32001D0844

L 317/1 *URADNI LIST EVROPSKIH SKUPNOSTI* 3.12.2001

SKLEP KOMISIJE
z dne 29. novembra 2001
o spremembah njenega poslovnika

(notificiran pod dokumentarno številko K (2001) 3031)

(2001/844/ES, ESPJ, Euratom)

KOMISIJA EVROPSKIH SKUPNOSTI JE –

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti in zlasti člena 218(2) Pogodbe,

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti za premog in jeklo in zlasti člena 16 Pogodbe,

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti za atomsko energijo in zlasti člena 131 Pogodbe,

ob upoštevanju Pogodbe o Evropski uniji in zlasti člena 28(1) in člena 41(1) Pogodbe –

SKLENILA:

Člen 1

Pravilnik Komisije o varnosti, ki je priložen temu sklepu, se doda Poslovniku Komisije kot priloga.

Člen 2

Ta sklep začne veljati na dan objave v *Uradnem listu Evropskih skupnosti*.

Uporabljati se začne s 1. decembrom 2001.

V Bruslju, 29. novembra 2001

Za Komisijo

Romano PRODI

Predsednik

PRILOGA

PRAVILNIK KOMISIJE O VARNOSTI

Ob upoštevanju naslednjega:

(1) Da bi razvijali dejavnosti Komisije na področjih, ki zahtevajo določeno stopnjo tajnosti, je treba vzpostaviti celovit varnostni sistem, ki se uporablja za Komisijo, ostale institucije, telesa, urade in agencije, ustanovljene zaradi ali na podlagi Pogodbe ES ali Pogodbe o Evropski uniji, države članice in tudi vse druge prejemnike tajnih podatkov Evropske unije, v nadaljnjem besedilu imenovani „tajni podatki EU".

(2) Za zagotavljanje učinkovitosti tako vzpostavljenega varnostnega sistema, posreduje Komisija tajne podatke EU samo tistim zunanjim telesom, ki zagotovijo, da so sprejela vse potrebne ukrepe za uporabo predpisov, ki so enakovredni temu pravilniku.

(3) Ta pravilnik se sprejme brez poseganja v Uredbo št. 3 z dne 31. julija 1958 o izvajanju člena 24 Pogodbe o ustanovitvi Evropske skupnosti za atomsko energijo [1], v Uredbo Sveta (ES) št. 1588/90 z dne 11. junija 1990 o prenosu zaupnih podatkov na Statistični urad Evropskih skupnosti [2], in v Sklep Komisije C (95) 1510 z dne 23. novembra 1995 o zaščiti informacijskega sistema.

(4) Varnostni sistem Komisije temelji na načelih, določenih v Sklepu Sveta 2001/264/ES z dne 19. marca 2001 o sprejetju predpisov Sveta o varovanju tajnosti [3], da bi se zagotovilo nemoteno sprejemanje odločitev v Uniji.

(5) Komisija poudarja pomembnost pridružitve ostalih institucij predpisom in standardom varovanja tajnosti, ki so potrebni za varstvo interesov Unije in njenih držav članic.

(6) Komisija ugotavlja potrebo po ustvarjanju lastnega koncepta varnosti ob upoštevanju vseh elementov varnosti in posebnega značaja Komisije kot institucije.

(7) Ta pravilnik se sprejme brez poseganja v člen 255 Pogodbe in v Uredbo (ES) št. 1049/2001 Evropskega parlamenta in Sveta z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije [4];

Člen 1

Pravilnik Komisije o varnosti je določen v Prilogi.

Člen 2

1. Član Komisije, pristojen za varnostne zadeve, sprejme ustrezne ukrepe za zagotovitev, da pri ravnanju s tajnimi podatki EU uradniki in drugi uslužbenci Komisije spoštujejo predpise iz člena 1 znotraj Komisije, prav tako osebje, začasno dodeljeno Komisiji, pa tudi znotraj vseh prostorov Komisije, vključno z njenimi predstavništvi in uradi v Uniji in njenimi delegacijami v tretjih državah in izvajalci izven Komisije.

2. Državam članicam, drugim institucijam, telesom, uradom in agencijam, ustanovljenim na podlagi Pogodb, je dovoljeno prejemati tajne podatke EU pod pogojem, da zagotovijo, da znotraj njihovih služb in prostorov pri ravnanju s tajnimi podatki EU spoštujejo predpise, ki so enakovredni tistim iz člena 1, predvsem:

(a) člani stalnih predstavništev držav članic v Evropski uniji kot tudi člani državnih delegacij, ki prisostvujejo sestankom Komisije ali njenih teles, ali ki sodelujejo v drugih dejavnostih Komisije,

(b) drugi predstavniki iz državnih uprav držav članic, ki upravljajo s tajnimi podatki EU, bodisi da delujejo na ozemlju držav članic ali v tujini,

(c) zunanji izvajalci in začasno dodeljeno osebje, ki upravlja s tajnimi podatki EU.

---

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

Člen 3

Tretjim državam, mednarodnim organizacijam in drugim telesom je dovoljeno prejemati tajne podatke EU pod pogojem, da zagotovijo, da se ob upravljanju s takimi podatki spoštuje predpise, ki so enakovredni tistim iz člena 1.

Člen 4

V skladu s temeljnimi načeli in minimalnimi varnostnimi standardi, ki jih vsebuje Del I Priloge, lahko član Komisije, pristojen za varnostne zadeve, sprejme ukrepe v skladu z Delom II Priloge.

Člen 5

Z dnem začetka njegove uporabe ta pravilnik nadomesti:

(a) Sklep Komisije C(94) 3282 z dne 30. novembra 1994 o varnostnih ukrepih, ki se uporabljajo za tajne podatke, ki nastajajo ali se prenašajo v zvezi z dejavnostmi Evropske unije;

(b) Sklep Komisije C(99) 423 z dne 25. februarja 1999 o postopkih, s katerimi se uradnikom in drugim uslužbencem Evropske Komisije lahko dovoli dostop do tajnih podatkov, ki jih ima Komisija.

Člen 6

Od dneva začetka uporabe tega pravilnika se vsi tajni podatki, ki jih do tega datuma poseduje Komisija, razen tajnih podatkov Euratoma:

(a) če jih je ustvarila Komisija, praviloma štejejo za ponovno določene kot „RESTREINT UE“, razen če jim njihov avtor do 31. januarja 2002 ne določi druge stopnje tajnosti. V takem primeru avtor obvesti vse naslovljence zadevnega dokumenta;

(b) obdržijo svojo prvotno stopnjo tajnosti, če jo določijo avtorji izven Komisije, in se tako obravnavajo kot tajni podatki EU na enakovredni ravni, razen če se avtor ne strinja z odvzemom stopnje tajnosti ali določitvijo nižje stopnje tajnosti.

PRILOGA

PRAVILNIK KOMISIJE O VARNOSTI

VSEBINA

DEL I: TEMELJNA NAČELA IN MINIMALNI STANDARDI VARNOSTI

1. UVOD

Ta pravilnik določa temeljna načela in minimalne standarde varnosti, ki jih mora Komisija spoštovati na ustrezen način v vseh svojih službah, kakor tudi vsi prejemniki tajnih podatkov EU, tako da je varnost zagotovljena in da je vsak lahko prepričan, da je vzpostavljen skupni standard varovanja.

2. SPLOŠNA NAČELA

Varnostna politika Komisije predstavlja sestavni del njene splošne notranje politike upravljanja in tako temelji na načelih, ki urejajo njeno splošno politiko.

Ta načela so načelo spoštovanja predpisov, načelo transparentnosti, načelo odgovornosti in načelo subsidiarnosti (sorazmernost).

Načelo spoštovanja predpisov pomeni, da se pri opravljanju varnostnih funkcij deluje v okviru pravnega sistema. Pomeni tudi, da morajo pristojnosti na področju varnosti temeljiti na ustreznih predpisih. Določbe uslužbenskih predpisov se v celoti uporabljajo, predvsem njihov člen 17 o dolžnosti osebja v zvezi s podatki Komisije, in njihov Naslov VI o disciplinskih ukrepih. Nadalje pomeni, da je treba kršitve varnosti v okviru pristojnosti Komisije obravnavati na način, ki je skladen s politiko Komisije o uresničevanju disciplinske odgovornosti in z njeno politiko o sodelovanju z državami članicami na področju kazenskega prava.

Načelo preglednosti pomeni jasnost varnostnih predpisov in določb o ravnotežju med različnimi službami in različnimi področji (fizično varovanje tajnih podatkov itd.) in potrebo po dosledni in organizirani politiki varnostnega ozaveščanja. Pomeni tudi potrebo po jasnih smernicah za izvajanje varnostnih ukrepov.

Načelo odgovornosti pomeni, da so pristojnosti na področju varnosti jasno določene. Poleg tega pomeni potrebo po rednem preverjanju, če se te pristojnosti pravilno uresničujejo.

Načelo subsidiarnosti ali sorazmernosti pomeni, da se varnost organizira na najnižji možni ravni in kolikor je mogoče blizu generalnih direktoratov in služb Komisije. Pomeni tudi, da se varnostne dejavnosti omejijo samo na tiste elemente, ki jo zares potrebujejo. Prav tako pomeni, da so varnostni ukrepi sorazmerni z interesi, ki jih je treba varovati, in z dejanskim ali možnim ogrožanjem teh interesov, pri čemer zagotavljajo varovanje, pri katerem so možne čim manjše motnje.

3. TEMELJI VARNOSTI

Temelji zanesljive varnosti so:

(a) V vsaki državi članici organi, pristojni za

   1. zbiranje in shranjevanje obveščevalnih podatkov o vohunstvu, sabotažah, terorizmu ter drugih subverzivnih dejavnostih, in

   2. posredovanje podatkov in nasvetov glede narave ogrožanja varnosti in o sredstvih varovanja pred njimi svojim vladam in preko njih Komisiji.

(b) V vsaki državi članici in v Komisiji tehnični organ INFOSEC (IA), pristojen za sodelovanje z zadevnim varnostnim organom, za posredovanje podatkov in nasvetov v zvezi z ogrožanjem varnosti iz tehničnega vidika in o sredstvih varovanja;

(c) Redno sodelovanje med službami vlad in pristojnimi službami Evropskih institucij, da bi, če je to primerno, določili in priporočili:

   1. katere osebe, podatke in vire je treba varovati in

   2. skupne standarde varovanja.

(d) Tesno sodelovanje med Varnostnim uradom Komisije in varnostnimi službami drugih evropskih institucij in z Uradom za varnost NATO (NOS).

4. NAČELA VAROVANJA PODATKOV

4.1 **Cilji**

Cilji varovanja tajnih podatkov so:

(a) varovati tajne podatke EU pred vohunstvom, ogrožanjem ali nedovoljenim razkritjem;

(b) varovati podatke EU, s katerimi se upravlja v komunikacijskih in informacijskih sistemih ter omrežjih, pred ogrožanjem njihove tajnosti, celovitosti in razpoložljivosti;

(c) varovati prostore Komisije, v katerih se nahajajo podatki EU, pred sabotažami in naklepnim poškodovanjem;

(d) v primeru napake oceniti povzročeno škodo, omejiti njene posledice in sprejeti potrebne sanacijske ukrepe.

4.2 **Definicije**

V tem pravilniku imajo posamezni izrazi naslednji pomen:

(a) Izraz „tajni podatki EU“ pomeni vse podatke in gradivo, katerih nedovoljeno razkritje bi lahko v različni meri škodovalo interesom EU ali eni ali več državam članicam, bodisi da taki podatki izvirajo znotraj EU ali prihajajo iz držav članic, tretjih držav ali mednarodnih organizacij.

(b) Izraz „dokument“ pomeni vsako pismo, zapis, zabeležko, poročilo, memorandum, signal/sporočilo, skico, fotografijo, diapozitiv, film, karto/zemljevid, grafični prikaz, načrt, zvezek/beležnico, matrico, kopirni papir, trak pisalnega stroja ali tiskalnika, magnetni trak, kaseto, računalniško disketo, CD ROM ali druge materialne nosilce shranjenih podatkov.

(c) Izraz „gradivo“ pomeni „dokument“, kot je opredeljen v (b) in tudi vsak del opreme, ki je bodisi že bil izdelan ali je v postopku izdelave.

(d) Izraz „potreba vedeti“ pomeni potrebo uradnika ali uslužbenca po dostopu do tajnih podatkov EU, da bi lahko opravljal svoje delo ali nalogo.

(e) „Pooblastilo“ pomeni sklep predsednika Komisije, da odobri posamezen dostop do tajnih podatkov EU do določene stopnje na podlagi pozitivnega rezultata varnostnega pregleda (preverjanja), ki ga izvede organ državne varnosti v skladu z notranjo zakonodajo.

(f) Izraz „stopnja tajnosti“ pomeni določitev ustrezne stopnje varnosti podatkom, katerih nedovoljeno razkritje bi lahko v določeni meri škodilo interesom Komisije ali držav članic.

(g) Izraz „znižanje stopnje tajnosti“ (déclassement) pomeni uvrstitev v nižjo stopnjo tajnosti .

(h) Izraz „odprava stopnje tajnosti“ (déclassification) pomeni odpravo kakršnekoli stopnje tajnosti.

(i) Izraz „oseba izvora“ pomeni ustrezno pooblaščenega avtorja tajnega dokumenta. Znotraj Komisije lahko vodje služb pooblastijo svoje osebje, da določa tajne podatke EU.

(j) Izraz „službe Komisije“ pomeni službe Komisije, vključno s kabineti, na vseh delovnih mestih, vključno s skupnim raziskovalnim centrom, predstavništvi in uradi v Uniji ter delegacijami v tretjih državah.

4.3 **Določanje stopenj tajnosti**

(a) Na področju tajnosti so pri izboru podatkov in gradiva, ki jih/ga je treba zavarovati in pri oceni zahtevane stopnje varovanja potrebni skrben pristop in izkušnje. Temeljnega pomena je, da stopnja varovanja ustreza kritični varnostni stopnji vsakega posameznega podatka in gradiva, ki ga je treba zavarovati. Da bi zagotovili nemoten pretok podatkov, se sprejmejo ukrepi za izognitev tako njihovi previsoki kot prenizki stopnji tajnosti.

(b) Sistem določanja stopenj tajnosti je sredstvo, ki omogoča uveljavitev teh načel; pri načrtovanju in organiziranju metod za boj proti vohunstvu, sabotažam, terorizmu in drugim nevarnostim se upošteva podoben sistem določanja stopenj tajnosti, tako da je najpomembnejšim prostorom, v katerih so shranjeni tajni podatki, in najobčutljivejšim točkam znotraj njih zagotovljena največja mera varovanja.

(c) Za določanje stopenj tajnosti podatkov je odgovorna izključno oseba izvora podatka.

(d) Stopnja tajnosti lahko temelji izključno na vsebini podatka.

(e) Kadar se različni podatki povežejo v celoto, velja za celoto stopnja tajnosti, ki je tako visoka kot najvišja stopnja posameznega podatka. Zbirka podatkov pa se lahko uvrsti višje kot njeni sestavni deli.

(f) Stopnje tajnosti se določijo samo takrat, kadar je potrebno in samo za tako dolgo kot je potrebno.

4.4 **Cilji varnostnih ukrepov**

Varnostni ukrepi:

(a) veljajo za vse osebe, ki imajo dostop do tajnih podatkov, za nosilce tajnih podatkov, za vse prostore, v katerih se nahajajo taki podatki in za pomembne objekte;

(b) so načrtovani tako, da odkrivajo osebe, ki bi s svojim položajem lahko ogrozile varnost tajnih podatkov in pomembnih objektov, v katerih se tajni podatki nahajajo, in da omogočijo njihovo izključitev ali odstranitev;

(c) vsem nepooblaščenim osebam onemogočajo dostop do tajnih podatkov ali do objektov, v katerih se ti nahajajo;

(d) zagotavljajo, da se tajni podatki razširjajo samo na podlagi „potrebe vedeti“, ki je temeljno načelo vseh vidikov v zvezi z varnostjo;

(e) zagotavljajo celovitost (t. j. preprečujejo ponarejanje ali nedovoljeno spreminjanje ali nedovoljen izbris) in razpoložljivost (t. j. da dostop ni prepovedan tistim, ki ga potrebujejo in so zanj pooblaščeni) vseh podatkov, bodisi tajnih ali ne, in še zlasti takih podatkov, ki so shranjeni, obdelani ali se prenašajo v elektromagnetni obliki.

5. ORGANIZACIJA VARNOSTI

5.1 **Skupni minimalni standardi**

Komisija zagotovi, da vsi prejemniki tajnih podatkov EU upoštevajo skupne minimalne standarde varnosti znotraj institucije in na podlagi njene pristojnosti, t. j. vse službe in izvajalci, tako da se tajni podatki EU lahko posredujejo z zaupanjem, da se bo z njimi ravnalo enako skrbno. Taki minimalni standardi vključujejo merila za preverjanje varnostne zanesljivosti osebja in postopke za varovanje tajnih podatkov EU.

Komisija omogoči dostop do tajnih podatkov EU zunanjim telesom samo pod pogojem, da zagotovijo, da se pri ravnanju s tajnimi podatki EU upoštevajo predpisi, ki so najmanj enakovredni tem minimalnim standardom.

5.2 **Organizacija**

Varnost v okviru Komisije je organizirana na dveh ravneh:

(a) na ravni Komisije kot celote je Varnostni urad Komisije s Službo za akreditacijo varnosti (SAA), ki deluje tudi kot Kripto služba (CrA) ter kot TEMPEST služba, in s službo INFOSEC (IA) in z eno ali več centralnimi registraturami tajnih podatkov EU, vsak z enim ali več registrskim nadzornim uradnikom (RCO).

(b) na ravni služb Komisije je za varnost odgovoren eden ali več lokalnih varnostnih uradnikov (LSO), eden ali več varnostnih uradnikov za centralno informatiko (CISO), lokalni varnostni uradniki za informatiko (LISO) in lokalne registrature za tajne podatke EU z enim ali več registrskimi nadzornimi uradniki.

(c) Centralne varnostne službe operativno usmerjajo lokalne varnostne službe.

6. VARNOST OSEBJA

6.1 **Varnostno preverjanje osebja**

Vse osebe, ki potrebujejo dostop do podatkov, določenih kot CONFIDENTIEL UE ali z višjo stopnjo, morajo biti ustrezno varnostno preverjene, preden se jim dovoli tak dostop. Podobno varnostno preverjanje se zahteva za osebe, katerih delovne naloge vključujejo tehnično delovanje ali vzdrževanje komunikacijskih in informacijskih sistemov, ki vsebujejo tajne podatke. Namen takega varnostnega preverjanja je ugotoviti, če take osebe:

(a) izražajo nedvomno lojalnost;

(b) imajo take osebnostne lastnosti in diskretnost, ki ne dopuščajo dvomov o njihovi integriteti pri ravnanju s tajnimi podatki, ali

(c) morda lahko hitro pridejo pod vpliv tujih ali drugih virov.

V postopkih varnostnega preverjanja se posebej natančno preverijo osebe:

(d) ki naj bi dobile dostop do podatkov TRÈS SECRET UE;

(e) ki zasedajo položaje, ki vključujejo redni dostop do velikega števila podatkov SECRET UE;

(f) ki imajo zaradi delovnih dolžnosti poseben dostop do varnih komunikacijskih ali informacijskih sistemov in s tem priložnost nedovoljenega dostopa do velikih količin tajnih podatkov EU ali povzročitve resne škode izvedbi naloge z dejanji tehnične sabotaže.

V okoliščinah, navedenih v pododstavkih (d), (e) in (f) se v največji možni meri uporablja metoda ugotavljanja zanesljivosti.

Če naj bi se osebe, za katere ne velja „potreba vedeti", zaposlile v okoliščinah, v katerih bi lahko imele dostop do tajnih podatkov EU (npr. sli, varnostni agenti, vzdrževalno in čistilno osebje itd.), morajo biti najprej ustrezno varnostno preverjene.

6.2 **Evidenca varnostnega preverjanja osebja**

Vse službe Komisije, ki imajo opravka s tajnimi podatki EU ali pri katerih se nahajajo varni komunikacijski ali informacijski sistemi, vodijo evidenco varnostnega preverjanja oseb, ki so jim dodeljene. Vsako potrdilo o varnostnem preverjanju se odvisno od okoliščin preveri, da se zagotovi njegova ustreznost za tekočo zadolžitev osebe; potrdilo se ponovno preveri kot prednostna zadeva vsakič ob prejemu novega podatka o tem, da nadaljnje delo s tajnimi podatki ni več v skladu z varnostnimi interesi. Lokalni varnostni uradnik službe Komisije vodi evidenco o varnostnem preverjanju oseb na svojem področju.

6.3 **Varnostna navodila za osebje**

Vse osebje na delovnih mestih, na katerih bi lahko imelo dostop do tajnih podatkov, mora biti ob začetku izvajanja nalog in v rednih časovnih presledkih temeljito seznanjeno s potrebo po varnosti in z ustreznimi postopki za njihovo izvajanje. Od takega osebja se zahteva, da pisno potrdi, da je prebralo in popolnoma razumelo veljavne predpise o varnosti.

6.4 **Odgovornosti vodstvenega osebja**

Vodstveno osebje mora biti seznanjeno, kateri sodelavci imajo pri svojem delu opravka s tajnimi podatki ali imajo dostop do zavarovanih komunikacijskih ali informacijskih sistemov in za evidentiranje ter poročanje o vseh incidentih ali očitnih slabostih, ki bi lahko imeli posledice za varnost.

6.5 **Varnostni status osebja**

Določijo se postopki, v katerih se v primeru ugotovitve negativnih podatkov o posamezniku ugotavlja, ali ima pri svojem delu opravka s tajnimi podatki in ali ima dostop do zavarovanih komunikacijskih ali informacijskih sistemov, o čemer se obvesti Varnostni urad Komisije. Če se ugotovi, da tak posameznik pomeni tveganje za varnost, se mu prepreči opravljanje nalog, kjer bi lahko škodoval interesom varnosti.

7. MATERIALNA VARNOST

7.1 **Potreba po varovanju**

Stopnja ukrepov materialne varnosti, ki se uporabljajo za zagotavljanje varovanja tajnih podatkov EU je v sorazmerju z določeno stopnjo tajnosti, obsegom in ogroženostjo shranjenih podatkov in gradiva. Vsi imetniki tajnih podatkov EU v zvezi s stopnjo tajnosti teh podatkov upoštevajo enotne prakse in izpolnjujejo skupne standarde glede varovanja, prenosa in uničenja podatkov in gradiva, ki zahteva varovanje.

7.2 **Preverjanje**

Pred odhodom s področij, kjer se nahajajo tajni podatki EU brez nadzora, zagotovijo osebe, ki so zadolžene za njihov nadzor, da so ti varno shranjeni in da so aktivirane vse varnostne naprave (ključavnice, alarmi itd.). Dodatna neodvisna preverjanja se izvajajo po izteku delovnega časa.

7.3 **Varnost zgradb**

Zgradbe, v katerih se nahajajo tajni podatki EU ali varni komunikacijski in informacijski sistemi, se zavarujejo pred dostopom nepooblaščenih oseb. Vrsta varovanja tajnih podatkov EU, npr. rešetke na oknih, vratne ključavnice/zapahi, vhodna straža, samodejni sistemi nadzora dostopa, varnostna preverjanja in obhodne patrulje, alarmni sistemi, sistemi odkrivanja dejavnosti nepooblaščenih oseb in psi čuvaji, je odvisna od:

(a) stopnje tajnosti in količine varovanih podatkov in gradiva ter njihove lokacije v stavbi;

(b) kvalitete varnostnih vsebnikov za hranjenje takih podatkov in gradiva; in

(c) tehničnih značilnosti in lokacije zgradbe.

Podobno je vrsta varovanja komunikacijskih in informacijskih sistemov odvisna od ocene vrednosti udeleženih sredstev in morebitne škode, ki bi lahko nastala v primeru ogrožanja varnosti, od fizičnih značilnosti in lokacije zgradbe, v kateri se sistem nahaja, ter od lokacije sistema v zgradbi.

7.4 **Načrt ukrepov ob nepredvidljivih dogodkih**

Pripravijo se podrobni načrti za varovanje tajnih podatkov v izrednih razmerah na lokalni ali državni ravni.

8. VAROVANJE PODATKOV

Varovanje podatkov (INFOSEC) se nanaša na opredelitev in uporabo varnostnih ukrepov za varovanje tajnih podatkov EU, ki se obdelujejo, hranijo ali prenašajo s komunikacijskimi, informacijskimi in drugimi elektronskimi sistemi pred izgubo tajnosti, celovitosti ali razpoložljivosti, bodisi slučajne ali namerne. Sprejmejo se primerni protiukrepi za preprečevanje dostopa do tajnih podatkov EU nepooblaščenim uporabnikom, preprečevanje onemogočanja dostopa do tajnih podatkov EU pooblaščenim uporabnikom in za preprečevanje ponarejanja ali nepooblaščenega spreminjanja ali brisanja tajnih podatkov EU.

9. UKREPI PROTI SABOTAŽAM IN NADZOR NAD DRUGIMI OBLIKAMI NAKLEPNEGA POŠKODOVANJA

Materialni previdnostni ukrepi za varovanje pomembnih objektov, v katerih se nahajajo tajni podatki, so najboljša varovalka pred sabotažami in naklepnim poškodovanjem in samo varnostno preverjanje osebja še ne pomeni učinkovitega nadomestila. Pristojni državni organ se zadolži za zbiranje podatkov glede vohunstva, sabotaž, terorizma in drugih subverzivnih dejavnosti.

10. POSREDOVANJE TAJNIH PODATKOV TRETJIM DRŽAVAM ALI MEDNARODNIM ORGANIZACIJAM

Odločitev o posredovanju tajnih podatkov EU z izvorom v Komisiji tretji državi ali mednarodni organizaciji sprejme Komisija kot kolegijski organ. Če organ izvora podatka, za katerega je posredovanje zaželeno, ni Komisija, Komisija organ izvora najprej zaprosi za njegov pristanek glede posredovanja. Če organa izvora ni mogoče ugotoviti, njegovo odgovornost prevzame Komisija.

Če Komisija prejme tajne podatke iz tretjih držav, mednarodnih organizacij ali od drugih tretjih strani, se ti podatki primerno zavarujejo glede na njihovo stopnjo tajnosti in enakovredno varovanje glede na standarde, določene v tem pravilniku, ki veljajo za tajne podatke EU, ali glede na take višje standarde, ki bi jih pri posredovanju podatkov lahko zahtevala tretja stran. Mogoče se je dogovoriti za vzajemni nadzor.

Zgornja načela se izvajajo v skladu s podrobnimi določbami, določenimi v Delu II, Oddelek 26 in Dodatkih 3, 4 in 5.

DEL II: ORGANIZACIJA VARNOSTI V KOMISIJI

11. ČLAN KOMISIJE, PRISTOJEN ZA VARNOSTNE ZADEVE

Član Komisije, pristojen za varnostne zadeve:

(a) izvaja varnostno politiko Komisije;

(b) preučuje varnostna vprašanja, ki mu jih predloži Komisija ali njena pristojna telesa;

(c) v sodelovanju z organi, pristojnimi za državno varnost (ali drugimi primernimi organi) držav članic (v nadaljnjem besedilu „NSA“) preučuje vprašanja v zvezi s spremembami varnostne politike Komisije.

Član Komisije, pristojen za varnostne zadeve, skrbi zlasti za:

(a) usklajevanje vseh varnostnih zadev v zvezi z dejavnostmi Komisije;

(b) naslavljanje zahtev uradno imenovanim organom držav članic za izdajo varnostnih dovoljenj osebju, zaposlenemu v Komisiji, s strani organov, pristojnih za državno varnost, v skladu z oddelkom 20;

(c) opravljanje preiskav ali vlaganje zahtev za preiskave v zvezi z vsemi odtekanji tajnih podatkov EU, za kar je predvidoma treba najti vzrok v Komisiji;

(d) predložitev zahtev ustreznim varnostnim organom, da uvedejo preiskave, če se zdi, da se je pojavilo odtekanje tajnih podatkov EU iz Komisije, in usklajevanje poizvedb, kadar je vpleten več kot en varnostni organ;

(e) stalen nadzor nad varnostno ureditvijo za varovanje tajnih podatkov EU;

(f) ohranjanje tesne povezave z vsemi zadevnimi varnostnimi organi zaradi doseganja vsesplošne varnostne usklajenosti;

(g) nenehno preverjanje varnostne politike Komisije in postopkov ter, če se to zahteva, pripravljanje ustreznih priporočil. Glede tega član Komisije, pristojen za varnostna vprašanja, Komisiji predloži letni načrt inšpekcijskih pregledov, ki ga pripravi Varnostna služba Komisije.

12. SVETOVALNA SKUPINA ZA VARNOSTNO POLITIKO KOMISIJE

Ustanovi se svetovalna skupina za varnostno politiko Komisije. Sestavljajo jo član/članica Komisije, pristojen/pristojna za varnostna vprašanja, ali njegov/njen namestnik, ki predseduje skupini, ter predstavniki organov, pristojnih za državno varnost (NSA) vsake države članice. Vabljeni so lahko tudi predstavniki drugih evropskih institucij. Poleg njih so lahko vabljeni tudi predstavniki ustreznih decentraliziranih agencij ES in EU, kadar se obravnavajo vprašanja v zvezi z njimi.

Svetovalna skupina za varnostno politiko Komisije se sestane na zahtevo njenega predsednika ali katerega koli od njenih članov. Naloga skupine je, da pregleda in oceni vsa ustrezna varnostna vprašanja in, če je potrebno, posreduje priporočila Komisiji.

13. VARNOSTNI ODBOR KOMISIJE

Ustanovi se Varnostni odbor Komisije. Sestavljajo ga generalni sekretar, ki predseduje Varnostnemu odboru, generalni direktorji Pravne službe, Službe za kadrovske zadeve in administracijo, Službe za zunanje odnose, pravosodja in notranjih zadev in Skupnega raziskovalnega centra ter vodje Službe za notranjo revizijo in Varnostnega urada Komisije. Vabljeni so lahko tudi drugi uradniki Komisije. Odbor je pristojen za oceno varnostnih ukrepov v okviru Komisije in sestavo priporočil s tega področja za člana Komisije, pristojnega za varnostne zadeve.

14. VARNOSTNI URAD KOMISIJE

Članu Komisije, pristojnemu za varnostne zadeve, pri opravljanju njegovih nalog iz oddelka 11, kot so usklajevanje, nadzor in izvajanje varnostnih ukrepov, pomaga Varnostni urad Komisije.

Vodja Varnostnega urada Komisije je glavni svetovalec člana Komisije, pristojnega za varnostne zadeve, kateremu svetuje glede varnostnih zadev in opravlja dolžnosti sekretarja Svetovalne skupine za varnostno politiko. V zvezi s tem je pristojen za pripravo potrebnih sprememb varnostnih predpisov in usklajuje varnostne ukrepe s pristojnimi organi držav članic ter, kjer je primerno, z mednarodnimi organizacijami, ki so s Komisijo sklenile varnostne sporazume. V ta namen opravlja naloge uradnika za zvezo.

Vodja Varnostnega urada Komisije je odgovoren za akreditacijo sistemov in omrežij informacijske tehnologije (IT) v okviru Komisije. Vodja Varnostnega urada Komisije se v soglasju s pristojnim organom za državno varnost (NSA) odloči o akreditaciji sistemov in omrežij IT, ki vključujejo na eni strani Komisijo na drugi pa katerega koli prejemnika tajnih podatkov EU.

15. VARNOSTNI PREGLEDI

Varnostni urad Komisije za varovanje tajnih podatkov EU opravlja redne preglede varnostne ureditve.

Varnostnemu uradu Komisije pri opravljanju te naloge lahko pomagajo varnostne službe drugih institucij EU, ki imajo tajne podatke EU, ali organi, pristojni za državno varnost (NSA) države članice ([1]).

Na zahtevo države članice lahko pregled tajnih podatkov EU opravi njen organ, pristojen za državno varnost (NSA) v okviru Komisije skupaj z Varnostno službo Komisije na podlagi medsebojnega dogovora.

([1]) Brez vpliva na Dunajsko konvencijo iz leta 1961 o diplomatskih odnosih in Protokol o posebnih privilegijih in imunitetah Evropskih Skupnosti z dne 8. aprila 1965.

16. STOPNJE TAJNOSTI, VARNOSTNI OZNAČEVALNIKI IN OZNAKE

16.1 **Stopnje tajnosti** [1]

Tajni podatki imajo naslednje stopnje tajnosti (glej tudi Dodatek 2):

TRÈS SECRET UE: ta stopnja tajnosti se uporablja le za podatke in gradivo, katerega nedovoljeno razkritje bi lahko povzročilo izjemno težke posledice za temeljne interese Evropske unije in ene ali več njenih držav članic.

SECRET UE: ta stopnja tajnosti se uporablja le za podatke in gradivo, katerega nedovoljeno razkritje bi lahko resno škodovalo temeljnim interesom Evropske unije ali ene ali več njenih držav članic.

CONFIDENTIEL UE: ta stopnja tajnosti se uporablja za podatke in gradivo, katerega nedovoljeno razkritje bi lahko škodovalo temeljnim interesom Evropske unije ali ene ali več njenih držav članic.

RESTREINT UE: ta stopnja tajnosti se uporablja le za podatke in gradivo, katerega nedovoljeno razkritje bi lahko bilo škodljivo za interese Evropske unije ali ene ali več njenih držav članic.

Druge stopnje tajnosti niso dopustne.

16.2 **Varnostni označevalniki**

Da bi se določile meje veljavnosti stopenj tajnosti (za tajne podatke, ki pomenijo avtomatično znižanje stopnje tajnosti ali odpravo stopnje tajnosti), se lahko uporabi dogovorjen varnostni označevalnik. Ta označevalnik se glasi bodisi „DO … (čas/datum)“ bodisi „DO … (dogodek)“.

Dodatni varnostni označevalniki, kot so označevalniki KRIPTO ali katerikoli drugi varnostni označevalnik, ki ga priznava EU, se uporabljajo v primeru potrebe po omejenem pošiljanju in posebnem ravnanju poleg tistega, ki je že označen s stopnjo tajnosti.

Varnostni označevalniki se uporabijo le skupaj s stopnjo tajnosti.

16.3 **Oznake**

Oznaka se lahko uporabi za določanje področja, ki ga pokriva dokument, ali določenega pošiljanja na podlagi „potrebe vedeti“ ali zato (pri podatkih, ki niso tajni), da se označi konec embarga.

Oznaka ni stopnja tajnosti in se ne sme uporabiti namesto nje.

Oznaka EVOP se uporabi pri dokumentih in njihovih kopijah v zvezi z varnostjo in obrambo Unije ali ene ali več njenih držav članic ali v zvezi z vojaškim ali nevojaškim kriznim upravljanjem.

16.4 **Namestitev stopenj tajnosti**

Stopnja tajnosti se označi:

(a) na dokumentih RESTREINT UE z mehanskimi ali elektronskimi sredstvi;

(b) na dokumentih CONFIDENTIEL UE z mehanskimi sredstvi, ročno ali s tiskanjem na predhodno žigosan, registrirani papir;

(c) na dokumentih SECRET UE in TRÈS SECRET UE z mehanskimi sredstvi ali ročno.

16.5 **Namestitev varnostnih označevalnikov**

Varnostni označevalniki se namestijo neposredno pod stopnjo tajnosti z uporabo enakih sredstev kot pri namestitvi stopenj tajnosti.

[1] Glej primerjalno tabelo varnostnih klasifikacij EU, NATO, ZEU in držav članic v Dodatku 1.

17. MERILA ZA DOLOČANJE STOPENJ TAJNOSTI

17.1 **Splošno**

Podatki se določijo kot tajni podatki le, če je to potrebno. Stopnja tajnosti se jasno in pravilno označi ter se ohrani samo toliko časa, kot je potrebno za varovanje podatkov.

Za določitev stopnje tajnosti podatka ter vsako znižanje stopnje tajnosti ali odpravo stopnje tajnosti je odgovorna samo oseba izvora.

Uradniki in drugi uslužbenci v Komisiji določajo stopnje tajnosti podatkom, jim znižujejo ali odpravljajo stopnje tajnosti po navodilu ali v dogovoru z vodjo službe.

Podrobni postopki za ravnanje s tajnimi dokumenti so določeni tako, da tem dokumentom zagotavljajo varovanje, ki ustreza podatkom, ki jih vsebujejo.

Število oseb, ki so pooblaščene za pripravo dokumentov TRÈS SECRET UE, se ohrani na minimumu, njihova imena pa se vnesejo v seznam, ki ga vodi Varnostni urad Komisije.

17.2 **Uporaba stopenj tajnosti**

Stopnja tajnosti dokumenta se določi glede na občutljivost njegove vsebine v skladu z opredelitvijo iz oddelka 16. Pomembno je, da se stopnja tajnosti uporablja na pravilen način in glede na stvarne potrebe. To zlasti velja za stopnjo tajnosti TRÈS SECRET UE.

Pri stopnji tajnosti dokumenta oseba izvora tega dokumenta upošteva zgoraj navedena pravila in se izogiba vsakršni težnji po previsoki ali prenizki stopnji tajnosti.

Navodilo za uporabo stopenj tajnosti je v Dodatku 2.

Za posamezne strani, odstavke, oddelke, priloge, dodatke, dodane in priložene dele posameznega dokumenta se lahko določijo različne stopnje tajnosti. Stopnja tajnosti dokumenta kot celote je tista, ki velja za njegov del, označen z najvišjo stopnjo tajnosti.

Stopnja tajnosti pisma ali zabeležke k priloženim delom je enaka najvišji stopnji tajnosti njenih priloženih delov. Če je pismo ali zabeležka ločena od priloženih delov, mora oseba izvora jasno določiti stopnjo tajnosti.

Dostop javnosti še naprej ureja Uredba (ES) št. 1049/2001.

17.3 **Zniževanje in odprava stopenj tajnosti**

Tajnim podatkom EU se lahko zniža ali odpravi stopnja tajnosti samo z dovoljenjem osebe izvora in, če je potrebno, po posvetovanju z drugimi zainteresiranimi stranmi. Zniževanje ali odprava stopenj tajnosti se potrdi pisno. Oseba izvora je dolžna o spremembi obvestiti svoje naslovnike, ti pa so dolžni o tej spremembi obvestiti vse nadaljnje naslovnike, katerim so poslali ali jim kopirali dokument.

Če je mogoče, osebe izvora na tajnem dokumentu določijo datum, čas ali dogodek, v katerem je vsebini mogoče znižati ali odpraviti stopnjo tajnosti. V nasprotnem primeru osebe izvora preverjajo dokumente najpozneje vsakih pet let, da bi zagotovili potrebno izvorno stopnjo tajnosti.

18. MATERIALNA VARNOST

18.1 **Splošno**

Glavni cilji ukrepov materialne varnosti so nepooblaščeni osebi preprečiti dostop do tajnih podatkov in/ali gradiva EU, preprečiti krajo ali poškodbo opreme in druge lastnine ter onemogočiti motenje osebja, drugih zaposlenih in obiskovalcev ali druge oblike pritiska na njih.

18.2 **Varnostne zahteve**

Vsi objekti, območja, zgradbe, prostori, komunikacijski in informacijski sistemi itd., v katerih se hranijo in/ali obdelujejo tajni podatki in gradivo EU, se zavarujejo z ustreznimi ukrepi materialne varnosti.

Pri odločanju o potrebni ravni ukrepov materialne varnosti je treba upoštevati vse pomembne dejavnike, kot so:

(a) stopnja tajnosti podatkov in/ali gradiva;

(b) količina in oblika (npr. papir, računalniški nosilci shranjevanja) varovanih podatkov;

(c) lokalno oceno nevarnosti s strani obveščevalnih služb, katerih delovanje je usmerjeno proti EU, državam članicam in/ali drugim institucijam ali tretjim strankam, ki razpolagajo s tajnimi podatki EU, in sicer v zvezi s sabotažami, terorizmom ter drugimi subverzivnimi in/ali kriminalnimi dejavnostmi.

Ukrepi materialne varnosti se načrtujejo zaradi:

(a) preprečevanja skrivnih ali nasilnih vdorov nepooblaščenih oseb;

(b) odvračanja, oviranja in odkrivanja dejanj nelojalnih članov osebja;

(c) onemogočanja dostopa do tajnih podatkov EU tistim, od katerih se ne zahteva, da so z njimi seznanjeni.

18.3 **Ukrepi materialne varnosti**

18.3.1 *Varnostna območja*

Območja, kjer se obdelujejo ali shranjujejo podatki s stopnjo tajnosti CONFIDENTIEL UE ali z višjo stopnjo tajnosti, se uredijo in strukturirajo tako, da ustrezajo eni od naslednjih kategorij:

(a) Varnostno območje razreda I: območje, kjer se podatki CONFIDENTIEL UE ali podatki z višjo stopnjo tajnosti obdelujejo in shranjujejo tako, da vstop na to območje dejansko pomeni dostop do tajnih podatkov. Za takšno območje se zahteva:

   (i) jasno določen in zavarovan obseg prostora, prek katerega se nadzorujejo vsi vhodi in izhodi;

   (ii) sistem vhodnega nadzora, ki vstop na območje dovoljuje samo ustrezno preverjenim in posebno pooblaščenim osebam;

   (iii) podroben opis stopnje tajnosti podatkov, ki se običajno hranijo na takem območju, tj. podatkov, ki z vstopom na območje postanejo dostopni.

(b) Varnostno območje razreda II: območje, kjer se podatki CONFIDENTIEL UE ali podatki z višjo stopnjo tajnosti obdelujejo in shranjujejo tako, da so pred dostopom nepooblaščenih oseb varovani s pomočjo notranjega nadzora, npr. objekti, kjer so službe, v katerih se redno obdelujejo in shranjujejo podatki CONFIDENTIEL UE ali podatki z višjo stopnjo tajnosti. Za takšno območje se zahteva:

   (i) jasno določen in zavarovan obseg prostora, prek katerega se nadzorujejo vsi vhodi in izhodi;

   (ii) sistem vhodnega nadzora, ki vstop na območje dovoljuje samo ustrezno preverjenim in posebno pooblaščenim osebam. Za vse druge osebe se zahteva spremstvo ali enakovreden nadzor, ki nepooblaščenim osebam preprečuje dostop do tajnih podatkov EU in nenadzorovan vstop na območja, ki so predmet tehničnih varnostnih inšpekcijskih pregledov.

   Tista območja, na katerih uslužbenci niso prisotni 24 ur na dan, se pregledajo takoj po izteku normalnega delovnega časa, da se zagotovi ustrezno zavarovanje tajnih podatkov EU.

18.3.2 *Upravno območje*

Okoli varnostnih območij razreda I in razreda II ali v smereh, ki vodijo na ta območja, se lahko vzpostavi upravno območje z nižjo stopnjo varovanja. Za tako območje se zahteva vidno določen obseg prostora, ki omogoča preverjanje osebja in vozil. V teh območjih se obdelujejo in shranjujejo samo podatki RESTREINT UE. in podatki, ki niso označeni s stopnjo tajnosti.

18.3.3 *Vhodni in izhodni nadzor*

Vhod v varnostna območja razreda I in razreda II in izhod iz njih se nadzoruje z dovolilnico ali s sistemom prepoznavanja oseb, ki velja za celotno osebje, ki običajno dela na teh območjih. Za preprečevanje nepooblaščenega dostopa do tajnih podatkov EU se vzpostavi tudi sistem preverjanja obiskovalcev. Sistem dovolilnic lahko dopolnjuje samodejno prepoznavanje kot dopolnilo k varnostnemu osebju, vendar ga v celoti ne nadomešča. Sprememba ocene ogrožanja lahko ima za posledico okrepitev ukrepov vhodnega in izhodnega nadzora, na primer med obiskom uglednih oseb.

18.3.4 *Varnostni obhodi*

Obhodi varnostnih območij razreda I in razreda II se morajo opravljati izven običajnega delovnega časa, da bi se premoženje EU zavarovalo pred ogrožanjem, poškodovanjem ali izgubo. Pogostost obhodov se določa glede na lokalne pogoje, vendar morajo obhodi praviloma potekati vsaki dve uri.

18.3.5 *Varnostni vsebniki in prostori-trezorji*

Za hranjenje tajnih podatkov EU se uporabljajo trije razredi vsebnikov:

— Razred A: vsebniki, ki so na nacionalni ravni odobreni za hranjenje tajnih podatkov TRÈS SECRET UE na varnostnih območjih razreda I ali razreda II;

— Razred B: vsebniki, ki so na nacionalni ravni odobreni za hranjenje tajnih podatkov SECRET UE in CONFIDENTIEL UE na varnostnih območjih razreda I ali razreda II;

— Razred C: pisarniško pohištvo, primerno samo za hranjenje tajnih podatkov RESTREINT UE.

V prostorih-trezorjih, zgrajenih na varnostnih območjih razreda I in razreda II in za vsa varnostna območja razreda I, kjer se tajni podatki CONFIDENTIEL UE in podatki z višjo stopnjo tajnosti hranijo na odprtih policah ali so predstavljeni na grafičnih prikazih, kartah/zemljevidih itd., mora stene, tla, strope in vrata s ključavnico(ami) potrditi Služba za akreditacijo varnosti (SAA) kot takšne, ki zagotavljajo enakovredno varovanje, kot jo zagotavlja razred varnostnih vsebnikov, odobrenih za shranjevanje tajnih podatkov iste stopnje tajnosti.

18.3.6 *Ključavnice*

Ključavnice, ki se uporabljajo pri varnostnih vsebnikih in prostorih-trezorjih, v katerih se hranijo tajni podatki EU, ustrezajo naslednjim standardom:

— Skupina A: biti morajo odobrene na nacionalni ravni za vsebnike razreda A;

— Skupina B: biti morajo odobrene na nacionalni ravni za vsebnike razreda B;

— Skupina C: biti morajo primerne samo za uporabo na pisarniškem pohištvu razreda C.

18.3.7 *Nadzor nad ključi in kombinacijami*

Ključi varnostnih vsebnikov se ne smejo nositi iz stavb Komisije. Nastavitve kombinacij za varnostne vsebnike si morajo osebe, ki jih morajo poznati, zapomniti. Nadomestni ključi in pisni zapisi vseh nastavitev kombinacij za uporabo v nujnih primerih so pri lokalnem varnostnem uradniku, zadolženem za varnost v pristojni službi Komisije; zapisi se hranijo ločeno, v zapečatenih neprozornih ovojnicah. Delovni ključi, nadomestni varnostni ključi in nastavitve kombinacij se hranijo v ločenih varnostnih vsebnikih. Za te ključe in nastavitve kombinacij mora biti zagotovljeno enako strogo varovanje kakor za gradivo, do katerega omogočajo dostop.

Poznavanje nastavitev kombinacij varnostnih vsebnikov je omejeno na najmanjše možno število oseb. Kombinacije se spremenijo:

(a) ob prejemu novega vsebnika;

(b) ob vsaki zamenjavi osebja;

(c) ob vsakem dejanskem ali predvidenem ogrožanju;

(d) po možnosti v presledkih šestih mesecev ali vsaj vsakih 12 mesecev.

18.3.8 *Naprave za odkrivanje dejavnosti nepooblaščenih oseb*

Če se za varovanje tajnih podatkov EU uporabljajo alarmni sistemi, televizija zaprtega kroga in druge električne naprave, mora biti na voljo rezervno električno napajanje, ki v primerih prekinitve glavnega električnega napajanja zagotavlja neprekinjeno delovanje sistema. Druga temeljna zahteva je, da se v primeru okvare v delovanju takšnih sistemov ali manipuliranju z njimi sproži ustrezen alarm ali kakšno drugo zanesljivo opozorilo nadzornemu osebju.

18.3.9 *Odobrena oprema*

Varnostni urad Komisije vodi in dopolnjuje sezname varnostne opreme po tipih in modelih, ki jo je odobril zaradi neposrednega ali posrednega varovanja tajnih podatkov v različnih razmerah in pogojih. Varnostni urad Komisije med drugim te sezname utemeljuje na podatkih organa, pristojnega za državno varnost (NSA).

18.3.10 *Fizično varovanje fotokopirnih strojev in telefaksov*

Fotokopirni stroji in telefaksi se fizično varujejo v potrebnem obsegu, s čimer se zagotovi, da jih lahko uporabljajo le pooblaščene osebe za obdelavo tajnih podatkov in da so vsi tajni podatki pod primernim nadzorom.

18.4 **Varovanje pred vpogledom in pred prisluškovanjem**

18.4.1 *Varovanje pred vpogledom*

Podnevi in ponoči se izvajajo vsi ustrezni ukrepi, ki zagotavljajo, da tajnih podatkov EU ne more videti, niti po naključju, nobena nepooblaščena oseba.

18.4.2 *Varovanje pred prisluškovanjem*

Pisarniški prostori ali območja, v katerih se redno razpravlja o podatkih s stopnjo tajnosti SECRET UE ali z višjo stopnjo tajnosti, se v primerih tveganja zavarujejo pred pasivnimi ali aktivnimi poskusi prisluškovanja. Za oceno tveganja takšnih poskusov je zadolžen Varnostni urad Komisije, ki se po potrebi posvetuje z organi, pristojnimi za državno varnost (NSA).

18.4.3 *Vnos elektronske in snemalne opreme*

Na varnostna območja ali tehnično zavarovana območja ni dovoljeno vnašati mobilnih telefonov, zasebnih računalnikov, snemalnih naprav, kamer in drugih elektronskih ali snemalnih naprav brez predhodnega dovoljenja vodje Varnostnega urada Komisije.

Pri določanju varnostnih ukrepov za prostore, ki so občutljivi na pasivno prisluškovanje (npr. izolacija zidov, tal, vrat, stropov, merjenja jakosti zvoka) in za aktivno prisluškovanje (npr. iskanje mikrofonov), lahko Varnostni urad Komisije zahteva pomoč strokovnjakov organov, pristojnih za državno varnost (NSA).

Podobno lahko, kadar tako zahtevajo okoliščine, strokovnjaki za tehnično varnost pri organih, pristojnih za državno varnost (NSA) na zahtevo vodje Varnostnega urada Komisije pregledajo telekomunikacijsko opremo in kakršno koli električno ali elektronsko pisarniško opremo, ki je bila uporabljena med sestanki stopnje SECRET UE ali višje stopnje.

18.5 **Tehnično varovana območja**

Nekatera območja se lahko določijo kot tehnično varovana območja. Ob vstopu vanje se izvede poseben pregled. Če v njih ni osebja, taka območja ostanejo zaklenjena po odobrenem postopku, vsi ključi pa se obravnavajo kot varnostni ključi. Taka območja so predmet rednih pregledov v okviru varovanja stavb, ki se opravijo tudi po dejanskem vstopu ali sumu vstopa nepooblaščenih oseb.

Vodi se natančen popis opreme in pohištva zaradi nadzora in spremembe njihove lokacije. V tako območje se ne sme vnesti nikakršen kos pohištva ali opreme, dokler ga posebno za to usposobljeno varnostno osebje skrbno ne pregleda zaradi odkritja morebitnih prisluškovalnih naprav. Splošno pravilo je, da namestitev komunikacijskih vodov na tehnično zavarovana območja ni dovoljena brez predhodnega pooblastila pristojnega organa.

19. SPLOŠNA PRAVILA O NAČELU POTREBE VEDETI IN VARNOSTNEM PREVERJANJU OSEBJA EU

19.1 **Splošno**

Dostop do tajnih podatkov EU se dovoli samo osebam, za katere zaradi opravljanja njihovih dolžnosti ali nalog velja „potreba vedeti“. Dostop do podatkov TRÈS SECRET UE, SECRET UE in CONFIDENTIEL UE se odobri le osebam, ki so varnostno preverjene.

Za določitev oseb, za katere velja „potreba vedeti“, je pristojna služba, v kateri se namerava zadevna oseba zaposliti.

Varnostno preverjanje osebja zahteva posamezna služba.

Ob koncu postopka se izda „varnostno potrdilo EU za osebje“, ki določa stopnjo tajnosti podatkov, do katerih lahko ima preverjena oseba dostop, in datum prenehanja veljavnosti potrdila.

Varnostno potrdilo EU za osebje, izdano za določeno stopnjo tajnosti, imetniku omogoči dostop do podatkov z nižjo stopnjo tajnosti.

Osebe, razen uradnikov ali drugih uslužbencev, kot so zunanji pogodbeniki, strokovnjaki ali svetovalci, s katerimi je treba obravnavati ali jim pokazati tajne podatke EU, morajo za tajne podatke EU imeti varnostno potrdilo in biti seznanjeni s svojo odgovornostjo za varnost.

Javni dostop še naprej ureja Uredba (ES) št. 1049/2001.

19.2 **Posebna pravila o dostopu do podatkov TRÈS SECRET UE**

Vse osebe, ki potrebujejo dostop do podatkov TRÈS SECRET UE, morajo najprej opraviti preverjanje za pridobitev dostopa do takih podatkov.

Vse osebe, za katere se zahteva dostop do podatkov TRÈS SECRET UE, imenuje član Komisije, pristojen za varnostne zadeve, njihova imena pa se hranijo v ustreznem registru TRÈS SECRET UE. Ta register vzpostavi in vodi Varnostni urad Komisije.

Vse osebe morajo pred pridobitvijo dostopa do podatkov TRÈS SECRET UE podpisati potrdilo, ki dokazuje, da so bile seznanjene z varnostnimi postopki Komisije in da se v celoti zavedajo svoje posebne odgovornosti za varovanje podatkov TRÈS SECRET UE ter posledic, ki jih predvidevajo predpisi EU in predpisi držav članic, če tajni podatki pridejo v roke nepooblaščeni osebi, bodisi namenoma ali iz malomarnosti.

Za osebe, ki imajo na sestankih itd. dostop do podatkov TRÈS SECRET UE, pristojni uradnik za nadzor službe ali organa, kjer je navedena oseba zaposlena, obvesti organ, ki je sklical sestanek, da zadevne osebe tako dovoljenje imajo.

Imena vseh oseb, ki ne opravljajo več nalog, za katere se zahteva dostop do podatkov TRÈS SECRET UE, se umaknejo s seznama TRÈS SECRET UE. Poleg tega so vse take osebe ponovno opozorjene na njihovo posebno odgovornost glede varovanja podatkov TRÈS SECRET UE. Osebe podpišejo tudi izjavo, s katero potrjujejo, da ne bodo niti uporabljale niti posredovale naprej podatkov TRÈS SECRET UE, s katerimi so se seznanile.

19.3 **Posebna pravila o dostopu do podatkov SECRET UE in CONFIDENTIEL UE**

Vse osebe, ki potrebujejo dostop do podatkov SECRET UE ali CONFIDENTIEL UE, morajo najprej opraviti preverjanje za pridobitev dostopa do ustrezne stopnje tajnosti podatkov.

Vse osebe, ki potrebujejo dostop do podatkov SECRET UE ali CONFIDENTIEL UE, se morajo seznaniti z ustreznimi varnostnimi predpisi in se zavedati posledic malomarnega odnosa do njih.

Za osebe, ki imajo na sestankih itd. dostop do podatkov SECRET UE in CONFIDENTIEL UE, varnostni uradnik organa, kjer je navedena oseba zaposlena, obvesti organ, ki je sklical sestanek, da imajo zadevne osebe tako pooblastilo.

19.4 **Posebna pravila o dostopu do podatkov RESTREINT UE**

Osebe, ki imajo dostop do podatkov RESTREINT UE, so opozorjene na ta pravilnik in posledice malomarnega odnosa do njih.

19.5 **Prenosi**

Če je uslužbenec premeščen z delovnega mesta, na katerem je imel opravka s tajnimi podatki EU, registrski urad nadzoruje, da prenos takih podatkov od odhajajočega k prihajajočemu uslužbencu poteka na pravilen način.

Če je uslužbenec premeščen na drugo delovno mesto, kjer ima opravka s tajnimi podatki EU, ga lokalni varnostni uradnik ustrezno pouči.

19.6 **Posebna navodila**

Osebe, od katerih se zahteva delo s tajnimi podatki EU, je treba ob nastopu dela in nato redno opozarjati na:

(a) nevarnosti za varnost, ki izhajajo iz prostih pogovorov;

(b) previdnostne ukrepe v njihovih odnosih s tiskom in predstavniki posebnih interesnih skupin;

(c) nevarnost, ki jo za EU in države članice v zvezi s tajnimi podatki in dejavnostmi EU predstavlja dejavnost obveščevalnih služb;

(d) obveznost takojšnjega poročanja pristojnim varnostnim organom o vsakem ravnanju, ki bi zbudilo sum o vohunski dejavnosti ali o kakršnih koli nenavadnih okoliščinah v zvezi z varnostjo.

Vse osebe, ki so običajno izpostavljene pogostim stikom s predstavniki držav, katerih obveščevalne službe delujejo proti EU in državam članicam v zvezi s tajnimi podatki in dejavnostmi EU, so poučene o tehnikah, za katere je znano, da jih uporabljajo različne obveščevalne službe.

Za zasebna potovanja osebja, ki je bilo za dostop do tajnih podatkov EU varnostno preverjeno, v katero koli namembno območje, Komisija nima nobenih varnostnih predpisov. Vendar pa Varnostni urad Komisije seznani uradnike in druge uslužbence, ki spadajo v njegovo pristojnost, s pravili potovanja, ki jih bodo morda morali spoštovati.

20. POSTOPEK VARNOSTNEGA PREVERJANJA URADNIKOV IN DRUGIH USLUŽBENCEV KOMISIJE

(a) Samo uradniki in drugi uslužbenci Komisije ali osebe, zaposlene v Komisiji, ki morajo zaradi opravljanja svojih nalog in zahtev službe poznati ali uporabljati tajne podatke Komisije, imajo dostop do takšnih podatkov.

(b) Da bi pridobile dostop do podatkov s stopnjo „TRÈS SECRET UE“, „SECRET UE“ in „CONFIDENTIEL UE“, morajo imeti osebe iz odstavka (a) pooblastilo v skladu s postopkom iz odstavkov (c) in (d) tega oddelka.

(c) Pooblastilo se izda samo osebam, ki so bile varnostno preverjene pri organih, pristojnih za državno varnost v državah članicah (NSA) v skladu s postopkom iz odstavkov (i) do (n).

(d) Vodja Varnostnega urada Komisije je pristojen za izdajanje pooblastil iz odstavkov (a), (b) in (c).

(e) Vodja izda pooblastilo po pridobitvi mnenja pristojnih državnih organov držav članic na podlagi opravljenega varnostnega pregleda, ki s izvede v skladu z odstavki (i) do (n).

(f) Varnostni urad Komisije vodi in dopolnjuje seznam vseh občutljivih mest v posameznih službah Komisije, ter vseh oseb, ki so pridobile (začasno) pooblastilo.

(g) Pooblastilo, ki velja pet let, ne sme presegati časa trajanja nalog, za katere je bilo izdano. V skladu s postopkom iz odstavka (e) se lahko obnovi.

(h) Vodja Varnostnega urada Komisije odvzame pooblastilo, kadar meni, da ima za to upravičene razloge. Vsaka odločitev o odvzemu pooblastila se sporoči zadevni osebi, ki lahko zahteva zaslišanje s strani vodje Varnostnega urada Komisije ali pristojnega državnega organa.

(i) Varnostni pregled se opravi s sodelovanjem zadevne osebe in na zahtevo vodje Varnostnega urada Komisije. Pristojni državni organ za preglede je organ tiste države članice, katere državljan je oseba, ki se ji izda pooblastilo. Kadar zadevna oseba ni državljan države članice EU, vodja Varnostnega urada Komisije zaprosi za varnostni pregled tisto državo članico EU, v kateri ima oseba stalno prebivališče ali navadno prebiva.

(j) Kot del postopka pregleda mora zadevna oseba izpolniti obrazec z osebnimi podatki.

(k) Vodja Varnostnega urada Komisije v svoji zahtevi določi vrsto in stopnjo tajnosti podatkov, ki bodo na razpolago zadevni osebi, tako da pristojni državni organi lahko opravijo postopek pregleda in dajo svoje mnenje glede obsega pooblastil, ki bi bil primeren za navedeno osebo.

(l) Za celotni proces varnostnega preverjanja skupaj z dobljenimi rezultati se upoštevajo ustrezna pravila in predpisi, ki veljajo v zadevni državi članici, vključno s pravili in predpisi, ki urejajo pravna sredstva.

(m) Kadar pristojni državni organi države članice izdajo pozitivno mnenje, lahko vodja Varnostnega urada Komisije izda zadevni osebi ustrezno pooblastilo.

(n) Kadar pristojni državni organi izdajo negativno mnenje, o tem uradno obvestijo zadevno osebo, ki lahko zaprosi vodjo Varnostnega urada Komisije za zaslišanje. Če vodja Varnostnega urada Komisije meni, da je to potrebno, lahko zaprosi pristojne državne organe za vsa dodatna pojasnila, ki jih lahko dajo. V primeru potrditve negativnega mnenja se pooblastilo ne izda.

(o) Vse osebe, ki jim je bilo izdano pooblastilo v smislu odstavkov (d) in (e) v času izdaje pooblastila in potem v rednih časovnih presledkih prejmejo vsa potrebna navodila v zvezi z varovanjem tajnih podatkov in sredstvi za zagotavljanje takega varovanja. Take osebe podpišejo izjavo, s katero potrjujejo, da so prejele navodila in se obvežejo, da jih bodo spoštovale.

(p) Vodja Varnostnega urada Komisije sprejme vse potrebne ukrepe za izvajanje tega oddelka, zlasti glede pravil, ki urejajo dostop do seznama pooblaščenih oseb.

(q) Izjemoma, če tako zahteva služba, lahko vodja Varnostnega urada Komisije, potem ko je uradno obvestil pristojne državne organe in pod pogojem, da od njih v roku enega meseca ni dobil odziva, izda začasno pooblastilo za obdobje, ki ne presega šest mesecev, do objave rezultata pregleda iz odstavka (i).

(r) Tako izdana prehodna in začasna pooblastila ne dajejo dostopa do podatkov TRÈS SECRET UE; dostop do takih podatkov je omejen na uradnike, ki so dejansko opravili pregled s pozitivnimi rezultati v skladu z odstavkom (i). Do objave rezultatov pregleda se uradnikom, za katere je bilo preverjanje zahtevano za stopnjo TRÈS SECRET UE, lahko začasno in prehodno dovoli dostop do podatkov s stopnjo tajnosti do in vključno z SECRET UE.

21. PRIPRAVA, POŠILJANJE, PRENOS, VARNOST KURIRJEV TER DODATNE KOPIJE ALI PREVODI IN IZVLEČKI IZ TAJNIH DOKUMENTOV EU

21.1 **Priprava**

1. Stopnje tajnosti EU, določene v oddelku 16, CONFIDENTIEL UE in višje stopnje se označijo zgoraj in spodaj na sredini vsake strani, vsaka stran pa je oštevilčena. Vsak tajni dokument EU je opremljen z referenčno številko in datumom. Pri dokumentih TRÈS SECRET UE in SECRET UE je referenčna številka na vsaki strani. Če je treba dokumente razdeliti v več izvodih, ima vsak izvod številko, ki je na prvi strani skupaj s skupnim številom strani. Seznam vseh dodatkov in prilog se navede na prvi strani dokumenta s stopnjo CONFIDENTIEL UE ali z višjo stopnjo tajnosti.

2. Dokumente s stopnjo CONFIDENTIEL UE in z višjo stopnjo tajnosti tipkajo, prevajajo, shranjujejo, fotokopirajo, reproducirajo na magnetni trak ali na mikrofilm samo osebe, ki so bile varnostno preverjene za dostop do tajnih podatkov EU vsaj do stopnje tajnosti zadevnega dokumenta.

3. Računalniško pripravo tajnih dokumentov ureja oddelek 25.

21.2 **Pošiljanje**

1. Tajni podatki EU se pošiljajo samo osebam, za katere velja „potreba vedeti“ in ki so ustrezno varnostno preverjene. Prvo pošiljanje določi oseba izvora.

2. Dokumenti TRÈS SECRET UE se pošiljajo preko registrskih uradov TRÈS SECRET UE (glej oddelek 22.2). Za sporočila TRÈS SECRET UE pristojni registrski urad lahko pooblasti vodjo komunikacijskega centra, da pripravi število izvodov, ki je določeno v seznamu naslovnikov.

3. Dokumente s stopnjo SECRET UE in z nižjo stopnjo tajnosti drugim naslovnikom lahko pošilja izvorni naslovnik na podlagi „potrebe vedeti“. Vendar pa organi izvora jasno navedejo vse potrebne omejitve. Kadarkoli so te omejitve uvedene, lahko naslovniki dokumente ponovno pošiljajo samo s pooblastilom oseb izvora.

4. Vsak dokument s stopnjo CONFIDENTIEL UE in z višjo stopnjo tajnosti, ob prihodu ali izhodu iz generalnega direktorata ali službe v evidenco vpiše lokalni registrski urad za tajne podatke EU v okviru posamezne službe. Podatki, ki jih je treba vpisati (reference, datum in po potrebi številka izvoda), morajo omogočati prepoznavo dokumentov in biti vpisani v kontrolno knjigo ali vneseni v posebno varovan računalniški nosilec. (glej 22.1).

21.3 **Prenos tajnih dokumentov EU**

21.3.1 *Pakiranje, potrdila*

1. Dokumenti s stopnjo CONFIDENTIEL UE in z višjo stopnjo, se posredujejo v odpornih, neprozornih dvojnih ovojnicah. Na notranji ovojnici se označijo ustrezna stopnja tajnosti EU in, če je možno, popolni podatki o nazivu delovnega mesta in naslova prejemnika.

2. Notranjo ovojnico lahko odpre in potrdi prejem priloženih dokumentov samo nadzorni uradnik registrskega urada (glej oddelek 22.1) ali njegov namestnik, razen če ta ovojnica ni naslovljena na posameznika. V takem primeru ustrezni registrski urad (glej oddelek 22.1) vpiše prejem ovojnice, notranjo ovojnico pa sme odpreti in potrditi prejem v njej vsebovanih dokumentov samo tista oseba, na katero je naslovljena.

3. V notranjo ovojnico se priloži potrdilo o prejemu. Na potrdilu, ki ne bo razvrščeno, morajo biti navedeni referenčna številka, datum in številka izvoda dokumenta, nikoli pa njegov predmet.

4. Notranja ovojnica se vloži v zunanjo ovojnico, ki nosi odpremno številko za namene prejema. Stopnja tajnosti v nobenem primeru ne sme biti vidna na zunanji ovojnici.

5. Za dokumente s stopnjo CONFIDENTIEL UE in z višjo stopnjo tanosti kurirji dobijo potrdila, na katerih se morajo podatki ujemati z odpremnimi številkami.

21.3.2 *Prenos znotraj zgradbe ali skupine zgradb*

Znotraj zgradbe ali skupine zgradb se tajni dokumenti lahko prenašajo v zapečatenih ovojnicah, na katerih je samo ime naslovnika, pod pogojem, da je oseba, ki jih prenaša, bila varnostno preverjena za stopnjo tajnosti dokumentov.

21.3.3 *Prenos znotraj države*

1. Znotraj države prenos dokumentov TRÈS SECRET UE opravlja samo uradna kurirska služba ali osebe, ki so pooblaščene za dostop do podatkov TRÈS SECRET UE.

2. Kadar se uporabi kurirska služba za prenos dokumenta TRÈS SECRET UE izven zgradbe ali skupine zgradb, je treba upoštevati določbe o odpremljanju in prejemu iz tega poglavja. Dostavne službe morajo imeti na voljo zadostno število osebja, da bi zagotovile, da pošiljke dokumentov TRÈS SECRET UE ves čas ostajajo pod neposrednim nadzorom odgovorne osebe.

3. Izjemoma lahko dokumente TRÈS SECRET UE izven zgradbe ali skupine zgradb za lokalno rabo na sestankih in razpravah prenašajo uslužbenci, ki niso kurirji, pod pogojem da:

   (a) je prenašalec pooblaščen za dostop do dokumentov TRÈS SECRET UE;

   (b) je način odpreme v skladu s pravili o prenosu dokumentov TRÈS SECRET UE;

   (c) uslužbenec v nobenem primeru ne pusti dokumentov TRÈS SECRET UE brez nadzora;

   (d) se uredi vse potrebno, da seznam dokumentov, ki se prenašajo na takšen način, ostane v registrskem uradu TRÈS SECRET UE, kjer se dokumenti hranijo, in da se vpiše v kontrolno knjigo ter omogoči preverjanje dokumentov ob njihovi vrnitvi.

4. Znotraj ene države se dokumenti SECRET UE in CONFIDENTIEL UE lahko pošiljajo po pošti, če tak prenos dovoljujejo nacionalni predpisi in če je prenos v skladu z določbami tega pravilnika, ali prenos opravi kurirska služba ali osebe, ki so bile varnostno preverjene v zvezi z dostopom do tajnih podatkov EU.

5. Varnostni urad Komisije pripravi navodila o osebnem prenašanju tajnih dokumentov EU, ki temeljijo na tem pravilniku. Od prenašalca se zahteva, da se s temi navodili seznani in jih podpiše. Navodila zlasti jasno določajo, da pod nobenim pogojem:

   (a) prenašalec dokumentov ne da iz rok, razen če so pod varnim nadzorom v skladu z določbami iz oddelka 18;

   (b) dokumenti ne smejo biti brez nadzora v sredstvih javnega prometa ali zasebnih vozilih ali na mestih, kot so restavracije ali hoteli. Ne smejo se hraniti v hotelskih trezorjih ali biti brez nadzora v hotelskih sobah;

   (c) se dokumenti ne smejo prebirati na javnih mestih, kot so letala ali vlaki.

21.3.4 *Prenos iz ene države v drugo*

1. Gradivo s stopnjo CONFIDENTIEL UE in z višjo stopnjo tajnosti, prenašajo diplomatske ali vojaške kurirske službe.

2. Vendar pa se osebni prenos gradiva s stopnjo SECRET UE in CONFIDENTIEL UE, dovoli, če določbe v zvezi s prenosom zagotavljajo, da dokumenti ne morejo priti v roke nobeni nepooblaščeni osebi.

3. Član Komisije, pristojen za varnostne zadeve, lahko odobri osebni prenos, če diplomatska ali vojaška kurirska služba nista na voljo ali če bi uporaba teh služb imela za posledico zamudo, ki bi škodila operacijam EU, in če naslovnik gradivo nujno potrebuje. Varnostni urad Komisije pripravi navodila za mednarodni osebni prenos tajnega gradiva s stopnjami do SECRET UE in vključno z njo s strani oseb, ki niso kurirji diplomatskih in vojaških kurirskih služb. Navodila določajo, da:

   (a) ima prenašalec ustrezno varnostno potrdilo;

   (b) se v pristojni službi ali registrskem uradu vodi evidenca o celotnem gradivu, ki se tako prenaša;

   (c) je na paketih ali vrečah, ki vsebujejo gradivo EU, nameščena uradna plomba, ki preprečuje carinski nadzor, ter nalepke za prepoznavo in navodila za najditelja;

   (d) ima prenašalec pri sebi kurirsko potrdilo in/ali potni nalog, ki ga priznavajo vse države EU, s katerim je pooblaščen za prenos ustrezno označenega paketa;

   (e) se na potovanju po kopnem ne prečka nobena od držav nečlanic EU ali njihovih meja, razen če ima država odpošiljateljica posebno jamstvo teh držav;

   (f) bo program potovanja prenašalca glede krajev namembnosti, potovalnih smeri in sredstev uporabljenega prevoza v skladu s predpisi EU ali - če so nacionalni predpisi v zvezi s takimi zadevami strožji - v skladu s temi predpisi;

(g) gradivo mora ostati v lasti prenašalca, razen če se varuje v skladu z določbami o varnem shranjevanju iz oddelka 18;

(h) gradivo ne sme ostati brez nadzora v sredstvih javnega prometa ali zasebnih vozilih ali na mestih, kot so restavracije ali hoteli. Ne sme se hraniti v hotelskih trezorjih ali biti brez nadzora v hotelskih sobah;

(i) če gradivo, ki se prenaša, vsebuje dokumente, se ti ne smejo prebirati na javnih mestih (npr. v letalih, vlakih itd.).

4. Oseba, ki je določena za prenos tajnega gradiva, mora prebrati in podpisati varnostna navodila, ki vsebujejo najmanj že navedena navodila, in postopke, po katerih je treba ravnati v nujnih primerih ali kadar carinski ali letališki varnostni organi zahtevajo pregled paketa, ki vsebuje tajno gradivo.

21.3.5 *Prenos dokumentov RESTREINT UE*

Za prenos dokumentov RESTREINT UE ni predvidenih posebnih določb, razen zagotovil, da ob prenosu dokumenti ne morejo preiti v roke nobeni nepooblaščeni osebi.

21.4 **Varnost kurirjev**

Vsi kurirji, ki so zadolženi za prenašanje dokumentov SECRET UE in CONFIDENTIEL UE, morajo biti ustrezno varnostno preverjeni.

21.5 **Elektronska in druga sredstva tehničnega prenosa**

1. Zaradi zagotovitve varnega prenosa tajnih podatkov EU se uvedejo varnostni ukrepi na področju komunikacij. Podrobna pravila, ki veljajo za prenos takih tajnih podatkov EU, določa oddelek 25.

2. Podatke s stopnjo CONFIDENTIEL UE in SECRET UE lahko prenašajo le akreditirani komunikacijski centri in omrežja in/ali terminali ter sistemi.

21.6 **Dodatne kopije in prevodi ter izvlečki iz tajnih dokumentov EU**

1. Kopijo ali prevod dokumentov TRÈS SECRET UE lahko odobri le organ izvora.

2. Če osebe brez varnostnega potrdila TRÈS SECRET UE potrebujejo podatke, ki, čeprav so vsebovani v dokumentu TRÈS SECRET UE, nimajo navedene stopnje tajnosti, se vodji registrskega urada TRÈS SECRET UE (glej oddelek 22.2) lahko dovoli, da pripravi potrebno število izvlečkov iz navedenega dokumenta. Hkrati vodja sprejme potrebne ukrepe, ki zagotovijo, da se takim izvlečkom določi ustrezna stopnja tajnosti

3. Dokumente s stopnjo SECRET UE in z nižjo stopnjo tajnosti, lahko razmnoži in prevaja naslovnik v skladu s tem pravilnikom in pod pogojem doslednega uresničevanja načela „potrebe vedeti“. Varnostni ukrepi, ki veljajo za izvorni dokument, veljajo tudi za njegove razmnožene primerke in/ali prevode.

22. REGISTRSKI URADI, INVENTURNI POPISI, PREVERJANJA, ARHIVIRANJE IN UNIČENJE TAJNIH PODATKOV EU

22.1 **Lokalni registrski uradi za tajne podatke EU**

1. V okviru Komisije je v vsaki službi, če je to potrebno, eden ali več lokalnih registrskih uradov za tajne podatke EU odgovornih za registracijo, razmnoževanje, odpremljanje, arhiviranje in uničenje dokumentov, označenih s stopnjo SECRET UE in CONFIDENTIEL UE.

2. Kadar služba nima lokalnega registrskega urada za tajne podatke EU, njegovo vlogo prevzame lokalni registrski urad za tajne podatke EU generalnega sekretariata.

3. Lokalni registrski uradi za tajne podatke EU poročajo vodji službe, od katerega prejemajo navodila. Vodja teh registrskih uradov je nadzorni uradnik registrskega urada (RCO).

4. Lokalni registrski uradi za tajne podatke EU so pod nadzorom lokalnega varnostnega uradnika, če gre za uporabo predpisov o ravnanju z dokumenti s tajnimi podatki EU in upoštevanje ustreznih varnostnih ukrepov.

5. Uradnikom, ki so dodeljeni lokalnim registrskim uradom za tajne podatke EU, je dovoljen dostop do tajnih podatkov EU v skladu z oddelkom 20.

6. Pod vodstvom pristojnega vodje službe so lokalni registrski uradi za tajne podatke EU zadolženi za:

(a) vodenje postopkov v zvezi z registracijo, razmnoževanjem, prevajanjem, prenosom, odpremljanjem in uničevanjem takih podatkov;

(b) vodenje registra o tajnih podatkih;

(c) redno preverjanje potrebe po ohranjanju stopenj tajnosti podatkov.

7. Lokalni registrski uradi za tajne podatke EU vodijo evidenco o naslednjih podatkih:

(a) datumu določitve tajnih podatkov;

(b) stopnje tajnosti;

(c) datumu prenehanja veljavnosti stopnje tajnosti;

(d) imenu in službi osebe izvora;

(e) prejemniku ali prejemnikih, z zaporedno številko;

(f) predmetu;

(g) številki;

(h) številu izvodov v obtoku;

(i) pripravi popisa tajnih podatkov, ki so bili posredovani službi;

(j) vpisniku o odpravi ali zniževanju stopenj tajnosti tajnih podatkov.

8. Splošna pravila, določena v oddelku 21, veljajo za lokalne registrske urade za tajne podatke EU v Komisiji, razen če jih spreminjajo posebna pravila iz tega oddelka.

22.2 **Registrski urad TRÈS SECRET UE**

22.2.1 *Splošno*

1. Centralni registrski urad TRÈS SECRET UE zagotavlja evidentiranje, obdelavo in razširjanje dokumentov TRÈS SECRET UE v skladu s tem pravilnikom. Vodja registrskega urada TRÈS SECRET UE je nadzorni uradnik registrskega urada TRÈS SECRET UE.

2. Centralni registrski urad TRÈS SECRET UE deluje kot glavni sprejemni in odpremni organ v Komisiji, pri drugih institucijah EU, državah članicah, mednarodnih organizacijah in tretjih državah, s katerimi ima Komisija sklenjene sporazume o varnostnih postopkih za izmenjavo tajnih podatkov.

3. Če je potrebno, se ustanovijo podregistrski uradi, ki so odgovorni za notranje upravljanje dokumentov TRÈS SECRET UE; njihova naloga je sprotno dopolnjevanje podatkov o kroženju vsakega dokumenta, za katerega so zadolženi.

4. Podregistrski uradi TRÈS SECRET UE se ustanovijo, kakor to določa oddelek 22.2.3, zaradi dolgoročnih potreb in so pridruženi centralnemu registrskemu uradu TRÈS SECRET UE. Če so potrebe po proučitvi dokumentov TRÈS SECRET UE samo začasne ali priložnostne, se ti dokumenti lahko razpošiljajo brez ustanovitve podregistrskega urada TRÈS SECRET UE, pod pogojem, da so predpisana pravila, ki zagotavljajo nadaljnji nadzor s strani ustreznega registrskega urada TRÈS SECRET UE in da se pri tem spoštujejo vsi ukrepi za materialno varnost in varnost osebja.

5. Podregistrski uradi ne smejo prenesti dokumentov TRÈS SECRET UE neposredno na druge podregistrske urade istega centralnega registrskega urada TRÈS SECRET UE brez izrecne odobritve slednjega.

6. Vse izmenjave dokumentov TRÈS SECRET UE med podregistrskimi uradi, ki niso pridruženi istemu centralnemu registrskemu uradu, potekajo prek centralnih registrskih uradov TRÈS SECRET UE.

22.2.2 *Centralni registrski urad TRÈS SECRET UE*

Kot nadzorni uradnik je vodja centralnega registrskega urada TRÈS SECRET UE pristojen za:

(a) prenos dokumentov TRÈS SECRET UE v skladu z določbami iz oddelka 21.3;

(b) vodenje seznama vseh svojih podrejenih podregistrskih uradov TRÈS SECRET UE skupaj z imeni in podpisi imenovanih uradnikov za nadzor in njihovih pooblaščenih namestnikov;

(c) shranjevanje potrdil registrskih uradov za vse dokumente TRÈS SECRET UE, ki jih je razposlal centralni registrski urad;

(d) vodenje evidence dokumentov TRÈS SECRET UE, ki se hranijo, in tistih, ki so bili razposlani naprej;

(e) vodenje dopolnjenega seznama vseh centralnih registrskih uradov TRÈS SECRET UE, s katerimi si običajno izmenjuje korespondenco, skupaj z imeni in podpisi njihovih imenovanih uradnikov za nadzor in njihovih pooblaščenih namestnikov;

(f) materialno varovanje vseh dokumentov TRÈS SECRET UE, ki se hranijo v registrskem uradu v skladu s pravili, ki jih določa oddelek 18.

22.2.3 *Podregistrski uradi* TRÈS SECRET UE

Kot nadzorni uradnik je vodja podregistrskega urada TRÈS SECRET UE pristojen za:

(a) prenos dokumentov TRÈS SECRET UE v skladu z določbami oddelka 21.3;

(b) vodenje dopolnjenega seznama vseh oseb, pooblaščenih za dostop do podatkov TRÈS SECRET UE, pod njegovim nadzorom;

(c) razpošiljanje dokumentov TRÈS SECRET UE v skladu z navodili osebe izvora ali na podlagi potrebe vedeti, pri čemer najprej preveri, ali ima naslovnik zahtevano varnostno potrdilo;

(d) vodenje evidence vseh dokumentov s stopnjo TRÈS SECRET UE, ki se hranijo ali so v obtoku pod njegovim nadzorom ali ki so bili poslani drugim registrskim uradom TRÈS SECRET UE, ter hranjenje vseh potrebnih potrdil;

(e) vodenje seznama registrskih uradov TRÈS SECRET UE, pri katerih je pooblaščen za izmenjavo dokumentov TRÈS SECRET UE, skupaj z imeni in podpisi njihovih uradnikov za nadzor in pooblaščenih namestnikov;

(f) materialno varovanje vseh dokumentov TRÈS SECRET UE, ki se hranijo v podregistrskem uradu v skladu z določbami oddelka 18.

22.3 **Inventurni popisi in preverjanja tajnih dokumentov EU**

1. Vsako leto registrski urad TRÈS SECRET UE, kot je navedeno v tem oddelku, opravi posamični popis vseh dokumentov TRÈS SECRET UE. Dokument velja za evidentiranega, če registrski urad fizično razpolaga z njim ali če ima urad potrdilo registrskega urada TRÈS SECRET UE, kateremu je bil poslan, s potrdilom o uničenju dokumenta ali z navodili o znižanju ali odpravi stopenj tajnosti navedenega dokumenta. Ugotovitve letnih popisov pošljejo članu Komisije, pristojnemu za varnostne zadeve, in sicer najpozneje do 1. aprila vsakega leta.

2. Podregistrski uradi TRÈS SECRET UE pošljejo ugotovitve svojih letnih popisov centralnemu registrskemu uradu, kateremu so odgovorni, do datuma, ki ga določi centralni registrski urad.

3. Tajni dokumenti z nižjo stopnjo tajnosti kot je TRÈS SECRET UE so predmet notranjih preverjanj v skladu z navodili člana Komisije, pristojnega za varnostne zadeve.

4. V teh postopkih lahko imetnik dokumenta izrazi mnenje glede:

   (a) možnosti znižanja ali odprave stopnje tajnosti nekaterih dokumentov;

   (b) dokumentov, ki jih je treba uničiti.

22.4 **Arhiviranje tajnih podatkov EU**

1. Tajni podatki EU se hranijo v pogojih, določenih v oddelku 18.

2. Zaradi lažjega arhiviranja se uradnikom, zadolženim za nadzor v vseh registrskih uradih, dovoli snemanje dokumentov TRÈS SECRET UE, SECRET UE in CONFIDENTIEL UE na mikrofilm ali drugačno shranjevanje na magnetna ali optična sredstva za namene arhiviranja pod pogojem, da:

   (a) postopek snemanja na mikrofim/shranjevanja opravlja osebje z veljavnim varnostnim potrdilom, ki ustreza stopnji tajnosti;

   (b) je mikrofilm/nosilec shranjenih podatkov varovan na enak način kakor izvirni dokumenti;

   (c) je o snemanju na mikrofilm/shranjevanju vsakega dokumenta TRÈS SECRET UE obveščen organ izvora;

   (d) filmski koluti ali druge vrste nosilcev vsebujejo samo dokumente iste stopnje tajnosti TRÈS SECRET UE, SECRET UE ali CONFIDENTIEL UE;

   (e) je snemanje na mikrofilm/shranjevanje dokumentov TRÈS SECRET UE ali SECRET UE razločno označeno v evidenci, ki se uporablja za letno inventuro;

   (f) se izvirni dokumenti, ki so bili posneti na mikrofilm ali kako drugače shranjeni, uničijo v skladu s pravili iz oddelka 22.5.

3. Ta pravila veljajo tudi za druge oblike dovoljenega shranjevanja, kot so elektromagnetni nosilci in optični diski.

22.5 **Uničenje tajnih dokumentov EU**

1. Da bi se preprečilo nepotrebno kopičenje tajnih dokumentov EU, se tisti, za katere je vodja službe, kjer se hranijo, mnenja, da so brezpredmetni in jih je preveč, uničijo takoj, ko je mogoče, in sicer na naslednji način:

   (a) Dokumente TRÈS SECRET UE uniči le centralni registrski urad, ki je za njih odgovoren. Vsak uničeni dokument se vpiše na potrdilo o uničenju, ki ga podpišeta uradnik, zadolžen za nadzor na stopnji TRÈS SECRET UE, in uradnik, ki je priča uničenju in ki mora imeti varnostno potrdilo na stopnji TRÈS SECRET UE. V ta namen se v vpisnik vnese ustrezna zabeležka;

   (b) Registrski urad hrani potrdila o uničenju skupaj z dokumentacijo o razpošiljanju za deset let. Kopije se posredujejo osebi izvora ali ustreznemu centralnemu registrskemu uradu le, kadar se to posebej zahteva;

   (c) Dokumenti TRÈS SECRET UE se skupaj z vsemi odpadki, ki se obravnavajo kot tajno gradivo in so nastali pri pripravi dokumentov TRÈS SECRET UE, kot so poškodovane kopije, delovni osnutki, natipkana sporočila, diskete, uničijo pod nadzorom nadzornega uradnika registrskega urada TRÈS SECRET UE z zažigom, zmletjem, razrezom v pramene ali z drugačno spremembo v neprepoznavno in nesestavljivo obliko.

2. Dokumente SECRET UE uniči registrski urad, ki je za navedene dokumente odgovoren, pod nadzorom varnostno preverjene osebe po enem od postopkov, navedenih v odstavku 1(c). Uničeni dokumenti SECRET UE se vpišejo na podpisana potrdila o uničenju, ki jih registrski urad hrani skupaj z dokumentacijo o razpošiljanju najmanj tri leta.

3. Dokumente CONFIDENTIEL UE uniči registrski urad, ki je za navedene dokumente odgovoren, pod nadzorom varnostno preverjene osebe po enem od postopkov, navedenih v odstavku 1(c). Njihovo uničenje se evidentira v skladu z navodili člana Komisije, pristojnega za varnostne zadeve.

4. Dokumente RESTREINT UE uniči registrski urad, odgovoren za navedene dokumente, ali uporabnik, v skladu z navodili člana Komisije, pristojnega za varnostne zadeve.

22.6 **Uničenje v nujnih primerih**

1. Službe Komisije ob upoštevanju lokalnih pogojev pripravijo načrte za varovanje tajnih podatkov EU v kriznih razmerah, vključno, če je to potrebno, z načrti za uničenje in evakuacijo v nujnih primerih. Na ta način razdelijo potrebna navodila, da tajni podatki EU ne bi prišli v roke nepooblaščenim osebam.

2. Ukrepi v zvezi z varovanjem in/ali uničenjem gradiva SECRET UE in CONFIDENTIEL UE v kriznih razmerah nikakor ne smejo biti v škodo varovanju ali uničenju gradiva TRÈS SECRET UE, vključno z (de)šifrirno opremo, katerih obravnava ima prednost pred vsemi drugimi nalogami.

3. Ukrepi, ki se sprejmejo za varovanje ali uničenje (de)šifrirne opreme v nujnih primerih, so določeni v posebnih navodilih.

4. Navodila morajo biti na voljo na kraju samem v zapečateni ovojnici. Na razpolago morajo biti sredstva/orodja za uničenje.

23. VARNOSTNI UKREPI ZA POSEBNE SESTANKE, KI POTEKAJO IZVEN PROSTOROV KOMISIJE IN VKLJUČUJEJO TAJNE PODATKE EU

23.1 **Splošno**

Če sestanki Komisije ali drugi pomembni sestanki potekajo izven prostorov Komisije in kjer zaradi visoke občutljivosti obravnavanih vprašanj ali podatkov to opravičujejo posebne varnostne zahteve, se uporabijo spodaj navedeni varnostni ukrepi. Ti ukrepi veljajo samo za varovanje tajnih podatkov EU; predvidijo se lahko tudi drugi varnostni ukrepi.

23.2 **Pristojnosti**

23.2.1 *Varnostni urad Komisije*

Varnostni urad Komisije sodeluje s pristojnimi organi države članice, na čigar območju poteka sestanek (država članica gostiteljica), da bi se zagotovila varnost sestankov Komisije ali drugih pomembnih sestankov ter zaradi varnosti samih delegatov in njihovega osebja. V zvezi z varovanjem urad posebej zagotovi, da:

(a) so pripravljeni načrti za primere ogrožanja varnosti in incidente v zvezi z varnostjo, pri čemer zadevni ukrepi zajemajo predvsem varno hrambo tajnih dokumentov EU v uradih;

(b) so sprejeti taki ukrepi, ki zagotavljajo možen dostop do komunikacijskega sistema Komisije za prejem in pošiljanje tajnih podatkov EU. Od države članice gostiteljice se zahteva, da po potrebi zagotovi tudi dostop do varnih telefonskih sistemov.

Varnostni urad Komisije ima vlogo svetovanja v zvezi z varnostjo pri pripravi sestanka; tam je zastopan zaradi pomoči in svetovanja uradniku, zadolženemu za varnost sestanka (MSO), in delegacijam, če je to potrebno.

Od vsake delegacije, prisotne na sestanku, se zahteva, da določi uradnika za varnost, ki bo odgovoren za obravnavanje varnostnih zadev v svoji delegaciji in za vzdrževanje povezav z uradnikom, zadolženim za varnost sestanka ter, če se to zahteva, s predstavnikom Varnostnega urada Komisije.

23.2.2 *Uradnik, zadolžen za varnost sestanka (MSO)*

Imenuje se uradnik, zadolžen za varnost sestanka, ki je odgovoren za splošno pripravo in nadzor nad splošnimi internimi varnostnimi ukrepi ter za uskladitev z drugimi zadevnimi varnostnimi organi. Ukrepi, ki jih sprejme nadzorni uradnik sestanka, na splošno veljajo za:

(a) varnostne ukrepe na kraju sestanka, ki zagotavljajo, da sestanek poteka brez vsakršnih incidentov, ki bi lahko ogrozili varnost katerih koli tam uporabljenih tajnih podatkov EU;

(b) preverjanje osebja z dovoljenjem za dostop na mesto sestanka, območja delegacij in v konferenčne sobe ter preverjanje celotne opreme;

(c) stalno usklajevanje s pristojnimi organi države članice gostiteljice in Varnostnim uradom Komisije;

(d) vključitev varnostnih navodil v gradivo za sestanek ob ustreznem upoštevanju določb tega pravilnika in vseh drugih varnostnih navodil, ki bi se izkazala za potrebna.

23.3 **Varnostni ukrepi**

23.3.1 *Varnostna območja*

Vzpostavijo se naslednja varnostna območja:

(a) Varnostno območje razreda II, ki ga sestavljajo prostor, v katerem se pripravljajo tajni dokumenti, pisarniški prostori Komisije, razmnoževalna grafična oprema in tudi pisarniški prostori za delegacije, kjer je to primerno;

(b) Varnostno območje razreda I, ki ga sestavlja konferenčna soba ter kabine za tolmače in tonske tehnike;

(c) Upravna območja, ki jih sestavljajo območje za tisk in tisti deli na kraju sestanka, ki se uporabljajo za upravo, gostinstvo in nastanitev, ter območje, ki neposredno meji na tiskovno središče in kraj sestanka.

23.3.2 *Dovolilnice*

Uradnik, zadolžen za varnost sestanka (MSO), poskrbi za ustrezne priponke, kakor to zahtevajo delegacije v skladu s svojimi potrebami. Če se zahteva, se lahko uvedejo razlike v dostopu do različnih varnostnih območij.

Varnostna navodila za sestanek od vseh zadevnih oseb zahtevajo, da nosijo in imajo pripete svoje priponke na vidnem mestu ves čas na kraju sestanka, tako da jih lahko po potrebi preveri varnostno osebje.

Z izjemo udeležencev, ki nosijo priponke, je praviloma na kraju sestanka prisotnih čim manj drugih oseb. Uradnik, zadolžen za varnost sestanka (MSO), dovoli le mednarodnim delegacijam, da na podlagi njihove zahteve v času sestanka sprejemajo obiske. Obiskovalci prejmejo priponko z oznako obiskovalca. Dovolilnica obiskovalca/ke se izpolni z imenom obiskovalca/ke in z imenom obiskane osebe. Obiskovalci/ke morajo ves čas biti v spremstvu varnostnika ali obiskane osebe. Spremljajoča oseba nosi dovolilnico obiskovalca, ki jo ob odhodu obiskovalca/ke s kraja sestanka skupaj z obiskovalčevo priponko vrne varnostnemu osebju.

23.3.3 *Nadzor fotografske in avdio opreme*

Na varnostno območje razreda I ni dovoljeno prinesti nikakršne fotografske ali snemalne opreme, z izjemo opreme, ki jo prinesejo fotografi in tonski tehniki, z dovoljenjem uradnika, zadolženega za varnost sestanka (MSO).

23.3.4 *Pregled aktovk, prenosnih računalnikov in paketov*

Imetniki dovolilnic, ki jim je dovoljen dostop na varnostno območje, lahko običajno vnašajo svoje aktovke in prenosne računalnike (samo s svojim lastnim napajanjem) brez pregleda. Pri pošiljkah, namenjenih delegacijam, lahko delegacije prevzamejo dostavo pošiljk, ki jih pregleda uradnik za nadzor delegacije, ali so pregledane s posebno opremo ali pa jih odpre varnostno osebje za inšpekcijski pregled. Če nadzorni uradnik sestanka meni, da je potrebno, se lahko določijo strožji ukrepi za inšpekcijski pregled aktovk in pošiljk.

23.3.5 *Tehnična varnost*

Sejno sobo tehnično zavaruje tehnična varnostna ekipa, ki lahko med samim sestankom izvaja tudi elektronski nadzor.

23.3.6 *Dokumenti delegacij*

Delegacije so odgovorne za prinašanje in odnašanje tajnih dokumentov EU na sestanke in z njih. Prav tako so odgovorne za potrjevanje in varnost navedenih dokumentov v času njihove uporabe v prostorih, ki so jim dodeljeni. Države članice gostiteljice lahko prosijo za pomoč pri prenosu tajnih dokumentov s kraja sestanka in na kraj sestanka.

23.3.7 *Varna hramba dokumentov*

Če Komisija ali delegacije ne morejo hraniti svojih tajnih dokumentov v skladu z veljavnimi standardi, lahko dajo dokumente v zapečatene ovojnice v hrambo uradniku, zadolženemu za varnost sestanka, za potrdilo, da lahko le-ta shrani dokumente v skladu z veljavnimi standardi.

23.3.8 *Pregled pisarniških prostorov*

Uradnik, zadolžen za varnost sestanka, ob koncu vsakega delovnega dne organizira pregled pisarn Komisije in delegacij, da bi zagotovil, da so tajni dokumenti EU hranjeni na varnem mestu. V nasprotnem primeru sprejme ustrezne ukrepe.

23.3.9 *Odstranjevanje gradiv v zvezi s tajnimi podatki EU*

Z vsem gradivom v zvezi s tajnimi podatki EU se ravna kot z le-temi, koše za smeti ali vreče pa je treba izročiti predstavnikom služb Komisije in delegacij, da jih odstranijo. Pred odhodom iz prostorov, ki so jim bili dodeljeni, predstavniki Komisije in delegacije izročijo vsa odpadna gradiva uradniku, zadolženemu za varnost sestanka, ki uredi vse potrebno za njihovo uničenje v skladu s pravili.

Na koncu sestanka se z vsemi dokumenti, s katerimi razpolagajo predstavniki Komisije in delegacije, vendar jih več ne potrebujejo, ravna kot z odpadnim gradivom. Še preden nehajo veljati varnostni ukrepi, sprejeti za namen sestanka, se opravi temeljit pregled prostorov Komisije in delegacij. Dokumente, za katere je bilo podpisano potrdilo o prejemu, je treba, kolikor je to primerno, uničiti, kot določa oddelek 22.5.

24. KRŠITVE VARNOSTI IN RAZKRITJE TAJNIH PODATKOV EU

24.1 **Opredelitve pojmov**

Kršitev varnosti nastane kot posledica dejanja ali opustitve dejanja, ki sta v nasprotju z varnostnimi predpisi Komisije, kar bi lahko povzročilo ogrozitev ali razkritje tajnih podatkov EU.

Do razkritja tajnih podatkov EU pride, kadar so ti podatki v celoti ali delno prišli v roke nepooblaščenim osebam, tj. osebam, ki nimajo niti ustreznega varnostnega potrdila niti zanje ne velja „potreba vedeti“ ali kadar gre za možnost, da se je kaj takega že zgodilo.

Tajni podatki EU se lahko razkrijejo zaradi neprevidnosti, malomarnosti ali lahkomiselnosti, razkrijejo pa se lahko tudi z dejavnostmi služb, katerih delovanje je usmerjeno proti EU ali državi članici v zvezi s tajnimi podatki in dejavnostmi EU, ali jih razkrijejo subverzivne organizacije.

24.2 **Poročanje o kršitvah varnosti**

Vse osebe, ki imajo opravka s tajnimi podatki EU, se temeljito seznanijo s svojimi dolžnostmi v zvezi s tem. O vseh kršitvah varnosti, za katere izvedo, poročajo takoj.

Kadar lokalni varnostni uradnik ali uradnik, zadolžen za varnost sestanka, ugotovita ali sta obveščena o kršitvah varnosti, ki se nanašajo na tajne podatke EU ali izgubo ali izginotje tajnega gradiva EU, takoj ukrepata, da bi:

(a) zavarovala dokaze;

(b) ugotovila dejstva;

(c) ocenila in zmanjšala povzročeno škodo;

(d) preprečila ponovno kršitev;

(e) obvestila pristojne organe o posledicah kršitve varnosti.

S tem v zvezi se posredujejo naslednji podatki:

(i) opis vključenih podatkov, vključno z njihovo stopnjo tajnosti, referenčno številko in številko izvoda, datumom, osebo izvora, predmetom in področjem uporabe;

(ii) kratek opis okoliščin kršitve varnosti, vključno z datumom in časom, v katerem so bili podatki izpostavljeni razkritju;

(iii) izjavo, da je bila oseba izvora seznanjena z razkritjem.

Dolžnost vsakega varnostnega organa je, da takoj, ko je obveščen o nastali kršitvi varnosti, o tem poroča Varnostnemu uradu Komisije.

O primerih, ki zadevajo podatke RESTREINT UE, je treba poročati le, če so neobičajni.

Ko je član Komisije, pristojen za varnostne zadeve, obveščen o nastali kršitvi varnosti:

(a) o tem obvesti organ, ki je določil zadevne tajne podatke;

(b) zaprosi ustrezne varnostne organe, da uvedejo preiskavo;

(c) usklajuje preiskave, kadar zadevajo več varnostnih organov;

(d) pridobi poročilo o okoliščinah kršitve, datumu ali času, v katerem se je kršitev zgodila in je bila odkrita, skupaj s podrobnim opisom vsebine in stopnje tajnosti zadevnega gradiva. Poroča se tudi o škodi, povzročeni interesom EU ali ene ali več njenih držav članic in o ukrepih, ki so bili sprejeti za preprečitev ponovitve kršitve.

Organ izvora o tem obvesti naslovnike in posreduje ustrezna navodila.

24.3 **Pravna sredstva**

Vsaka oseba, ki je odgovorna za razkritje tajnih podatkov EU, je disciplinsko odgovorna v skladu z ustreznimi pravili in predpisi, zlasti z Naslovom VI uslužbenskih predpisov. Takšno ukrepanje ne posega v nobene nadaljnje pravne ukrepe.

Član Komisije, pristojen za varnostne zadeve, v posameznih primerih na podlagi poročila, navedenega v oddelku 24.2, sprejme vse potrebne ukrepe, da bi pristojnim državnim organom omogočil, da sprožijo kazenske postopke.

25. VAROVANJE TAJNIH PODATKOV EU V SISTEMIH INFORMACIJSKE TEHNOLOGIJE IN V KOMUNIKACIJSKIH SISTEMIH

25.1 **Uvod**

25.1.1 *Splošno*

Varnostna politika in varnostne zahteve veljajo za vse komunikacijske in informacijske sisteme ter omrežja (v nadaljevanju sistemi), ki obdelujejo podatke s stopnjo tajnosti CONFIDENTIEL UE in z višjo stopnjo tajnosti. Uporabljajo se kot dopolnilo k Sklepu Komisije K(95) 1510 z dne 23. novembra 1995 o varovanju informacijskih sistemov.

Sistemi, ki obdelujejo podatke RESTREINT UE, tudi zahtevajo varnostne ukrepe za varovanje tajnosti navedenih podatkov. Pri vseh sistemih so potrebni varnostni ukrepi za varstvo integritete in razpoložljivosti navedenih sistemov in podatkov, ki jih vsebujejo.

Varnostna politika informacijske tehnologije (IT), ki jo uporablja Komisija, vsebuje naslednje elemente:

— je sestavni del splošne varnosti in dopolnjuje vse elemente informacijske varnosti, varnosti osebja in materialne varnosti;

— delitev odgovornosti med imetniki tehničnih sistemov, imetniki tajnih podatkov EU, shranjenih in obdelanih v tehničnih sistemih, strokovnjaki za varstvo informacijske tehnologije (IT) in uporabniki;

— varnostna načela in zahteve vsakega sistema informacijske tehnologije (IT);

— odobritev teh načel in zahtev s strani imenovanega organa;

— upoštevanje posebnih ogrožanj in ranljivosti na področju informacijske tehnologije (IT).

25.1.2 *Ogroženost in ranljivost sistemov*

Ogroženost se lahko opredeli kot možnost za naključno ali namerno zmanjšanje varnosti. Pri sistemih tako zmanjšanje obsega izgubo ene ali več lastnosti kot so tajnost, celovitost in razpoložljivost. Ranljivost se lahko opredeli kot slabost ali pomanjkanje nadzora, ki lahko pospeši ali omogoči nevarnost za določeno sredstvo ali cilj.

Tajni podatki EU in podatki, ki niso tajni, obdelani v sistemih v koncentrirani obliki, zasnovani za hiter dostop, posredovanje in uporabo, so izpostavljeni mnogim nevarnostim. Te obsegajo dostop nepooblaščenih uporabnikov do podatkov ali, nasprotno, odvzem dostopa pooblaščenim osebam. Obstajajo tudi tveganja nepooblaščenega razkritja, ponarejanja, spreminjanja ali brisanja podatkov. Poleg tega je kompleksna in včasih občutljiva oprema draga ter se pogosto težko popravi ali hitro zamenja.

25.1.3 *Glavni namen varnostnih ukrepov*

Glavni namen varnostnih ukrepov, navedenih v tem oddelku, je omogočiti varovanje pred nepooblaščenim razkritjem tajnih podatkov EU (izgubo tajnosti) in proti izgubi celovitosti in razpoložljivosti podatkov. Da bi se doseglo ustrezno varovanje sistema, ki obdeluje tajne podatke EU, Varnostni urad Komisije določi ustrezne standarde običajne varnosti skupaj z ustreznimi posebnimi varnostnimi postopki in tehnikami, posebno oblikovanimi za vsak sistem.

25.1.4 *Opredelitev varnostnih zahtev, ki so specifične za sistem (SSRS)*

Za vse sisteme, ki obdelujejo tajne podatke, s stopnjo tajnosti CONFIDENTIEL UE in z višjo stopnjo tajnosti, se zahteva, da imetnik tehničnega sistema (TSO, glej oddelek 25.3.4) in imetnik podatkov (glej oddelek 25.3.5), skupaj s prispevki in pomočjo projektnega osebja in Varnostnega urada Komisije (v vlogi organa INFOSEC - IA, glej oddelek 25.3.3) in s pooblastilom Službe za akreditacijo varnosti (SAA, glej oddelek 25.3.2), opredelita varnostne zahteve, ki so specifične za sistem (SSRS).

Opredelitev varnostnih zahtev, ki so specifične za sistem (SSRS), se zahteva tudi, kadar Služba za akreditacijo varnosti (SAA) meni, da sta razpoložljivost in celovitost podatkov RESTREINT UE ali podatkov, ki niso tajni, kritični.

Opredelitev varnostnih zahtev, ki so specifične za sistem (SSRS), se pripravi na najzgodnejši stopnji priprave projekta ter se razvije in okrepi v času razvoja projekta, pri tem pa izpolnjuje različne naloge na različnih projektnih stopnjah v celotnem obdobju delovanja sistema.

25.1.5 *Načini varnostnega delovanja*

Vsi sistemi, v katerih se obdelujejo tajni podatki s stopnjo tajnosti CONFIDENTIEL UE in z višjo stopnjo tajnosti, smejo delovati na en sam način ali, kjer je to odobreno z zahtevami v različnih časovnih obdobjih, na več kakor enega od naslednjih načinov varnostnega delovanja ali na način, ki ga določa posamezna država članica, če je enakovreden:

(a) dedicated

(b) system high, in

(c) multi-level.

25.2 **Opredelitve pojmov**

„Akreditacija“ pomeni: pooblastilo in dovoljenje, dano sistemu za obdelavo tajnih podatkov EU v svojem operativnem okolju.

Opomba:

Takšna akreditacija se da po izvedbi vseh ustreznih varnostnih postopkov in ko je dosežena zadostna stopnja varovanja sistemskih virov. Akreditacija se običajno opravi v skladu z varnostnimi zahtevami, ki so specifične za sistem (SSRS), vključno z:

(a) določitvijo cilja akreditacije za sistem; zlasti katera stopnja ali stopnje tajnosti podatkov se obdelujejo in kateri način ali načini sistemske ali omrežne varnosti se predlagajo;

(b) priprava pregleda obvladovanja tveganja za namen prepoznavanja nevarnosti in ranljivosti ter ukrepi za njihovo preprečevanje;

(c) varnostni postopki obratovanja (SecOPs) s podrobnim opisom predlaganih operacij (npr. načini, storitve, ki jih je treba zagotoviti) in vključno z opisom lastnosti sistemske varnosti, ki predstavlja podlago za akreditacije;

(d) načrt izvajanja in vzdrževanja varnostnih lastnosti;

(e) načrt začetnega in nadaljevalnega preizkusa, ocene in potrditve sistemske in omrežne varnosti, ter

(f) certificiranje, kjer se to zahteva, skupaj z drugimi elementi akreditacije.

„Varnostni uradnik za centralno informatiko“ (CISO) je uradnik v centralni službi informacijske tehnologije, ki usklajuje in nadzoruje varnostne ukrepe v centralno organiziranih sistemih.

„Certificiranje“ pomeni: izdajo uradnega potrdila na podlagi neodvisnega pregleda izvajanja in rezultatov ocenjevanja, obsega, do katerega sistem izpolnjuje varnostne zahteve, ali do katerega računalniški varnostni produkt izpolnjuje vnaprej opredeljene varnostne zahteve.

„Komunikacijska varnost“ (COMSEC) pomeni: uporabo varnostnih ukrepov na področju telekomunikacij za preprečevanje dostopa nepooblaščenim osebam do pomembnih podatkov, ki bi se lahko pridobili s posedovanjem ali preučevanjem takšnih telekomunikacij, ali za zagotovitev verodostojnosti teh telekomunikacij.

Opomba:

To so ukrepi za kriptografsko varnost, varnost prenosov in varnost oddajanja; to so tudi ukrepi za proceduralno in materialno varnost, varnost osebja, dokumentov ter računalniško varnost.

„Računalniška varnost“ (COMPUSEC) pomeni: uporabo varnostnih elementov strojne opreme, sistemskih programov in programske opreme v računalniškem sistemu za varovanje pred nepooblaščenim razkritjem, manipulacijo, spreminjanjem/brisanjem podatkov ali izpadom sistema ali preprečitvijo le-tega.

„Računalniški varnostni produkt“ pomeni: produkt za računalniško varnost, ki je namenjen vključitvi v sistem informacijske tehnologije (IT) za uporabo pri izboljšanju ali zagotavljanju tajnosti, celovitosti ali razpoložljivosti obdelanih podatkov.

Namenski varnostni način delovanja pomeni: način delovanja, pri katerem so VSI posamezniki, ki imajo dostop do sistema, varnostno preverjeni do najvišje stopnje tajnosti podatkov, ki se v sistemu obdelujejo in za katere velja splošna „potreba vedeti“ za VSE podatke, ki se v sistemu obdelujejo.

Opombe:

(1) Splošna „potreba vedeti“ pomeni, da ni obvezne zahteve za varnostne značilnosti računalnikov za zagotavljanje ločevanja podatkov znotraj sistema.

(2) Druge varnostne lastnosti (na primer materialna varnost, varnost osebja in proceduralna varnost) se prilagodijo zahtevam za najvišjo stopnjo tajnosti in za vse oznake kategorij podatkov, ki se obdelujejo v sistemu.

„Ocenjevanje“ pomeni: podroben tehničen pregled varnostnih vidikov sistema, kriptografskega produkta ali računalniškega varnostnega produkta, ki ga opravi pristojen organ.

Opombe:

(1) Pri ocenjevanju se preverja prisotnost zahtevane varnostne funkcionalnosti in odsotnost negativnih stranskih učinkov takšne funkcionalnosti ter ocenjuje možnost vplivanja na takšno funkcionalnost.

(2) Z ocenjevanjem se določi obseg izpolnitve varnostnih zahtev sistema ali varnostnih zahtev računalniškega varnostnega produkta ter določi stopnja zanesljivosti sistema ali zanesljivega delovanja kriptografskega produkta ali produkta računalniške varnosti.

„Imetnik podatka“ (IO) je organ (vodja službe), ki je pristojen za oblikovanje, obdelavo in uporabo podatkov, vključno z odločanjem o tem, komu se dovoli dostop do podatkov.

„Varnost podatkov“ (INFOSEC) pomeni: uporabo varnostnih ukrepov za varovanje podatkov, ki se obdelujejo, hranijo ali prenašajo v komunikacijskih, informacijskih in drugih elektronskih sistemih, pred izgubo tajnosti, celovitosti ali razpoložljivosti, bodisi naključne bodisi namerne, ter za preprečitev izgube celovitosti in razpoložljivosti samih sistemov.

„Ukrepi INFOSEC“ vključujejo ukrepe računalniške varnosti, varnosti prenosa, oddajanja in kriptografske varnosti, ter odkrivanje, dokumentiranje in preprečevanje ogroženosti podatkov in sistemov.

„Območje informacijske tehnologije (IT)“ pomeni: območje, ki vsebuje enega ali več računalnikov, njihove lokalne periferne in shranjevalne enote, enote za nadzor in njim podrejena omrežja ter komunikacijsko opremo.

Opomba:

Sem ne spada ločeno območje, v katerem so oddaljene periferne naprave ali terminali/delovne postaje, četudi so te naprave povezane z opremo na območju informacijske tehnologije (IT).

„Omrežje informacijske tehnologije (IT)“ pomeni: geografsko razširjeno organizacijo sistemov informacijske tehnologije (IT), ki so med seboj povezani zaradi izmenjave podatkov in ki vključujejo sestavne dele med seboj povezanih sistemov informacijske tehnologije (IT) ter njihov vmesnik s podpirajočimi podatkovnimi ali komunikacijskimi omrežji.

Opombe:

(1) Omrežje informacijske tehnologije (IT) lahko uporabi storitve enega ali več med seboj povezanih komunikacijskih omrežij za izmenjavo podatkov; več omrežij informacijske tehnologije (IT) lahko uporabi storitve skupnega komunikacijskega omrežja.

(2) Omrežje informacijske tehnologije (IT) se označi za „lokalno“, če povezuje več računalnikov na isti lokaciji.

„Varnostne lastnosti omrežja informacijske tehnologije (IT)“ vključujejo varnostne lastnosti posameznih sistemov informacijske tehnologije (IT), ki sestavljajo omrežje skupaj s tistimi dodatnimi komponentami in lastnostmi, povezanimi z omrežjem kot takim (na primer komunikacije omrežij, mehanizmi in postopki varnostnega prepoznavanja in označevanja, kontrole dostopa, programi in revizijske sledi), ki so potrebne zaradi zagotavljanja sprejemljive stopnje varovanja tajnih podatkov.

„Sistem informacijske tehnologije (IT)“ pomeni: celoto opreme, metod in postopkov in, če je potrebno, osebja, organiziranega za opravljanje nalog v zvezi z obdelavo podatkov.

Opombe:

(1) To pomeni celoto naprav, konfiguriranih za obdelavo podatkov znotraj sistema.

(2) Takšni sistemi lahko služijo v podporo posvetovanju, vodenju, nadzoru, komunikacijam, znanstvenim ali administrativnim aplikacijam, vključno z obdelovanjem besedil.

(3) Meje sistema so na splošno določene kot elementi, ki so pod nadzorom enega samega imetnika tehničnega sistema.

(4) Sistem informacijske tehnologije (IT) lahko vsebuje podsisteme, od katerih so nekateri tudi sami sistemi informacijske tehnologije (IT).

„Varnostne lastnosti sistema informacijske tehnologije (IT)“ obsegajo vse funkcije, značilnosti in lastnosti strojne opreme/sistemskih programov/programske opreme; obratovalne postopke, postopke odgovornosti in kontrole dostopa, območje informacijske tehnologije (IT), oddaljena območja terminalov/delovnih postaj in okvir upravljanja, fizično strukturo in naprave, nadzor nad osebjem in komunikacijami, potreben za zagotavljanje sprejemljive stopnje varovanja tajnih podatkov, ki se obdelujejo znotraj sistema informacijske tehnologije (IT).

„Varnostni uradnik za lokalno informatiko“ (LISO) je uradnik v službi Komisije, ki je pristojen za koordinacijo in nadzor varnostnih ukrepov na svojem področju.

„Varnostni način delovanja na več stopnjah“ pomeni: način delovanja, pri katerem NISO VSI posamezniki, ki imajo dostop do sistema, varnostno preverjeni do najvišje stopnje tajnosti podatkov, ki se v tem sistemu obdelujejo, ter kjer splošna „potreba vedeti“ za podatke, ki se v sistemu obdelujejo, NE velja za VSE osebe, ki imajo dostop do sistema.

Opombe:

(1) Ta način delovanja trenutno dovoljuje obdelavo podatkov različnih stopenj tajnosti in različnih oznak kategorij podatkov.

(2) Dejstvo, da vse osebe niso upravičene do dostopa do podatkov z najvišjo stopnjo tajnosti in da za vse osebe ne velja „potreba vedeti“, pomeni, da se pri varnostnih lastnostih računalnikov zahteva, da zagotovijo selektiven dostop do in ločevanje podatkov znotraj sistema.

„Dislocirano območje terminala/delovne postaje“ pomeni: območje, kjer so računalniška oprema, njene lokalne periferne naprave ali terminali/delovne postaje ter vsa pripadajoča komunikacijska oprema, ki je ločeno od območja informacijske tehnologije (IT).

„Varnostni postopki obratovanja“ so postopki imetnika tehničnih sistemov, ki določajo načela, ki jih je treba sprejeti glede varnostnih zadev, obratovalne postopke, po katerih je treba delovati ter dolžnosti osebja.

„Varnostni način delovanja SYSTEM-HIGH“ je način delovanja, pri katerem so VSI posamezniki, ki imajo dostop do sistema, varnostno preverjeni do najvišje stopnje tajnosti podatkov, ki se v tem sistemu obdelujejo, vendar kjer splošna potreba vedeti glede podatkov, ki se v sistemu obdelujejo, NE velja za VSE posameznike, ki imajo dostop do sistema.

Opombe:

(1) Ker nimajo vsi uporabniki splošne „potrebe vedeti“ pomeni, da se pri varnostnih lastnostih računalnika zahteva, da zagotavljajo selektiven dostop do ali ločevanje podatkov znotraj sistema.

(2) Druge varnostne lastnosti (na primer, materialna varnost, varnost osebja in proceduralna varnost) se prilagodijo zahtevam za najvišjo stopnjo tajnosti in vse oznake kategorij podatkov, obdelanih znotraj sistema.

(3) Vsi podatki, ki se obdelujejo ali so na razpolago sistemu v tem načinu delovanja skupaj z ustvarjenimi izhodnimi podatki, se zavarujejo, dokler ni drugače določeno, kakor da bi spadali pod oznako kategorij podatkov in v najvišjo stopnjo tajnosti, razen če ni za vsako prisotno funkcionalnost označevanja na voljo sprejemljiva raven zanesljivosti.

„Opredelitev varnostnih zahtev, ki so specifične za sistem“ (SSRS), je popolna in izključna opredelitev varnostnih načel, ki jih je treba upoštevati, in podrobnih varnostnih zahtev, ki jih je treba izpolniti. Temelji na varnostni politiki Komisije in oceni tveganja ali pa jo oblikujejo parametri, ki zajemajo operacijsko okolje, najnižjo stopnjo varnostnega preverjanja osebja, najvišjo stopnjo tajnosti obdelanih podatkov, varnostni način delovanja ali zahteve za uporabnike. Opredelitev varnostnih zahtev, ki so specifične za sistem (SSRS), je sestavni del dokumentacije projekta, ki se predloži pristojni službi za tehnično, proračunsko in varnostno odobritev. V svoji končni obliki opredelitev varnostnih zahtev, ki so specifične za sistem (SSRS), pomeni popolno opredelitev varnega sistema.

„Imetnik tehničnih sistemov“ (TSO) je služba, ki je pristojna za oblikovanje, vzdrževanje, delovanje in zapiranje sistema.

Protiukrepi „TEMPEST“: so varnostni ukrepi, namenjeni varovanju opreme in komunikacijske infrastrukture proti ogrožanju tajnih podatkov s strani nenamernih elektromagnetnih oddajanj in s prevodnostjo.

25.3 **Pristojnosti na področju varnosti**

25.3.1 *Splošno*

Med naloge svetovalne skupine za varnostno politiko Komisije, opredeljene v oddelku 12, sodijo zadeve INFOSEC. Ta skupina organizira svoje dejavnosti tako, da lahko zagotavlja strokovno svetovanje o zgoraj navedenih zadevah.

Varnostni urad Komisije je pristojen za sprejem podrobnejših predpisov o INFOSEC na podlagi določb tega poglavja.

V primeru problemov v zvezi z varnostjo (nezgode, kršitve itd.) Varnostni urad Komisije takoj ukrepa.

Varnostni urad Komisije ima enoto INFOSEC.

25.3.2 *Služba za akreditacijo varnosti (SAA)*

Vodja Varnostnega urada Komisije vodi službo za akreditacijo varnosti (SAA) za Komisijo. Služba za akreditacijo varnosti (SAA) je pristojna na splošnem področju varnosti in na specializiranih področjih INFOSEC, komunikacijske varnosti, varnosti kripto in varnosti tempest.

Služba za akreditacijo varnosti (SAA) je pristojna za zagotovitev skladnosti sistemov z varnostno politiko Komisije. Ena od njenih nalog je izdati sistemu odobritev za obdelavo tajnih podatkov EU do določene stopnje tajnosti v svojem operativnem okolju.

Pristojnost službe za akreditacijo varnosti (SAA) Komisije zajema vse delujoče sisteme znotraj prostorov Komisije. Kadar različne komponente sistema pridejo v pristojnost Službe za akreditacijo varnosti (SAA) Komisije in drugih služb za akreditacijo varnosti (SAA), lahko vse zadevne stranke imenujejo skupen odbor za akreditacijo, katerega usklajevanje vodi Služba za akreditacijo varnosti Komisije.

25.3.3 *Služba INFOSEC (IA)*

Vodja enote INFOSEC Varnostnega urada Komisije vodi službo INFOSEC za Komisijo. Služba INFOSEC je pristojna za:

— strokovno svetovanje in pomoč službam za akreditacijo varnosti (SAA);

— pomoč pri pripravi opredelitve varnostnih zahtev, ki so specifične za sisteme (SSRS);

— pregled opredelitve varnostnih zahtev, ki so specifične za sisteme (SSRS), za zagotovitev skladnosti s temi varnostnimi pravili in dokumenti o politiki in zasnovi INFOSEC;

— udeležba v akreditacijskih skupinah/odborih, kot je zahtevano, ter posredovanje priporočil glede akreditacije INFOSEC službi za akreditacijo varnosti (SAA);

— podpora dejavnostim usposabljanja in izobraževanja INFOSEC;

— strokovno svetovanje pri preiskavah nezgod, povezanih z INFOSEC;

— pripravo tehnično-strateških navodil, da bi se zagotovila uporaba samo odobrene programske opreme.

25.3.4 *Imetnik tehničnih sistemov (TSO)*

Za izvedbo ter delovanje nadzora in posebnih varnostnih lastnosti sistema je pristojen imetnik sistema, imenovan Imetnik tehničnega sistema (TSO). Za centralne sisteme je imenovan varnostni uradnik za centralno informatiko (CISO). Vsaka služba, če je potrebno, imenuje varnostnega uradnika za lokalno informatiko (LISO). Imetnik tehničnega sistema (TSO) je pristojen tudi za določitev varnostnih postopkov obratovanja (SecOPs), ta pristojnost pa velja v celotnem obdobju delovanja sistema od stopnje zasnove projekta do dokončne ukinitve.

Imetnik tehničnega sistema (TSO) določi varnostne standarde in prakse, ki jih mora izpolniti dobavitelj sistema.

Imetnik tehničnega sistema (TSO) lahko prenese del svojih nalog, če je potrebno, varnostnemu uradniku za lokalno informatiko (LISO). Ena sama oseba lahko izvaja različne funkcije INFOSEC.

25.3.5 *Imetnik podatkov (IO)*

Imetnik podatkov (IO) je odgovoren za tajne podatke EU (in druge podatke), ki jih je treba uvesti, obdelati in izdelati v tehničnih sistemih. Imetnik podatkov opredeli zahteve za dostop do teh podatkov v sistemih. To pristojnost lahko prenese na upravitelja podatkov ali upravitelja podatkovne baze znotraj svojega področja.

25.3.6 *Uporabniki*

Vsi uporabniki so dolžni ravnati tako, da njihova dejanja ne ogrožajo varnosti sistema, ki ga uporabljajo.

25.3.7 *Usposabljanje INFOSEC*

Izobraževanje in usposabljanje INFOSEC je na razpolago celotnemu osebju, ki ga potrebuje.

25.4 **Netehnični varnostni ukrepi**

25.4.1 *Varnost osebja*

Uporabniki sistema morajo opraviti varnostno preverjanje in imeti „potrebo vedeti“, kakor je to primerno za stopnjo tajnosti in vsebino podatkov, ki se obdelujejo znotraj določenega sistema. Za dostop do nekatere opreme ali podatkov, značilnih za varnost sistemov, je potrebno posebno pooblastilo, izdano po predpisanem postopku Komisije.

Služba za akreditacijo varnosti (SAA) določi vsa občutljiva mesta in opredeli stopnjo odobritve in nadzora, ki se zahteva za celotno osebje, ki mesta zaseda.

Sistemi se določijo in opredelijo tako, da se olajša porazdelitev nalog in odgovornosti med osebje, s čimer se prepreči, da bi samo ena oseba vedela vse o ključnih točkah varnosti sistema ali imela nad njimi popoln nadzor.

Območja informacijske tehnologije (IT) in dislocirana območja terminalov/delovnih postaj, v katerih je mogoče spreminjati varnost sistema, ne zaseda samo en pooblaščen uradnik ali drug uslužbenec.

Varnostne nastavitve sistema spreminjata najmanj dve pooblaščeni osebi v medsebojnem sodelovanju.

25.4.2 *Materialna varnost*

Območja informacijske tehnologije (IT) in dislocirana območja terminalov/delovnih postaj (kot so opredeljena v oddelku 25.2), v katerih se s sredstvi informacijske tehnologije (IT) obdelujejo podatki s stopnjo tajnosti CONFIDENTIEL UE in z višjo stopnjo, ali kjer je omogočen potencialni dostop do teh podatkov, se opredelijo kot varnostna območja EU razreda I ali razreda II.

25.4.3 *Nadzor dostopa do sistema*

Vsi podatki in gradivo, ki omogočajo nadzor dostopa do sistema, se zavarujejo z ukrepi, ki so sorazmerni z najvišjo stopnjo tajnosti in oznako stopnje tajnosti podatkov, do katere se dostop lahko dovoli.

Podatki in gradivo za nadzor dostopa do podatkov se, kadar ne služijo več temu namenu, uničijo v skladu z določbami iz oddelka 25.5.4.

25.5 **Tehnični varnostni ukrepi**

25.5.1 *Varnost podatkov*

Dolžnost osebe izvora podatkov je, da opredeli in razvrsti vse dokumente, ki so nosilci podatkov, bodisi na papirju ali na računalniškem nosilcu shranjevanja. Vsaka stran izpisa na papirju je zgoraj in spodaj označena s stopnjo tajnosti. Izpis, bodisi na papirju ali na računalniškem shranjevalnem nosilcu, ima enako stopnjo tajnosti, kakor je najvišja stopnja tajnosti podatkov, ki se uporabljajo pri njihovi izdelavi. Način delovanja sistema lahko vpliva tudi na stopnjo tajnosti izdaj tega sistema.

Dolžnost služb Komisije in njihovih imetnikov podatkov je upoštevati težave kopičenja posameznih elementov podatkov in sklepov, ki jih je mogoče pridobiti iz sorodnih elementov, ter določiti, ali je višja stopnja tajnosti ustrezna za celoto podatkov ali ne.

Dejstvo, da so lahko podatki v obliki okrajšane kode, kode prenosa ali v kakršnikoli obliki binarnega prikaza, ne zagotavlja varnosti in zaradi tega ne sme vplivati na stopnjo tajnosti podatkov.

Kadar se podatki prenesejo iz enega sistema v drugega, se zavarujejo med prenosom in v sprejemnem sistemu na način, ki je sorazmeren z originalno stopnjo tajnosti in kategorijo podatkov.

Vsi računalniški nosilci podatkov se obravnavajo na način, ki je v sorazmerju z najvišjo stopnjo tajnosti shranjenih podatkov ali oznake nosilcev in morajo biti vedno ustrezno zavarovani.

Računalniški nosilci shranjevanja za ponovno uporabo, ki se uporabljajo za zapisovanje tajnih podatkov EU, ohranijo najvišjo stopnjo tajnosti, za katero so bili kadarkoli uporabljeni, vse dokler navedenim podatkom ni ustrezno znižana ali odpravljena stopnja tajnosti in nosilcem ustrezno ponovno določena stopnja tajnosti ali dokler nosilcem ni odpravljena stopnja tajnosti ali pa dokler nosilci niso uničeni v skladu s postopkom, ki ga določi Služba za akreditacijo varnosti (SAA) (glej 25.5.4).

25.5.2 *Nadzor in vknjižba podatkov*

Evidenca dostopa do tajnih podatkov s stopnjo SECRET UE in z višjo stopnjo, se vodi avtomatsko (revizijska sled) ali z ročnimi vpisi v vpisnik. Ta evidenca se hrani v skladu s tem pravilnikom.

Izhodni izpisi tajnih podatkov EU, hranjeni znotraj področja informacijske tehnologije (IT), se lahko obravnavajo kot eno tajno gradivo in jih ni treba vpisovati v vpisnik, pod pogojem, da je to gradivo prepoznavno opredeljeno, označeno s svojo stopnjo tajnosti in pod primernim nadzorom.

Kadar izhodni izpisi pridejo iz sistema, ki obdeluje tajne podatke EU, in se prenesejo na območje terminala/delovne postaje, ki je dislocirano od področja informacijske tehnologije (IT), se s soglasjem Službe za akreditacijo varnosti (SAA) določijo postopki za nadzor in registracijo izdanih podatkov. Za podatke s stopnjo SECRET UE in z višjo stopnjo takšni postopki vključujejo posebna navodila za vknjižbo podatkov.

25.5.3 *Ravnanje z računalniškimi nosilci podatkov in nadzor nad njimi*

Z vsemi računalniškimi nosilci podatkov s stopnjo CONFIDENTIEL UE in z višjo stopnjo se ravna kot z gradivom, pri čemer veljajo splošna pravila. Identifikacijske oznake in oznake stopenj tajnosti se zaradi jasne prepoznave prilagodijo specifičnemu fizičnemu izgledu nosilca.

Uporabniki so dolžni zagotoviti, da so tajni podatki EU shranjeni na nosilcih skupaj z ustrezno oznako stopnje tajnosti in zavarovani. Določijo se postopki, da se za vse stopnje tajnosti podatkov EU zagotovi, da je shranjevanje podatkov na računalniškem nosilcu podatkov opravljeno v skladu s tem pravilnikom.

25.5.4 *Odprava stopenj tajnosti in uničenje računalniških nosilcev podatkov*

Računalniškim nosilcem podatkov, uporabljenim za evidentiranje tajnih podatkov EU, se lahko znižajo ali odpravijo stopnje tajnosti v skladu s postopkom, ki ga določi Služba za akreditacijo varnosti (SAA).

Računalniškim nosilcem podatkov, na katerih so bili shranjeni podatki TRÈS SECRET UE ali posebna kategorija podatkov, se stopnja tajnosti ne odpravi niti se ponovno ne uporabijo.

Če računalniškemu nosilcu podatkov ni mogoče odpraviti stopnje tajnosti ali če ni namenjen ponovni uporabi, se uniči v skladu z zgoraj navedenim postopkom.

25.5.5 *Varnost komunikacij*

Vodja Varnostnega urada Komisije je pristojen za Kripto.

Kadar se tajni podatki EU prenašajo po elektromagnetni poti, se izvajajo posebni ukrepi za varovanje tajnosti, celovitosti in razpoložljivosti takšnih prenosov. Služba za akreditacijo varnosti (SAA) določi zahteve za varstvo prenosov pred odkritjem in prekinitvijo. Podatki, ki se prenašajo po komunikacijskem sistemu, se varujejo na podlagi zahtev po tajnosti, celovitosti in razpoložljivosti.

Kadar so zahtevane kriptografske metode za zagotavljanje tajnosti, celovitosti in razpoložljivosti, takšne metode in z njimi povezane produkte posebej za ta namen odobri Služba za akreditacijo varnosti (SAA) v funkciji službe Kripto.

Med prenosom se tajnost podatkov s stopnjo tajnosti SECRET UE in z višjo stopnjo zavaruje s kriptografskimi metodami ali produkti, ki jih odobri član Komisije, pristojen za varnostne zadeve, po posvetu s Svetovalno skupino za varnostno politiko Komisije. Med prenosom se tajnost podatkov s stopnjo tajnosti CONFIDENTIEL UE ali RESTREINT UE, zavaruje s kriptografskimi metodami ali produkti, ki jih odobri služba Kripto pri Komisiji po posvetu s Svetovalno skupino za varnostno politiko Komisije.

Podrobna pravila, ki veljajo za prenos tajnih podatkov EU, se določijo v posebnih varnostnih navodilih, ki jih sprejme Varnostni urad Komisije po posvetu s Svetovalno skupino za varnostno politiko Komisije.

V izjemnih delovnih okoliščinah se lahko podatki s stopnjo tajnosti RESTREINT UE, CONFIDENTIEL UE in SECRET UE prenesejo kot čisto besedilo, pod pogojem, da vsak tak primer izrecno odobri in ustrezno registrira imetnik podatkov (IO). Do takšnih izjemnih okoliščin pride:

(a) v času preteče ali dejanske krize, spopada ali vojnih razmer, in

(b) kadar je hitrost dostave največjega pomena, sredstva kodiranja pa niso na voljo in se ocenjuje, da prenesenih podatkov ni mogoče pravočasno izkoristiti za negativno vplivanje na potek operacij.

Sistem mora biti sposoben onemogočiti dostop do tajnih podatkov EU v katerem koli ali v vseh dislociranih delovnih postajah ali terminalih, če jih je treba izključiti na fizičen način ali s pomočjo posebnih elementov programske opreme, ki jih odobri Služba za akreditacijo varnosti (SAA).

25.5.6 *Varnost v zvezi z namestitvijo in sevanjem*

Začetna postavitev sistemov in vse večje spremembe v zvezi z njo se določijo tako, da postavitev izvajajo varnostno preverjeni delavci pod stalnim nadzorstvom tehnično usposobljenega osebja, ki je varnostno preverjeno glede dostopa do tajnih podatkov EU na stopnji, ki je enaka najvišji stopnji tajnosti, ki jo bo sistem predvidoma hranil in obdeloval.

Sistemi, v katerih se obdelujejo podatki s stopnjo tajnosti CONFIDENTIEL UE in z višjo stopnjo, se varujejo tako, da njihove varnosti ne morejo ogroziti nevarna sevanja in/ali prevodnost, katerih preučevanje in nadzor se označi kot „Tempest“.

Protiukrepe Tempest pregleda in odobri služba Tempest (glej 25.3.2).

25.6 **Varnost med obdelavo**

25.6.1 *Varnostni postopki delovanja (SecOPs)*

Varnostni postopki delovanja (SecOPs) opredeljujejo načela, ki jih je treba sprejeti v zvezi z varnostnimi zadevami, operativne postopke, ki jih je treba opravljati, ter odgovornosti osebja. Varnostni postopki delovanja se določijo v okviru pristojnosti imetnika tehničnih sistemov (TSO).

25.6.2 *Varovanje programske opreme/upravljanje konfiguracije*

Varovanje uporabniških programov se vzpostavi na podlagi ocene stopnje tajnosti samega programa in ne na podlagi stopnje tajnosti podatkov, ki jih obdeluje. Uporabljene različice programske opreme se potrdijo v rednih časovnih obdobjih, da bi se zagotovila njihova celovitost in pravilno delovanje.

Nove ali spremenjene različice programske opreme se ne uporabljajo za obdelovanje tajnih podatkov EU, dokler jih ne potrdi imetnik tehničnih sistemov (TSO).

25.6.3 *Preverjanje prisotnosti škodljive programske opreme/računalniških virusov*

Preverjanje prisotnosti škodljive programske opreme/računalniških virusov se izvaja redno v skladu z zahtevami Službe za akreditacijo varnosti (SAA).

Preden se računalniški nosilci podatkov vključijo v katerikoli sistem, se na njih, ko prispejo v Komisijo, preveri prisotnost kakršne koli škodljive programske opreme ali računalniških virusov.

25.6.4 *Vzdrževanje*

Pogodbe in postopki časovno načrtovanega in pravočasnega vzdrževanja sistemov, za katere je bila pripravljena opredelitev varnostnih zahtev, ki so specifične za sistem (SSRS), določajo zahteve in dogovore za vzdrževalno osebje in z njimi povezano opremo, ki vstopa na območje informacijske tehnologije (IT).

Zahteve so jasno navedene v opredelitvi varnostnih zahtev, ki so specifične za sistem (SSRS), postopki pa se jasno določijo v varnostnih postopkih delovanja (SecOPs). Pogodbeno vzdrževanje, ki zahteva postopke diagnosticiranja oddaljenega dostopa, se dovoli le v izjemnih okoliščinah pod strogim varnostnim nadzorom in le z dovoljenjem Službe za akreditacijo varnosti (SAA).

25.7 **Naročila**

25.7.1 *Splošno*

Vsak varnostni produkt, ki ga je treba naročiti za uporabo v sistemu, mora biti ocenjen in certificiran ali biti v postopku ocenjevanja in certificiranja s strani ustreznega ocenjevalnega organa ali organa za certificiranje po mednarodno priznanih merilih (npr. Skupna merila za varnostno ocenitev informacijske tehnologije (IT), glej ISO 15408). V posebnem postopku je treba pridobiti soglasje Svetovalnega odbora za naročila in pogodbe (ACPC).

Pri presoji, ali naj se oprema, zlasti računalniški nosilci podatkov, najamejo ali kupijo, je treba upoštevati, da takšne opreme, ki je bila enkrat že uporabljena za obdelavo tajnih podatkov EU, ni mogoče odnesti iz ustrezno zavarovanega okolja brez predhodne odprave stopnje tajnosti z odobritvijo Službe za akreditacijo varnosti (SAA), ter da takšna odobritev ni vedno možna.

25.7.2 *Akreditacija*

Vse sisteme, za katere so bile določene varnostne zahteve, ki so specifične za sistem (SSRS), pred obdelavo tajnih podatkov EU akreditira Služba za akreditacijo varnosti (SAA) na podlagi podatkov iz opredelitve varnostnih zahtev, ki so specifične za sistem (SSRS), varnostnih postopkov delovanja (SecOPs) in vse druge ustrezne dokumentacije. Podsistemi in dislocirani terminali/delovne postaje se akreditirajo kot del vseh sistemov, s katerimi so povezani. Kadar sistem uporablja Komisija in druge organizacije, se Komisija in pristojni varnostni organi dogovorijo o akreditaciji.

Postopek akreditacije se lahko izvede v skladu s strategijo akreditacije, ki ustreza določenemu sistemu in ga določi Služba za akreditacijo varnosti (SAA).

25.7.3 *Ocenjevanje in certificiranje*

Pred akreditacijo se v nekaterih primerih varnostne lastnosti strojne opreme, sistemskih programov in programske opreme ocenijo in certificirajo glede zmožnosti varovanja podatkov na predvideni stopnji tajnosti.

Zahteve za ocenitev in certificiranje se vključijo v načrtovanje sistema in se jasno navedejo v opredelitvi varnostnih zahtev, ki so specifične za sistem (SSRS).

Postopki ocenjevanja in certificiranja se izvedejo v skladu s sprejetimi smernicami, izvaja pa jih tehnično usposobljeno in varnostno preverjeno osebje, ki deluje v imenu imetnika tehničnih sistemov **(TSO).**

Osebje lahko da na voljo pristojna služba za ocenjevanje in certificiranje države članice ali njeni imenovani predstavniki, na primer pristojni in varnostno preverjeni pogodbeni partner.

Postopki ocenjevanja in certificiranja se lahko skrajšajo (na primer tako, da zajemajo samo vidike integracije), kadar sistemi temeljijo na obstoječih nacionalno ocenjenih in certificiranih računalniških varnostnih produktih.

25.7.4 **Redno preverjanje varnostnih značilnosti za kontinuirano akreditacijo**

Imetnik tehničnih sistemov (TSO) določi postopke rednega nadzora, ki zagotavlja vse varnostne lastnosti sistema.

Vrste sprememb, ki bi sprožile ponovno akreditacijo ali zahtevale predhodno odobritev službe za akreditacijo varnosti (SAA), se jasno opredelijo in navedejo v opredelitvi varnostnih zahtev, ki so specifične za sistem (SSRS). Po vsaki spremembi, popravilu ali napaki, ki bi lahko vplivala na varnostne lastnosti sistema, imetnik tehničnih sistemov (TSO) zagotovi, da je opravljen pregled za zagotovitev varnostnih lastnosti. Kontinuirana akreditacija sistema je praviloma odvisna od pozitivne ocene pregledov.

Vse sisteme, ki imajo varnostne lastnosti, redno pregleda ali preveri Služba za akreditacijo varnosti (SAA). V zvezi s sistemi, ki obdelujejo podatke s stopnjo tajnosti TRÈS SECRET UE, se izvedejo pregledi najmanj enkrat letno.

25.8 *Začasna ali občasna uporaba*

25.8.1 **Varnost mikroračunalnikov/osebnih računalnikov**

Mikroračunalniki/osebni računalniki (PC-ji) z vgrajenimi diski (ali drugimi nosilci s trajnim shranjevanjem), ki delujejo bodisi samostojno ali so mrežno konfigurirani, ter prenosne računalniške naprave (na primer prenosni osebni računalniki in elektronski „notesniki“) z vgrajenimi trdimi diski, se upoštevajo kot nosilci podatkov v istem pomenu kakor računalniške diskete ali drugi računalniški nosilci podatkov.

Za to opremo se zagotovi stopnja varovanja v smislu dostopa, obdelave, shranjevanja in prenosa, ki je sorazmerna z najvišjo stopnjo tajnosti podatkov, ki so bili kdaj koli shranjeni ali obdelovani (do znižanja ali odprave stopnje tajnosti v skladu z odobrenimi postopki).

25.8.2 **Uporaba zasebne opreme IT za delo v službene namene Komisije**

Uporaba zasebnih računalniških nosilcev podatkov, programske opreme in strojne opreme informacijske tehnologije (IT) (na primer osebnih računalnikov in prenosnih računalniških naprav), ki imajo zmogljivost shranjevanja, za obdelavo tajnih podatkov EU ni dovoljena.

Strojna oprema, programska oprema in nosilci v zasebni lasti se ne vnašajo na območja razreda I ali razreda II, kjer se obdelujejo tajni podatki EU, brez pisnega dovoljenja vodje Varnostnega urada Komisije. Ta odobritev se lahko zagotovi le iz tehničnih razlogov v izjemnih primerih.

25.8.3 **Uporaba opreme IT, ki je v lasti izvajalca ali države članice, za delo v službene namene Komisije**

Uporabo opreme informacijske tehnologije (IT), ki je v lasti izvajalca, in programske opreme v organizacijah za podporo pri delu v službene namene Komisije lahko dovoli vodja Varnostnega urada Komisije. Prav tako se lahko dovoli uporaba opreme informacijske tehnologije (IT) in programske opreme države članice; v tem primeru se oprema informacijske tehnologije (IT) prenese pod nadzor ustreznega inventurnega popisa Komisije. Če je treba opremo informacijske tehnologije (IT) uporabiti za obdelavo tajnih podatkov EU, se je treba v obeh primerih posvetovati s Službo za akreditacijo varnosti (SAA), da bi se ustrezno upoštevali in izvajali elementi INFOSEC, ki veljajo za uporabo navedene opreme.

26. POSREDOVANJE TAJNIH PODATKOV EU TRETJIM DRŽAVAM ALI MEDNARODNIM ORGANIZACIJAM

26.1.1 *Načela posredovanja tajnih podatkov EU*

Komisija kot kolegijski organ odloča o posredovanju tajnih podatkov EU tretjim državam ali mednarodnim organizacijam na podlagi:

— narave in vsebine takih podatkov;

— prejemnikove potrebe vedeti;

— prednosti za EU.

Osebo izvora tajnih podatkov EU, ki naj se posredujejo, se zaprosi za soglasje.

Navedene odločitve se sprejmejo od primera do primera, odvisno od:

— zaželene stopnje sodelovanja z zadevnimi tretjimi državami ali mednarodnimi organizacijami;

— tajnosti, ki jim jo je mogoče pripisati – ki izhaja iz stopnje varnosti, ki bi veljala za tajne podatke EU, zaupane tem državam ali organizacijam, ter skladnosti med varnostnimi pravili, ki veljajo tam, ter pravili, ki veljajo v EU. Svetovalna skupina za varnostno politiko Komisije o tej zadevi posreduje svoje mnenje Komisiji.

Ob sprejetju tajnih podatkov EU tretje države ali mednarodne organizacije zagotovijo, da se bodo podatki uporabili zgolj za spodbujanje posredovanja ali izmenjave podatkov in da se bo zagotovilo varovanje, ki ga zahteva Komisija.

26.1.2 *Stopnje*

Ko Komisija sklene, da se tajni podatki lahko posredujejo zadevni državi ali mednarodni organizaciji ali z njima izmenjajo, se odloči tudi o stopnji možnega sodelovanja. To je zlasti odvisno od varnostne politike in predpisov, ki veljajo v navedeni državi ali organizaciji.

Stopnje sodelovanja so:

Stopnja 1

Sodelovanje s tretjimi državami ali mednarodnimi organizacijami, katerih varnostna politika in predpisi so zelo sorodni varnostni politiki in predpisom EU.

Stopnja 2

Sodelovanje s tretjimi državami ali mednarodnimi organizacijami, katerih varnostna politika in predpisi se bistveno razlikujejo od varnostne politike in predpisov EU.

Stopnja 3

Občasno sodelovanje s tretjimi državami ali mednarodnimi organizacijami, katerih politike in varnostnih predpisov ni mogoče oceniti.

Za vsako stopnjo sodelovanja so določeni postopki in varnostni predpisi, vsebovani v Dodatkih 3, 4 in 5.

26.1.3 *Varnostna ureditev*

Ko se Komisija odloči, da obstaja trajna ali dolgoročna potreba po izmenjavi tajnih podatkov med Komisijo in tretjimi državami ali drugimi mednarodnimi organizacijami, skupaj z njimi sestavi „sporazume o varnostnih postopkih za izmenjavo tajnih podatkov“, v katerih se opredelijo namen sodelovanja in vzajemna pravila glede varovanja izmenjanih podatkov.

V primeru občasnega sodelovanja na stopnji 3, ki je po opredelitvi omejeno s časom in namenom, je mogoče „sporazum o postopkih za izmenjavo tajnih podatkov“ nadomestiti s preprostim memorandumom o soglasju, ki opredeljuje naravo tajnih podatkov za izmenjavo in vzajemne obveznosti v zvezi z navedenimi podatki, pod pogojem, da nima višje stopnje tajnosti kot RESTREINT UE.

O osnutkih sporazumov o varnostnih postopkih ali memorandumih o soglasju razpravlja Svetovalna skupina za varnostno politiko Komisije, še preden se predložijo Komisiji v odločanje.

Član Komisije, pristojen za varnostne zadeve, organe, pristojne za državno varnost (NSA) držav članic zaprosi za vso potrebno pomoč, da bi zagotovil, da se podatki, ki jih je treba posredovati, uporabljajo in varujejo v skladu z določbami iz sporazumov o varnostnih postopkih ali memorandumov o soglasju.

Dodatek 1

PRIMERJAVA STOPENJ TAJNOSTI NA PODROČJU DRŽAVNE VARNOSTI

Stopnja tajnosti EU	TRÈS SECRET UE	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Stopnja tajnosti NATO (1)				
Stopnja tajnosti ZEU	Focal Top Secret	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Stopnja tajnosti EURATOM (2)	EURATOM Top Secret	EURATOM SECRET	EURATOM Confidential	EURATOM Restricted
Belgija	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Danska	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Nemčija	STRENG GEHEIM	GEHEIM	VS (3) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGE-BRAUCH
Grčija	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Španija	Secreto	Reservado	Confidencial	Difusión limitada
Francija	Très Secret Défense (4)	Secret Défense	Confidentiel Défense	Diffusion restreinte
Irska	Top Secret	Secret	Confidential	Restricted
Italija	Segretissimo	Segreto	Riservatissimo	Riservato
Luksemburg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Nizozemska	Stg. Zeer Geheim	Stg. Geheim	Stg. Confidentieel	
Avstrija	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Portugalska	Muito Secreto	Secreto	Confidencial	Reservado
Finska	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Švedska	Luottamuksellinen	Hemlig	Hemlig	Hemlig
Združeno kraljestvo	Top Secret	Secret	Confidential	Restricted

(1) NATO – skladnost s stopnjami tajnosti NATO bo vzpostavljena, ko se bodo končala pogajanja o Varnostnem sporazumu med Komisijo in NATO-m.

(2) Uredba EURATOM št. 3 z dne 31. julija 1958 o varovanju tajnih podatkov EURATOM.

(3) Nemčija: VS = Verschlusssache (tajni podatki)

(4) Francija: stopnja tajnosti „Très Secret Défense“, ki zajema vladna prednostna vprašanja, se lahko spremeni le z dovoljenjem predsednika vlad

DODATEK 2

NAVODILO ZA UPORABO STOPENJ TAJNOSTI

To navodilo je samo usmeritvene narave in ga ni možno razumeti kot da spreminja temeljne določbeiz oddelkov 16, 17, 20 in 21.

Stopnja tajnosti	Kdaj	Kdo	Namestitve stopenj tajnosti	Znižanje/odprava stopnje tajnosti/uničenje	
				Kdo	Kdaj
TRÈS SECRET UE: Ta stopnja tajnosti velja le za podatke in gradivo, katerega nedovoljeno razkritje bi lahko povzročilo izjemno težko škodo za bistvene interese Evropske unije ali ene ali več njenih držav članic [16.1].	Seznanitev z zadevami s stopnjo tajnosti TRÈS SECRET UE s strani nepooblaščenih oseb bi lahko: — neposredno ogrozila notranjo stabilnost EU ali ene od njenih držav članic ali prijateljskih držav — povzročila izredno resno škodo odnosom med prijateljskimi vladami — neposredno pripeljala do številnih izgub življenja — povzročila izredno resno škodo operativni učinkovitosti ali varnosti oboroženih sil držav članic ali drugih sodelujočih ali trajni učinkovitosti izredno dragocenih varnostnih ali obveščevalnih operacij — povzročila resno dolgoročno škodo gospodarstvu EU ali držav članic.	Formalno pooblaščene osebe (osebe izvora), generalni direktorji, vodje služb [17.1] Osebe izvora določijo datum, čas ali dogodek, ko se lahko vsebini zniža ali odpravi njena stopnja tajnosti [16.2] Osebe izvora pregledujejo dokumente najmanj vsakih pet let, da bi se zagotovila potrebnost originalne stopnje tajnosti [17.3].	Na dokumente TRÈS SECRET UE se namesti stopnja tajnosti TRÈS SECRET UE ali, kjer je primerno, varnostni označevalnik in/ali obrambna oznaka – SEVOP, in sicer z mehanskimi sredstvi in ročno [16.4, 16.5, 16.3]. Stopnje tajnosti in varnostni označevalniki EU se označijo zgoraj in spodaj na sredini vsake strani, vsaka stran pa se oštevilči. Vsak dokument je opremljen z referenčno številko in datumom; ta referenčna številka je na vsaki strani. Če je treba dokumente razdeliti v več izvodih, ima vsak izvod številko izvoda, ki je na prvi strani skupaj s skupnim številom strani. Vse priloge in dodatki se navedejo na prvi strani [21.1].	Za odpravo ali znižanje stopnje tajnosti skrbi le oseba izvora, ki o vsaki spremembi obvesti vse nadaljnje naslovnike, katerim pošlje ali kopira dokument [17.3]. Dokumente TRÈS SECRET UE uniči centralni registrski urad ali podregistrski urad, ki je za dokumente odgovoren. Vsak uničen dokument se vpiše v potrdilo o uničenju, ki ga podpiše uradnik za nadzor TRÈS SECRET UE ter uradnik, ki je priča pri uničenju in je varnostno preverjen na ravni TRÈS SECRET UE. To se zapiše v vpisnik. Registrski urad hrani potrdila o uničenju skupaj z dokazili o razdelitvi, in sicer deset let [22.5].	Odvečni izvodi in dokumenti, ki niso več potrebni, se morajo uničiti [22.5]. Dokumenti TRÈS SECRET UE, vključno z vsemi odpadki, ki se obravnavajo kot tajni podatki in so nastali ob pripravi dokumentov TRÈS SECRET UE, kot so poškodovani izvodi, delovni osnutki, natipkana sporočila in indigo papir, se uničijo pod nadzorom uradnika za nadzor na ravni TRÈS SECRET UE, in sicer z zažigom, zmletjem, razrezom v pramene ali z drugačno spremembo v neprepoznavno in nesestavljivo obliko [22.5].

Stopnja tajnosti	Kdaj	Kdo	Namestitve stopenj tajnosti	Znižanje/odprava stopnje tajnosti/uničenje	
				Kdo	Kdaj
SECRET UE: Ta stopnja tajnosti velja le za tiste podatke in gradivo, katerega nedovoljeno razkritje bi lahko resno škodovalo bistvenim interesom Evropske unije ali ene ali več njenih držav članic [16.1].	Seznanitev z zadevami s stopnjo tajnosti SECRET UE, s strani nepooblaščenih oseb bi lahko: — povzročila napete mednarodne odnose — resno škodila odnosom med prijateljskimi vladami — neposredno ogrozila življenja ali resno škodila javnemu redu ali varnosti ali svobodi posameznika — povzročila izredno resno škodo operativni učinkovitosti ali varnosti oboroženih sil držav članic ali drugih sodelujočih ali trajni učinkovitosti izredno dragocenih varnostnih ali obveščevalnih operacij — povzročila znatno materialno škodo finančnim, monetarnim, gospodarskim in komercialnim interesom EU ali ene od njenih držav članic.	Pooblaščene osebe (osebe izvora), generalni direktorji, vodje služb [17.1]. Osebe izvora določijo datum ali časovno obdobje, ko se lahko vsebini zniža ali odpravi njena stopnja tajnosti [16.2] Osebe izvora pregledujejo dokumente najmanj vsakih pet let, da bi se zagotovila potrebnost originalne stopnje tajnosti [17.3].	Na dokumente SECRET UE se namesti stopnja tajnosti SECRET UE ali, kjer je primerno, varnostni označevalnik in/ali obrambna oznaka – SEVOP, in sicer z mehanskimi sredstvi in ročno [16.4, 16.5, 16.3]. Stopnje tajnosti in varnostni označevalniki EU se označijo zgoraj in spodaj na sredini vsake strani, vsaka stran pa se oštevilči. Vsak dokument je opremljen z referenčno številko in datumom; ta referenčna številka je na vsaki strani. Če je treba dokumente razdeliti v več izvodov, ima vsak izvod številko, ki je na prvi strani skupaj s skupnim številom strani. Vse priloge in dodatki se navedejo na prvi strani [21.1].	Za odpravo ali znižanje stopnje tajnosti skrbi le oseba izvora, ki o vsaki spremembi obvesti vse nadaljnje naslovnike, katerim pošlje ali kopira dokument [17.3]. Dokumente SECRET UE uniči registrski urad, ki je za te dokumente odgovoren, pod nadzorom varnostno preverjene osebe. Uničeni dokumenti SECRET UE se navedejo na podpisanih potrdilih o uničenju, ki jih hrani registrski urad skupaj z obrazci o uničenju najmanj tri leta [22.5].	Odvečni izvodi in dokumenti, ki niso več potrebni, se morajo uničiti [22.5]. Dokumenti SECRET UE, vključno z vsemi odpadki, ki se obravnavajo kot tajni podatki in so nastali ob pripravi dokumentov SECRET UE, kot so poškodovani izvodi, delovni osnutki, natipkana sporočila in indigo papir, se uničijo, in sicer z zažigom, zmletjem, razrezom v pramene ali z drugačno spremembo v neprepoznavno in nesestavljivo obliko [22.5].

Stopnja tajnosti	Kdaj	Kdo	Namestitve stopenj tajnosti	Znižanje/odprava stopnje tajnosti/uničenje	
				Kdo	Kdaj
CONFIDENTIEL UE: Ta stopnja tajnosti velja le za tiste podatke in gradivo, katerega nedovoljeno razkritje bi lahko škodovalo bistvenim interesom Evropske unije ali ene ali več njenih držav članic. [16.1].	Seznanitev z zadevami s stopnjo tajnosti CONFIDENTIEL UE s strani nepooblaščenih oseb bi lahko: — materialno škodovala diplomatskim odnosom, tj. povzročilo formalne proteste ali druge sankcije; — škodila varnosti ali svobodi posameznika; — povzročila izredno resno škodo operativni učinkovitosti ali varnosti oboroženih sil držav članic ali drugih sodelujočih ali trajni učinkovitosti izredno dragocenih varnostnih ali obveščevalnih operacij; — bistveno oslabila finančno sposobnost večjih organizacij; — ovirala preiskave ali omogočila izvršitev resnih kaznivih dejanj; — resno delovala proti finančnim, monetarnim, gospodarskim in komercialnim interesom EU ali držav članic; — resno ovirala razvoj ali delovanje glavnih politik EU; — ustavila ali kako drugače bistveno prekinjala pomembne dejavnosti EU.	Pooblaščene osebe (osebe izvora), generalni direktorji, vodje služb [17.1] Osebe izvora določijo datum ali časovno obdobje, ko se vsebini lahko zniža ali odpravi njena stopnja tajnosti. Osebe izvora pregledujejo dokumente najmanj vsakih pet let, da bi se zagotovila potrebnost originalne stopnje tajnosti [17.3].	Na dokumente CONFIDENTIEL UE se namesti stopnja tajnosti CONFIDENTIEL UE ali, kjer je primerno, varnostni označevalnik in/ali obrambna oznaka – SEVOP, in sicer z mehanskimi sredstvi in ročno ali s tiskanjem na predhodno žigosan registrirni papir [16.4, 16.5, 16.3]. Stopnje tajnosti EU se označijo zgoraj in spodaj na sredini vsake strani, vsaka stran pa se oštevilči. Vsak dokument je opremljen z referenčno številko in datumom; Vse priloge in dodatki se navedejo na prvi strani [21.1].	Za znižanje ali odpravo stopnje tajnosti skrbi le oseba izvora, ki o vsaki spremembi obvesti vse nadaljnje naslovnike, katerim pošlje ali kopira dokument [17.3]. Dokumente CONFIDENTIEL UE uniči registrski urad, ki je za te dokumente odgovoren, pod nadzorom varnostno preverjene osebe. Uničenje teh dokumentov se evidentira v skladu s predpisi držav članic in, v primeru decentraliziranih agencij Komisije ali EU, v skladu z navodili predsednika [22.5].	Odvečni izvodi in dokumenti, ki niso več potrebni, se morajo uničiti [22.5]. Dokumenti CONFIDENTIEL UE, vključno z vsemi odpadki, ki se obravnavajo kot tajni podatki in so nastali ob pripravi dokumentov CONFIDENTIEL UE, kot so poškodovane kopije, delovni osnutki, natipkana sporočila in indigo papir, se uničijo, in sicer z zažigom, zmletjem, razrezom v pramene ali z drugačno spremembo v neprepoznavno in nesestavljivo obliko. [22.5].

Stopnja tajnosti	Kdaj	Kdo	Namestitve stopenj tajnosti	Znižanje/odprava stopnje tajnosti/uničenje	
				Kdo	Kdaj
RESTREINT UE: Ta stopnja tajnosti velja za tiste podatke in gradivo, katerega nedovoljeno razkritje bi lahko bilo škodljivo za interese Evropske unije ali ene ali več njenih držav članic. [16.1].	Seznanitev z zadevami RESTREINT UE s strani nepooblaščenih oseb bi lahko: — imela škodljiv vpliv na diplomatske odnose — posameznikom povzročila resno stisko — otežila ohranitev operativne učinkovitosti ali varnosti oboroženih sil držav članic ali drugih sodelujočih — povzročila finančne izgube ali pospešila neprimerne pridobitve ali prednosti posameznikom ali podjetjem — kršila ustrezne spodbude k ohranitvi tajnosti podatkov, ki jih prispevajo tretje osebe — kršila pravne omejitve glede razkrivanja podatkov — škodila preiskavam ali omogočilo izvršitev kaznivega dejanja — slabo vplivala na EU ali države članice pri komercialnih ali političnih pogajanjih z drugimi — ovirala učinkovit razvoj ali izvajanje politik EU — ogrozila ustrezno upravljanje EU in njenih dejavnosti.	Pooblaščene osebe (osebe izvora), generalni direktorji, vodje služb [17.1]. Osebe izvora določijo datum, čas ali dogodek, ko se vsebini lahko zniža ali odpravi njena stopnja tajnosti [16.2]. Osebe izvora pregledujejo dokumente najmanj vsakih pet let, da bi se zagotovila potrebnost originalne stopnje tajnosti [17.3].	Na dokumente RESTREINT UE se namesti stopnja tajnosti RESTREINT UE in, kjer je primerno, varnostni označevalnik in/ali obrambna oznaka – SEVOP, in sicer z mehanskimi ali elektronskimi sredstvi [16.4, 16.5, 16.3]. Stopnja tajnosti in varnostni označevalniki EU so na vrhu prve strani, vsaka stran pa se oštevilči. Vsak dokument ima referenčno številko in datum [21.1].	Za odpravo stopnje tajnosti skrbi le oseba izvora, ki o vsaki spremembi obvesti vse nadaljnje naslovnike, katerim pošlje ali kopira dokument [17.3]. Dokumente RESTREINT UE uniči registrski urad, ki je za te dokumente odgovoren, ali uporabnik v skladu z navodili predsednika [22.5].	Odvečni izvodi in dokumenti, ki niso več potrebni, se uničijo [22.5].

Dodatek 3

Smernice za posredovanje tajnih podatkov EU tretjim državam ali mednarodnim organizacijam: stopnja sodelovanja 1

POSTOPKI

1. Pooblastilo za posredovanje tajnih podatkov EU državam, ki niso članice Evropske unije, ali drugim mednarodnim organizacijam, katerih varnostna politika in predpisi so primerljivi z varnostno politiko in predpisi EU, ima Komisija kot kolegijski organ.

2. Do sklenitve varnostnega sporazuma je član Komisije, pristojen za varnostne zadeve, pristojen za obravnavo zahtev za posredovanje tajnih podatkov EU.

3. Član Komisije pri tem:

   — prosi za mnenja oseb izvora tajnih podatkov EU, ki naj se posredujejo;

   — vzpostavi potrebne stike z organi, pristojnimi za varnost, držav ali mednarodnih organizacij upravičenk, da bi potrdil, ali so njihova varnostna politika in predpisi takšni, da zagotavljajo varovanje posredovanih tajnih podatkov v skladu s tem pravilnikom;

   — prosi za mnenje Svetovalno skupino za varnostno politiko Komisije glede možne tajnosti do držav upravičenk ali mednarodnih teles upravičencev.

4. Član Komisije, pristojen za varnostne zadeve, posreduje prošnjo in mnenje Svetovalne skupine za varnostno politiko Komisije v odločanje Komisiji.

VARNOSTNI PREDPISI ZA RAVNANJE UPRAVIČENCEV

5. Član Komisije, pristojen za varnostne zadeve, obvesti države ali mednarodne organizacije upravičenke o odločitvi Komisije glede odobritve posredovanja tajnih podatkov EU.

6. Odločitev glede posredovanja začne veljati, ko upravičenke dajo pisno zagotovilo, da bodo:

   — uporabile podatke le za dogovorjene namene;

   — varovale podatke v skladu z navedenimi varnostnimi predpisi in zlasti posebnimi pravili, določenimi v nadaljevanju.

7. Osebje

   (a) Število uradnikov, ki imajo dostop do tajnih podatkov EU, je na podlagi načela „potrebe vedeti“ strogo omejeno na tiste osebe, katerih naloge zahtevajo takšen dostop.

   (b) Vsi uradniki ali državljani, pooblaščeni za dostop do podatkov s stopnjo tajnosti CONFIDENTIEL UE ali z višjo stopnjo, imajo bodisi varnostno potrdilo za ustrezno stopnjo bodisi enakovredno varnostno dovoljenje, ki ju je izdala vlada njihove države.

8. Prenos dokumentov

   (a) Operativni postopki za prenos dokumentov se določijo s sporazumom. Do sklenitve takšnega sporazuma veljajo določbe iz oddelka 21. Sporazum zlasti določa registrske urade, katerim se tajni podatki EU posredujejo.

   (b) Če tajni podatki, katerih posredovanje je odobrila Komisija, zajemajo podatke TRÈS SECRET UE, država ali mednarodna organizacija upravičenka ustanovi centralni registrski urad EU in, če je potrebno, podregistrske urade EU. Ti registrski uradi uporabljajo določbe, ki so v celoti enakovredne določbam iz oddelka 22 tega pravilnika.

9. Registracija

   Takoj ko registrski urad prejme dokument CONFIDENTIEL UE ali z višjo stopnjo, ga uvrsti v poseben register, ki ga ima organizacija, s stolpci za datum prejema, podrobnosti dokumenta (datum, referenčna številka in številka kopije), njegovo stopnjo tajnosti, naslov, ime ali naziv prejemnika, datum vračila potrdila o prejemu in datum, ko se dokument vrne organu izvora EU ali ko se uniči.

10. Uničenje

(a) Tajni podatki EU se uničijo v skladu z navodili, določenimi v oddelku 22 tega pravilnika. Kopije potrdil o uničenju za dokumente SECRET UE in TRÈS SECRET UE se pošljejo registrskemu uradu EU, ki je dokumente posredoval.

(b) Tajni podatki EU se vključijo v načrte o nujnem uničenju za tajne dokumente pristojnih služb upravičencev.

11. Varovanje dokumentov

Sprejmejo se vsi ukrepi, da se nepooblaščenim osebam prepreči dostop do tajnih podatkov EU.

12. Kopije, prevodi in povzetki

Dokumenti CONFIDENTIEL UE ali SECRET UE se ne fotokopirajo in ne prevajajo niti se iz njih ne jemljejo povzetki brez dovoljenja vodje zadevne varnostne organizacije, ki te kopije, prevode in povzetke registrira in preveri ter jih po potrebi označi z žigom.

Reprodukcijo ali prevod dokumenta TRÈS SECRET UE odobri le organ izvora, ki opredeli število odobrenih kopij; če organa izvora ni mogoče določiti, se prošnja naslovi na Varnostno službo Komisije.

13. Kršitve varnosti

Kadar se krši varnost tajnih podatkov EU ali se sumi kršitev, se ob upoštevanju sklenjenega varnostnega sporazuma takoj sprejmejo naslednji ukrepi:

(a) opravi se preiskava, da se ugotovijo okoliščine kršitve varnosti;

(b) obveščen je Varnostni urad Komisije, pristojni organ za državno varnost (NSA) in organ izvora, ali pa se jasno navede, da slednji ni bil obveščen, če to ni bilo storjeno;

(c) sprejmejo se ukrepi za zmanjšanje vplivov kršitve varnosti;

(d) pretehtajo in izvedejo se ukrepi za preprečitev ponovne kršitve;

(e) izvedejo se vsi ukrepi, ki jih predlaga Varnostni urad Komisije, da se prepreči ponovna kršitev.

14. Inšpekcije

Varnostni urad Komisije lahko na podlagi soglasja z zadevnimi državami ali mednarodnimi organizacijami opravi presojo učinkovitosti ukrepov za varovanje tajnih podatkov EU.

15. Poročanje

Na podlagi sklenjenega varnostnega sporazuma država ali mednarodna organizacija v času, ko ima tajne podatke EU, predloži letno poročilo do datuma, določenega pri izdaji pooblastila za posredovanje podatkov, v katerem potrjuje spoštovanje določb tega pravilnika.

Dodatek 4

Smernice za posredovanje tajnih podatkov EU tretjim državam ali mednarodnim organizacijam: stopnja sodelovanja 2

POSTOPKI

1. Pooblastilo za posredovanje tajnih podatkov EU tretjim državam ali mednarodnim organizacijam, katerih varnostna politika in predpisi se znatno razlikujejo od varnostne politike in predpisov EU, ima oseba izvora. Pooblastilo za posredovanje tajnih podatkov EU, ustvarjenih znotraj Komisije, ima Komisija kot kolegijski organ.
2. Načeloma je to omejeno na podatke, katerih stopnja tajnosti je določena do stopnje SECRET UE in vključno z njo; izključeni so tajni podatki, varovani s posebnimi varnostnimi označevalniki ali oznakami.
3. Do sklenitve varnostnega sporazuma je član Komisije, pristojen za varnostne zadeve, pristojen za obravnavo zahtev za posredovanje tajnih podatkov EU.
4. Član Komisije pri tem:

   — prosi za mnenja oseb izvora tajnih podatkov EU, ki naj se posredujejo;

   — vzpostavi potrebne stike z varnostnimi telesi držav ali mednarodnih organizacij upravičenk, da bi pridobil podatke o njihovi varnostni politiki in predpisih in zlasti sestavil tabelo primerjave stopenj tajnosti, ki veljajo v EU in v zadevni državi ali organizaciji;

   — organizira sestanek Svetovalne skupine za varnostno politiko Komisije ali, če je potrebno, s pisnim postopkom opravi poizvedbo pri državnih varnostnih organih držav članic zaradi pridobitve mnenja Svetovalne skupine za varnostno politiko Komisije.
5. Mnenje Svetovalne skupine za varnostno politiko Komisije zadeva:

   — tajnost, ki jo je mogoče vzpostaviti do držav ali mednarodnih organizacij upravičenk zaradi ocenitve varnostnega tveganja, ki se mu izpostavljene EU ali njene države članice;

   — ocena sposobnosti upravičenk, da varujejo tajne podatke, ki jih posreduje EU;

   — predloge glede operativnih postopkov za ravnanje s tajnimi podatki EU (na primer, posredovanje prečiščenih različic besedila) in prenesenimi dokumenti (zadržanje ali brisanje tajnih napisov EU, posebnih oznak itd.);

   — zniževanje ali odprava stopnje tajnosti, še preden se podatki posredujejo državam ali mednarodnim organizacijam upravičenkam.
6. Član Komisije, pristojen za varnostne zadeve, posreduje prošnjo in mnenje Svetovalne skupine za varnostno politiko Komisije v odločanje Komisiji.

VARNOSTNI PREDPISI ZA RAVNANJE UPRAVIČENCEV

7. Član Komisije, pristojen za varnostne zadeve, obvesti države ali mednarodne organizacije upravičenke o odločitvi Komisije glede odobritve posredovanja tajnih podatkov EU in njenih omejitev.

8. Odločitev glede posredovanja začne veljati, ko uporabnice pisno zagotovijo, da bodo:

   — uporabile podatke le za dogovorjene namene;

   — varovale podatke v skladu s predpisi Komisije.

9. Naslednji predpisi glede varovanja veljajo le, če se Komisija po prejemu strokovnega mnenja Svetovalne skupine za varnostno politiko Komisije ne odloči o posebnem postopku za obdelovanje tajnih dokumentov EU (brisanje omemb stopenj tajnosti EU, posebnih oznak itd.).

10. Osebje

    (a) Število uradnikov, ki imajo dostop do tajnih podatkov EU, je na podlagi načela „potrebe vedeti“ strogo omejeno na tiste osebe, katerih naloge zahtevajo takšen dostop;

    (b) Vsi uradniki ali državljani, pooblaščeni za dostop do tajnih podatkov, ki jih izda Komisija, imajo dovoljenje s strani države ali dovoljenje za dostop do ustrezne ravni, enakovredne ravni EU, kakor je opredeljeno v primerjalni tabeli;

    (c) Dovoljenja s strani države ali druga dovoljenja se posredujejo v vednost predsedniku.

11. Prenos dokumentov

(a) Operativni postopki za prenos dokumentov se določijo s sporazumom. Do sklenitve takšnega sporazuma veljajo določbe iz oddelka 21. Sporazum zlasti določa registrske urade, katerim je treba tajne podatke EU posredovati, in natančne naslove, kamor se dokumenti posredujejo, ter kurirske ali poštne storitve, uporabljene za prenos tajnih podatkov EU.

12. Registracija ob prispetju

Državni varnostni organ države naslovnice ali njegov enakovredni organ v državi, ki v imenu svoje vlade prejme tajne podatke, ki jih posreduje Komisija, ali varnostni urad mednarodne organizacije prejemnice, odpre poseben register, kamor vpiše tajne podatke EU ob njihovem prejemu. Register vsebuje stolpce z datumom prejema, podrobnostmi dokumenta (datum, referenčna številka in številka izvoda), njegovo stopnjo tajnosti, naslovom, imenom ali nazivom naslovnika, datumom vračila potrdila o prejemu in datumom, ko se dokument vrne v EU ali ko se uniči.

13. Vračanje dokumentov

Kadar prejemnik vrne tajni dokument Komisiji, to stori, kot je označeno v zgoraj navedenem odstavku „Prenos dokumentov“.

14. Varovanje

(a) Kadar dokumenti niso v rabi, se shranijo v varnostnem vsebniku, odobrenem za shranjevanje državnega tajnega gradiva z enako stopnjo tajnosti. Vsebnik ne nosi nikakršnih navedb o svoji vsebini, ki je dostopna samo osebam s pooblastili za ravnanje s tajnimi podatki EU. Kadar se uporabijo ključavnice s kombinacijami, je kombinacija znana le tistim uradnikom v državi ali organizaciji, ki imajo pooblastilo za dostop do tajnih podatkov EU, shranjenih v vsebniku, spremeni pa se vsakih šest mesecev ali prej ob premestitvi uradnika, ob odvzemu varnostne odobritve enemu ali več uradnikom, ki kombinacijo poznajo, ali če gre za ogrožanje varnosti.

(b) Tajne podatke EU iz varnostnega vsebnika odstranijo le tisti uradniki, ki so varnostno preverjeni za dostop do tajnih podatkov EU ter imajo „potrebo vedeti“. So še naprej odgovorni za varno hranjenje navedenih dokumentov, dokler so le-ti v njihovi lasti, in zlasti za zagotovitev, da do dokumentov nima dostopa nobena nepooblaščena oseba. Zagotavljajo tudi, da so dokumenti po končani uporabi in izven delovnega časa shranjeni v varnostnem vsebniku.

(c) Dokumenti CONFIDENTIEL UE ali z višjo stopnjo se ne fotokopirajo niti se iz njih ne jemljejo izvlečki brez dovoljenja Varnostnega urada Komisije.

(d) Postopek hitrega in celotnega uničenja dokumentov v sili določi Varnostni urad Komisije.

15. Materialna varnost

(a) Kadar varnostni vsebniki, uporabljeni za shranjevanje tajnih podatkov EU, niso v uporabi, so ves čas zaklenjeni.

(b) Kadar mora vzdrževalno ali čistilno osebje stopiti v prostor ali delati v prostoru, kjer so takšni varnostni vsebniki, jih ves čas spremlja član varnostne službe države ali organizacije ali uradnik, ki je posebno odgovoren za nadzor varnosti v prostoru.

(c) Izven običajnega delovnega časa (ponoči, ob koncu tedna in praznikih) so varnostni vsebniki, ki vsebujejo tajne podatke EU, pod nadzorom stražarja ali samodejnega alarmnega sistema.

16. Kršitve varnosti

Kadar se krši varnost v zvezi s tajnimi dokumenti EU ali se sumi kršitev varnosti, se takoj sprejmejo naslednji ukrepi:

(a) takoj se posreduje poročilo Varnostnemu uradu Komisije ali organu, pristojnemu za državno varnost države članice, ki je prevzela pobudo za posredovanje dokumentov (kopija se pošlje Varnostnemu uradu Komisije);

(b) izvede se preiskava, po zaključku katere se odda popolno poročilo službi, pristojni za varnost (glej (a) zgoraj). Nato se sprejmejo potrebni ukrepi za ureditev nastale situacije.

17. Inšpekcije

Varnostni urad Komisije lahko po dogovoru z zadevnimi državami ali mednarodnimi organizacijami oceni učinkovitost ukrepov za varovanje tajnih podatkov EU.

18. Poročanje

Na podlagi sklenjenega varnostnega sporazuma država ali mednarodna organizacija, dokler ima tajne podatke EU, predloži letno poročilo do datuma, določenega, ko je bilo izdano pooblastilo za posredovanje podatkov, v katerem potrjuje spoštovanje določb tega pravilnika.

Dodatek 5

Smernice za posredovanje tajnih podatkov EU tretjim državam ali mednarodnim organizacijam: stopnja sodelovanja 3

POSTOPKI

1. Komisija občasno v nekaterih posebnih okoliščinah lahko izrazi željo po sodelovanju z državami ali organizacijami, ki ne morejo nuditi zagotovil, kot jih zahteva ta pravilnik, vendar lahko navedeno sodelovanje zahteva posredovanje tajnih podatkov EU.

2. Pooblastilo za posredovanje tajnih podatkov EU tretjim državam ali mednarodnim organizacijam, katerih varnostna politika in predpisi se znatno razlikujejo od varnostne politike in predpisov EU, ima oseba izvora. Pooblastilo za posredovanje tajnih podatkov EU, ustvarjenih znotraj Komisije, ima Komisija kot kolegijsko telo.

   Načeloma je to omejeno na podatke, katerih stopnja tajnosti je določena s stopnjo SECRET UE in vključno z njo; izključeni so tajni podatki, zavarovani s posebnimi varnostnimi označevalniki ali oznakami.

3. Komisija preuči smotrnost posredovanja tajnih podatkov, oceni „potrebo vedeti“ upravičenk in se odloči o naravi tajnih podatkov, ki se lahko posredujejo.

4. Če Komisija pristane na posredovanje, član Komisije, pristojen za varnostne zadeve:

   — prosi za mnenja oseb izvora tajnih podatkov EU, ki naj se posredujejo;

   — organizira sestanek Svetovalne skupine za varnostno politiko Komisije ali, če je potrebno, s pisnim postopkom opravi poizvedbo pri državnih varnostnih organih držav članic za pridobitev mnenja Svetovalne skupine za varnostno politiko Komisije.

5. Mnenje Svetovalne skupine za varnostno politiko Komisije zadeva:

   (a) oceno varnostnega tveganja, ki so mu izpostavljene EU ali njene države članice;

   (b) stopnjo tajnosti podatkov, ki se lahko posredujejo;

   (c) zniževanje ali odpravo stopenj tajnosti, še preden se podatki posredujejo;

   (d) postopke za obdelovanje dokumentov, ki naj se posredujejo (glej odstavek spodaj);

   (e) možne metode prenosa (uporaba nacionalnih poštnih služb, javnih ali varovanih telekomunikacijskih sistemov, diplomatskih pošiljk, preverjenih kurirjev itd.).

6. Dokumenti, posredovani državam ali organizacijam, na katere se nanaša ta dodatek, se načeloma pripravijo ne glede na vir ali stopnjo tajnosti EU. Svetovalna skupina za varnostno politiko Komisije lahko priporoči:

   — uporabo posebne oznake ali kode;

   — uporabo posebnega sistema določanja stopenj tajnosti, ki povezuje občutljivost podatkov z nadzornimi ukrepi, ki se zahtevajo od metod prenosa dokumentov, po katerih ravna upravičenka.

7. Predsednik posreduje mnenje Svetovalne skupine za varnostno politiko Komisije v odločanje Komisiji.

8. Ko Komisija odobri posredovanje tajnih podatkov EU ter operativno izvajanje postopkov, Varnostni urad Komisije vzpostavi potrebne stike s pristojno varnostno službo zadevne države ali organizacije, da bi pospešil uporabo predvidenih varnostnih ukrepov.

9. Član Komisije, pristojen za varnostne zadeve, obvesti države članice o naravi in stopnji tajnosti podatkov, pri čemer navede organizacije in države, katerim se ti podatki smejo posredovati, kakor je odločila Komisija.

10. Varnostni urad Komisije sprejme vse potrebne ukrepe, da omogoči vse nadaljnje ocene škod in postopkov pregledovanja.

    Kadar se pogoji sodelovanja spremenijo, Komisija ponovno preuči zadevo.

VARNOSTNI PREDPISI ZA RAVNANJE UPRAVIČENCEV

11. Član Komisije, pristojen za varnostne zadeve, obvesti države ali mednarodne organizacije upravičenke o odločitvi Komisije glede odobritve posredovanja tajnih podatkov skupaj s podrobnimi predpisi o varovanju, ki jih predlaga Svetovalna skupina za varnostno politiko Komisije in potrdi Komisija.

12. Odločitev začne veljati samo, če upravičenke pisno zagotovijo, da:

— podatkov ne bodo uporabile za druge namene razen za sodelovanje, o katerem odloči Komisija;

— bodo za podatke zagotovile varovanje, ki ga zahteva Komisija.

13. Prenos dokumentov

(a) O operativnih postopkih za prenos dokumentov odloči Varnostni urad Komisije skupaj s pristojnimi službami držav ali mednarodnih organizacij prejemnic. Zlasti se opredelijo natančni naslovi, kamor se morajo dokumenti poslati.

(b) Dokumenti CONFIDENTIEL UE ali z višjo stopnjo se prenašajo v dvojni ovojnici. Na notranji ovojnici je poseben žig ali koda, o kateri se predhodno odloča, ter navedba posebne stopnje tajnosti, odobrene za dokument. Za vsak tajni dokument se priloži potrdilo o prejemu. Potrdilo o prejemu, ki nima stopnje tajnosti, navaja samo podrobnosti o dokumentu (njegovo referenčno številko, datum, številko izvoda) in jezik, ne pa tudi naslova.

(c) Notranja ovojnica se potem vloži v zunanjo ovojnico, na kateri je številka pošiljke za namene potrditve prejema. Na zunanji ovojnici ni stopnje tajnosti.

(d) Kurirjem se vedno izroči potrdilo o prejemu s številko pošiljke.

14. Registracija ob prispetju

Organ, pristojen za državno varnost (NSA) države naslovnice ali njegov enakovredni organ v državi, ki v imenu svoje vlade prejme tajne podatke, ki jih posreduje Komisija, ali varnostni urad mednarodne organizacije prejemnice, odpre poseben register, v katerem evidentira tajne podatke EU ob njihovem prejemu. Register vsebuje stolpce z datumom prejema, podrobnostmi dokumenta (datum, referenčno številko in številko izvoda), njegovo stopnjo tajnosti, naslovom, imenom ali nazivom naslovnika, datumom vračila potrdila o prejemu in datumom vračila potrdila o prejemu v EU ter datumom uničenja dokumenta.

15. Uporaba in varovanje izmenjanih tajnih podatkov

(a) Podatke s stopnjo tajnosti SECRET UE obdelujejo posebej za to imenovani uradniki s pooblastili za dostop do podatkov s to stopnjo tajnosti. Hranijo se v kakovostnih varnostnih omarah, ki jih lahko odpirajo samo osebe, pooblaščene za dostop do podatkov, ki so v njih. Območja z navedenimi omarami so ves čas varovana, vzpostavi pa se še sistem preverjanja, s katerim se zagotovi, da je vstop dovoljen le osebam z ustreznimi pooblastili. Podatki s stopnjo tajnosti SECRET UE se pošiljajo z diplomatsko pošto, varovano poštno službo ali varovanimi telekomunikacijami. Dokument s stopnjo tajnosti SECRET UE se kopira le s pisnim soglasjem organa izvora. Vse kopije se registrirajo in spremljajo. Izdajo se potrdila za vse dejavnosti, ki se nanašajo na dokumente SECRET UE;

(b) Dokumente CONFIDENTIEL UE obdelujejo le ustrezno imenovani uradniki, ki imajo pooblastila za to, da so obveščeni o predmetu. Dokumenti se hranijo v zaklenjenih varnostnih omarah v nadzorovanih območjih;

Podatki CONFIDENTIEL UE se pošiljajo z diplomatsko pošto, vojaško poštno službo in z varovanimi telekomunikacijami. Prejemnik lahko naredi kopije, njihovo število in razdelitev pa se evidentirata v posebnih registrih;

(c) Podatki RESTREINT UE se obdelujejo v prostorih, ki niso dostopni nepooblaščenemu osebju, hranijo pa se v zaklenjenih vsebnikih. Dokumenti se lahko pošiljajo z javnimi poštnimi storitvami kot registrirana pošta v dvojni ovojnici ter v nujnih primerih med operacijami z nezavarovanimi javnimi telekomunikacijskimi sistemi. Prejemniki lahko naredijo kopije;

(d) Za dokumente, katerim ni bila določena stopnja tajnosti, se ne zahtevajo posebni varnostni ukrepi in se lahko pošiljajo z elektronsko pošto in javnimi telekomunikacijskimi sistemi. Naslovniki lahko izdelajo kopije.

16. Uničenje

Dokumenti, ki niso več potrebni, se uničijo. Pri dokumentih RESTREINT UE in CONFIDENTIEL UE se v posebne registre vnese ustrezna opomba. Pri dokumentih SECRET UE se izdajo potrdila o uničenju, ki jih podpišeta dve osebi, ki sta priči uničenju.

17. Kršitve varnosti

Kadar je ogrožena integriteta podatkov CONFIDENTIEL UE ali SECRET UE ali če obstaja sum za to, državni varnostni organ države članice ali vodja varnosti v organizaciji izvede preiskavo o okoliščinah. O rezultatih je obveščen Varnostni urad Komisije. Sprejmejo se potrebni ukrepi za odpravo neustreznih postopkov ali metod hranjenja, če so ti vzrok ogrožanja integritete podatkov.

Dodatek 6

SEZNAM KRATIC

ACPC	Svetovalni odbor za (javna) naročila in pogodbe
CrA	Služba Kripto
CISO	Varnostni uradnik za centralno informatiko
COMPUSEC	Računalniška varnost
COMSEC	Komunikacijska varnost
CSO	Varnostni urad Komisije
EVOP	Evropska varnostna in obrambna politika
EUCI	Tajni podatki EU
IA	Organ INFOSEC
INFOSEC	Varnost podatkov
IO	Imetnik podatkov
ISO	Mednarodna organizacija za standardizacijo
IT	Informacijska tehnologija
LISO	Varnostni uradnik za lokalno informatiko
LSO	Lokalni varnostni uradnik
MSO	Uradnik, zadolžen za varnost sestanka
NSA	Organ, pristojen za državno varnost
PC	Osebni računalnik
RCO	Nadzorni uradnik registrskega urada
SAA	Služba za akreditacijo varnosti
SecOPS	Varnostni postopki delovanja
SSRS	Opredelitev varnostnih zahtev, ki so specifične za sistem
TA	Organ Tempest
TSO	Imetnik tehničnega sistema