustava. Primatelji smiju izrađivati preslike;

(d) podaci koji nisu klasificirani ne trebaju posebne zaštitne mjere i mogu se upućivati poštom i javnim telekomunikacijskim sustavima. Naslovnici smiju izrađivati preslike.

16. Uništavanje

Dokumenti koji nisu više potrebni, uništavaju se. U slučaju dokumenata sa stupnjem klasifikacije RESTREINT UE i CONFIDENTIEL UE unose se u posebne registre odgovarajuće bilješke. U slučaju dokumenata sa stupnjem klasifikacije SECRET UE izdaju se potvrde o uništenju koje potpisuju dvije osobe koje su svjedočile njihovom uništenju.

17. Kršenja sigurnosti

Ako su podaci CONFIDENTIEL UE ili SECRET UE ugroženi ili se na to sumnja, tijelo nacionalne sigurnosti države ili čelnik za sigurnost u organizaciji raspituje se o okolnostima ugrožavanja. O rezultatima tog raspitivanja obavještava se Sigurnosni ured Komisije. Poduzimaju se koraci potrebni za ispravljanje neodgovarajućih postupaka ili načina pohranjivanja koji su mogli dovesti do ugrožavanja podataka.

Dodatak 6.

POPIS SKRAĆENICA

ACPC	Savjetodavni odbor za nabavku i ugovore
CrA	tijelo Crypto
CISO	službenik za informacijsku sigurnost na središnjoj razini
COMPUSEC	sigurnost računala
COMSEC	sigurnost komunikacija
CSO	Sigurnosni ured Komisije
ESDP	europska sigurnosna i obrambena politika
EUCI	klasificirani podaci EU-a
IA	tijelo INFOSEC
INFOSEC	sigurnost podataka
IO	imatelj podataka
ISO	međunarodna organizacija za normizaciju
IT	informacijska tehnologija
LISO	službenik za informacijsku sigurnost na lokalnoj razini
LSO	lokalni službenik sigurnosti
MSO	službenik za sigurnost sastanka
NSA	tijelo nacionalne sigurnosti
PC	osobno računalo
RCO	nadzorni službenik registarskog ureda
SAA	tijelo za akreditaciju u vezi sa sigurnosti
SecOPS	sigurnosni postupci rada
SSRS	određenje sigurnosnih zahtjeva koji su specifični za sustav
TA	tijelo TEMPEST
TSO	imatelj tehničkih sustava