32001D0264

L 101/1 URADNI LIST EVROPSKIH SKUPNOSTI 11.4.2001

SKLEP SVETA
z dne 19. marca 2001
o sprejetju predpisov Sveta o varovanju tajnosti

(2001/264/ES)

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti in zlasti člena 207(3) Pogodbe,

ob upoštevanju Sklepa Sveta 2000/396/ES, ESPJ, Euratom z dne 5. junija 2000 o sprejetju poslovnika Sveta [1], in zlasti člena 24 Sklepa,

ob upoštevanju naslednjega:

(1) Zaradi razvoja dejavnosti Sveta na področjih, kjer je potrebna določena stopnja zaupnosti, je primerno vzpostaviti celovit sistem varovanja tajnosti, ki bi vključeval Svet, njegov Generalni sekretariat in države članice.

(2) Tak sistem naj bi v enem samem besedilu združeval vsebine, ki jih obravnavajo vsi prejšnji sklepi in določbe na istem področju.

(3) V praksi se večina podatkov EU stopnje tajnosti CONFIDENTIEL UE in višje nanaša na skupno varnostno in obrambno politiko.

(4) Da bi zavarovali učinkovitost tako vzpostavljenega sistema varovanja tajnosti, se bi morale države članice povezati z njegovim delovanjem tako, da sprejmejo ukrepe na državni ravni, potrebne za spoštovanje določb tega sklepa, kadar njihovi pristojni organi in uradniki delajo s tajnimi podatki EU.

(5) Svet pozdravlja namero Komisije, da bo zaradi nemotenega izvajanja postopka odločanja Unije do datuma začetka uporabe tega sklepa uvedla obširen sistem, ki bo usklajen s prilogami k sklepu.

(6) Svet poudarja pomen vključevanja, kadar je to ustrezno, Evropskega parlamenta in Komisije v pravila in standarde o zaupnosti, potrebne za varstvo interesov Unije in njenih držav članic.

(7) Ta sklep ne vpliva na člen 255 Pogodbe in ustrezne izvedbene instrumente.

(8) Ta sklep ne vpliva na obstoječe običajne postopke v državah članicah glede informiranja nacionalnih parlamentov o dejavnostih Unije –

SKLENIL:

Člen 1

Potrdijo se predpisi Sveta o varovanju tajnosti, ki jih vsebuje Priloga.

Člen 2

1. Generalni sekretar/visoki predstavnik sprejme ustrezne ukrepe, s katerimi zagotovi, da v Generalnem sekretariatu Sveta (v nadaljevanju imenovanem „GSS“) ter v prostorih Sveta in decentraliziranih agencij EU [2] uradniki in drugi uslužbenci GSS, zunanji pogodbeni sodelavci GSS in osebje, dodeljeno GSS, pri delu s tajnimi podatki EU upoštevajo predpise iz člena 1.

[1] UL L 149, 23.6.2000, str. 21.

[2] Glej Sklepe Sveta z dne 10. novembra 2000.

2. Države članice sprejmejo ustrezne ukrepe v skladu z nacionalnimi predpisi, da bi zagotovile, da pri delu s tajnimi podatki EU znotraj svojih služb in prostorov naslednje osebe spoštujejo predpise iz člena 1:

(a) člani stalnih predstavništev držav članic pri Evropski uniji in člani državnih delegacij, ki se udeležujejo sestankov Sveta ali njegovih organov ali pa sodelujejo pri drugih dejavnostih Sveta;

(b) drugi člani državnih uprav držav članic, ki delajo s tajnimi podatki EU, če so nameščeni na ozemlju držav članic ali v tujini; in

(c) zunanji pogodbeni sodelavci in dodeljeno osebje držav članic, ki delajo s tajnimi podatki EU.

Države članice o sprejetih ukrepih nemudoma obvestijo GSS.

3. Ukrepi iz odstavkov 1 in 2 se sprejmejo pred 30. novembrom 2001.

Člen 3

Ob spoštovanju temeljnih načel in minimalnih standardov varovanja tajnosti iz dela I Priloge lahko generalni sekretar/visoki predstavnik sprejme ukrepe v skladu z delom II, oddelkom I(1) in (2) Priloge.

Člen 4

Z dnevom začetka uporabe ta sklep nadomesti:

(a) Sklep Sveta 98/319/ES z dne 27. aprila 1998 o postopkih, po katerih je mogoče uradnikom in uslužbencem Generalnega sekretariata Sveta dovoliti dostop do tajnih podatkov Sveta [1];

(b) Sklep generalnega sekretarja/visokega predstavnika z dne 27. julija 2000 o ukrepih za zaščito tajnih podatkov, ki veljajo za Generalni sekretariat Sveta [2];

(c) Sklep 433/97 generalnega sekretarja Sveta z dne 22. maja 1997 o postopku varnostnega preverjanja uradnikov, odgovornih za delovanje omrežja Cortesy.

Člen 5

1. Ta sklep začne učinkovati na dan objave.

2. Uporablja se od 1. decembra 2001.

V Bruslju, 19. marca 2001

Za Svet

Predsednik

A. LINDH

[1] UL L 140, 12.5.1998, str. 12.
[2] UL C 239, 23.8.2000, str. 1.

PRILOGA

PREDPISI SVETA EVROPSKE UNIJE O VAROVANJU TAJNOSTI

VSEBINA

Stran

Dodatki

DEL I

TEMELJNA NAČELA IN MINIMALNI STANDARDI VAROVANJA TAJNOSTI

UVOD

1. Te določbe predpisujejo temeljna načela in minimalne standarde varovanja tajnosti, ki jih morajo na primeren način spoštovati Svet, Generalni sekretariat Sveta (v nadaljevanju „GSS“), države članice in decentralizirane agencije Evropske unije (v nadaljevanju „decentralizirane agencije EU“), tako da se s tem zagotovi varovanje tajnosti in potrdi prepričanje vsake od njih, da so vzpostavljeni skupni standardi zaščite.

2. Izraz „tajni podatki EU“ pomeni vsak podatek in gradivo, katerega razkritje nepoklicani osebi bi lahko v različni meri škodovalo interesom EU ali eni ali več državam članicam, če imajo taki podatki svoj izvor bodisi znotraj EU ali pa prihajajo iz držav članic, tretjih držav ali mednarodnih organizacij.

3. V teh predpisih:

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

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

4. Glavni cilji varovanja tajnosti so:

   (a) varovati tajne podatke EU pred vohunjenjem, ogrožanjem ali razkritjem nepoklicani osebi;

   (b) varovati podatke EU v komunikacijskih in informacijskih sistemih ter omrežjih, pred nevarnostjo poseganja v njihovo celovitost in razpoložljivost;

   (c) varovati objekte, v katerih so podatki EU, pred sabotažami in zlonamernim naklepnim poškodovanjem;

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

5. Temelji zanesljivega varovanja tajnosti so:

   (a) nacionalna organizacija za varnost v vsaki državi članici, ki je odgovorna za:

      (i) zbiranje in evidentiranje obveščevalnih podatkov o vohunjenju, sabotažah, terorizmu in drugih uničevalnih dejavnostih; in

      (ii) obveščanje svoje vlade in preko nje Sveta ter svetovanje obema o značaju groženj za varnost in o sredstvih zavarovanja pred njimi;

   (b) tehnični organ INFOSEC v vsaki državi članici in v okviru GSS, ki je skupaj z zadevnim varnostnim organom odgovoren za zagotavljanje podatkov in nasvetov o nevarnostih tehničnega značaja za varovanje tajnosti in za sredstva zaščite pred njimi;

   (c) redno sodelovanje med vladnimi sektorji, agencijami in ustreznimi službami GSS z namenom določiti in priporočiti, kot je ustrezno:

      (i) katere podatke, sredstva in objekte je treba zaščititi; in

      (ii) skupne standarde zaščite.

6. Kadar gre za zaupnost, so potrebne skrbnost in izkušnje za izbor podatkov in gradiv, ki jih je treba zaščititi, ter za oceno potrebne stopnje zaščite. Temeljnega pomena je, da stopnja zaščite ustreza kritični stopnji tajnosti vsakega posameznega podatka in gradiva, ki ju je treba zaščititi. Da bi bil zagotovljen tekoč pretok podatkov, se sprejmejo ukrepi za izognitev preobsežnemu razvrščanju podatkov po tajnosti. Sistem razvrščanja je instrument, ki omogoča uveljavitev teh načel; pri načrtovanju in organiziranju načinov boja proti vohunjenju, sabotažam, terorizmu in drugim nevarnostim se je treba držati podobnega sistema za razvrščanje, tako da je najpomembnejšim prostorom, v katerih se hranijo tajni podatki, in najbolj občutljivim točkam znotraj njih zagotovljena najvišja stopnja zaščite.

TEMELJNA NAČELA

7. **Ukrepi varovanja tajnosti:**

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

(b) so načrtovani tako, da omogočajo odkrivanje oseb, ki bi s svojim položajem lahko ogrozile varnost tajnih podatkov in pomembnih objektov, v katerih se taki podatki nahajajo, in zagotavljajo njihovo nedostopnost ali prenos drugam;

(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 načela potrebe po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog, ki je temeljno načelo za vse vidike v zvezi z varovanjem tajnosti;

(e) zagotavljajo celovitost (t.j. preprečujejo ponarejanje, 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 ali obdelani v elektromagnetni obliki ali se v njej prenašajo.

ORGANIZIRANOST VAROVANJA TAJNOSTI

Skupni minimalni standardi

8. Svet in vsaka država članica morajo zagotoviti, da vse upravne in/ali vladne službe, druge institucije EU, agencije in pogodbeni partnerji spoštujejo skupne minimalne standarde varovanja tajnosti, tako da je mogoče vsak tajni podatek EU posredovati naprej v prepričanju, da bo vsaka od navedenih strani z njim ravnala na enak način. Taki minimalni standardi morajo obsegati merila o preverjeni varnostni zanesljivosti osebja in postopke za zaščito tajnih podatkov EU.

VARNOSTNA PREVERJENOST OSEBJA

Varnostno preverjanje osebja

9. Vse osebe, ki potrebujejo dostop do tajnih podatkov stopnje CONFIDENTIEL UE ali višje, morajo biti ustrezno varnostno preverjene, preden se jim tak dostop dovoli. Podobna varnostna preverjenost se zahteva od oseb, katerih delovne naloge so v zvezi s tehničnim delovanjem ali vzdrževanjem komunikacijskih in informacijskih sistemov, ki vsebujejo tajne podatke. Namen takega preverjanja je ugotoviti, ali te osebe:

(a) izpričujejo popolno lojalnost;

(b) imajo tako osebnost in kvalitete diskretnosti, ki ne dopuščajo dvomov o njihovi integriteti pri delu s tajnimi podatki; ali

(c) ne podlegajo pritisku iz zunanjih ali drugih virov, npr. v zvezi s prejšnjim prebivališčem ali preteklimi zvezami, kar bi lahko pomenilo tveganje za varnost.

Pri postopkih varnostnega preverjanja se posebno natančno preverijo osebe:

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

(e) ki zasedajo položaje z rednim dostopom do velikega števila podatkov stopnje SECRET UE;

(f) ki imajo zaradi delovnih nalog poseben dostop do za izvedbo naloge ključno pomembnih 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.

Za primere iz pododstavkov (d), (e) in (f) se v največji možni meri uporablja metoda preverjanja ozadja.

10. Če se zaposlijo osebe, za katere ne velja načelo potrebe po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog v okoliščinah, v katerih bi lahko dobile dostop do tajnih podatkov EU (npr. sli, varnostni agenti, vzdrževalno in čistilno osebje, itd.), je treba te osebe najprej ustrezno varnostno preveriti.

Evidenca varnostnega preverjanja osebja

11. Vse službe, telesa ali ustanove, ki imajo opravka s tajnimi podatki EU ali pri katerih so komunikacijski in informacijski sistemi, ki so ključnega pomena za izvedbo naloge, vodijo evidenco varnostnih preverjanj pri njih zaposlenega osebja. Vsako varnostno potrdilo se glede na okoliščine preveri zaradi zagotavljanja njegove ustreznosti tekoči zadolžitvi osebe; potrdilo se ponovno preveri kot prednostna zadeva, kadarkoli novi podatki kažejo na to, da nadaljnje izpolnjevanje nalog pri delu s tajnimi podatki ni več v skladu z interesi varovanja tajnosti. Evidenca o varnostnem preverjanju oseb je pri vodji varnosti ustrezne službe, telesa ali ustanove.

Seznanjenost osebja z ukrepi varovanja tajnosti

12. Vse osebje, zaposleno na položajih, kjer bi lahko imelo dostop do tajnih podatkov, je treba ob začetku izvajanja nalog in v rednih časovnih presledkih temeljito seznaniti s potrebo po ukrepih varovanja tajnosti in z ustreznimi postopki za njihovo izvajanje. Od vseh članov takega osebja je koristno zahtevati pisno potrditev o tem, da v celoti razumejo predpise o varovanju tajnosti, ki se nanašajo na izvajanje njihovih nalog.

Odgovornosti vodstvenega osebja

13. Vodstveno osebje je zadolženo za poznavanje tistih članov osebja, ki delajo s tajnimi podatki ali ki imajo dostop do komunikacijskih ali informacijski sistemov, ključnih za izvedbo naloge in za beleženje in poročanje o incidentih ali očitnih slabostih članov osebja, za katere je verjetno, da bi lahko imele posledice za varovanje tajnosti.

Status varnostne preverjenosti osebja

14. Določijo se postopki, ki v primeru negativnih informacij o neki osebi zagotavljajo ugotovitve o tem, če ta oseba dela s tajnimi podatki ali ima dostop do komunikacijskih ali informacijskih sistemov, ki so ključnega pomena za izvedbo naloge, in zagotavljajo, da je o tem obveščen pristojni organ. Če se ugotovi, da taka oseba pomeni tveganje za varnost, se mu/ji prepreči ali se ga/jo odstrani od izvajanja nalog, kjer bi lahko škodoval/a interesom varnosti.

FIZIČNO VAROVANJE TAJNOSTI

Potreba po zaščiti

15. Stopnja ukrepov fizičnega varovanja tajnosti, ki se uporabljajo zaradi zagotavljanja zaščite tajnih podatkov EU je v sorazmerju z razvrstitvijo, obsegom in ogroženostjo, ki se nanašajo na tajne podatke in gradivo. Poskrbeti je treba, da se pri razvrščanju podatkov po stopnji tajnosti izognemo previsoki ali prenizki stopnji tajnosti; razvrstitev podatkov mora biti predmet rednih preverjanj. Vsi imetniki tajnih podatkov EU se v zvezi z razvrstitvijo takih podatkov po stopnjah tajnosti držijo enotnih postopkov in spoštujejo skupne standarde zaščite glede nadzora, prenosa in uničenja podatkov in gradiv, ki jih je treba zaščititi.

Preverjanje

16. Pred odhodom z območij, kjer so tajni podatki EU, morajo osebe, zadolžene za njihov nadzor, zagotoviti, da so ti varno shranjeni in da so aktivirane vse varnostne naprave (ključavnice, alarmi, itd.). Dodatno neodvisno preverjanje se izvaja izven delovnega časa.

Varnost zgradb

17. Zgradbe, v katerih so tajni podatki EU ali komunikacijski in informacijski sistemi, ki so ključnega pomena za izvedbo nalog, se ščitijo pred dostopom nepooblaščenih oseb. Vrsta zaščite tajnih podatkov EU, npr. rešetke na oknih, vratne ključavnice/zapahi, vhodna straža, samodejni sistemi nadzora dostopa, varnostne kontrole in obhodne patrulje, alarmni sistemi, sistemi odkrivanja vsiljivcev in psi čuvaji, je odvisna od:

(a) razvrščenosti po stopnjah tajnosti, obsega in notranje lokacije podatkov in gradiva, ki jih je treba zaščititi, znotraj zgradbe;

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

(c) tehničnih značilnosti in lokacije zgradbe.

18. Podobno je vrsta zaščite komunikacijskih in informacijskih sistemov odvisna od ocene vrednosti sredstev v nevarnosti in morebitne škode, ki bi lahko nastala v primeru ogrožanja varovanja tajnosti, od tehničnih značilnosti in lokacije zgradbe, v kateri je sistem, in od lokacije sistema v zgradbi.

Načrti za izredne razmere

19. Vnaprej se pripravijo podrobni načrti za zaščito tajnih podatkov v izrednih razmerah na lokalni ali nacionalni ravni.

VAROVANJE TAJNOSTI PODATKOV (INFOSEC)

20. INFOSEC se nanaša na opredelitev in uporabo ukrepov varovanja tajnosti, s katerimi se podatki, ki se obdelujejo, hranijo ali prenašajo s pomočjo komunikacijskih, informacijskih in drugih elektronskih sistemov, zaščitijo pred izgubo zaupnosti, celovitosti ali razpoložljivosti, bodisi naključne ali namerne. Sprejmejo se primerni protiukrepi za preprečevanje dostopa do podatkov EU nepooblaščenim uporabnikom, za preprečevanje onemogočanja dostopa do podatkov EU pooblaščenim uporabnikom in za preprečevanje izkrivljanja ali nepooblaščenega spreminjanja ali brisanja podatkov EU.

UKREPI PROTI SABOTAŽI IN DRUGIM OBLIKAM ZLONAMERNEGA NAKLEPNEGA POŠKODOVANJA

21. Fizični ukrepi za zaščito pomembnih objektov, v katerih so tajni podatki, so najboljša zaščitna varovalka pred sabotažo in zlonamernim naklepnim poškodovanjem; samo varnostno preverjanje osebja še ne pomeni učinkovitega nadomestila. Pristojni državni organ se zadolži za zbiranje podatkov glede vohunjenja, sabotaž, terorizma in drugih uničevalnih dejavnosti.

SPOROČANJE TAJNIH PODATKOV TRETJIM DRŽAVAM ALI MEDNARODNIM ORGANIZACIJAM

22. Odločitev o sporočanju tajnih podatkov EU z izvorom v Svetu tretji državi ali mednarodni organizaciji sprejme Svet. Če organ izvora podatka, za katerega je sporočanje zaželeno, ni Svet, mora Svet ta organ najprej zaprositi za njegov pristanek glede sporočanja. Če organa izvora ni mogoče ugotoviti, njegovo odgovornost prevzame Svet.

23. Če Svet prejme tajne podatke od tretjih držav, mednarodnih organizacij ali drugih tretjih strani, se ti podatki primerno zaščitijo glede na stopnjo tajnosti in enakovredno glede na standarde sprejete s temi predpisi, ki veljajo za tajne podatke EU ali glede na take višje standarde, ki bi jih pri sporočanju podatkov lahko zahtevala tretja stran. Mogoče se je dogovoriti za vzajemni nadzor.

24. Zgornja načela se izvajajo v skladu s podrobno navedenimi določbami iz Dela II.

DEL II

ODDELEK I

ORGANIZIRANOST VAROVANJA TAJNOSTI V SVETU EVROPSKE UNIJE

Generalni sekretar/visoki predstavnik

1. Generalni sekretar/visoki predstavnik

   (a) izvaja varnostno politiko Sveta;

   (b) preučuje varnostna vprašanja, ki mu jih predloži Svet ali njegova pristojna telesa;

   (c) v tesni povezavi z organi za nacionalno varnost (v nadaljevanju „ONV“) ali drugimi primernimi organi držav članic preučuje vprašanja v zvezi s spremembami varnostne politike Sveta. Seznam teh organov vsebuje Dodatek 1.

2. Generalni sekretar/visoki predstavnik je še zlasti odgovoren za:

   (a) usklajevanje vseh varnostnih zadev, ki se nanašajo na dejavnosti Sveta;

   (b) dajanje zahtev državam članicam za ustanovitev centralnih arhivskih uradov na stopnji TRES SECRET UE/EU TOP SECRET in za ustanovitev takih uradov v decentraliziranih agencijah EU po potrebi;

   (c) sporočanje zahtev ONV v državah članicah za pridobitev varnostnih potrdil o osebju, zaposlenemu v GSS, v skladu z Oddelkom VI;

   (d) opravljanje ali naročanje preiskav v zvezi z vsakršnim odtekanjem tajnih podatkov EU na podlagi dokazov, izkazanih z verjetnostjo, do katerega pride v GSS ali v katerikoli decentralizirani agenciji EU;

   (e) od ustreznih varnostnih organov zahtevati začetek preiskav, če je videti, da naj bi do odtekanja podatkov prišlo zunaj GSS ali decentraliziranih agencij EU, in usklajevanje poizvedb, če v njih sodeluje več kakor en varnostni organ;

   (f) izvajanje periodičnih preverjanj, skupaj in v dogovoru z zadevnimi ONV, ureditve varovanja tajnosti, s katero so zaščiteni tajni podatki EU v državah članicah;

   (g) vzdrževanje tesnih stikov z vsemi zadevnimi varnostnimi organi zaradi uresničevanja vsesplošne usklajenosti na področju varovanja tajnosti;

   (h) nenehno preverjanje varnostne politike Sveta in postopkov in po potrebi pripravljanje ustreznih priporočil. Glede tega Svetu v odobritev predloži letni inšpekcijski načrt, ki ga pripravi Varnostni urad GSS.

Varnostni odbor Sveta

3. Ustanovi se Varnostni odbor. Sestavljajo ga predstavniki ONV iz vsake države članice. Predseduje mu generalni sekretar/visoki predstavnik ali njegov/njen pooblaščeni predstavnik. Na sestanke odbora so lahko vabljeni in jim prisostvujejo tudi predstavniki decentraliziranih agencij EU, kadar se obravnavajo vprašanja v zvezi z njimi.

4. Varnostni odbor se sestaja po navodilih Sveta, na zahtevo generalnega sekretarja/visokega predstavnika ali enega od ONV. Odbor je pristojen za preverjanje in ocenjevanje vseh varnostnih vprašanj, ki se nanašajo na delovanje Sveta in za dajanje priporočil Svetu, glede na potrebe. Glede dejavnosti GSS je Odbor pristojen za dajanje priporočil o varnostnih vprašanjih generalnemu sekretarju/visokemu predstavniku.

Varnostni urad generalnega sekretariata Sveta

5. Za izpolnjevanje nalog iz odstavkov 1 in 2, ima generalni sekretar/visoki predstavnik za usklajevanje, nadzor in izvajanje ukrepov varovanja tajnosti na voljo Varnostni urad GSS.

6. Vodja Varnostnega urada GSS je glavni svetovalec generalnega sekretarja/visokega predstavnika za varnostne zadeve in opravlja dolžnosti sekretarja Varnostnega odbora. V tem pogledu vodi posodabljanje predpisov o varovanju tajnosti in usklajuje ukrepe varovanja tajnosti s pristojnimi organi držav članic in, po potrebi, z mednarodnimi organizacijami, ki jih s Svetom povezujejo sporazumi o varovanju tajnosti. V ta namen opravlja vlogo uradnika za zvezo.

7. Vodja Varnostnega urada GSS je odgovoren za akreditacijo sistemov informacijske tehnologije in omrežij v okviru GSS. Vodja Varnostnega urada GSS in zadevni ONV po potrebi skupaj odločita o akreditaciji sistemov informacijske tehnologije in omrežij, pri katerih so udeleženi GSS, države članice, decentralizirane agencije EU in/ali tretje strani (države ali mednarodne organizacije).

Decentralizirane agencije EU

8. Vsak direktor decentralizirane agencije EU je odgovoren za izvajanje varnostnih predpisov v okviru svoje ustanove. Direktor običajno imenuje enega od članov svojega osebja, ki je odgovoren za to področje in mu o tem poroča. Ta član osebja je imenovan za varnostnega uradnika, pristojnega za varovanje tajnosti.

Države članice

9. Vsaka država članica imenuje svoj organ za nacionalno varnost (ONV), ki je pristojen za varovanje tajnih podatkov EU ([1]).

10. V okviru državne uprave vsake države članice je ustrezni ONV pristojen za:

(a) trajno varovanje tajnih podatkov EU, s katerimi razpolaga katerikoli javni ali zasebni nacionalni organ, telo ali agencija, doma ali na tujem;

(b) izdajo dovoljenj za ustanavljanje arhivskih uradov na stopnji TRES SECRET UE/EU TOP SECRET (to pooblastilo se lahko prenese na nadzornega uradnika Centralnega arhivskega urada TRÈS SECRET UE/EU TOP SECRET);

(c) periodične inšpekcije sistemov za zaščito tajnih podatkov EU;

(d) zagotavljanje, da so bili vsi domači državljani kot tudi tujci, zaposleni v nacionalnem organu telesu ali agenciji, ki bi lahko imeli dostop do podatkov EU označenih s TRES SECRET UE/EU TOP SECRET, SECRET UE in CONFIDENTIEL UE ustrezno varnostno preverjeni;

(e) oblikovanje takih načrtov varovanja tajnosti, kot so potrebni za preprečevanje prehajanja tajnih podatkov EU v roke nepooblaščenim osebam.

Vzajemne varnostne inšpekcije

11. Periodične inšpekcije sistemov za zaščito tajnih podatkov EU v GSS in v stalnih predstavništvih držav članic v Evropski uniji ter v prostorih zgradb Sveta, ki jih zasedajo države članice, izvajajo Varnostni urad GSS in zadevni ONV, skupaj in v medsebojnem soglasju ([2]).

12. Periodične inšpekcije sistemov za zaščito tajnih podatkov EU v decentraliziranih agencijah EU izvaja Varnostni urad GSS ali na zahtevo generalnega sekretarja ONV države članice gostiteljice.

([1]) Za seznam ONV, zadolženih za varnost tajnih podatkov EU, glej Dodatek 1

([2]) Brez vpliva na Dunajsko konvencijo iz 1961 o diplomatskih odnosih.

ODDELEK II

RAZVRŠČANJE IN OZNAČEVANJE

RAZVRŠČANJE PO STOPNJAH TAJNOSTI [1]

Stopnje razvrstitve tajnosti podatkov so naslednje:

1. TRES SECRET UE/EU TOP SECRET: ta stopnja tajnosti se uporablja samo za podatke in gradivo, katerih razkritje nepooblaščeni osebi bi lahko imelo izjemno težke posledice za bistvene interese Evropske unije ali ene ali več njenih držav članic.

2. SECRET UE: ta stopnja tajnosti se uporablja samo za podatke in gradivo, katerih razkritje nepooblaščeni osebi bi lahko resno škodovalo bistvenim interesom Evropske unije ali ene ali več njenih držav članic.

3. CONFIDENTIEL UE: ta stopnja tajnosti se uporablja za podatke in gradivo, katerih razkritje nepooblaščeni osebi bi lahko škodovalo bistvenim interesom Evropske unije ali ene ali več njenih držav članic.

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

OZNAKE

5. Opozorilna oznaka se lahko uporablja za določitev področja, na katerega se nanaša dokument, ali za posebno razpošiljanje na podlagi načela potrebe po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog.

6. Oznaka ESDP/PESD se uporablja za dokumente in njihove kopije v zvezi z varnostjo in obrambo Unije ali ene ali več njenih držav članic, ali pa v zvezi z vojaškim ali nevojaškim obvladovanjem kriznih razmer.

7. Nekateri dokumenti, predvsem tisti, ki se nanašajo na sisteme informacijske tehnologije, se lahko opremijo z dodatno oznako, ki pomeni uporabo dodatnih ukrepov varovanja tajnosti, določenih z ustreznimi predpisi.

OPREMLJANJE S STOPNJAMI TAJNOSTI IN OZNAKAMI

8. Dokumenti se opremijo s stopnjami tajnosti in oznakami na naslednji način:

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

   (b) na dokumente CONFIDENTIEL UE z mehanskimi sredstvi ali ročno ali s tiskom na predhodno ožigosan in registran papir;

   (c) na dokumente SECRET UE in TRÈS SECRET UE/EU TOP SECRET z mehanskimi sredstvi in ročno.

[1] Primerjalna tabela varnostnih stopenj tajnosti EU, NATO, ZEU in držav članic je v Dodatku 2.

ODDELEK III

SISTEM RAZVRŠČANJA TAJNIH PODATKOV

1. Stopnje tajnosti podatkov se določijo samo, če je to potrebno. Stopnja tajnosti se določi na jasen in pravilen način in se zadrži samo tako dolgo, kot je potrebno za zaščito podatkov.

2. Odgovornost za določanje stopnje tajnosti in za vsa njena naknadna znižanja ali preklic ([1]) nosi samo organ izvora.

   Uradniki in drugi uslužbenci GSS razvrščajo, znižujejo ali preklicujejo stopnjo tajnosti podatkov po navodilu svojega generalnega direktorja ali v dogovoru z njim.

3. Podrobni postopki za ravnanje s tajnimi dokumenti so zasnovani tako, da tem dokumentom zagotavljajo zaščito, ki je ustrezna glede na podatke, ki jih vsebujejo.

4. Število oseb, pooblaščenih za izdajanje dokumentov TRES SECRET UE/EU TOP SECRET, se skrči na minimum; njihova imena so na seznamu, ki ga sestavi GSS, vsaka država članica in po potrebi vsaka decentralizirana agencija EU.

UPORABA STOPENJ TAJNOSTI

5. Stopnja tajnosti dokumenta se določi glede na stopnjo občutljivosti njegove vsebine v skladu z definicijo iz odstavkov 1 do 4 Oddelka II. Pomembno je, da se stopnja tajnosti uporablja na pravilen način in glede na stvarne potrebe. To velja zlasti za stopnjo tajnosti TRÈS SECRET UE/EU TOP SECRET.

6. Pri določanju stopnje tajnosti nekega dokumenta organ izvora tega dokumenta upošteva zgoraj navedene predpise in se izogiba vsakršni težnji po previsoki ali prenizki stopnji razvrstitve.

   Čeprav visoka stopnja tajnosti na prvi pogled zagotavlja boljšo zaščito dokumenta, lahko rutinsko določanje previsokih stopenj povzroči izgubo zaupanja v vrednost sistema razvrščanja.

   Po drugi strani pa dokumenti zaradi izogibanja omejitvam v zvezi z njihovo zaščito ne smejo imeti prenizke stopnje tajnosti.

   Praktična navodila za razvrstitev po stopnjah tajnosti so v Dodatku 3.

7. Posamezne strani, odstavki, oddelki, priloge, dodatki in dodani ter priloženi deli nekega dokumenta lahko zahtevajo različne stopnje tajnosti in se temu ustrezno označijo. Za stopnjo tajnosti dokumenta kot celote velja stopnja, ki se nanaša na njegov najbolj tajni del.

8. Stopnja tajnosti pisma ali zabeležke, ki se nanaša na priloge, je enaka najvišji stopnji tajnosti ene od prilog. V primeru ločenosti od prilog mora organ izvora jasno določiti stopnjo njegove/njene tajnosti.

ZNIŽANJE IN PREKLIC STOPENJ TAJNOSTI

9. Tajnim dokumentom EU se stopnja tajnosti lahko zniža ali prekliče samo z dovoljenjem organa izvora in, če je potrebno, po posvetovanju z drugimi zainteresiranimi stranmi. Znižanje stopnje tajnosti ali njen preklic se potrdi pisno. Institucija izvora, država članica, urad, nasledstvena organizacija ali organ z višjo pristojnostjo so o spremembi dolžni obvestiti svoje naslovnike, ti pa so v zvezi s spremembo odgovorni za obveščanje vseh nadaljnjih naslovnikov, katerim so poslali ali kopirali dokument.

10. Če je mogoče, organi izvora na tajnih dokumentih določijo datum ali obdobje, ko je stopnjo tajnosti vsebine mogoče znižati ali ukiniti. V nasprotnem primeru ti organi dokumente preverjajo najpozneje vsakih pet let, da tako zagotovijo potrebno izvorno razvrstitev dokumenta.

([1]) Znižanje stopnje tajnosti pomeni nižjo stopnjo razvrstitve; preklic stopnje tajnosti pa pomeni odpravo vseh razvrstitev.

ODDELEK IV

FIZIČNO VAROVANJE TAJNOSTI

SPLOŠNO

1. Glavni cilj ukrepov fizičnega varovanja tajnosti je nepooblaščenim osebam preprečiti dostop do tajnih podatkov in/ali gradiva EU.

ZAHTEVE ZA VAROVANJE TAJNOSTI

2. Vsi prostori, območja, zgradbe, uradi, sobe, komunikacijski in informacijski sistemi, itd., v katerih se hranijo in/ali obdelujejo tajni podatki EU, se zavarujejo s primernimi ukrepi fizičnega varovanja tajnosti.

3. Pri odločanju o potrebni stopnji ukrepov fizičnega varovanja tajnosti je treba upoštevati naslednje pomembne dejavnike:

   (a) razvrstitev tajnosti podatkov in/ali gradiva;

   (b) količino in obliko (npr. papir, računalniški nosilci shranjevanja) varovanih podatkov;

   (c) lokalno oceno nevarnosti, ki jo za EU, države članice in/ali druge institucije ali tretje strani, ki razpolagajo s tajnimi podatki EU, pomenijo obveščevalne službe, predvsem glede sabotaž, terorizma in drugih uničevalnih in/ali kaznivih dejavnosti.

4. Ukrepi fizičnega varovanja tajnosti se načrtujejo zaradi:

   (a) preprečevanja skrivnih ali nasilnih vdorov vsiljivcev;

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

   (c) preprečevanja dostopa do tajnih podatkov EU tistim uradnikom in drugim uslužbencem GSS, vladnih sektorjev držav članic in/ali drugih institucij ali tretjih strank, za katere ne velja načelo potrebe po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog.

UKREPI FIZIČNEGA VAROVANJA TAJNOSTI

Varnostna območja

5. Območja, kjer se obdelujejo in shranjujejo tajni podatki CONFIDENTIEL UE ali višje, se uredijo in strukturirajo tako, da ustrezajo eni od naslednjih kategorij:

   (a) Varnostno območje razreda I: območje, kjer se tajni podatki stopnje CONFIDENTIEL UE ali višje obdelujejo in shranjujejo na tak način, da vstop na to območje praktično pomeni dostop do tajnih podatkov. Za tako območje se zahteva:

      (i) razločno določen in zavarovan obseg prostora preko katerega se nadzorujejo vsi vhodi in izhodi;

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

      (iii) podroben opis razvrščenosti podatkov, ki se običajno hranijo na takem območju, to je podatkov, za katere vstop na območje pomeni dostop do njih.

   (b) Varnostno območje razreda II: območje, kjer se podatki stopnje CONFIDENTIEL UE ali višje obdelujejo in shranjujejo tako, da so pred dostopom nepooblaščenih oseb zaščitene s pomočjo notranjega nadzora, t.j. poslopja s prostori, v katerih se redno obdelujejo in shranjujejo tajni podatki stopnje CONFIDENTIEL UE ali višje. Za tako območje se zahteva:

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

      (ii) sistem vhodnega nadzora, ki vstop brez spremstva na območje dovoljuje samo ustrezno preverjenim in posebej pooblaščenim osebam. Za vse druge osebe je predvideno spremstvo ali enakovreden nadzor, ki nepooblaščenim osebam preprečuje dostop do tajnih podatkov EU in nenadzorovan vstop na območja, ki so predmet tehnično varnostnih inšpekcij.

Območja, v katerih se delovno osebje ne nahaja 24 ur, se pregledajo takoj po izteku delovnega časa z namenom zagotoviti, da so tajni podatki EU pravilno varovani.

Upravno območje

6. Okoli varnostnih območij razreda I in razreda II ali na pristopih k njim se lahko vzpostavi upravno območje z nižjo stopnjo varovanja. Za tako območje se zahteva vidno določen obseg prostora, ki omogoča preverjanje oseb in vozil. V upravnih območjih se obdelujejo in hranijo samo podatki stopnje RESTREINT UE.

Vhodni in izhodni nadzor

7. Vstop v varnostna območja razreda I in razreda II se nadzoruje z dovolilnico ali s sistemom prepoznavanja oseb, ki velja za stalno zaposleno osebje. Zaradi preprečevanja nepooblaščenega dostopa do tajnih podatkov EU se vzpostavi tudi sistem preverjanja obiskovalcev. Sistem dovolilnic lahko dopolnjuje samodejno prepoznavanje, ki ima vlogo dopolnila k sistemu, in ne more v celoti nadomestiti varnostnega osebja. Sprememba ocene nevarnosti ima lahko za posledico okrepitev ukrepov vhodnega in izhodnega nadzora, npr. med obiskom uglednih oseb.

Varnostni obhodi

8. Obhodi varnostnih območij razreda I in II se morajo opravljati izven običajnega delovnega časa in imajo za namen zaščito premoženja EU pred ogrožanjem, poškodovanjem ali izgubo. Pogostost obhodov se določi glede na lokalne okoliščine, vendar morajo obhodi praviloma potekati vsaki dve uri.

Varnostni vsebniki in sobe-trezorji

9. Za hranjenje tajnih podatkov EU se uporabljajo trije tipi vsebnikov:

   — tip A: vsebniki, ki so bili na nacionalni ravni odobreni za hranjenje tajnih podatkov stopnje TRÈS SECRET UE/EU TOP SECRET na varnostnih območjih razreda I ali razreda II,

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

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

10. V sobah-trezorjih, zgrajenih za varnostna območja razreda I in razreda II in za vsa varnostna območja razreda I, kjer se tajni podatki CONFIDENTIEL UE in višje hranijo na odprtih policah ali so predstavljeni na grafičnih prikazih, kartah/zemljevidih, itd., stenah, tleh in stropih, mora vrata in ključavnice odobriti ONV, kar pomeni enakovredno zaščito, kot jo nudi razred varnostnih vsebnikov, odobrenih za shranjevanje tajnih podatkov enake varnostne stopnje.

Ključavnice

11. Ključavnice, ki se uporabljajo pri varnostnih vsebnikih in sobah-trezorjih, v katerih se hranijo tajni podatki EU, morajo ustrezati naslednjim standardom:

   — Skupina A: odobrene na nacionalni ravni za vsebnike razreda A,

   — Skupina B: odobrene na nacionalni ravni za vsebnike razreda B,

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

Nadzor nad ključi in kombinacijami

12. Ključi varnostnih vsebnikov se ne smejo nositi izven pisarniških zgradb. Nastavitve kombinacij za varnostne vsebnike si osebe, ki jih morajo poznati, zapomnijo po spominu. Nadomestni ključi in pisni zapisi vseh nastavitev kombinacij za uporabo v nujnih primerih so pri uradniku, zadolženem za varnost v zadevni ustanovi; slednji se hranijo ločeno, v zapečatenih neprozornih ovojnicah. Delovni ključi, nadomestni varnostni ključi in nastavitve kombinacij se hranijo v ločenih varnostnih vsebnikih. Ti ključi in nastavitve kombinacij morajo biti deležni enako stroge varnostne zaščite kakor gradivo, do katerega omogočajo dostop.

13. Poznavanje nastavitev kombinacij varnostnih vsebnikov je omejeno na najmanjše praktično dopustno število ljudi. Kombinacije se spremenijo:

(a) ob prejemu novega vsebnika;

(b) ob vsaki spremembi osebja;

(c) ob vsakršnem razkritju ali sumu razkritja;

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

Naprave za odkrivanje vsiljivcev

14. 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 voda zagotavlja neprekinjeno delovanje sistema. Druga temeljna zahteva je, da se v primeru napak v delovanju sistema ali nedovoljenih posegov vanj sproži ustrezen alarm ali kakšno drugo zanesljivo opozorilo nadzornemu osebju.

Odobrena oprema

15. Organi za nacionalno varnost (ONV) vodijo svoje lastne ali na bilateralnih virih temelječe sproti dopolnjene sezname varnostne opreme po tipih in modelih, ki so jo odobrili za neposredno ali posredno varovanje tajnih podatkov v različnih določenih razmerah in pogojih. Varnostni urad GSS vodi podoben seznam, ki med drugim temelji na podatkih, prejetih od ONV. Pred nakupom take opreme, se decentralizirane agencije EU posvetujejo z Varnostnim uradom GSS in po potrebi z ONV države članice gostiteljice.

Fizična zaščita fotokopirnih strojev in telefaksov

16. Fotokopirni stroji in telefaksi se fizično zaščitijo v takšnem obsegu, ki zagotavlja, da jih lahko uporabljajo le pooblaščene osebe in da so vsi tajni produkti pod primernim nadzorom.

ZAŠČITA PRED PREGLEDOVANJEM IN PRISLUŠKOVANJEM

Zaščita pred pregledovanjem

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

Zaščita pred prisluškovanjem

18. Pisarniški prostori ali območja, v katerih se redno razpravlja o tajnih podatkih SECRET UE ali višje, se v primerih tveganja zaščitijo pred pasivnimi ali aktivnimi poskusi prisluškovanja. Za oceno tveganja takih poskusov je zadolžen pristojni varnostni organ, ki se po potrebi posvetuje z ONV.

19. Pri določanju zaščitnih ukrepov za prostore, ki so občutljivi na pasivno prisluškovanje (npr. izolacija zidov, tal, vrat, stropov, merjenja jakosti kompromitirajočega zvoka) in za aktivno prisluškovanje (npr. iskanje mikrofonov), Varnostni urad GSS lahko zahteva pomoč ONV. Varnostno osebje decentraliziranih agencij EU lahko od Varnostnega urada GSS zahteva izvedbo tehničnih inšpekcij in/ali pomoč strokovnjakov ONV.

20. Podobno, kadar tako zahtevajo okoliščine, lahko specialisti ONV za tehnično varnost na zahtevo pristojnega varnostnega uradnika pregledajo telekomunikacijsko opremo in električno ali elektronsko pisarniško opremo katerekoli vrste, ki je bila uporabljena med sestanki na stopnji SECRET UE ali višje.

TEHNIČNO VAROVANA OBMOČJA

21. Nekatera območja se lahko določijo kot tehnično varovana območja. Ob vstopu vanje se izvaja posebni nadzor. Če v njih ni osebja, morajo biti taka območja po odobrenem postopku zaklenjena, vsi ključi pa se obravnavajo kot varnostni ključi. Taka območja so predmet rednih fizičnih pregledov, ki se opravijo tudi po dejanskem vstopu ali sumu vstopa nepooblaščenih oseb.

22. Vodi se natančen popis opreme in pohištva zaradi nadzora nad njihovimi premiki. V tako območje ne sme biti vnesen nikakršen kos opreme ali pohištva, preden posebej za to usposobljeno varnostno osebje ne opravi skrbnega pregleda zaradi odkritja morebitnih prisluškovalnih naprav. Splošno pravilo je, da se je namestitvi komunikacijskih vodov v tehnično varovanih območjih treba izogibati.

ODDELEK V

SPLOŠNA PRAVILA O NAČELU POTREBE PO SEZNANITVI S PODATKI ZARADI OPRAVLJANJA FUNKCIJE ALI DELOVNIH NALOG IN VARNOSTNO PREVERJANJE

1. Dostop do tajnih podatkov EU se dovoli samo osebam, za katere zaradi opravljanja funkcije ali delovnih nalog velja načelo potrebe po seznanitvi s podatki. Dostop do tajnih podatkov stopenj TRÈS SECRET UE/EU TOP SECRET, SECRET UE in CONFIDENTIEL UE se dovoli samo osebam, ki imajo ustrezno varnostno potrdilo.

2. Odgovornost za določitev oseb, ki morajo biti seznanjene s podatki zaradi opravljanja funkcije ali delovnih nalog, nosijo GSS, decentralizirane agencije EU in služba ali organ države članice, v kateri naj bi se zadevna oseba zaposlila glede na zahteve, ki jih narekuje izvedba naloge.

3. Za varnostna potrdila osebja na temelju relevantnih veljavnih postopkov je odgovoren delodajalec. Za uradnike GSS in druge uslužbence je postopek preverjanja varnostne zanesljivosti predviden v Oddelku VI.

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

   Varnostno potrdilo za določeno stopnjo tajnosti daje imetniku pravico dostopa do podatkov na nižjih stopnjah tajnosti.

4. Osebe, ki niso uradniki ali drugi uslužbenci GSS ali držav članic, npr. člani, uradniki ali uslužbenci institucij EU, s katerimi je treba obravnavati ali jim pokazati tajne podatke EU, morajo v zvezi s tajnimi podatki EU imeti varnostno potrdilo in biti seznanjeni z lastno odgovornostjo glede varovanja tajnosti. Isto pravilo v podobnih okoliščinah velja za zunanje pogodbene partnerje, strokovnjake ali svetovalce.

POSEBNA PRAVILA O DOSTOPU DO PODATKOV TRÈS SECRET UE/EU TOP SECRET

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

6. Vse osebe, za katere se zahteva dostop do podatkov TRÈS SECRET UE/EU TOP SECRET, imenuje vodja njihovega oddelka, njihova imena pa se hranijo v ustreznem arhivskem uradu TRÈS SECRET UE/EU TOP SECRET.

7. Vse osebe morajo pred pridobitvijo dostopa do podatkov TRÈS SECRET UE/EU TOP SECRET podpisati potrdilo, s katerim potrjujejo, da so bile seznanjene z varnostnimi postopki Sveta in da popolnoma razumejo pomen svoje lastne posebne odgovornosti za varovanje podatkov TRÈS SECRET UE/EU TOP SECRET in posledice, ki jih predvidevajo pravila EU in nacionalno pravo ali upravna pravila, če tajni podatki pridejo v nepooblaščene roke bodisi namenoma ali iz malomarnosti.

8. Za osebe, ki imajo na sestankih, itd. dostop do podatkov TRÈS SECRET UE/EU TOP SECRET, pristojni uradnik za nadzor službe ali telesa, kjer je ta oseba zaposlena, uradno obvesti organ, ki sestanek organizira, da zadevne osebe tako dovoljenje imajo.

9. Imena vseh oseb, ki ne opravljajo več nalog, za katere se zahteva dostop do podatkov TRES SECRET UE/EU TOP SECRET, se umaknejo s seznama TRES SECRET UE/EU TOP SECRET. Poleg tega, se vse take osebe ponovno opozorijo na njihovo posebno odgovornost glede varovanja podatkov TRÈS SECRET UE/EU TOP SECRET. Podpisati morajo izjavo s katero potrjujejo, da ne bodo uporabljale ali naprej posredovale podatkov TRÈS SECRET UE/EU TOP SECRET, s katerimi razpolagajo.

POSEBNA PRAVILA O DOSTOPU DO PODATKOV SECRET UE IN CONFIDENTIEL UE

10. Vse osebe, ki potrebujejo dostop do podatkov SECRET UE ali CONFIDENTIEL UE, morajo biti najprej ustrezno preverjene.

11. Vse osebe, ki potrebujejo dostop do podatkov SECRET UE ali CONFIDENTIEL UE, se morajo seznaniti z ustreznimi predpisi o varovanju tajnosti in se zavedati posledic malomarnosti.

12. Za osebe, ki imajo na sestankih, itd. dostop do podatkov SECRET UE ali CONFIDENTIEL UE, pristojni uradnik za nadzor službe ali telesa, kjer je ta oseba zaposlena, uradno obvesti organ, ki sestanek organizira, da zadevne osebe taka dovoljenja imajo.

POSEBNA PRAVILA O DOSTOPU DO PODATKOV RESTREINT UE

13. Osebe, ki imajo dostop do podatkov RESTREINT UE se opozorijo na pomembnost teh predpisov o varovanju tajnosti in na posledice malomarnosti.

PREMESTITVE

14. Če je član osebja premeščen z delovnega mesta, na katerem je imel opravka s tajnimi podatki EU, arhivski urad nadzoruje, da predaja take dokumentacije od odhajajočega k prihajajočemu uradniku poteka na pravilen način.

POSEBNA NAVODILA

15. Osebe, od katerih se zahteva delo s tajnimi podatki EU, je treba ob prvem prevzemu nalog in nato v periodičnih presledkih opozarjati na:

    (a) nevarnosti, ki jih za varovanje tajnosti pomenijo indiskretni pogovori;

    (b) previdnostne ukrepe v njihovih stikih s tiskom;

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

    (d) obveznost takojšnjega poročanja ustreznim varnostnim organom o vsakem poskusu ali ravnanju, ki bi zbudil sum o vohunski dejavnosti, ali o kakršnihkoli nenavadnih okoliščinah v zvezi z varovanjem tajnosti.

16. Vse osebe, ki so običajno izpostavljene pogostim stikom s predstavniki držav, katerih obveščevalne službe imajo za cilj EU in države članice v zvezi s tajnimi podatki in dejavnostmi EU, se pouči o tehnikah, za katere je znano, da jih uporabljajo različne obveščevalne službe.

17. Za zasebna potovanja osebja, ki je bilo glede dostopa do tajnih podatkov EU varnostno preverjeno, v katero koli smer, Svet ne predvideva predpisov o varovanju tajnosti. Vendarle pristojni varnostni organi uradnike in druge uslužbence, ki spadajo v njihovo pristojnost, seznanijo s pravili potovanja, ki jih bodo morali spoštovati v danih primerih. Pristojni uradniki za varovanje tajnosti so zadolženi za organiziranje sestankov, na katerih članom osebja osvežijo ta posebna navodila.

ODDELEK VI

POSTOPEK VARNOSTNEGA PREVERJANJA URADNIKOV GSS IN DRUGIH USLUŽBENCEV

1. Samo uradniki in drugi uslužbenci GSS ali osebe zaposlene v GSS, ki morajo zaradi opravljanja svojih nalog in zahtev službe poznati ali uporabljati tajne podatke Sveta, imajo pravico dostopa do takih podatkov.

2. Da bi pridobile dostop do tajnih podatkov, razvrščenih na stopnje TRES SECRET UE/EU TOP SECRET, SECRET UE in CONFIDENTIEL UE, se osebe iz odstavka 1 za ta namen pooblastijo v skladu s postopkom iz odstavkov 4 in 5.

3. Pooblastilo se izda samo osebam, za katere so pristojni nacionalni varnostni organi držav članic (ONV) opravili varnostno preverjanje v skladu s postopkom iz odstavkov 6 do 10.

4. Pristojni organ za imenovanje v smislu člena 2, prvi pododstavek, Kadrovskih predpisov je zadolžen za izdajo pooblastil iz odstavkov 1, 2 in 3.

   Pristojni organ za imenovanje izda pooblastilo po pridobitvi mnenja pristojnih nacionalnih organov držav članic na podlagi preverjanja varnostne zanesljivosti, ki se opravi v skladu z odstavki 6 do 12.

5. Pooblastilo, ki velja pet let, ne sme preseči časa trajanja nalog, na podlagi katerih je bilo izdano. Organ, pristojen za imenovanje, ga lahko podaljša v skladu s postopkom iz odstavka 4.

   Organ za imenovanje pooblastilo umakne, če meni, da za to obstajajo upravičeni razlogi. Vsaka odločitev o umiku pooblastila se uradno sporoči zadevni osebi, ki lahko zahteva, da jo zasliši organ za imenovanje, in pristojnemu nacionalnemu organu.

6. Cilj preverjanja varnostne zanesljivosti je ugotoviti odsotnost zadržkov, ki bi osebi preprečevali dostop do tajnih podatkov Sveta.

7. Preverjanje varnostne zanesljivosti ob sodelovanju zadevne osebe in na zahtevo organa za imenovanje opravijo pristojni nacionalni organi države članice, katere državljan je oseba, ki naj dobi pooblastilo. Če zadevna oseba biva na ozemlju druge države članice, pristojni nacionalni organi lahko zagotovijo sodelovanje organov države, kjer ima oseba prebivališče.

8. Kot del postopka preverjanja mora zadevna oseba izpolniti obrazec z osebnimi podatki.

9. Organ za imenovanje v svoji zahtevi opredeli vrsto in stopnjo tajnosti podatkov s katerimi bo razpolagala zadevna oseba, tako da pristojni nacionalni organi lahko opravijo postopek preverjanja in podajo svoje mnenje glede stopnje pooblaščenosti, ki bi bila primerna za to osebo.

10. Celotni proces varnostnega preverjanja skupaj z dobljenimi rezultati se opravi v skladu z relevantnimi pravili in predpisi, ki veljajo v zadevni državi članici, vključno s pravili in predpisi, ki se nanašajo na pritožbe.

11. Kadar pristojni nacionalni organi države članice izdajo pozitivno mnenje, organ za imenovanje zadevni osebi lahko podeli ustrezno pooblastilo.

12. Kadar pristojni nacionalni organi izdajo negativno mnenje, o tem uradno obvestijo zadevno osebo, ki lahko zaprosi za zaslišanje pri organu za imenovanje. Če meni, da je tako potrebno, organ za imenovanje lahko zaprosi pristojne nacionalne organe za vsa dodatna pojasnila, ki jih lahko podajo. V primeru potrditve negativnega mnenja se pooblastilo ne izda.

13. Oseba, ki ji je bilo podeljeno pooblastilo v smislu odstavkov 4 in 5, v času izdaje pooblastila in potem v rednih časovnih presledkih prejme vsa potrebna navodila v zvezi z zaščito tajnih podatkov in sredstvi za zagotavljanje take zaščite. Te osebe podpišejo izjavo, s katero potrjujejo, da so prejele navodila in se obvežejo, da jih bodo spoštovale.

14. Organ za imenovanje sprejme vse potrebne ukrepe za izvajanje določb tega oddelka, še posebej glede pravil, ki urejajo dostop do seznama pooblaščenih oseb.

15. Izjemoma, če tako zahteva služba, organ za imenovanje lahko — potem ko je uradno obvestil pristojne organe in pod pogojem, da od njih v roku enega meseca ni dobil odziva — podeli začasno pooblastilo za obdobje, ki ne presega šest mesecev, med čakanjem na rezultat preverjanja iz odstavka 7.

16. Tako podeljena začasna in pogojna pooblastila ne dajejo dostopa do podatkov TRES SECRET UE/EU TOP SECRET; dostop do takih podatkov je omejen na uradnike, ki so dejansko opravili preverjanje s pozitivnim rezultatom v skladu z odstavkom 7. Do objave rezultatov se uradnikom, za katere je bilo preverjanje zahtevano na stopnji TRÈS SECRET UE/EU TOP SECRET, lahko začasno in pogojno dovoli dostop do tajnih podatkov do stopnje SECRET UE in vključno z njo.

ODDELEK VII

PRIPRAVA, RAZPOŠILJANJE, PRENOS, SHRANJEVANJE IN UNIČEVANJE TAJNEGA GRADIVA EU

Vsebina

Splošne določbe

Ta oddelek podrobno navaja ukrepe za pripravo, razpošiljanje, prenos, shranjevanje in uničevanje tajnih dokumentov EU, kot določa odstavek 3(a) Temeljnih načel in minimalnih standardov varovanja tajnosti iz Dela I te priloge. Uporablja se kot referenca pri prilagajanju teh ukrepov drugemu gradivu EU glede na vrsto gradiva in glede na posamezne primere.

Poglavje I

Priprava in razpošiljanje tajnih dokumentov EU

PRIPRAVA

1. Stopnje tajnosti in oznake EU se uporabljajo, kot je določeno v Oddelku II, in so vidne zgoraj in spodaj na sredini vsake strani; vsaka stran je oštevilčena. Vsak tajni dokument EU je opremljen z opravilno številko in datumom. Pri dokumentih TRÈS SECRET UE/EU TOP SECRET in SECRET UE mora biti opravilna številka vidna na vsaki strani. Če se razpošiljajo v več primerkih, mora biti številka kopije vsakega primerka navedena na prvi strani skupaj s celotnim številom strani. Seznam vseh dodatkov in prilog mora biti naveden na prvi strani tajnega dokumenta stopnje CONFIDENTIEL UE in višje.

2. Dokumente na stopnji CONFIDENTIEL UE in višje lahko tipkajo, prevajajo, shranjujejo, fotokopirajo in reproducirajo na magnetni trak ali mikrofilm samo osebe, ki so bile varnostno preverjanje za dostop do tajnih podatkov EU do vsaj ustrezne stopnje tajnosti zadevnega dokumenta, z izjemo posebnega primera, ki je opisan v odstavku 27 tega oddelka.

   Določbe, ki urejajo računalniško pripravo tajnih dokumentov, so navedene v Oddelku XI.

RAZPOŠILJANJE

3. Tajni podatki EU se razpošiljajo samo osebam, za katere velja načelo potrebe po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog in ki imajo ustrezno varnostno potrdilo. Prvo razpošiljanje določi organ izvora.

4. Dokumenti TRÈS SECRET UE/EU TOP SECRET krožijo preko arhivskih uradov TRÈS SECRET UE/EU TOP SECRET (glej Oddelek VIII). V primeru sporočil s stopnjo tajnosti TRES SECRET UE/EU TOP SECRET pristojni arhivski urad pooblasti vodjo komunikacijskega centra, da pripravi število kopij, ki je določeno v seznamu naslovnikov.

5. Dokumente na stopnji SECRET UE in nižje drugim naslovnikom lahko razpošilja izvorni naslovnik na podlagi potrebe po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog. Organi izvora morajo jasno določiti vse opozorilne oznake, ki jih želijo uvesti. Ob navedbi takih opozorilnih oznak naslovniki dokumente lahko ponovno razpošiljajo samo s pooblastilom organa izvora.

6. Arhivski urad ustanove mora vsak dokument na stopnji CONFIDENTIEL UE in višje ob prihodu ali izhodu iz ustanove vpisati v evidenco. Podatki, ki jih je treba vpisati (reference, datum in po potrebi številka kopije), morajo omogočati prepoznavo dokumentov in biti vpisani v vpisnik ali vneseni v posebno varovan računalniški nosilec.

Poglavje II

Prenos tajnih dokumentov EU

ODPREMLJANJE

7. Dokumenti stopnje tajnosti CONFIDENTIEL UE se prenašajo v odpornih, neprozornih dvojnih ovojnicah. Notranja ovojnica se označi s primerno varnostno stopnjo tajnosti EU in, če je možno, s popolnimi podatki o uradnem delovnem nazivu in naslovu naslovnika.

8. Notranjo ovojnico lahko odpre in sprejem priloženih dokumentov potrdi samo nadzorni uradnik arhivskega urada ali njegov namestnik, razen če ta ovojnica ni naslovljena na posamezno osebo. V takem primeru ustrezni arhivski urad vpiše sprejem ovojnice, notranjo ovojnico pa sme odpreti in potrditi sprejem v njej vsebovanih dokumentov samo oseba, na katero je naslovljena.

9. V notranjo ovojnico se priloži potrdilo o sprejemu. Na potrdilu, ki ni predmet razvrstitve po tajnosti, morajo biti navedeni opravilna številka, datum in številka kopije dokumenta, nikoli pa predmet dokumenta.

10. Notranja ovojnica se vloži v zunanjo ovojnico, ki nosi odpremno številko zaradi formalnosti ob prejemu. Varnostna razvrstitev v nobenem primeru ne sme biti vidna na zunanji ovojnici.

11. Pri oddaji dokumentov stopnje CONFIDENTIEL UE ali višje, kurirji in sli dobijo potrdilo, na katerem se morajo podatki ujemati z odpremnimi podatki.

PRENAŠANJE ZNOTRAJ ZGRADBE ALI SKUPINE ZGRADB

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

PRENOS DOKUMENTOV EU ZNOTRAJ DRŽAVE

13. Znotraj države smejo prenos dokumentov TRES SECRET UE/EU TOP SECRET opravljati samo uradna kurirska služba ali osebe, ki so pooblaščene za dostop do podatkov TRES SECRET UE/EU TOP SECRET.

14. Kadar kurirska služba opravlja prenos dokumentov TRES SECRET UE/EU TOP SECRET zunaj meja zgradbe ali skupine zgradb, je treba upoštevati določbe o odpremljanju in sprejemu iz tega poglavja. Dostavne službe morajo imeti na voljo zadostno število osebja, da bi zagotovile, da pošiljke dokumentov TRES SECRET UE/EU TOP SECRET ves čas ostajajo pod neposrednim nadzorom odgovorne osebe.

15. Izjemoma dokumente TRÈS SECRET UE/EU TOP SECRET zunaj meja zgradbe ali skupine zgradb zaradi lokalne rabe na sestankih in razpravah lahko prenašajo uradniki, ki niso kurirji, pod pogojem da:

(a) je prenašalec pooblaščen za dostop do dokumentov TRES SECRET UE/EU TOP SECRET;

(b) je način prenosa v skladu z nacionalnimi pravili o prenosu nacionalnih dokumentov TOP SECRET;

(c) uradnik dokumentov TRÈS SECRET UE/EU TOP SECRET v nobenem primeru ne pusti brez nadzora;

(d) se uredi vse potrebno, da seznam tako prenesenih dokumentov ostane v arhivskem uradu TRÈS SECRET UE/EU TOP SECRET, kjer se dokumenti hranijo, in da se vpiše v vpisnik ter tako omogoči preverjanje dokumentov ob njihovi vrnitvi.

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

17. Vse države članice ali decentralizirane agencije EU morajo pripraviti navodila o osebnem prenosu tajnih dokumentov EU, ki imajo podlago v teh predpisih. Od prenašalca je treba zahtevati, da ta navodila prebere in se pod njih podpiše. Navodila morajo zlasti jasno določati, da pod nobenim pogojem:

(a) prenašalec dokumentov ne da iz rok, razen če so varno shranjeni v skladu z določbami iz Oddelka IV;

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

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

PRENOS IZ ENE DRŽAVE ČLANICE V DRUGO

18. Tajno gradivo stopnje CONFIDENTIEL UE in višje iz ene države članice v drugo prenašajo diplomatske poštne ali vojaške kurirske službe.

19. Osebni prenos tajnega gradiva stopenj SECRET UE in CONFIDENTIEL UE se dovoli, če določbe v zvezi s prenosom zagotavljajo, da dokumenti ne morejo priti v roke nobenih nepooblaščenih oseb.

20. Organi nacionalne varnosti (ONV) lahko dovolijo osebni prenos, če diplomatska pošta ali vojaška kurirska služba nista na voljo ali če bi uporaba teh služb imela za posledico zamudo, ki bi bila škodljiva za delovanje EU, medtem ko naslovnik gradivo nujno potrebuje. Vsaka država članica mora pripraviti navodila za osebni prenos tajnega gradiva do stopnje SECRET UE in vključno z njo v mednarodnem okolju za osebe, ki niso člani diplomatskih in vojaških poštno-kurirskih služb. V navodilih je treba zahtevati, da:

(a) ima prenašalec ustrezno varnostno potrdilo, ki ga izdajo države članice;

(b) se v ustrezni pisarni ali arhivskem uradu vodi evidenca o vsem gradivu, ki se tako prenaša;

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

(d) ima prenašalec pri sebi kurirsko potrdilo in/ali potni nalog, priznan od vseh držav EU, s katerim je pooblaščen za prenos ustrezno označenega paketa;

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

(f) je potovalni aranžma prenašalca glede kraja namembnosti, potovalnih smeri in sredstev prevoza v skladu s predpisi EU, ali če so nacionalni predpisi v tem oziru strožji, v skladu s temi predpisi;

(g) gradivo ne sme biti dano iz rok prenašalca, razen če se varuje v skladu z določbami o varnem shranjevanju iz Oddelka IV;

(h) gradivo ne sme ostati brez nadzora v sredstvih javnega transporta ali zasebnih vozilih, ali na mestih kot so restavracije ali hoteli. Ne sme biti shranjeno v hotelskih sefih 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.).

Oseba, ki je določena za prenos tajnih podatkov, mora prebrati in podpisati varnostna navodila, ki morajo vsebovati vsaj zgoraj navedena navodila in postopke, ki jih je treba spoštovati v nujnih primerih ali kadar carinski ali letališki varnostni organi zahtevajo pregled paketa, ki vsebuje tajno gradivo.

PRENOS DOKUMENTOV RESTREINT UE

21. Za prenos dokumentov stopnje RESTREINT UE niso predvidene posebne določbe; te morajo zagotavljati, da ob prenosu dokumenti ne morejo preiti v nepooblaščene roke.

VARNOSTNA PREVERJENOST KURIRSKEGA OSEBJA

22. Vsi kurirji in sli, ki so zaposleni zaradi prenašanja dokumentov SECRET UE in CONFIDENTIEL UE, morajo biti ustrezno varnostno preverjeni.

Poglavje III

Električna in druga tehnična sredstva prenosa

23. Zaradi zagotavljanja varnega prenosa tajnih podatkov EU se na področju telekomunikacij oblikujejo varnostni ukrepi. Podrobna pravila, ki veljajo za prenos takih podatkov, obravnava Oddelek XI.

24. Tajne podatke CONFIDENTIEL UE in SECRET UE lahko prenašajo le pooblaščeni komunikacijski centri in omrežja in/ali terminali ter sistemi.

Poglavje IV

Dodatne kopije in prevodi ter izvlečki iz tajnih dokumentov EU.

25. Kopiranje ali prevajanje dokumentov TRÈS SECRET UE/EU TOP SECRET lahko dovoli le organ izvora.

26. Če osebe brez varnostnega potrdila za stopnjo TRES SECRET UE/EU TOP SECRET potrebujejo podatke, ki so v dokumentu TRES SECRET UE/EU TOP SECRET, vendar pa nimajo te stopnje tajnosti, se vodji arhivskega urada TRES SECRET UE/EU TOP SECRET lahko dovoli, da pripravi potrebno število izvlečkov iz takega dokumenta. Ta istočasno sprejme potrebne ukrepe, ki naj zagotovijo, da bodo taki izvlečki opremljeni z ustrezno stopnjo tajnosti.

27. Dokumente, razvrščene na stopnjo SECRET UE in nižje, lahko razmnožuje ali prevaja naslovnik v okviru nacionalnih predpisov o varovanju tajnosti in pod pogojem strogega spoštovanja načela o potrebnosti seznanitve s podatki zaradi opravljanja funkcije ali delovnih nalog. Varnostni ukrepi, ki veljajo za izvorni dokument, veljajo tudi za njegove razmnožene primerke in/ali prevode. Po teh predpisih o varovanju tajnosti se ravnajo tudi decentralizirane agencije EU.

Poglavje V

Inventurni popisi in preverjanja, shranjevanje in uničevanje tajnih dokumentov EU

INVENTURNI POPISI IN PREVERJANJA

28. Vsi arhivski uradi TRÈS SECRET UE/EU TOP SECRET, kot je navedeno v Oddelku VIII, vsako leto opravijo podroben popis posamičnih dokumentov TRÈS SECRET UE/EU TOP SECRET v skladu s predpisi iz Oddelka VIII, (9) do (11). Tajni dokumenti EU pod stopnjo TRÈS SECRET UE/EU TOP SECRET so predmet internih preverjanj v skladu z nacionalnimi smernicami in, v primeru GSS ali decentraliziranih agencij EU, v skladu z navodili generalnega sekretarja/visokega predstavnika.

Ti postopki dajejo priložnost za oblikovanje mnenja lastnikov dokumentov glede:

(a) možnosti znižanja stopnje tajnosti ali njenega preklica za nekatere dokumente;

(b) dokumentov, ki jih je treba uničiti.

ARHIVSKO SHRANJEVANJE TAJNIH PODATKOV EU

29. Zaradi zmanjšanja težav pri shranjevanju se uradnikom, zadolženim za nadzor v vseh arhivskih uradih dovoli snemanje dokumentov TRES SECRET UE/EU TOP SECRET, SECRET UE ali CONFIDENTIEL UE na mikrofilm ali shranjevanje na magnetna ali optična sredstva v namene arhiviranja pod pogojem, da:

(a) postopek snemanja na mikrofilm/shranjevanje opravlja osebje z veljavnim varnostnim potrdilom, ki ustreza primerni stopnji tajnosti dokumentov;

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

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

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

(e) je snemanje na mikrofilm/shranjevanje dokumentov TRÈS SECRET UE/EU TOP SECRET ali SECRET UE razločno označeno v evidenci, ki se uporablja ob letni inventuri;

(f) so izvirni dokumenti, ki so bili posneti na mikrofilm ali kako drugače shranjeni, uničeni v skladu s predpisi, navedenimi v odstavkih od 31 do 36.

30. Ta pravila veljajo tudi za vse druge oblike shranjevanja, ki jih odobrijo ONV, kot so elektromagnetni nosilci in optični disk.

RUTINSKO UNIČEVANJE TAJNIH DOKUMENTOV EU

31. Da bi preprečili nepotrebno kopičenje tajnih dokumentov EU, se tisti, za katere je vodja ustanove, kjer se hranijo, mnenja, da so zastareli in v odvečnem številu, uničijo takoj, ko je mogoče, in sicer na naslednji način:

(a) dokumente stopnje TRÈS SECRET UE/EU TOP SECRET uniči samo Centralni arhivski urad, ki je za njih odgovoren. Vsak uničeni dokument se vpiše na potrdilo o uničenju, ki ga podpiše uradnik, zadolžen za nadzor na stopnji TRES SECRET UE/EU TOP SECRET, in uradnik, ki je priča ob uničenju in ki mora imeti varnostno potrdilo na stopnji TRES SECRET UE/EU TOP SECRET. V ta namen se v vpisnik zavede ustrezna zabeležka;

(b) potrdila o uničenju skupaj z dokumentacijo o razpošiljanju arhivski urad hrani deset let. Kopije se organu izvora ali ustreznemu centralnemu arhivskemu uradu pošljejo le na izrecno zahtevo;

(c) Dokumenti TRÈS SECRET UE/EU TOP SECRET, skupaj z vsemi tajnimi odpadki, ki so nastali pri pripravi dokumentov TRÈS SECRET UE/EU TOP SECRET kot so poškodovane kopije, delovni osnutki, natipkana sporočila in indigo papir se uničijo pod nadzorom uradnika, preverjenega na stopnji TRES SECRET UE/EU TOP SECRET, z zažigom, zmletjem, razrezanjem v pramene ali z drugačno spremembo v neprepoznavno in nesestavljivo obliko.

32. Dokumente SECRET UE uniči arhivski urad, ki je odgovoren za take dokumente, pod nadzorom varnostno preverjene osebe ob uporabi enega od postopkov navedenih v odstavku 31 (c). Dokumenti SECRET UE, ki so uničeni, se vpišejo na podpisana potrdila o uničenju, ki jih arhivski urad skupaj z dokumentacijo o razpošiljanju zadrži najmanj tri leta.

33. Dokumente CONFIDENTIEL UE uniči arhivski urad, ki je odgovoren za te dokumente, pod nadzorom varnostno preverjene osebe po enem od postopkov navedenih v odstavku 31 (c). Njihovo uničenje se vpiše v arhiv v skladu z nacionalnimi predpisi in, v primeru GSS ali decentraliziranih agencij EU, v skladu z navodili generalnega sekretarja/visokega predstavnika.

34. Dokumente RESTREINT UE uniči arhivski urad, ki je odgovoren za te dokumente ali uporabnik, v skladu z nacionalnimi predpisi in, v primeru GSS ali decentraliziranih agencij EU, v skladu z navodili generalnega sekretarja/visokega predstavnika.

UNIČENJE V NUJNIH PRIMERIH

35. GSS, države članice in decentralizirane agencije EU ob upoštevanju lokalnih pogojev pripravijo načrte za varovanje tajnega gradiva EU v kriznih razmerah vključno z, glede na potrebe, načrti za uničenje in evakuacijo v nujnih primerih; znotraj svojih organizacij razdelijo navodila, za katera menijo da so potrebna, da tajni podatki EU ne bi prišli v roke nepooblaščenih oseb.

36. Režim varovanja in/ali uničenja gradiva SECRET UE in CONFIDENTIEL UE v kriznih razmerah ne sme biti v ničemer na škodo varovanju ali uničenju gradiva TRES SECRET UE/EU TOP SECRET, vključno z (de)šifrirno opremo, kjer ima ravnanje z njo prednost pred vsemi drugimi nalogami. Ukrepi, ki se sprejmejo za varovanje ali uničenje (de)šifrirne opreme v nujnih primerih, so vsebovani v ad hoc navodilih.

POGLAVJE VI

Posebna pravila za dokumente, namenjene Svetu

37. Spremljanje in nadzor tajnih podatkov stopnje tajnosti SECRET UE ali CONFIDENTIEL UE, ki jih vsebujejo dokumenti, namenjeni Svetu, znotraj GSS izvaja „Urad za tajne podatke“.

V okviru pooblastil generalnega direktorja za osebje in upravo so naloge Urada:

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

(b) sprotno dopolnjevanje seznama s podatki o tajnih podatkih;

(c) periodično preverjanje vprašanj o potrebi ohranjanja tajnosti podatkov;

(d) predpisovanje, v sodelovanju z Varnostnim uradom, praktičnih postopkov za določanje stopenj tajnosti podatkov ali njihovega preklica.

38. Urad za tajne podatke vodi vpisnik o naslednjih podatkih:

(a) datum priprave tajnega podatka;

(b) stopnjo tajnosti;

(c) datum prenehanja tajnosti;

(d) ime in oddelek izdajatelja;

(e) prejemnik ali prejemniki, z zaporedno številko;

(f) predmet;

(g) številka;

(h) število kopij v obtoku;

(i) priprava popisa tajnih podatkov, ki so bile predložene Svetu;

(j) vpisnik o preklicu tajnosti ali o znižanju stopenj tajnosti podatkov.

39. Splošna pravila, predvidena v poglavjih I do V tega Oddelka veljajo za Urad za tajne podatke pri GSS, razen če jih ne spreminjajo posebna pravila iz tega poglavja.

ODDELEK VIII

ARHIVSKI URADI TRÈS SECRET UE/EU TOP SECRET

1. Namen arhivskih uradov TRÈS SECRET UE/EU TOP SECRET je zagotoviti arhiviranje, rokovanje z dokumenti TRÈS SECRET UE/EU TOP SECRET in njihovo razpošiljanje v skladu s predpisi o varovanju tajnosti. Vodja arhivskega urada TRÈS SECRET UE/EU TOP SECRET v vsaki državi članici, v GSS in po potrebi v decentraliziranih agencijah EU je uradnik, zadolžen za nadzor na stopnji TRES SECRET UE/EU TOP SECRET.

2. Centralni arhivski uradi imajo vlogo glavnega sprejemnega in odpremnega organa v državah članicah, v GSS in v decentraliziranih agencijah EU, pri katerih so bili taki uradi ustanovljeni, po potrebi pa tudi v drugih institucijah EU, mednarodnih organizacijah in tretjih državah, s katerimi ima Svet sklenjene sporazume o varnostnih postopkih za izmenjavo tajnih podatkov.

3. Če je potrebno, se ustanovijo podarhivski uradi, ki so zadolženi za notranje upravljanje z dokumenti TRÈS SECRET UE/EU TOP SECRET; njihova naloga je posodabljanje podatkov o kroženju vsakega dokumenta, za katerega so zadolženi.

4. Podarhivski uradi TRÈS SECRET UE/EU TOP SECRET se ustanovijo, kot določa Oddelek I, zaradi zadovoljevanja dolgoročnih potreb in so pridruženi centralnemu arhivskemu uradu TRES SECRET UE/EU TOP SECRET. Če so potrebe po dokumentih TRES SECRET UE/EU TOP SECRET samo začasne ali priložnostne, se ti dokumenti lahko razpošiljajo brez ustanovitve podarhivskih uradov TRES SECRET UE/EU TOP SECRET pod pogojem, da so predpisana pravila, ki zagotavljajo nadaljnji nadzor s strani ustreznega arhivskega urada TRÈS SECRET UE/EU TOP SECRET, in da se pri tem upoštevajo vsi ukrepi za fizično varovanje tajnosti in ukrepi varovanja tajnosti v zvezi z osebjem.

5. Podarhivski uradi ne smejo pošiljati dokumentov TRÈS SECRET UE/EU TOP SECRET neposredno drugim podarhivskim uradom istega centralnega arhivskega urada TRÈS SECRET UE/EU TOP SECRET brez njegove izrecne odobritve.

6. Vse izmenjave dokumentov TRÈS SECRET UE/EU TOP SECRET med podarhivskimi uradi, ki niso pridruženi istemu centralnemu arhivskemu uradu, morajo potekati preko centralnih arhivskih uradov TRÈS SECRET UE/EU TOP SECRET.

CENTRALNI ARHIVSKI URADI TRÈS SECRET UE/EU TOP SECRET

7. Kot uradnik za nadzor je vodja centralnega arhivskega urada TRÈS SECRET UE/EU TOP SECRET odgovoren za:

   (a) pošiljanje dokumentov TRÈS SECRET UE/EU TOP SECRET v skladu s predpisi, ki jih določa Oddelek VII;

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

   (c) shranjevanje potrdil vseh arhivskih uradov za vse dokumente TRÈS SECRET UE/EU TOP SECRET, ki so bili razposlani preko centralnega arhivskega urada;

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

   (e) vodenje posodobljenega seznama vseh centralnih arhivskih uradov TRÈS SECRET UE/EU TOP SECRET, s katerimi običajno izmenjuje korespondenco, skupaj z imeni in podpisi imenovanih uradnikov za nadzor in njihovih pooblaščenih namestnikov;

   (f) fizično varovanje vseh dokumentov TRÈS SECRET UE/EU TOP SECRET, ki se hranijo v arhivskem uradu v skladu s predpisi iz Oddelka IV.

PODARHIVSKI URADI TRÈS SECRET UE/EU TOP SECRET

8. Kot uradnik za nadzor, je vodja podarhivskega urada TRÈS SECRET UE/EU TOP SECRET odgovoren za:

   (a) prenos dokumentov TRÈS SECRET UE/EU TOP SECRET v skladu s predpisi, ki jih vsebujejo Oddelek VII in odstavka 5 in 6 Oddelka VIII;

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

(c) razpošiljanje dokumentov TRÈS SECRET UE/EU TOP SECRET v skladu z navodili organa izvora ali na podlagi potrebe po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog, ob poprejšnjem preverjanju ustreznosti zahtevanega varnostnega potrdila naslovnika;

(d) vodenje posodobljenega seznama vseh dokumentov stopnje TRÈS SECRET UE/EU TOP SECRET, ki se hranijo ali so v obtoku pod njegovim nadzorom ali ki so bili poslani drugim arhivskim uradom TRÈS SECRET UE/EU TOP SECRET, ter hranjenje vseh potrebnih potrdil;

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

(f) fizično varovanje vseh dokumentov TRES SECRET UE/EU TOP SECRET, ki se hranijo v podarhivskem uradu, v skladu s predpisi iz Oddelka IV.

INVENTURNI POPISI

9. Vsakih dvanajst mesecev vsi arhivski uradi TRÈS SECRET UE/EU TOP SECRET opravijo posamični popis vseh dokumentov stopnje TRES SECRET UE/EU TOP SECRET, za katere so odgovorni. Dokument velja za evidentiranega, če ga je arhivski urad fizično pregledal ali če urad razpolaga s potrdilom arhivskega urada TRES SECRET UE/EU TOP SECRET, kateremu je bil poslan, s potrdilom o uničenju dokumenta ali z navodili o znižanju ali preklicu stopenj tajnosti dokumenta.

10. Podarhivski uradi ugotovitve letnega popisa pošljejo centralnemu arhivskemu uradu, kateremu so podrejeni, do datuma, ki ga ta določi.

11. ONV ter tiste institucije EU, mednarodne organizacije in decentralizirane agencije EU, pri katerih so bili ustanovljeni arhivski uradi TRÈS SECRET UE/EU TOP SECRET, ugotovitve letnih popisov, opravljenih v centralnih arhivskih uradih TRÈS SECRET UE/EU TOP SECRET, pošljejo generalnemu sekretarju/visokemu predstavniku najpozneje do 1. aprila vsakega leta.

ODDELEK IX

UKREPI VAROVANJA TAJNOSTI, KI SE IZVAJAJO V ČASU POSEBNIH SESTANKOV O POSEBEJ OBČUTLJIVIH VPRAŠANJIH, KI POTEKAJO ZUNAJ PROSTOROV SVETA

SPLOŠNO

1. Ukrepe varovanja tajnosti, navedene v nadaljevanju, je treba uporabljati, kadar sestanki Evropskega Sveta, Sveta, ministrski ali drugi pomembni sestanki potekajo zunaj prostorov Sveta v Bruslju ali Luksemburgu in kadar zaradi visoke občutljivosti obravnavanih vprašanj ali podatkov to opravičujejo posebne varnostne zahteve. Ti ukrepi se nanašajo samo na zaščito tajnih podatkov EU; za potrebne pa se lahko izkažejo tudi drugi varnostni ukrepi.

ODGOVORNOSTI

Države članice gostiteljice

2. Država članica, na katere ozemlju poteka sestanek (država članica gostiteljica) je v sodelovanju z Varnostnim uradom GSS odgovorna za varnost sestankov Evropskega sveta, Sveta in ministrskih ali drugih pomembnih sestankov ter za fizično varnost glavnih delegatov in članov njihovega osebja.

V zvezi z varnostno zaščito tajnih podatkov mora država članica posebej zagotoviti, da:

(a) so izdelani načrti za primere ogrožanja varnosti tajnih podatkov in incidente v zvezi z varnostjo, pri čemer se predvideni ukrepi nanašajo predvsem na varno hrambo tajnih dokumentov EU v uradih;

(b) so sprejeti taki ukrepi, ki omogočajo dostop do komunikacijskega sistema Sveta za sprejem in pošiljanje tajnih sporočil EU. Država članica gostiteljica na zahtevo zagotovi tudi dostop do varnih telefonskih sistemov.

Države članice

3. Organi oblasti držav članic morajo sprejeti potrebne ukrepe, ki zagotavljajo, da:

(a) je za njihove nacionalne delegate predvideno overjanje ustreznih varnostnih potrdil, če je potrebno, v obliki signalnega sporočila ali po telefaksu bodisi neposredno uradniku, ki je zadolžen za varnost sestanka, ali preko Varnostnega urada GSS;

(b) so o vsaki značilni nevarnosti zaradi ustreznega ukrepanja obveščeni organi oblasti države članice gostiteljice in po potrebi Varnostni urad GSS.

Uradnik, zadolžen za varnost sestanka

4. Imenuje se uradnik, ki je zadolžen za varnost sestanka in je odgovoren za splošno pripravo in nadzor nad splošnimi internimi ukrepi varovanja tajnosti ter za uskladitev z drugimi varnostnimi organi. Ukrepi, ki jih sprejme, se v splošnem nanašajo na:

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

(ii) preverjanje osebja, ki mu je dovoljen dostop do kraja sestanka, do prostora, namenjenega delegacijam, in do konferenčnih dvoran, ter preverjanje vse opreme;

(iii) stalno usklajevanje s pristojnimi organi države članice gostiteljice in z Varnostnim uradom GSS.

(b) vključitev navodil o varovanju tajnosti v dosje sestanka ob ustreznem upoštevanju zahtev iz teh predpisov o varovanju tajnosti in vseh drugih navodil za varovanje tajnosti, ki bi se izkazala kot potrebna.

Varnostni urad GSS

5. Varnostni urad GSS mora imeti vlogo svetovalca v zvezi z varovanjem tajnosti pri pripravi sestanka; tam mora biti zastopan zaradi pomoči in svetovanja uradniku, zadolženemu za varnost sestanka, in, po potrebi, delegacijam.

6. Vsaka na sestanku prisotna delegacija mora določiti uradnika za varovanje tajnosti, ki je odgovoren za obravnavanje zadev v zvezi z varovanjem tajnosti v svoji delegaciji in za vzdrževanje stikov z uradnikom, zadolženim za varnost sestanka, po potrebi pa tudi z zastopnikom Varnostnega urada GSS.

VARNOSTNI UKREPI

Varnostna območja

7. Vzpostavijo se naslednja varnostna območja:

(a) varnostno območje Razreda II, ki ga sestavljajo redakcijski prostor, pisarniški prostori GSS z razmnoževalno grafično opremo ter pisarniški prostori za delegacije;

(b) varnostno območje Razreda I, ki ga sestavljajo konferenčna dvorana ter kabine za prevajalce in za tehnično osebje, zadolženo za ozvočenje;

(c) upravna območja, ki jih sestavljajo območje za tisk in tisti deli na kraju sestanka, ki jih uporabljajo uprava, službe za postrežbo in sprejem ter območje, ki neposredno meji na tiskovno središče in kraj sestanka.

Prepustnice

8. Uradnik, zadolžen za varnost sestanka, mora glede na zahteve in potrebe delegacij poskrbeti za ustrezne priponke. Kadar se to zahteva, se lahko uvedejo razlike v dostopu do različnih varnostnih območij.

9. Varnostna navodila v zvezi s sestankom morajo od vseh zadevnih oseb zahtevati, da v območju kraja sestanka svoje priponke stalno nosijo na vidnem mestu, tako da jih varnostno osebje po potrebi lahko preveri.

10. Z izjemo udeležencev, ki nosijo priponke, naj bi bilo na kraju sestanka prisotnih čim manj drugih oseb. Nacionalne delegacije, ki želijo med sestankom sprejeti obiskovalce, morajo o tem obvestiti uradnika, zadolženega za varnost sestanka. Obiskovalci morajo nositi priponko z oznako obiskovalca. Prepustnico obiskovalca je treba izpolniti z imenom obiskovalca in z imenom obiskane osebe. Obiskovalci morajo biti ves čas v spremstvu varnostnika ali obiskane osebe. Spremljevalna oseba mora nositi prepustnico obiskovalca, ki jo ob odhodu obiskovalca s kraja sestanka skupaj z obiskovalčevo priponko vrne varnostnemu osebju.

Nadzor fotografske in avdio opreme

11. V varnostno območje Razreda I ni dovoljen vnos naprav za snemanje slike ali zvoka, z izjemo opreme fotografov in tonskih tehnikov, ki imajo za to ustrezno dovoljenje uradnika, zadolženega za varnost sestanka.

Preverjanje aktovk, prenosnih računalnikov in paketov

12. Imetniki prepustnic z dovoljenim dostopom do varnostnega območja s seboj lahko običajno prinesejo svoje aktovke in prenosne računalnike (samo z lastnim napajanjem) brez preverjanja. Pakete, ki so namenjeni delegacijam, te lahko sprejmejo potem, ko jih je bodisi pregledal uradnik delegacije, zadolžen za varnost, ko so bili varnostno pregledani s specialno opremo ali ko jih je odprlo varnostno osebje, zadolženo za pregled. Če uradnik, zadolžen za varnost sestanka, presodi za potrebno, se za pregled aktovk in paketov lahko predpišejo strožji ukrepi.

Tehnična varnost

13. Za tehnično varnost prostora, v katerem poteka sestanek, lahko poskrbi tehnična varnostna ekipa, ki med sestankom lahko izvaja elektronski nadzor.

Dokumenti delegacij

14. Za prinašanje in odnašanje tajnih dokumentov EU na sestanke in z njih so odgovorne delegacije. Odgovorne so tudi za preverjanje in varovanje tajnosti tistih dokumentov, ki jih uporabljajo v njim dodeljenih prostorih. Za dostavo na kraj sestanka in odnašanje tajnih dokumentov s kraja sestanka delegacije za pomoč lahko zaprosijo državo članico gostiteljico.

Varna hramba dokumentov

15. Če GSS, Komisija ali delegacije tajnih dokumentov ne morejo shraniti v skladu z odobrenimi standardi, te dokumente lahko ob povratnem potrdilu v zapečateni ovojnici predajo uradniku, zadolženemu za varovanje tajnosti, tako da ta dokumente lahko shrani v skladu z odobrenimi standardi.

Pregled prostorov

16. Ob koncu vsakega delovnega dne mora uradnik, zadolžen za varnost sestanka, poskrbeti za pregled prostorov GSS in delegacij z namenom zagotoviti, da so vsi tajni dokumenti EU shranjeni na varnem kraju; v nasprotnem mora ustrezno ukrepati.

Odstranjevanje odpadkov s tajnimi podatki EU

17. Z vsemi odpadki je treba ravnati kot s tajnimi podatki EU, zato morajo zaradi njihove odstranitve GSS in delegacijam biti na voljo koši ali vreče za odpadke. Preden zapustijo prostore, ki so jim določeni, morajo GSS in delegacije svoje odpadke odnesti do uradnika, zadolženega za varnost sestanka, ki mora poskrbeti za njihovo uničenje v skladu s predpisi.

18. Ob koncu sestanka se vsi dokumenti, ki so pri GSS ali delegacijah a jih ti več ne potrebujejo, obravnavajo kot odpadki. Pred prenehanjem izvajanja varnostnih ukrepov, ki so bili sprejeti zaradi sestanka, je treba opraviti temeljit pregled prostorov GSS in delegacij. Dokumenti, za katere je bil podpisan sprejem, morajo v dopustnem obsegu biti uničeni po določbah Oddelka VII.

ODDELEK X

KRŠITVE VAROVANJA TAJNOSTI IN OGROŽANJE TAJNIH PODATKOV EU

1. Kršitve varnosti nastanejo kot posledica dejanja ali opustitve, ki nasprotujeta nekemu predpisu Sveta ali države o varovanju tajnosti, kar bi lahko ogrozilo ali izpostavilo nevarnosti tajne podatke EU.

2. Do ogrožanja tajnih podatkov EU pride, če taki podatki v celoti ali delno pridejo v roke nepooblaščenih oseb, to je tistih, ki nimajo ustreznega varnostnega potrdila ali za katere ne velja potreba po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog, ali če obstaja verjetnost, da se je to tudi zgodilo.

3. Tajni podatki EU se lahko ogrozijo kot posledica nepazljivosti, malomarnosti ali indiskretnosti, pa tudi zaradi dejavnosti služb, ki imajo za cilj EU ali njene države članice glede tajnih podatkov in dejavnosti EU, ali zaradi uničevalnih organizacij.

4. Pomembno je, da so vse osebe, od katerih se zahteva delo s tajnimi podatki EU, temeljito seznanjene z varnostnimi postopki, z nevarnostmi, ki jo pomenijo indiskretni razgovori in njihovi odnosi s tiskom. Zavedati se morajo pomena tega, da o vsaki kršitvi varnosti, ki jo opazijo, takoj obvestijo varnostni organ države članice, institucije ali agencije, v kateri so zaposlene.

5. Če varnostni organ odkrije kršitev varovanja tajnosti, ki se nanaša na tajne podatke EU ali na izgubo ali izginotje tajnega gradiva EU, ali je o njej obveščen, nemudoma ukrepa z namenom:

   (a) ugotoviti dejstva;

   (b) oceniti in zmanjšati povzročeno škodo na minimum;

   (c) preprečiti ponovitev;

   (d) obvestiti pristojne organe o posledicah kršitve varnosti..

   V tej zvezi je treba pridobiti naslednje podatke:

   (i) opis zadevnega tajnega podatka vključno s stopnjo tajnosti, opravilno številko in številko kopije, datumom, organom izvora, predmetom in razsežnostjo tajnega podatka;

   (ii) kratek opis okoliščin, v katerih je prišlo do kršitve varnosti, vključno z datumom in obdobjem, v katerem je bil tajni podatek izpostavljen ogrožanju;

   (iii) izjavo o obveščenosti organa izvora.

6. Dolžnost vsakega varnostnega organa je, da takoj, ko je bil obveščen o možni kršitvi varovanja tajnosti, o tem poroča po naslednjem postopku: podarhivski urad TRÈS SECRET UE/EU TOP SECRET o zadevi poroča Varnostnemu uradu GSS preko svojega centralnega arhivskega urada TRÈS SECRET UE/EU TOP SECRET; če je do ogrožanja tajnih podatkov EU prišlo na področju pristojnosti države članice, je o tem treba poročati Varnostnemu uradu GSS preko pristojnega ONV, kakor to določa odstavek 5.

7. O primerih v zvezi s tajnimi podatki RESTREINT UE je treba poročati le če imajo neobičajne lastnosti.

8. Ob obvestilu, da je prišlo do kršitve varovanja tajnosti, generalni sekretar/visoki predstavnik:

   (a) uradno obvesti organ izvora zadevnega tajnega podatka;

   (b) zaprosi pristojne varnostne organe za začetek preiskav;

   (c) usklajuje poizvedovanja, če je v zadevi udeleženih več varnostnih organov;

(d) pridobi poročilo o okoliščinah kršitve, datumu in obdobju, v katerem naj bi se zgodila in bila odkrita, skupaj s podrobnim opisom vsebine in stopnjo tajnosti zadevnega gradiva. Poročati je treba tudi o škodi, povzročeni interesom EU ali eni ali več njenih držav članic in o ukrepih, ki so bili sprejeti za preprečitev ponovitve kršitve.

9. Organ izvora obvesti naslovnike tajnega podatka in izda ustrezna navodila.

10. Oseba, ki jo bremeni odgovornost za ogrožanje tajnih podatkov EU, je disciplinsko odgovorna v skladu z ustreznimi pravili in predpisi. Disciplinsko ukrepanje je brez vpliva na pravne posege.

ODDELEK XI

ZAŠČITA PODATKOV V SISTEMIH INFORMACIJSKE TEHNOLOGIJE IN V KOMUNIKACIJSKIH SISTEMIH

Vsebina

Poglavje I

Uvod

SPLOŠNI VIDIKI

1. Varnostna politika in zahteve v tem oddelku se nanašajo na vse komunikacijske in informacijske sisteme ter omrežja (v nadaljevanju SISTEMI), v katerih se obdelujejo tajni podatki na stopnji CONFIDENTIEL UE in višje.

2. SISTEMI, v katerih se obdelujejo tajni podatki RESTREINT UE, prav tako zahtevajo ukrepe za zaščito zaupnosti takih podatkov. Pri vseh SISTEMIH se zahtevajo ukrepi za varovanje celovitosti in razpoložljivosti tistih sistemov in podatkov, ki jih vsebujejo. Ukrepe varovanja tajnosti, ki se uporabljajo pri teh sistemih, določi imenovani organ za varnost akreditacije (Security Accreditation Authority — SAA) in so sorazmerni glede na ocenjeno tveganje ter skladni z ureditvijo teh predpisov o varovanju tajnosti.

3. Varovanje senzorskih sistemov, ki vsebujejo vgrajene SISTEME IT, se določi in specificira v splošnem kontekstu sistemov, katerih del so, v mejah možne uporabe veljavnih določb tega oddelka.

OGROŽENOST IN RANLJIVOST SISTEMOV

4. V splošnem je mogoče ogroženost opredeliti kot možnost naključnega ali namernega ogrožanja tajnih podatkov. V zvezi s SISTEMI tako ogrožanje pomeni izgubo ene ali več značilnosti zaupnosti, celovitosti in razpoložljivosti. Ranljivost je mogoče definirati kot šibkost ali pomanjkanje nadzora, ki lahko olajša ali dopusti pojav ogroženosti nekega specifičnega sredstva ali cilja. Ranljivost lahko izhaja iz opustitve ali se nanaša na slabosti v moči nadzora, njegovi celovitosti ali doslednosti; lahko je tehničnega, postopkovnega ali operativnega značaja.

5. Tajni in drugi podatki EU, ki se obdelujejo v SISTEMIH v zgoščeni obliki zaradi možnosti hitre ponovne pridobitve, komuniciranja in uporabe, so izpostavljeni številnim tveganjem. Ta obsegajo dostop nepooblaščenih uporabnikov do podatkov ali nasprotno, zavrnitev dostopa pooblaščenim uporabnikom. Tu so še tveganja v zvezi z razkritjem nepooblaščeni osebi, ponarejanjem, spreminjanjem ali izbrisom tajnih podatkov. Poleg tega je zapletena in včasih občutljiva oprema draga in jo je pogosto težko popraviti ali na hitro zamenjati. Ti SISTEMI so zatorej privlačen cilj operacij zbiranja podatkov in sabotaž, zlasti če obstaja mišljenje, da so ukrepi varovanja tajnosti neučinkoviti.

UKREPI VAROVANJA TAJNOSTI

6. Poglavitni namen ukrepov varovanja tajnosti, navedenih v tem oddelku, je zagotoviti zaščito pred razkritjem podatkov nepooblaščeni osebi (izguba zaupnosti) in pred izgubo celovitosti in razpoložljivosti podatkov. Za zagotovitev ustrezne varnostne zaščite SISTEMA, v katerem se obdelujejo tajni podatki EU, je treba določiti primerne standarde konvencionalnega varovanja tajnosti skupaj s primernimi posebnimi postopki in tehnikami varovanja tajnosti, načrtovanimi za vsak SISTEM posebej.

7. Za vzpostavitev varnega okolja, v katerem SISTEM deluje, je treba opredeliti in izvajati uravnotežen sklop ukrepov varovanja tajnosti. Področja uporabe teh ukrepov zadevajo fizične elemente, osebje, netehnične postopke in postopke v zvezi z delovanjem računalnikov in komunikacij.

8. Ukrepi varovanja tajnosti v računalnikih (varnostne značilnosti strojne in programske opreme) morajo vsebovati zahteve po uporabi načela potrebe po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog in preprečevati ali odkrivati razkritje podatkov nepooblaščeni osebi. Obseg zanesljivosti ukrepov varovanja tajnosti pri računalnikih se določi med postopkom določanja zahtev za varovanje tajnosti. Postopek akreditacije določa, da je prisotna primerna stopnja zanesljivosti, ki opravičuje zaupanje v ukrepe varovanja tajnosti pri računalnikih.

IZJAVA O ZAHTEVAH ZA VAROVANJE TAJNOSTI, KI SO ZNAČILNE ZA SISTEM (SSRS)

9. Za vse SISTEME, v katerih se obdelujejo tajni podatki CONFIDENTIEL UE in višje, mora organ pristojen za delovanje sistema IT (IT System Operational Authority — ITSOA), po potrebi v sodelovanju s prispevki in pomočjo projektnega osebja in organa INFOSEC, pripraviti izjavo o zahtevah za varovanje tajnosti, značilnih za SISTEM (SSRS — SYSTEM-Specific Security Requirement Statement), ki jo potrdi SAA. SSRS se zahteva tudi, kadar SAA oceni, da je razpoložljivost in celovitost tajnih podatkov RESTREINT UE ali netajnih podatkov bistvenega pomena za varovanje tajnosti.

10. SSRS se izoblikuje v najzgodnejši fazi zasnove projekta in se razvija ter dograjuje vzporedno z razvojem projekta; v različnih fazah projekta in v življenjskem ciklusu delovanja SISTEMA ima različne vloge.

11. SSRS predstavlja zavezujoč sporazum med organom, pristojnim za delovanje sistema IT, in SAA, na podlagi katerega se SISTEMU dodeli akreditacija.

12. SSRS je izčrpna in izrecna izjava o načelih varovanja tajnosti, ki jih je treba upoštevati, in o natančno določenih zahtevah za varovanje tajnosti, ki jih je treba izpolnjevati. Podlago ima v varnostni politiki Sveta in v ocenah tveganj ali v parametrih, ki se določajo glede na okolje delovanja, najnižjo stopnjo preverjene varnostne zanesljivosti osebja, najvišjo stopnjo tajnosti obdelovanih podatkov, način delovanja z varovanjem tajnosti ali zahteve uporabnikov. SSRS je sestavni del dokumentacije projekta, ki se predloži ustreznim organom za namene tehnične, proračunske in varnostne odobritve. V svoji končni obliki je SSRS izčrpna izjava o vsem, kar je pomembno za varnostne značilnosti SISTEMA.

NAČINI DELOVANJA Z VAROVANJEM TAJNOSTI

13. Zaradi zahtev v različnih časovnih obdobjih se vsi SISTEMI, v katerih se obdelujejo tajni podatki CONFIDENTIEL UE in višje, akreditirajo za delovanje na en ali več naslednjih načinov delovanja z varovanjem tajnosti glede na njihov nacionalni ekvivalent:

(a) „dedicated“;

(b) „system high“; in

(c) „multi-level“

Poglavje II

Opredelitve pojmov

DODATNE OZNAKE

14. Poleg oznak iz razvrstitve po stopnji tajnosti se uporabljajo oznake CRYPTO ali katerakoli druga oznaka, ki jo priznava EU, kadar se pojavi potreba po omejenem razpošiljanju nekega dokumenta in posebnem rokovanju z njim.

15. NAČIN DELOVANJA Z VAROVANJEM TAJNOSTI „DEDICATED“ pomeni način delovanja, pri katerem so VSE osebe, ki imajo dostop do SISTEMA, varnostno preverjene do najvišje stopnje tajnosti podatkov, ki se v SISTEMU obdelujejo, in za katere velja splošna potreba po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog za VSE podatke, ki se v SISTEMU obdelujejo.

Opombe:

(1) Splošno načelo potrebe po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog pomeni, da zahteve glede obveznosti za varnostne značilnosti računalnikov ne predvidevajo ločevanja podatkov znotraj SISTEMA.

(2) Druge določbe o varnostnih značilnostih (npr. glede fizične zaščite, osebja in postopkov) se prilagodijo zahtevam po najvišji stopnji tajnosti in vsem oznakam kategorij podatkov, ki se obdelujejo v okviru SISTEMA.

16 NAČIN DELOVANJA Z VAROVANJEM TAJNOSTI „HIGH SECURITY“ pomeni način delovanja, pri katerem so VSE osebe, ki imajo dostop do SISTEMA, varnostno preverjene do najvišje stopnje tajnosti podatkov, ki se v tem SISTEMU obdelujejo, vendar pa splošna potreba po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog glede podatkov, ki se v SISTEMU obdelujejo, NE velja za VSE osebe, ki imajo dostop do SISTEMA.

Opombe:

(1) Neuveljavljanje splošnega načela o potrebnosti seznanitve s podatki zaradi opravljanja funkcije ali delovnih nalog za nekatere osebe pomeni, da morajo določbe o varnostnih značilnostih računalnikov predvidevati selektiven dostop do SISTEMA in ločevanje podatkov znotraj njega.

(2) Druge določbe o varnostnih značilnostih (npr. glede fizične zaščite, osebja in postopkov) se prilagodijo zahtevam po najvišji stopnji tajnosti in vsem oznakam kategorij podatkov, ki se obdelujejo v okviru SISTEMA.

(3) Vse podatke, ki se obdelujejo ali so na razpolago SISTEMU v tem načinu delovanja z varovanjem tajnosti skupaj z izhodnimi podatki, se zaščitijo, dokler ni drugače določeno, kot podatki za potencialne kategorijske oznake in na najvišji stopnji tajnosti, razen če ni na voljo taka funkcionalnost obstoječih oznak, ki omogoča zadovoljivo stopnjo zaupanja vanje.

17. NAČIN DELOVANJA Z VAROVANJEM TAJNOSTI „MULTI-LEVEL“ pomeni način delovanja pri katerem VSE osebe, ki imajo dostop do SISTEMA, NISO varnostno preverjene do najvišje stopnje glede tajnosti podatkov, ki se v tem SISTEMU obdelujejo in kjer splošna potreba po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog glede podatkov, ki se v SISTEMU obdelujejo, NE velja za VSE osebe, ki imajo dostop do SISTEMA.

Opombe:

(1) Ta način delovanja dopušča sprotno obdelovanje podatkov različnih stopenj tajnosti in podatkov z različnimi kategorijskimi oznakami.

(2) Ker vse osebe niso varnostno preverjene do najvišje stopnje tajnosti in ker splošno načelo potrebe po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog ne velja za vse osebe, to pomeni, da morajo določbe o varnostnih značilnostih računalnikov predvideti selektiven dostop do SISTEMA in ločevanje podatkov v njegovem okviru.

18. INFOSEC pomeni uporabo ukrepov za zaščito podatkov, ki se obdelujejo, hranijo ali prenašajo s pomočjo komunikacijskih, informacijskih in drugih elektronskih sistemov pred naključno ali namerno izgubo zaupnosti, celovitosti ali razpoložljivosti, in za preprečevanje izgube celovitosti in razpoložljivosti samih sistemov. Ukrepi INFOSEC vsebujejo ukrepe varovanja tajnosti pri računalnikih, prenosih, oddajanju in kriptografski metodi ter odkrivanju, dokumentiranju in zoperstavljanju grožnjam, uperjenim proti podatkom in SISTEMOM.

19. VAROVANJE TAJNOSTI PRI RAČUNALNIKIH (COMPUSEC) pomeni uporabo določb o varovanju tajnosti za strojno opremo, sistemske programe in programsko opremo zaradi preprečitve razkritja nepooblaščeni osebi, manipulacij, spreminjanja/brisanja podatkov ali izpada sistema ali zaščite pred njimi.

20. VARNOSTNI RAČUNALNIŠKI PRODUKT pomeni generični produkt varovanja tajnosti pri računalnikih, ki je namenjen vključitvi v sistem IT zaradi uporabe pri izboljšanju ali zagotavljanju zaupnosti, celovitosti ali razpoložljivosti obdelovanih podatkov.

21. VAROVANJE TAJNOSTI PRI KOMUNIKACIJAH (COMSEC) pomeni uporabo ukrepov varovanja tajnosti v telekomunikacijah zaradi preprečevanja dostopa nepooblaščenim osebam do pomembnih podatkov, do katerih bi lahko prišle s prilastitvijo in proučevanjem telekomunikacijskih sporočil, ali zaradi zagotavljanja avtentičnosti takih sporočil.

Opomba:

Taki ukrepi vsebujejo ukrepe varovanja tajnosti pri kriptografski metodi, pri prenosih in pri oddajanju; nanašajo se tudi na varovanje tajnosti v zvezi s postopki, fizičnimi elementi, osebjem, dokumenti in računalniki.

22. OCENA pomeni, da ustrezni organ natančno tehnično preuči varnostne vidike SISTEMA ali kriptografskega ali računalniškega produkta.

Opombe:

(1) Ocena pomeni, da je preverjena prisotnost zahtevane varnostne funkcionalnosti in odsotnost nezaželenih ogrožajočih stranskih učinkov v zvezi z njimi ter ocenjena možnost vplivanja na to funkcionalnost.

(2) Ocena določa obseg, v katerem so izpolnjene zahteve varovanja tajnosti SISTEMA ali zahteve varovanja tajnosti glede varnostnega računalniškega produkta, in določa stopnjo zanesljivosti SISTEMA ali kriptografskih funkcij ali zaupanja v funkcije varnostnega računalniškega produkta.

23. OVERJANJE pomeni izdajo formalne izjave, ki ima podlago v neodvisnem pregledu izvajanja in rezultatov ocene, o obsegu, v katerem SISTEM ustreza zahtevam za varovanje tajnosti ali v katerem varnostni računalniški produkt ustreza vnaprej določenim zahtevam za varovanje tajnosti.

24. AKREDITACIJA pomeni dovoljenje in odobritev SISTEMA za obdelovanje tajnih podatkov EU v njegovem operativnem okolju.

Opomba:

Akreditacija se odobri potem, ko so izpeljani vsi ustrezni postopki varovanja tajnosti in ko je dosežena zadostna stopnja zaščite sistemskih elementov. Akreditacija se običajno odobri na podlagi SSRS skupaj z:

(a) izjavo o cilju akreditacije za sistem, zlasti glede na stopnjo tajnosti obravnavanih podatkov in glede na predlagani način delovanja z varovanjem tajnosti v sistemu ali omrežju;

(b) analizo obvladovanja tveganj zaradi ugotavljanja ogroženosti in ranljivih točk ter ustreznih protiukrepov;

(c) varnostno operativnimi postopki (SecOP) z natančnim opisom predlaganih operacij (npr. načini delovanja, potrebne prihodnje storitve) ter opisom varnostnih značilnosti SISTEMA, ki so temelj akreditacije;

(d) načrtom za izvajanje in vzdrževanje varnostnih značilnosti;

(e) načrtom za prvo in nadaljnja preverjanja varnosti sistema ali varnosti omrežja, ocenjevanje in overjanje; in

(f) overitvijo, če je potrebna, skupaj z ostalimi elementi akreditacije.

25. IT SISTEM pomeni sklop opreme, metod in postopkov in po potrebi osebja, ki je organiziran zaradi izvajanja nalog obdelave podatkov.

Opombe:

(1) To pomeni sklop zmogljivosti, ki so prirejene za obdelovanje podatkov znotraj sistema.

(2) Taki sistemi se lahko uporabljajo v podporo posvetovanju, vodenju, nadzoru, komunikacijam in znanstvenim ali administrativnim aplikacijam skupaj z obdelovanjem besedil.

(3) Meje sistema so na splošno določene kot elementi, ki so pod nadzorom enega organa, pristojnega za delovanje sistema IT (ITSOA).

(4) Sistem IT lahko vsebuje take podsisteme, ki so sami po sebi sistemi IT.

26. VARNOSTNE ZNAČILNOSTI SISTEMA IT obsegajo vse funkcije strojne, sistemsko programske in programske opreme, lastnosti in značilnosti; postopke za delovanje, postopke glede odgovornosti in nadzora dostopa, območje IT, območje oddaljenih terminalov/delovnih postaj, omejitve v pravilih upravljanja, fizično strukturo in naprave, ukrepe nadzora za osebje in komunikacije, ki so potrebni za zagotavljanje sprejemljive stopnje zaščite tajnih podatkov, ki se obdelujejo v sistemu IT.

27. OMREŽJE IT pomeni geografsko razpršen, organiziran sklop sistemov IT, medsebojno povezanih zaradi izmenjave podatkov, ki vsebuje komponente medsebojno povezanih sistemov IT ter njihove uporabniške vmesnike z dopolnilnimi podatki ali komunikacijskimi omrežji.

Opombe:

(1) Omrežje IT lahko pri izmenjavi podatkov uporablja storitve enega ali več medsebojno povezanih komunikacijskih omrežij; več omrežij IT lahko uporablja storitve skupnega komunikacijskega omrežja.

(2) Omrežje IT se imenuje „lokalno“, če povezuje več računalnikov, ki so na enem mestu.

28. VARNOSTNE ZNAČILNOSTI OMREŽJA IT vključujejo varnostne značilnosti sistema IT posameznih sistemov IT, ki tvorijo omrežje skupaj s tistimi dodatnimi komponentami in značilnostmi v navezavi z omrežjem (npr. omrežne komunikacije, mehanizmi in postopki varnostnega prepoznavanja in označevanja, nadzor dostopa, programi in kontrolni zapisi), ki so potrebne zaradi zagotavljanja sprejemljive stopnje zaščite tajnih podatkov.

29. OBMOČJE IT pomeni območje, kjer se nahaja eden ali več računalnikov, njihove lokalne periferne in shranjevalne enote, enote za nadzor in njim podrejena omrežna in komunikacijska oprema.

Opomba:

To ne vključuje ločenega območja, v katerem so oddaljene periferne naprave ali terminali/delovne postaje, čeprav so te naprave priključene na opremo v območju IT.

30. OBMOČJE Z ODDALJENIMI TERMINALI/DELOVNIMI POSTAJAMI pomeni območje, ločeno od območja IT, z določeno računalniško opremo, njenimi perifernimi napravami ali terminali/delovnimi postajami in vso pripadajočo komunikacijsko opremo.

31. Protiukrepi TEMPEST so ukrepi varovanja tajnosti, katerih namen je varovanje opreme in komunikacijske infrastrukture pred ogrožanjem tajnih podatkov zaradi nenamernih elektromagnetnih oddajanj.

Poglavje III

Odgovornost za varovanje tajnosti

SPLOŠNO

32. Odgovornosti Varnostnega odbora, določene v Oddelku I, odstavek 4, vključujejo tudi vprašanja INFOSEC. Varnostni odbor svoje dejavnosti organizira tako, da lahko daje strokovne nasvete o zgornjih vprašanjih.

33. Če se pojavijo problemi v zvezi z varovanjem tajnosti (incidenti, kršitve, itd.), nemudoma ukrepata pristojni nacionalni organ in/ali Varnostni urad GSS. O vseh problemih je treba poročati Varnostnemu uradu GSS.

34. Generalni sekretar/visoki predstavnik ali, kadar je to potrebno, vodja decentralizirane agencije EU ustanovi Urad INFOSEC zaradi dajanja navodil varnostnemu organu o izvajanju in nadzoru določb o posebnih varnostnih značilnostih, ki so zasnovane kot del SISTEMOV.

ORGAN ZA VARNOSTNO AKREDITACIJO (SAA)

35. SAA je lahko:

— nacionalni organ za varnost (ONV),

— organ, ki ga določi generalni sekretar/visoki predstavnik,

— varnostni organ decentralizirane agencije EU, ali

— njegovi imenovani zastopniki glede na SISTEM, ki potrebuje akreditacijo.

36. SAA je odgovoren za zagotavljanje skladnosti SISTEMOV z varnostno politiko Sveta. Ena od njegovih nalog je odobritev SISTEMA za obdelavo tajnih podatkov EU do določene stopnje tajnosti v njegovem operativnem okolju. Glede GSS in po potrebi decentraliziranih agencij EU je SAA odgovoren za varovanje tajnosti v imenu generalnega sekretarja/visokega predstavnika ali vodij decentraliziranih agencij.

Pristojnosti organa za varnostno akreditacijo (SAA) pri GSS se nanašajo na vse SISTEME, ki delujejo v prostorih GSS. SISTEMI in komponente SISTEMOV, ki delujejo v državi članici, ostajajo v pristojnosti te države članice. Če različne komponente SISTEMA pridejo pod pristojnosti SAA pri GSS in drugih SAA, vse zadevne strani imenujejo skupni akreditacijski svet, za čigar usklajevanje je zadolžen SAA pri GSS.

ORGAN INFOSEC (IA)

37. Organ INFOSEC je odgovoren za dejavnosti urada INFOSEC. Glede GSS in, po potrebi, decentraliziranih agencij EU, je organ INFOSEC odgovoren za naslednje:

— tehnično svetovanje in dajanje pomoči SAA,

— pomoč pri oblikovanju SSRS,

— preverjanje SSRS zaradi zagotavljanja skladnosti s temi predpisi o varovanju tajnosti in politiko INFOSEC in arhitekturno dokumentacijo,

— sodelovanje v akreditacijskih odborih/svetih, če se zahteva, in dajanje priporočil INFOSEC o akreditacijah organu SAA,

— podporo dejavnostim izobraževanja in usposabljanja INFOSEC,

— dajanje tehničnih nasvetov pri preiskavah incidentov v zvezi z INFOSEC,

— vzpostavitev tehnične metodologije s smernicami, ki zagotavljajo izključno uporabo odobrene programske opreme.

ORGAN, PRISTOJEN ZA DELOVANJE SISTEMA IT (ITSOA)

38. Organ INFOSEC odgovornost za izvajanje in delovanje nadzora ter določb o posebnih varnostnih značilnostih SISTEMA prenese na ITSOA v najzgodnejši možni fazi. Ta odgovornost velja za celotno trajanje življenjskega ciklusa SISTEMA, od zasnove projekta do zaključene končne faze.

39. ITSOA je odgovoren za vse ukrepe varovanja tajnosti, ki so zasnovani kot sestavni del celotnega SISTEMA. Ta odgovornost se nanaša tudi na pripravo varnostno operativnih postopkov (SecOP). ITSOA podrobno določi standarde varovanja tajnosti in postopke, ki jih mora spoštovati dobavitelj SISTEMA.

40. ITSOA lahko del svoje odgovornosti, kadar je to primerno, prenese npr. na uradnika INFOSEC, zadolženega za varnost in na uradnika, zadolženega za varnost lokacije INFOSEC. V okviru INFOSEC ena oseba lahko opravlja več funkcij.

UPORABNIKI

41. Vsi uporabniki so odgovorni zagotoviti, da njihovo delovanje ne bo imelo škodljivih posledic za varnost SISTEMA, ki ga uporabljajo.

IZOBRAŽEVANJE INFOSEC

42. Izobraževanje in usposabljanje INFOSEC je na voljo na več ravneh in, po potrebi, za različno osebje v okviru GSS, decentraliziranih agencij EU ali vladnih oddelkov držav članic.

Poglavje IV

Netehnični ukrepi varovanja tajnosti

VARNOSTNA PREVERJENOST OSEBJA

43. Uporabniki SISTEMA morajo biti varnostno preverjeni in mora zanje veljati potreba po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog, če je tako potrebno zaradi tajnosti in vsebine podatkov, ki se obdelujejo znotraj njihovega SISTEMA. Za dostop do nekatere opreme ali podatkov, ki so značilni za SISTEME varovanja tajnosti, se zahteva posebno potrdilo, ki se izda v skladu s postopki Sveta.

44. SAA določi vsa občutljiva delovna mesta in opredeli stopnjo preverjene varnostne zanesljivosti in nadzora, ki velja za vse osebje na teh mestih.

45. SISTEMI so definirani in zasnovani na način, ki omogoča tako razdelitev nalog in odgovornosti osebju, da nobena posamezna oseba ne more v celoti poznati sistema ali imeti nadzora nad njegovimi ključnimi varnostnimi točkami. Cilj tega je doseči, da nihče ne bi mogel povzročiti spremembe ali namerno poškodovati sistema ali omrežja brez sodelovanja ene ali več drugih oseb.

FIZIČNO VAROVANJE TAJNOSTI

46. IT in oddaljena območja s terminali/delovnimi postajami (kakor je določeno v odstavkih 29 in 30), v katerih se tajni podatki CONFIDENTIEL UE in višje obdelujejo s pomočjo informacijske tehnologije ali kadar je dostop do takih podatkov potencialno mogoč, se vzpostavijo kot varnostna območja EU razreda I ali razreda II ali, po potrebi, glede na njihov nacionalni ekvivalent.

47. Na območjih IT in oddaljenih terminalih/delovnih postajah, kjer je mogoče vplivati na varnost SISTEMA, se ne sme nikoli zadrževati en sam pooblaščeni uradnik ali drug uslužbenec.

NADZOR DOSTOPA DO SISTEMA

48. Vsi podatki in gradivo, ki omogočajo nadzor dostopa do SISTEMA, se zavarujejo z ukrepi, ki so sorazmerni glede na najvišjo stopnjo tajnosti in kategorijsko oznako podatka, do katerega se dostop lahko dovoli.

49. Kadar ne služijo več temu namenu, se podatki in gradivo za nadzor dostopa do podatkov uničijo v skladu z odstavkoma 61 in 63.

Poglavje V

Tehnični ukrepi varovanja tajnosti

VAROVANJE TAJNOSTI PODATKOV

50. Dolžnost organa izvora podatkov je, da opredeli in po stopnjah tajnosti razvrsti vse dokumente, ki so nosilci podatkov, bodisi na papirju ali na računalniškem shranjevalnem nosilcu. Vsaka stran primerkov, izpisanih na papirju je zgoraj in spodaj označena s stopnjo tajnosti. Izhodni izpisi, bodisi na papirju ali na računalniškem shranjevalnem nosilcu, imajo isto stopnjo tajnosti kot je najvišja stopnja tajnosti podatkov, ki se uporabljajo pri njihovi izdelavi. Način delovanja SISTEMA tudi lahko vpliva na stopnjo tajnosti izpisanih primerkov takega sistema.

51. Dolžnost organizacije in lastnikov podatkov v njenem okviru je preučiti probleme pri sestavljanju posameznih elementov podatka v celoto in povzetke, ki jih je mogoče ustvariti ob povezavi zadevnih elementov ter odločiti, če je zaradi celovitosti podatka temu potrebna višja stopnja tajnosti ali ne.

52. Dejstvo, da ima podatek lahko obliko skrajšane kode, kode, namenjene za prenos ali predstavljene v kakršnikoli binarni obliki, ne zagotavlja varnostne zaščite in zato ne bi smelo imeti vpliva na stopnjo tajnosti podatkov.

53. Pri prenosu podatkov iz enega SISTEMA v drugega se podatki med prenosom in v sprejemnem SISTEMU zaščitijo na način, ki ustreza izvirni razvrstitvi po stopnjah tajnosti in kategoriji podatkov.

54. Z vsemi računalniškimi shranjevalnimi nosilci je treba ravnati v sorazmerju z najvišjo stopnjo tajnosti shranjenih podatkov ali oznak na nosilcu in nenehno skrbeti za njihovo ustrezno zaščitenost.

55. Ponovno uporabni računalniški nosilci, ki se uporabljajo za vnos tajnih podatkov EU, obdržijo najvišjo stopnjo tajnosti, za katero so bili uporabljeni, dokler stopnja tajnosti teh podatkov ni primerno znižana ali preklicana in je nosilec ponovno naravnan na ustrezno stopnjo tajnosti ali je bila stopnja tajnosti nosilca preklicana in ta uničen v skladu s postopkom, ki ga odobri GSS ali nacionalni organi (glej odstavke od 61 do 63).

NADZOR IN SLEDLJIVOST PODATKOV

56. Evidenca dostopa do tajnih podatkov stopnje SECRET UE in višje se vodi avtomatsko (kontrolni zapisi) ali z ročnimi vpisi v vpisnik. Ta evidenca se hrani v skladu s temi predpisi o varovanju tajnosti.

57. Izhodni izpisi tajnih podatkov EU znotraj območja IT se lahko obravnavajo kot ena tajna zadeva in jih ni treba vpisovati v vpisnik, pod pogojem, da je to gradivo prepoznavno opredeljeno, označeno glede na stopnje in pod primernim nadzorom.

58. Pri pošiljanju izpisov, nastalih v SISTEMU, ki obdeluje tajne podatke EU, iz območja IT na območje oddaljenega terminala/delovne postaje, se za nadzor nad pošiljanjem na daljavo določijo postopki, ki jih odobri SAA. Pri podatkih stopnje SECRET UE in višje taki postopki vsebujejo posebna navodila glede sledljivosti takih podatkov.

ROKOVANJE Z IN NADZOR NAD IZMENLJIVIMI RAČUNALNIŠKIMI NOSILCI

59. Vsi izmenljivi računalniški shranjevalni nosilci s stopnjo CONFIDENTIEL UE in višje se obravnavajo kot material in za njih veljajo splošna pravila. Primerne prepoznavne in razvrstitvene oznake o stopnji tajnosti morajo biti zaradi jasne prepoznave prilagojene značilnemu fizičnemu izgledu nosilca.

60. Uporabniki so dolžni zagotoviti, da so tajni podatki EU shranjeni na nosilcih skupaj z ustrezno označeno stopnjo tajnosti in zaščite. Določijo se postopki, ki zagotavljajo, da shranjevanje tajnih podatkov EU na računalniške shranjevalne nosilce na vseh ravneh poteka v skladu s temi predpisi o varovanju tajnosti.

PREKLIC STOPENJ TAJNOSTI IN UNIČENJE RAČUNALNIŠKIH NOSILCEV PODATKOV

61. Stopnja tajnosti pri računalniških nosilcih, ki se uporabljajo za vnos tajnih podatkov EU, se lahko zniža ali prekliče z uporabo odobrenih postopkov GSS ali nacionalnih postopkov.

62. Stopnja tajnosti pri računalniških shranjevalnih nosilcih tajnih podatkov TRÈS SECRET UE/EU TOP SECRET ali posebnih kategorij podatkov se ne prekliče, ti pa se ne smejo ponovno uporabljati.

63. Kadar stopnje tajnosti za računalniški shranjevalni nosilec ni mogoče preklicati ali se ta ne sme ponovno uporabiti, se računalniški nosilec uniči po odobrenem postopku GSS ali nacionalnem postopku.

VAROVANJE TAJNOSTI KOMUNIKACIJ

64. Pri elektromagnetnih prenosih tajnih podatkov EU se zaradi zaščite zaupnosti, celovitosti in razpoložljivosti takih prenosov izvajajo posebni ukrepi. SAA določi zahteve za zaščito prenosov pred odkrivanjem in prestrezanjem. Podatki, ki se prenašajo v komunikacijskem sistemu se zaščitijo na podlagi zahtev po zaupnosti, celovitosti in razpoložljivosti.

65. Če se zaradi zagotavljanja zaupnosti, celovitosti in razpoložljivosti zahteva uporaba kriptografskih metod, mora te metode in zadevne produkte posebej za te namene odobriti SAA.

66. Med prenosom se zaupnost podatkov, razvrščenih na stopnjo SECRET UE in višje, zaščiti s kriptografskimi metodami ali produkti, ki jih odobri Svet na priporočilo Varnostnega odbora Sveta. Med prenosom se zaupnost podatkov, razvrščenih na stopnji CONFIDENTIEL UE ali RESTREINT UE, zaščiti s kriptografskimi metodami ali produkti, ki jih odobri generalni sekretar/visoki predstavnik na priporočilo Varnostnega odbora Sveta ali država članica.

67. Podrobna pravila za prenos tajnih podatkov EU se predpišejo s posebnimi navodili o varovanju tajnosti, ki jih odobri Svet na priporočilo Varnostnega odbora Sveta.

68. V izrednih okoliščinah se tajni podatki na stopnjah RESTREINT UE, CONFIDENTIEL UE in SECRET UE lahko prenašajo kot razvidno besedilo pod pogojem, da se za vsak tak prenos izrecno izda dovoljenje. Take izredne okoliščine so naslednje:

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

(b) kadar je hitrost dostave bistvenega pomena ter sredstva za kriptografski zapis niso na voljo in se ocenjuje, da poslanih podatkov ni mogoče pravočasno uporabiti zaradi vplivanja na potek operacij.

69. SISTEM mora imeti zmogljivost, da zanesljivo zavrne dostop do tajnih podatkov EU na vsaki ali vseh delovnih postajah ali terminalih, če se tako zahteva s pomočjo fizičnega odklopa ali s posebnimi lastnostmi programske opreme, ki jih odobri SAA.

VAROVANJE TAJNOSTI V ZVEZI Z NAMESTITVIJO IN SEVANJEM

70. Začetna namestitev SISTEMOV in vse večje spremembe v zvezi z njo se določijo tako, da namestitev izvajajo varnostno preverjeni delavci pod stalnim nadzorstvom tehnično usposobljenega osebja, ki je varnostno preverjeno glede dostopa do tajnih podatkov EU na ravni, ki je enaka najvišji stopnji tajnosti, na kateri jih bo SISTEM hranil in obdeloval.

71. Vsa oprema se namesti v skladu s tekočo varnostno politiko Sveta.

72. SISTEMI, ki obdelujejo tajne podatke na stopnji CONFIDENTIEL UE in višje, se zaščitijo tako, da njihove varnosti ne morejo ogroziti škodljiva sevanja, katerih proučevanje in nadzor sta določena kot „TEMPEST“.

73. Protiukrepe TEMPEST, ki veljajo za namestitve v GSS in v decentraliziranih agencijah EU, pregleda in odobri organ TEMPEST-a, ki ga določi varnostni organ GSS. Za namestitve na nacionalni stopnji, v katerih se obdelujejo tajni podatki EU, odobritev izda na nacionalni ravni priznani organ TEMPEST.

Poglavje VI

Varovanje tajnosti med obdelavo

POSTOPKI DELOVANJA Z VAROVANJEM TAJNOSTI

74. SecOP določijo načela, ki jih je treba sprejeti na področju varnosti, potrebne operativne postopke in odgovornosti zaposlenega osebja. Za pripravo varnostno operativnih postopkov je zadolžen organ ITSOA.

ZAŠČITA PROGRAMSKE OPREME/UPRAVLJANJE KONFIGURACIJE

75. Varnostna zaščita aplikacijskih programov se določi na podlagi ocene varnostne razvrstitve po stopnji tajnosti programa samega in ne na podlagi stopnje tajnosti podatka, ki ga je treba obdelati. Verzije programske opreme v uporabi je treba pregledovati v rednih presledkih, da se zagotovi njihova celovitost in pravilno delovanje.

76. Nove ali spremenjene verzije programske opreme se ne smejo uporabljati za obdelavo tajnih podatkov EU, preden jih ne preveri ITSOA.

PREVERJANJE PRISOTNOSTI ŠKODLJIVE PROGRAMSKE OPREME/RAČUNALNIŠKIH VIRUSOV

77. Preverjanje prisotnosti škodljive programske opreme/računalniških virusov se opravlja v periodičnih presledkih v skladu z zahtevami SAA.

78. Vsi računalniški shranjevalni nosilci, ki pridejo v GSS, decentralizirane agencije EU ali v države članice, morajo pred priključitvijo na kakršenkoli SISTEM biti preverjeni zaradi prisotnosti škodljive programske opreme ali računalniških virusov.

VZDRŽEVANJE

79. Vse pogodbe in postopki v zvezi z rednim vzdrževanjem in vzdrževanjem SISTEMOV po naročilu, za katere je bila izdelana SSRS, morajo vsebovati zahteve in predpise za vzdrževalno osebje in njegovo opremo, ki prihaja na območje IT.

80. Zahteve morajo biti jasno navedene v SSRS, postopki pa morajo biti jasno navedeni v SecOP. Pogodbenemu izvajalcu, ki med vzdrževanjem zahteva uporabo diagnostičnih postopkov na daljavo, se to dovoli samo v izjemnih okoliščinah, ob strogem varnostnem nadzoru in samo ob odobritvi SAA.

Poglavje VII

Naročila

81. Vse varnostne produkte, ki jih je treba naročiti zaradi uporabe v SISTEMU, mora oceniti in overiti ali dati v postopek ocenitve ali overitve ustrezen ocenjevalni ali overitveni organ po mednarodno priznanih merilih (npr. Common Criteria for Information Technology Security Evaluation, glej ISO 15 408).

82. Pri odločanju za izposojo, ki naj bi imela prednost pred nakupom zlasti računalniških shranjevalnih nosilcev, se je treba zavedati, da taka oprema, potem ko je bila uporabljena za obdelavo tajnih podatkov EU, ne sme zapustiti primerno zavarovanega okolja brez poprejšnjega preklica tajnosti ob odobritvi SAA in da taka odobritev ni vedno mogoča.

AKREDITACIJA

83. Vse SISTEME, za katere je treba izdelati SSRS, je treba pred začetkom obdelovanja tajnih podatkov EU akreditirati s strani SAA na podlagi podatkov iz SSRS, SecOP in vse druge ustrezne dokumentacije. Podsistemi in oddaljeni terminali/delovne postaje se akreditirajo kot sestavni del SISTEMOV, na katere so priključeni. Če neki SISTEM opravlja storitve za Svet in druge organizacije, se GSS in zadevni varnostni organi o akreditaciji sporazumejo v medsebojnem soglasju.

84. Akreditacijski postopek se lahko izvede v skladu z akreditacijsko strategijo, primerno za tak SISTEM, ki jo določi SAA.

OCENITEV IN OVEROVITEV

85. V nekaterih primerih je pred akreditacijo treba oceniti in overoviti varnostne lastnosti strojne opreme, sistemskih programov in programske opreme SISTEMA kot primerne za zagotavljanje varovanja podatkov na želeni stopnji tajnosti.

86. Zahteve za ocenitev in overovitev morajo biti vključene v načrtovanje sistema in jasno navedene v SSRS.

87. Ocenitveni in overitveni postopek izvede tehnično usposobljeno in ustrezno varnostno preverjeno osebje v imenu ITSOA, v skladu z odobrenimi smernicami.

88. Ekipe lahko da na voljo organ za ocenjevanje ali overitev, imenovan pri državi članici, ali njegovi imenovani zastopniki, npr. pristojni in varnostno preverjeni pogodbeni partner.

89. Stopnja ocenitve in overitveni postopki se lahko poenostavijo (npr. omejitev na samo integracijske vidike), če imajo SISTEMI podlago v obstoječih računalniških varnostnih produktih, ki so ocenjeni in overjeni na nacionalni ravni.

RUTINSKO PREVERJANJE VARNOSTNIH ZNAČILNOSTI ZA PODALJŠANJE AKREDITACIJE

90. ITSOA določi rutinske postopke nadzora, ki zagotavljajo, da so vse varnostne značilnosti SISTEMA še veljavne.

91. SSRS jasno opredeli in navede vrsto sprememb, ki omogočajo ponovno akreditacijo ali jih mora predhodno odobriti SAA. Po vsaki spremembi, popravilu ali okvari, ki bi lahko škodljivo vplivale na varnostne značilnosti SISTEMA, ITSOA zagotovi ustrezno preverjanje zaradi pravilnega delovanja varnostnih značilnosti. Podaljšanje akreditacije SISTEMA je običajno odvisno od zadovoljivosti rezultatov takih preverjanj.

92. Vse SISTEME, pri katerih so uporabljene varnostne značilnosti, na periodični podlagi preveri in pregleda SAA. Pri SISTEMIH, ki obdelujejo tajne podatke TRÈS SECRET UE/TOP SECRET EU ali dodatne oznake, se pregledi opravijo vsaj enkrat letno.

Poglavje VIII

Začasna ali priložnostna uporaba

VAROVANJE TAJNOSTI PRI MIKRORAČUNALNIKIH/OSEBNIH RAČUNALNIKIH

93. Mikroračunalniki/osebni računalniki (PC) z vgrajenimi diski (ali drugi nosilci s trajnim pomnjenjem), ki delujejo bodisi samostojno ali so mrežno konfigurirani in prenosne računalniške naprave (npr. prenosni PC in elektronske „beležnice“) z vgrajenimi trdimi diski, se upoštevajo kot nosilci shranjenih podatkov v istem pomenu kakor računalniške diskete ali drugi izmenljivi računalniški nosilci.

94. Ta oprema je glede dostopa do nje, ravnanja z njo, hranjenja in prevozov upravičena do zaščite na ravni, ki je sorazmerna najvišji stopnji tajnosti kdajkoli shranjenih ali obdelanih podatkov (do znižanja ali preklica stopenj tajnosti v skladu z odobrenimi postopki).

UPORABA ZASEBNE OPREME IT ZA DELO V SLUŽBENE NAMENE SVETA

95. Uporaba zasebnih izmenljivih računalniških nosilcev, programske opreme in strojne opreme IT (npr. PC in prenosnih računalniških naprav) z zmogljivostjo shranjevanja za delo s tajnimi podatki EU ni dovoljena.

96. Računalniška strojna oprema, programska oprema in nosilci v zasebni lasti se ne smejo vnašati na območja razreda I ali razreda II, kjer se obdelujejo tajni podatki EU, brez dovoljenja vodje Varnostnega urada GSS ali ustreznega oddelka države članice ali zadevne decentralizirane agencije EU.

UPORABA POGODBENO LASTNIŠKE ALI NACIONALNE OPREME IT ZA DELO V SLUŽBENE NAMENE SVETA

97. Uporabo pogodbeno lastniške opreme IT in pogodbeno lastniške programske opreme v organizacijah pri delu v službene namene Sveta lahko dovoli vodja Varnostnega urada GSS ali oddelka države članice ali zadevne decentralizirane agencije EU. Uslužbencem GSS ali decentraliziranih agencij EU se lahko dovoli tudi uporaba opreme IT in programske opreme, ki jo je dobavila država; v takem primeru nadzor nad opremo IT prevzame ustrezni inventurno popisni oddelek GS. V vsakem primeru velja, da če se oprema IT uporablja za obdelovanje tajnih podatkov EU, se je zaradi pravilnega upoštevanja in izvajanja elementov INFOSEC, ki se nanašajo na uporabo take opreme, treba posvetovati z ustreznim SAA.

ODDELEK XII

SPOROČANJE TAJNIH PODATKOV EU TRETJIM DRŽAVAM ALI MEDNARODNIM ORGANIZACIJAM

NAČELA, KI UREJAJO SPOROČANJE TAJNIH PODATKOV EU

1. O sporočanju tajnih podatkov EU tretjim državam ali mednarodnim organizacijam odloči Svet na podlagi:

   — značaja in vsebine takih podatkov,

   — prejemnikove potrebe po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog,

   — obsega ugodnosti za EU.

   Glede sporočanja tajnih podatkov EU, ki imajo izvor v državi članici, je za pristanek treba zaprositi to državo članico.

2. Odločitve o tem se sprejemajo na podlagi posamičnih primerov v odvisnosti od:

   — zaželene ravni sodelovanja s tretjimi državami ali zadevnimi mednarodnimi organizacijami,

   — zaupanja vanje, izhajajočega iz stopnje tajnosti, ki bi jo te države ali organizacije uporabljale za zaupane jim tajne podatke EU, in od skladnosti med njihovimi veljavnimi pravili o varovanju tajnosti in tistimi, ki se uporabljajo v EU; Varnostni odbor Sveta o tem Svetu da tehnično mnenje.

3. Prejem tajnih podatkov EU s strani tretjih držav ali mednarodnih organizacij pomeni njihovo zagotovilo, da bodo te podatke uporabljale zgolj v namene, ki imajo za cilj sporočanje ali izmenjavo podatkov in da bodo zagotovile zaščito, ki jo zahteva Svet.

STOPNJE SODELOVANJA

4. Potem ko Svet sprejme odločitev, da se tajni podatki lahko sporočajo ali izmenjujejo z določeno državo ali mednarodno organizacijo, sprejme tudi odločitev o ravni mogočega sodelovanja. To je odvisno zlasti od varnostne politike in predpisov, ki jih uporablja zadevna država ali organizacija.

5. Gre za tri ravni sodelovanja:

   Stopnja 1

   Obsega sodelovanje s tretjimi državami ali mednarodnimi organizacijami, katerih varnostna politika in predpisi so zelo blizu politiki in predpisom EU.

   Stopnja 2

   Obsega sodelovanje s tretjimi državami ali mednarodnimi organizacijami, katerih varnostna politika in predpisi so razvidno različni od take politike in predpisov EU.

   Stopnja 3

   Obsega občasno sodelovanje s tretjimi državami ali mednarodnimi organizacijami, o katerih varnostni politiki in predpisih ni mogoče podati ocene.

6. Za vsako stopnjo sodelovanja so določeni predpisi o varovanju tajnosti, kjer so besedila prilagojena posameznim primerom v luči tehničnega mnenja Varnostnega odbora Sveta, za katerega bodo uporabniki zaprošeni, da ga uporabljajo pri zaščiti sporočenih jim tajnih podatkov. Ti postopki in ukrepi varovanja tajnosti so podrobno predstavljeni v Dodatkih 4, 5 in 6.

DOGOVORI

7. Potem ko Svet sprejme odločitev o trajni ali dolgoročni potrebi po izmenjavi tajnih podatkov med EU in tretjimi državami ali drugimi mednarodnimi organizacijami, z njimi oblikuje „dogovore o postopkih varovanja tajnosti za izmenjavo tajnih podatkov“, ki določajo namen sodelovanja in medsebojna pravila za zaščito izmenjanih podatkov.

8. V primeru občasnega sodelovanja na Stopnji 3, ki je že po definiciji časovno in namensko omejeno, se lahko sklene preprost memorandum o soglasju, ki določi vrsto tajnih podatkov, namenjenih za izmenjavo, in medsebojne obveznosti v zvezi s temi podatki, in ki lahko nadomesti „dogovor o postopkih za izmenjavo tajnih podatkov“ pod pogojem, da niso razvrščeni višje od RESTREINT UE.

9. Osnutke dogovorov o postopkih varovanja tajnosti ali memorandume o soglasju odobri Varnostni odbor še preden so v odločanje predloženi Svetu.

10. ONV dajo generalnemu sekretarju/visokemu predstavniku vso potrebno podporo, ki zagotavlja, da bodo sporočeni podatki uporabljeni in zaščiteni v skladu z določbami dogovorov o postopkih varovanja tajnosti ali z memorandumi o soglasju.

Dodatek 1

Seznam organov nacionalne varnosti

BELGIJA

Ministère des Affaires Étrangères, du Commerce Extérieur et de la Coopération au Développement
Direction de la sécurité — A 01
Rue des Petits Carmes, 15
B-1000 Bruxelles
Telefon: 32–2–501 85 14
Faks: 32–2–501 80 58
Teleks: 21376
Telegrafski naslov: Direction de Sécurité A01 — MINAFET

DANSKA

Politiets Efterretningstjeneste
Borups Alle 266
DK-2400 Copenhagen NV
Telefon: 45-33 14 88 88
Faks: 45-38 19 07 05

Forsvarsministeriet
Forsvarets Efterretningstjeneste
Kastellet 30
DK-2100 Copenhagen Ø
Telefon: 45-33 32 55 66
Faks: 45-33 93 13 20

NEMČIJA

Bundesministerium des Innern
Referat IS 4
Alt-Moabit 101D
D-10559 Berlin
Telefon: 49–30–39 81 15 28
Faks: 49–30–39 81 16 10

GRČIJA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Υπηρεσία Στρατιωτικών Πληροφοριών (ΥΣΠ — Β' Κλάδος)
Γραφείο Ασφάλειας
ΣΤΓ 1020- Χολαργός (Αθήνα)
Ελλαδα
Τηλέφωνα: 30–1–655 22 03 (ώρες γραφείου)
30–1–655 22 05 (εικοσιτετράωρο)
Φαξ: 30–1–642 69 40

Hellenic National Defence
General Staff (HNDGS)
Intelligence Branch/Security
(INT. BR:/SEC:)
STG 1020, Holargos - Athens
Greece
Telefon: 30–1–655 22 03 (uradne ure)
30–1–655 22 05 (24 ur)
Faks: 30–1–642 69 40

ŠPANIJA

AUTORIdad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera Nacional Radial VI, km 8 500
E-28023 Madrid
Telefon: 34–91–372 57 07
Faks: 34–91–372 58 08
E-pošta: nsa-sp@areatec.com

FRANCIJA

Secrétariat général de la Défense Nationale
Service de Sécurité de Défense (SGDN/SSD)
51 Boulevard de la Tour-Maubourg
F—75700 Pariz 07 SP
Telefon: 330-144 18 81 80
Faks: 33–0–144 18 82 00
Teleks: SEGEDEFNAT 200019
Telegrafski naslov: SEGEDEFNAT PARIS

IRSKA

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
Dublin 2
Telefon: 353–1–478 08 22
Faks: 353–1–478 14 84

ITALIJA

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Ufficio Centrale per la Sicurezza
Via della Pineta Sacchetti, 216
I-00168 Roma
Telefon: 39–06–627 47 75
Faks: 39–06–614 33 97
Teleks: 623876 AQUILA 1
Telegrafski naslov: ess: PCM-ANS-UCSI-ROMA

LUKSEMBURG

Autorité Nationale de Sécurité
Ministère d'État
Boîte Postale 2379
L-1023 Luksemburg
Telefon: 352-478 22 10 centrala
352-478 22 35 neposredno
Faks: 352-478 22 43
352-478 22 71
Teleks: 3481 SERET LU
Telegrafski naslov: MIN D'ETAT — ANS

NIZOZEMSKA

Ministerie van Binnenlandse Zaken
Postbus 20010
NL-2500 EA Den Haag
Telefon: 31–70–320 44 00
Faks: 31–70–320 07 33
Teleks: 32166 SYTH NL

Ministerie van Defensie
Militaire Inlichtingendienst (MID)
Postbus 20701
NL-2500 ES Den Haag
Telefon: 31–70–318 70 60
Faks: 31–70–318 79 51

AVSTRIJA

Bundesministerium für auswärtige Angelegenheiten
Abteilung I.9
Ballhausplatz 2
A-1014 Wien
Telefon: 43–1–531 15 34 64
Faks: 43–1–531 8 52 19

PORTUGALSKA

Presidencia do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1449-004 Lisboa
Telefon: 351–21–301 55 10
351–21–301 00 01, int. 20 45 37
Faks: 351–21–302 03 50

FINSKA

Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Ulkoasiainministeriö/Utrikesministeriet
Laivastokatu/Maringatan 22
PL/PB 176
FIN-00161 Helsinki/Helsingfors
Telefon: 358–9–13 41 53 38
Faks: 358–9–13 41 53 03

ŠVEDSKA

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Telefon: 46–8–405 54 44
Faks: 46–8–723 11 76

ZDRUŽENO KRALJESTVO

The secretary (for DIR/5)
PO Box 5656
London EC1A 1AH
Telefon: 44–20–72 70 87 51
Faks: 44–20–76 30 14 28
Telegrafski naslov: UK Delegation to Security Policy Dept FCO, z oznako (in Box 5656 for DIR/5).

Dodatek 2

Primerjava nacionalnih oznak stopenj tajnosti

Razvrstitev EU	Très secret UE/EU Top Secret	Secret UE	Confidentiel UE	Restreint UE
Razvrstitev NATO (1)				
Razvrstitev ZEU	Focal Top Secret	WEU Secret	WEU Confidential	WEU 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 (2)— Vertraulich	VS — Nur fur den Dienstgebrauch
Grčija	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Španija	Secreto	Reservado	Confidencial	Difusion Limitada
Francija	Très Secret Defense (3)	Secret Defense	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	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Združeno kraljestvo	Top Secret	Secret	Confidential	Restricted

(1) NATO: ustreznice stopnjam tajnosti NATO bodo določene ob sklenitvi Varnostnega sporazuma med Evropsko unijo in NATO.

(2) Nemčija: VS = Verschlusssache

(3) Francija: razvrstitev „Très Secret Défense“, ki se nanaša na prednostna vprašanja vlade, se lahko spremeni le z dovoljenjem predsednika vlade.

Dodatek 3

Praktični vodnik za razvrščanje

Ta vodnik je orientacijske narave in se ne sme razlagati v smislu spreminjanja temeljnih določb, ki jih določata Oddelka II in III.

Razvrstitev	Kdaj	Kdo	Oznake	Znižanje/Preklic/Uničenje	
				Kdo	Kdaj
TRÈS SECRET UE/EU TOP SECRET: Ta stopnja tajnosti se uporablja samo za podatke in gradivo, katerih razkritje nepooblaščenim osebam bi lahko povzročilo izjemno težke posledice za bistvene interese Evropske unije ali ene ali več njenih držav članic[SII(1)].	Ogrožanje premoženja pod oznako TRÈS SECRET UE/EU TOP SECRET bi lahko: — neposredno ogrozilo notranjo stabilnost EU ali ene od držav članic ali prijateljske države — povzročilo izjemno resno škodo odnosom s prijateljskimi vladami — pripeljalo neposredno do izgube življenja velikega števila ljudi — povzročilo izjemno resno škodo operativni učinkovitosti ali varnosti držav članic ali drugim silam, ki dajejo svoj prispevek, ali poteku izredno koristnih varnostnih ali obveščevalnih operacij — povzročilo hudo dolgoročno škodo gospodarstvu EU ali držav članic.	Države članice: ustrezno pooblaščene osebe (stran izvora) [SIII(4)] GSS: ustrezno pooblaščene osebe (stran izvora) [SIII(4)], GS/VP in DSG. Stran izvora določi datum ali obdobje, ko se tajnost vsebine lahko zniža ali prekliče. V nasprotnem primeru strani izvora dokumente preverjajo najpozneje na vsakih pet let, da tako zagotovijo potrebno izvorno razvrstitev dokumenta [SIII(10)].	Razvrstitev pod TRÈS SECRET UE/EU TOP SECRET se uporablja za dokumente TRÈS SECRET UE/EU TOP SECRET; kadar je primerno, se dokument opremi z obrambno oznako EVOP na mehanski način in ročno [SII(8)]. Stopnje tajnosti EU so zgoraj in spodaj na sredini strani; vsaka stran je oštevilčena. Vsak dokument je opremljen z opravilno številko in datumom; opravilna številka mora biti na vsaki strani. Če se razpošiljajo v več primerkih, je treba na prvi strani vsakega primerka navesti številko kopije in skupno število strani. Vse priloge in priloženo gradivo morajo biti navedeni v seznamu na prvi strani [SVII(1)].	Stopnjo tajnosti lahko prekliče ali zniža samo stran izvora ali GS/VP ali DSG, ki o spremembi obvestijo vse naslove, katerim so poslali ali kopirali dokument [SVIII(9)]. Dokumente stopnje TRÈS SECRET UE/EU TOP SECRET uniči Centralni arhivski urad ali podarhivski urad, ki je za njih odgovoren. Vsak uničeni dokument se vpiše na potrdilo o uničenju, ki ga podpiše uradnik, zadolžen za nadzor na ravni TRES SECRET UE/EU TOP SECRET, in uradnik, ki je priča ob uničenju in ki mora imeti varnostno potrdilo na ravni TRES SECRET UE/EU TOP SECRET. V ta namen se v vpisno knjigo zavede ustrezna zabeležka. Potrdilo o uničenju skupaj z dokumentacijo o razpošiljanju arhivski urad hrani deset let [SVII(31)].	Odvečne kopije in dokumente, ki niso več v rabi, je treba uničiti [SVII(31)]. Dokumenti TRÈS SECRET UE/EU TOP SECRET, skupaj z vsemi odpadki, ki so nastali pri pripravi zaupnih dokumentov TRÈS SECRET UE/EU TOP SECRET, kot so poškodovane kopije, delovni osnutki, natipkana sporocila in indigo papir, se uničijo pod nadzorom uradnika, preverjenega na stopnji TRÈS SECRET UE/EU TOP SECRET, z zažigom, zmletjem, razrezanjem v pramene ali z drugačno spremembo v neprepoznavno in nesestavljivo obliko [SVII(31)].

Razvrstitev	Kdaj	Kdo	Oznake	Znižanje/Preklic/Uničenje	
				Kdo	Kdaj
SECRET: Ta stopnja tajnosti se uporablja samo za podatke in gradivo katerih in/ali katerega razkritje nepooblaščenim osebam bi lahko resno škodovalo bistvenim interesom Evropske unije ali ene ali več njenih držav članic [SII(2)].	Premoženja pod oznako SECRET UE bi lahko: — povzročilo mednarodne napetosti — resno škodovalo odnosom s prijateljskimi državami — neposredno ogrozilo življenje ali resno vplivalo na javni red ali varnost posameznikov ali svobodo — povzročilo resno škodo operativni učinkovitosti ali varnosti držav članic ali drugim silam, ki dajejo svoj prispevek ali poteku zelo koristnih varnostnih ali obveščevalnih operacij — povzročilo občutno materialno škodo finančnim, monetarnim, ekonomskim in trgovskim interesom EU ali ene od držav članic.	Države članice ustrezno pooblaščene osebe (stran izvora)[SIII(2)]; Decentralizirane agencije GSS in EU: ustrezno pooblaščene osebe (stran izvora) [SIII(2)]; generalni direktorji, GS/VP in DSG. Stran izvora določi datum ali obdobje, ko se tajnost vsebine lahko zniža ali prekliče. V nasprotnem primeru strani izvora dokumente preverjajo najpozneje na vsakih pet let, da tako zagotovijo potrebno izvorno razvrstitev dokumenta [SVII(1)].	Razvrstitev SECRET UE se uporablja za dokumente SECRET UE; kadar je primerno, se dokument opremi z obrambno oznako EVOP na mehanski način in ročno [SIII(8)]. Stopnje tajnosti EU so zgoraj in spodaj na sredini strani; vsaka stran je oštevilčena. Vsak dokument je opremljen z opravilno številko in datumom; opravilna številka mora biti na vsaki strani. Če se razpošiljajo v več primerkih, je treba na prvi strani vsakega primerka navesti številko kopije in skupno število strani. Vse priloge in priloženo gradivo morajo biti navedeni v seznamu na prvi strani [SVII(1)].	Stopnjo tajnosti lahko prekliče in zniža samo stran izvora ali GS/VP ali DSG, ki o spremembi obvestijo vse naslove, katerim so poslali ali kopirali dokument [SVII(9)]. Dokumente SECRET UE uniči arhivski urad, ki je zanje odgovoren pod nadzorom varnostno preverjene osebe. Dokumenti SECRET UE, ki so uničeni, se vpišejo na podpisana potrdila o uničenju, ki jih zadrži arhivski urad skupaj z dokumentacijo o razpošiljanju za najmanj tri leta [SVII(32)].	Odvečne kopije in dokumente, ki niso več v rabi, je treba uničiti [SVII(31)]. Dokumente SECRET UE skupaj z vsemi odpadki, ki so nastali pri pripravi zaupnih dokumentov SECRET UE kot so poškodovane kopije, delovni osnutki, natipkana sporočila in indigo papir se uničijo z zažigom, zmletjem, razrezanjem v pramene ali z drugačno spremembo v neprepoznavno ali nesestavljivo obliko [SVII(31), (32)].

Razvrstitev	Kdaj	Kdo	Oznake	Znižanje/Preklic/Uničenje	
				Kdo	Kdaj
CONFIDENTIEL UE: Ta stopnja tajnosti se uporablja samo za podatke in gradivo, katerih razkritje nepooblaščenim osebam bi lahko škodovalo bistvenim interesom Evropske unije ali ene ali več njenih držav članic [SII(3)].	Ogrožanje premoženja pod oznako CONFIDENTIEL UE bi lahko: — bistveno škodovalo diplomatskim odnosom, kar bi povzročilo formalne proteste ali druge sankcije — vplivalo na osebno varnost ali svobodo — povzročilo škodo operativni učinkovitosti ali varnosti držav članic ali drugim silam, ki dajejo svoj prispevek, ali poteku koristnih varnostnih ali obveščevalnih operacij — občutno načelo finančno sposobnost za preživetje večjih organizacij — oviralo preiskave ali olajšalo izvajanje resnega kriminala — v veliki meri omogočilo dejavnosti proti finančnim, monetarnim, ekonomskim in trgovskim interesom EU ali držav članic — resno oviralo razvoj ali delovanje poglavitnih politik EU — zatrlo ali drugače občutno načelo pomembne dejavnosti EU	Države članice ustrezno pooblaščene osebe (stran izvora) [SIII(2)]; Decentralizirane agencije GSS in EU: ustrezno pooblaščene osebe (stran izvora) [SIII(2)], generalni direktorji, GS/VP in DSG. Stran izvora določi datum ali obdobje, ko se tajnost vsebine lahko zniža ali prekliče. V nasprotnem primeru strani izvora dokumente preverjajo najpozneje na vsakih pet let, da tako zagotovijo potrebno izvorno razvrstitev dokumenta [SIII(10)].	Razvrstitev pod CONFIDENTIEL UE se uporablja za dokumente CONFIDENTIEL UE; kadar je primerno, se dokument opremi z obrambno oznako EVOP na mehanski način in ročno ali s tiskom na predžigosan, registrirni papir, [SII(8)]. Stopnje tajnosti EU so zgoraj in spodaj na sredini vsake strani; vsaka stran je oštevilčena. Vsak dokument je opremljen z opravilno številko in datumom. Vse priloge in priložena gradiva se navedejo na prvi strani [SVII(1)].	Stopnjo tajnosti lahko prekliče in zniža samo stran izvora ali GS/VP ali DSG, ki o spremembi obvestijo vse naslove, katerim so poslali ali kopirali dokument [SVII(31)]. Dokumente CONFIDENTIEL UE uniči arhivski urad, ki je zanje odgovoren, pod nadzorom varnostno preverjene osebe, v skladu z nacionalnimi predpisi in, v primeru decentraliziranih agencij GSS ali EU, v skladu z navodili GS/VP ali DSG [SVII(33)].	Odvečne kopije in dokumente, ki niso več v rabi, je treba uničiti [SVII(31)]. Dokumente CONFIDENTIEL UE skupaj z vsemi odpadki, ki so nastali pri pripravi zaupnih dokumentov CONFIDENTIEL UE kot so poškodovane kopije, delovni osnutki, natipkana sporočila in indigo papir se uničijo z zažigom, zmletjem, razrezanjem v pramene ali z drugačno spremembo v neprepoznavno ali nesestavljivo obliko [SVII(31), (33)]

Razvrstitev	Kdaj	Kdo	Oznake	Znižanje/Preklic/Uničenje	
				Kdo	Kdaj
RESTREINT UE: Ta stopnja tajnosti se uporablja za podatke in gradivo katerih in/ali katerega razkritje nepooblaščenim osebam bi lahko bilo neugodno za interese EU ali ene ali več njenih držav članic [SII(4)].	Ogrožanje premoženja pod oznako RESTREINT UE bi lahko: — negativno vplivalo na diplomatske odnose — povzročilo stiske posameznikom — otežilo vzdrževanje operativne učinkovitosti ali varnosti držav članic ali drugih sil, ki dajejo svoj prispevek — povzročilo finančne izgube ali omogočilo neprimerno dobit ali ugodnosti posameznikom ali družbam — škodovalo ustreznim podjetjem pri vzdrževanju zaupnosti podatkov, ki jih dajo tretje strani — povzročilo kršitve zakonskih omejitev o razkritju informacij — vplivalo na preiskave ali olajšalo izvajanje kriminala — prikrajšalo EU ali države članice v trgovskih ali političnih pogajanjih z ostalimi — oviralo učinkovit razvoj ali delovanje politik EU — izpodkopavalo pravilno upravljanje EU in njenih dejavnosti.	Države članice: ustrezno pooblaščene osebe (stran izvora) [SIII(2)]; Decentralizirane agencije GSS in EU: ustrezno pooblaščene osebe (stran izvora) [SIII(2)], generalni direktorji, GS/VP in DSG. Stran izvora določi datum ali obdobje, ko se tajnost vsebine lahko zniža ali prekliče. V nasprotnem primeru strani izvora dokumente preverjajo najpozneje na vsakih pet let, da tako zagotovijo potrebno izvorno razvrstitev dokumenta [SIII(10)].	Razvrstitev pod RESTREINT UE se uporablja za dokumente RESTREINT UE; kadar je primerno, se dokument opremi z obrambno oznako EVOP na mehanski način ali z elektronskimi sredstvi [SII(8)]. Stopnje tajnosti EU so zgoraj in spodaj na sredini strani; vsaka stran je oštevilčena. Vsak dokument je opremljen z opravilno številko in datumom [SVII(1)].	Stopnjo tajnosti lahko prekliče in zniža samo stran izvora ali GS/VP ali DSG, ki o spremembi obvestijo vse naslove, katerim so poslali ali kopirali dokument [SIII(9)]. Dokumente RESTREINT UE uniči arhivski urad, ki je zanje odgovoren, v skladu z nacionalnimi predpisi in, v primeru decentraliziranih agencij GSS ali EU, v skladu z navodili GS/VP ali DSG [SVII(34)].	Odvečne kopije in dokumente, ki niso več v rabi, je treba uničiti [SVII(31)].

Dodatek 4

Smernice za sporočanje tajnih podatkov EU tretjim državam ali mednarodnim organizacijam.

Sodelovanje na stopnji 1

POSTOPKI

1. Za sporočanje tajnih podatkov EU državam, ki niso podpisnice Pogodbe o Evropski uniji ali drugim mednarodnim organizacijam, katerih varnostna politika in predpisi so primerljivi s tistimi v EU, je pristojen Svet.

2. Svet odločitev o sporočanju tajnih podatkov lahko prenese na drugega. V tem prenosu navede vrsto podatkov, ki se lahko sporočijo, in stopnjo razvrščenosti, ki običajno ne sme biti višja od CONFIDENTIEL UE.

3. Ob upoštevanju sklenitve varnostnega dogovora varnostni organi zadevnih držav ali mednarodnih organizacij prošnje za sporočanje tajnih podatkov EU naslovijo na generalnega sekretarja/visokega predstavnika in navedejo namene, v katere bodo uporabili tako sporočene tajne podatke ter vrsto želenih tajnih podatkov.

   Prošnjo za sporočanje lahko naredijo tudi država članica ali decentralizirane agencije EU, ki so mnenja, da je sporočanje tajnih podatkov EU zaželeno; v njih navedejo cilje in koristi takega pošiljanja za EU, skupaj z vrsto in razvrščenostjo želenih tajnih podatkov.

4. Prošnjo obravnava GSS, ki:

   — pridobi mnenje države članice ali po potrebi decentralizirane agencije EU, pri kateri imajo podatki, ki se sporočajo, svoj izvor,

   — vzpostavi potrebne stike z varnostnimi organi držav uporabnic ali mednarodnih organizacij zaradi preverjanja, če so njihova varnostna politika in predpisi taki, ki jamčijo, da bodo tajni podatki, ki se sporočajo, zaščiteni v skladu s temi predpisi o varovanju tajnosti,

   — pridobi tehnična mnenja nacionalnih varnostnih organov držav članic glede zaupanja, ki ga lahko vložijo v države uporabnice ali mednarodne organe.

5. GSS prošnjo skupaj s priporočilom Varnostnega urada v odločanje pošlje Svetu.

PREDPISI O VAROVANJU TAJNOSTI, KI JIH MORAJO SPOŠTOVATI UPORABNIKI

6. Generalni sekretar/visoki predstavnik uradno obvesti države uporabnice ali mednarodne organizacije o odločitvi Sveta glede dovoljenja za sporočanje tajnih podatkov EU in jim pošlje toliko kopij teh predpisov o varovanju tajnosti, kolikor meni, da je potrebno. Če je prošnjo naredila država članica, ta država uporabnika uradno obvesti o dovoljenju za sporočanje.

   Odločitev o sporočanju tajnih podatkov postane veljavna samo takrat, ko uporabnice pisno zagotovijo, da bodo:

   — podatke uporabljale samo v dogovorjene namene,

   — zaščitile podatke v skladu s temi predpisi o varovanju tajnosti in zlasti s posebnimi določbami, navedenimi v nadaljevanju.

7. *Osebje*

   (a) Število uslužbencev, ki imajo dostop do tajnih podatkov EU, je na podlagi potrebe po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog strogo omejeno na osebe, za katere se tak dostop zahteva zaradi izpolnjevanja delovnih nalog.

(b) Vsi uslužbenci ali državljani, ki so pooblaščeni za dostop do podatkov na stopnji CONFIDENTIEL UE ali višje, morajo imeti varnostno potrdilo za ustrezno stopnjo ali enakovredno varnostno pooblastilo, ki ju izda vlada njihove države.

8. *Prenos dokumentov*

(a) Praktični postopki za prenos dokumentov se določijo z dogovorom na podlagi določb Oddelka VII Varnostnih predpisov Sveta. V njih se določijo zlasti arhivski uradi, na katere je treba nasloviti tajne podatke EU.

(b) Če tajni podatki, katerih sporočanje dovoli Svet, obsegajo podatke stopnje TRÈS SECRET UE/EU TOP SECRET, država uporabnica ali mednarodna organizacija ustanovi centralni arhivski urad EU in, če je potrebno, podarhivske urade EU. Omenjeni arhivski uradi se urejajo po določbah Oddelka VIII teh predpisov.

9. *Vpis v evidenco*

Takoj ko arhivski urad prejme tajni dokument na stopnji CONFIDENTIEL UE ali višje, tega vpiše v posebni evidenčni vpisnik organizacije po stolpcih za datum sprejema, podatke o dokumentu (datum, opravilna številka in številka kopije), razvrstitev, naslov, ime ali delovni naslov naslovnika, datum povratnice in datum vrnitve dokumenta organu izvora v EU ali datum uničenja.

10. *Uničenje*

(a) Tajni dokumenti EU se uničijo v skladu z navodili, določenimi v Oddelku VI teh predpisov o varovanju tajnosti. Kopije potrdil o uničenju tajnih dokumentov na stopnji SECRET UE in TRÈS SECRET UE/EU TOP SECRET se pošljejo arhivskemu uradu EU kot pošiljatelju dokumentov.

(b) Tajni dokumenti EU se vključijo v načrte za uničenje v nujnih primerih, ki jih uporabniki obravnavajo kot tajne dokumente.

11. *Zaščita dokumentov*

Treba je sprejeti vse ukrepe za preprečitev dostopa nepooblaščenim osebam do tajnih podatkov EU.

12. *Kopije, prevodi in izvlečki*

Tajnih dokumentov na stopnji CONFIDENTIEL UE ali SECRET UE ni dovoljeno fotokopirati ali prevajati ali delati izvlečkov iz njih brez dovoljenja vodje zadevne varnostne organizacije, ki kopije, prevode ali izvlečke vpiše v vpisnik, jih preveri in po potrebi opremi z žigom.

Reprodukcijo ali prevajanje tajnih dokumentov stopnje TRÈS SECRET UE/EU TOP SECRET lahko dovoli samo organ izvora, ki določi dovoljeno število kopij; če organa izvora ni mogoče določiti, se prošnja napoti na Varnostni urad GSS.

13. *Kršitve varnosti*

Kadar pride do kršitve varnosti v zvezi s tajnimi dokumenti EU ali do suma kršitve, je treba ob upoštevanju sklenitve varnostnega dogovora nemudoma ukrepati na naslednji način:

(a) izpeljati preiskavo zaradi ugotovitve okoliščin kršitve varnosti;

(b) uradno obvestiti Varnostni urad GSS, nacionalni organ za varnost in organ izvora ali jasno razvidno navesti, da slednji organ ni bil obveščen, če je temu res bilo tako;

(c) ukrepati z namenom na minimum zmanjšati posledice kršitve varnosti;

(d) ponovno preučiti ukrepe in jih izvajati z namenom preprečiti ponovitev kršitve;

(e) izvajati vse ukrepe, ki jih priporoči Varnostni urad GSS, z namenom preprečiti ponovitev.

14. *Inšpekcije*

Varnostnemu uradu GSC se, po dogovoru z zadevnimi državami ali mednarodnimi organizacijami, dovoli, da opravi oceno učinkovitosti ukrepov za varovanje sporočenih tajnih podatkov EU.

15. *Poročanje*

Ob upoštevanju sklenitve varnostnega dogovora mora država ali mednarodna organizacija, za čas ko je v posesti tajnih podatkov EU, predložiti letno poročilo do datuma, ko se izda dovoljenje za sporočanje tajnih podatkov, v katerem potrjuje, da so bili ti predpisi o varovanju tajnosti ustrezno spoštovani.

Dodatek 5

Smernice za sporočanje tajnih podatkov EU tretjim državam ali mednarodnim organizacijam.

Sodelovanje na stopnji 2

POSTOPKI

1. Sporočanje tajnih podatkov EU tretjim državam ali mednarodnim organizacijam, katerih varnostna politika in predpisi se opazno razlikujejo od teh pri EU, je v pristojnosti Sveta. Načeloma je omejeno na podatke, razvrščene do stopnje SECRET UE in vključno z njo; ne obsega podatkov na nacionalni ravni, ki so posebej rezervirani za države članice in kategorije tajnih podatkov EU, zaščitenih s posebnimi oznakami.

2. Svet lahko svojo odločitev delegira; pri tem ob upoštevanju omejitev iz odstavka 1 navede vrsto podatkov, ki se lahko sporočajo in njihovo stopnjo razvrščenosti, ki ne sme presegati stopnje RESTREINT UE.

3. Ob upoštevanju sklenitve varnostnega dogovora varnostni organi zadevnih držav ali mednarodnih organizacij prošnje za sporočanje tajnih podatkov EU naslovijo na generalnega sekretarja/visokega predstavnika in pri tem navedejo namene, v katere bodo uporabili tako sporočene tajne podatke, ter vrsto in stopnjo razvrstitve tajnih podatkov.

   Prošnje za sporočanje lahko sestavijo tudi države članice ali decentralizirane agencije EU, ki so mnenja, da je sporočanje tajnih podatkov EU zaželeno; v njih navedejo cilje in koristi takega pošiljanja za EU, skupaj z vrsto in stopnjo razvrščenosti tajnih podatkov.

4. Prošnjo obravnava GSS, ki:

   — pridobi mnenje države članice ali po potrebi decentralizirane agencije EU, pri kateri imajo podatki, ki se sporočajo, svoj izvor,

   — vzpostavi predhodne stike z varnostnimi organi držav uporabnic ali mednarodnih organizacij, zato da pridobi podatke o njihovi varnostni politiki in predpisih in zlasti zaradi izdelave primerjalne tabele o razvrščanju, ki velja v EU in v državi članici ali zadevni organizaciji,

   — skliče sestanek Varnostnega odbora Sveta ali, če je potrebno, s pisnim postopkom opravi poizvedbo pri nacionalnih varnostnih organih držav članic zaradi pridobitve tehničnega menja Varnostnega odbora.

5. Tehnično mnenje Varnostnega odbora Sveta se nanaša na:

   — zaupanje do držav uporabnic ali mednarodnih organizacij zaradi ocenitve varnostnega tveganja za EU ali njene države članice,

   — ocenitev sposobnosti uporabnikov za varovanje tajnih podatkov, ki jih sporoča EU,

   — predloge glede praktičnih postopkov za ravnanje s tajnimi podatki EU (na primer posredovanje okleščenih verzij besedil) in poslanimi dokumenti (ohranitev ali brisanje oznak EU za tajnost, posebnih oznak, itd.),

   — znižanje ali preklic stopenj tajnosti s strani organa izvora pred sporočanjem podatkov državi uporabnici ali mednarodnim organizacijam ([1]).

([1]) To ima za posledico, da organ izvora uporabi postopek iz odstavka 9 Oddelka III za vse kopije, ki krožijo znotraj EU

6. Generalni sekretar/visoki predstavnik Svetu v odločanje pošlje prošnjo in tehnično mnenje Varnostnega odbora Sveta, ki ga pridobi Varnostni urad GSS.

PREDPISI O VAROVANJU TAJNOSTI, KI JIH MORAJO SPOŠTOVATI UPORABNIKI

7. O odločitvi Sveta v zvezi z dovoljenjem za pošiljanje tajnih podatkov EU države uporabnice ali mednarodne organizacije seznani generalni sekretar/visoki predstavnik skupaj s primerjalno tabelo o razvrščanju, ki velja v EU in v zadevnih državah ali organizacijah. Če je prošnjo vložila država članica, ta država uporabnika uradno obvesti o dovoljenju za sporočanje.

Odločitev o sporočanju tajnih podatkov postane veljavna samo takrat, ko uporabnice pisno zagotovijo, da bodo:

— podatke uporabljale samo v dogovorjene namene,

— podatke varovale v skladu s predpisi, ki jih določi Svet.

8. Če Svet po pridobitvi tehničnega mnenja Varnostnega odbora Sveta ne določi posebnega postopka za delo s tajnimi dokumenti EU (izbris navedbe razvrstitve EU, posebne oznake itd.), se vzpostavijo varovalna pravila, navedena v nadaljevanju:

V takem primeru se pravila prilagodijo.

9. *Osebje*

(a) Število uradnikov, ki imajo dostop do tajnih podatkov EU, mora biti na podlagi potrebe po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog strogo omejeno na osebe, ki tak dostop potrebujejo zaradi izpolnjevanja delovnih nalog.

(b) Vsi uradniki ali državljani z dovoljenim dostopom do tajnih podatkov, ki jih sporoča EU, morajo imeti nacionalno varnostno potrdilo ali pooblastilo za dostop, ki morata, če gre za tajne podatke na nacionalni ravni, biti na primerni ravni, enakovredni EU, kakor je to določeno v primerjalni tabeli.

(c) Nacionalna varnostna potrdila ali pooblastila se pošljejo v vednost generalnemu sekretarju/visokemu predstavniku.

10. *Prenos dokumentov*

(a) O praktičnih postopkih za prenos dokumentov se dogovorijo Varnostni urad GSS in varnostni organi držav prejemnic ali mednarodnih organizacij na podlagi pravil, določenih v Oddelku VII teh predpisov o varovanju tajnosti. V pravilih morajo biti navedeni zlasti točni naslovi, na katere se dokumenti pošiljajo, skupaj s kurirskimi ali poštnimi službami, ki opravljajo prenos tajnih podatkov EU.

(b) Dokumenti na stopnji CONFIDENTIEL UE in višje se prenašajo v dvojnih ovojnicah. Notranja ovojnica nosi oznako „UE“ skupaj s stopnjo razvrstitve dokumenta. Vsakemu tajnemu dokumentu je priložen obrazec o prejemu (sprejemnica). Obrazec o prejemu, ki sam po sebi ni razvrščen po tajnosti, vsebuje samo podatke o dokumentu (opravilna številka, datum, številka kopije) in jeziku dokumenta, ne pa naslova.

(c) Notranja ovojnica je položena v zunanjo ovojnico, ki je označena z odpremno številko zaradi prejema dokumenta. Zunanja ovojnica je brez označene razvrstitve po tajnosti.

(d) Kurirju se vedno izda potrdilo o prejemu z označeno odpremno številko pošiljke.

11. *Evidentiranje ob prejemu*

ONV države naslovnice ali njegov ekvivalent v državi, ki v imenu vlade sprejema tajne podatke, ki jih pošilja EU ali varnostni urad mednarodne organizacije kot prejemnice, odpre posebni vpisnik, v katerega ob prejemu vpiše tajne podatke EU. Vpisnik vsebuje stolpce z datumom prejema, podatki o dokumentu (datum, opravilna številka in številka kopije), razvrstitvijo, naslovom, imenom ali delovnim naslovom naslovnika, datumom povratnice in datumom vrnitve dokumenta EU ali njegovega uničenja.

12. *Vračanje dokumentov*

Če prejemnik tajni dokument vrne Svetu ali državi članici, ki ga je poslala, se pri tem ravna po postopku iz odstavka 10.

13. *Varovanje*

(a) Kadar se dokumenti ne uporabljajo, so shranjeni v varnostnem vsebniku, ki je bil odobren za varovanje tajnega nacionalnega gradiva na isti stopnji tajnosti. Vsebnik nima nikakršnih oznak o hranjeni vsebini, ki je dostopna samo osebam, pooblaščenim za delo s tajnimi podatki EU. Pri uporabi ključavnic na kombinacijo, je ta znana samo tistim uradnikom v državi ali organizaciji, ki so pooblaščeni za dostop do v vsebniku shranjenih tajnih podatkov EU; kombinacija se spreminja na šest mesecev ali prej, t.j. ob zamenjavi uradnika, ob odvzemu varnostnega potrdila uradniku, ki pozna kombinacijo, ali če obstaja tveganje glede ogrožanja.

(b) Tajne dokumente EU iz varnostnega vsebnika lahko vzamejo samo uradniki z varnostnim potrdilom za dostop do tajnih dokumentov EU in s potrebo po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog. Odgovorni so za varno hrambo teh dokumentov toliko časa, dokler se ti nahajajo v njihovi posesti, in zlasti za zagotavljanje, da nobena nepooblaščena oseba ne dobi dostopa do dokumentov. Zagotavljajo tudi, da so dokumenti po končani uporabi in izven delovnega časa shranjeni v varnostnem vsebniku.

(c) Fotokopiranje ali delanje izvlečkov iz dokumentov na stopnji CONFIDENTIEL UE ali višje ni dovoljeno brez dovoljenja Varnostnega urada GSS.

(d) Postopek za hitro in popolno uničenje dokumentov v nujnih primerih je treba določiti in potrditi skupaj z Varnostnim uradom GSS.

14. *Fizično varovanje tajnosti*

(a) Izven uporabe morajo biti varnostni vsebniki, ki se uporabljajo za shranjevanje tajnih dokumentov EU, ves čas zaklenjeni.

(b) Kadar mora v prostor, v katerem so varnostni vsebniki, vstopiti in tam delati vzdrževalno ali čistilno osebje, tega ves čas spremlja član varnostne službe države ali mednarodne organizacije ali uradnik s posebej določeno odgovornostjo za nadzor varnosti prostora.

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

15. *Kršitve varnosti*

Kadar v zvezi s tajnimi dokumenti EU pride do suma ali dejanske kršitve varnosti, je treba nemudoma:

(a) poslati poročilo Varnostnemu uradu GSS ali nacionalnemu varnostnemu organu države članice, ki je dala pobudo za pošiljanje dokumentov (s kopijo Varnostnemu uradu GSS);

(b) izpeljati preiskavo s predložitvijo izčrpnega poročila varnostnemu organu ob koncu preiskave (glej (a) zgoraj). Temu sledi sprejem zahtevanih ukrepov za popravo stanja.

16. *Inšpekcije*

Varnostnemu uradu GSS se po dogovoru z zadevnimi državami ali mednarodnimi organizacijami dovoli, da opravi oceno učinkovitosti ukrepov za varovanje sporočenih tajnih podatkov EU.

17. *Poročanje*

Za čas, ko ima država ali mednarodna organizacija v posesti tajne podatke EU, mora predložiti letno poročilo do datuma, ko se izda dovoljenje za sporočanje tajnih podatkov, v katerem potrjuje, da so bili ti predpisi o varovanju tajnosti ustrezno spoštovani.

Dodatek 6

Smernice za sporočanje tajnih podatkov EU tretjim državam ali mednarodnim organizacijam.

Sodelovanje na stopnji 3

POSTOPKI

1. Občasno se Svet lahko odloči za sodelovanje v nekaterih posebnih okoliščinah z državami ali organizacijami, ki ne morejo dati ustreznih zagotovil, kot jih zahtevajo ti predpisi o varovanju tajnosti, kjer pa utegne biti zaradi sodelovanja potrebno sporočanje tajnih podatkov EU. Iz takšnega sporočanja so izvzeti nacionalni podatki, ki so posebej rezervirani za države članice.

2. V takih posebnih okoliščinah prošnje za sodelovanje z EU, ki jih vložijo tretje države ali mednarodne organizacije ali jih predlagajo države članice ali, kadar je to primerno, decentralizirane agencije EU, najprej vsebinsko preuči Svet, ki mora po potrebi pridobiti mnenje države članice ali decentralizirane agencije, pri kateri imajo podatki izvor. Svet presodi o priporočljivosti sporočanja tajnih podatkov, oceni potrebo po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog za uporabnika in sprejme odločitev o vrsti tajnih podatkov, ki se lahko pošljejo.

3. Če Svet na sporočanje pristane, je generalni sekretar/visoki predstavnik odgovoren za sklic Varnostnega odbora Sveta ali za poizvedbo pri nacionalnih varnostnih organih držav članic, če je primerno, po pisni poti, zaradi pridobitve tehničnega mnenja Varnostnega odbora.

4. Tehnično mnenje Varnostnega odbora Sveta se nanaša na naslednje:

   (a) oceno varnostnega tveganja za EU ali države članice;

   (b) stopnjo tajnosti podatkov, ki se lahko sporočajo glede na njihovo vrsto, kadar je tako primerno;

   (c) znižanje ali preklic stopenj tajnosti s strani organa izvora pred sporočanjem zadevnim državam ali mednarodnim organizacijam ([1]);

   (d) postopke za delo z dokumenti, ki naj bi se sporočali (glej odstavek 5 spodaj);

   (e) možne načine pošiljanja (uporaba javnih poštnih služb, javni ali varovani sistemi telekomunikacij, diplomatska pošta, varnostno preverjeni kurirji, itd.).

5. Dokumenti, ki se sporočajo državam ali organizacijam v okviru tega dodatka se načeloma pripravijo brez sklicevanja na vir ali razvrstitev tajnosti EU. Varnostni odbor Sveta lahko priporoči:

   — uporabo posebne oznake ali kodiranega imena,

   — uporabo značilnega sistema razvrstitev po stopnji tajnosti, ki občutljivost podatkov povezuje z ukrepi nadzora, ki se zahtevajo pri načinih prenosa dokumentov s strani uporabnikov (glej primere iz odstavka 14).

6. Varnostni urad GSS Svetu predloži tehnično mnenje Varnostnega odbora in, kadar je to potrebno, priloži predlagane prenose pooblastil, ki so potrebni zaradi izvedbe naloge, zlasti v nujnih primerih.

7. Potem ko je Svet odobril sporočanje tajnih podatkov EU in praktične postopke za izvajanje, Varnostni urad GSS zaradi lažjega izvajanja ukrepov varovanja tajnosti vzpostavi potrebne stike z varnostnim organom zadevne države ali organizacije.

([1]) To ima za posledico, da organ izvora uporabi postopek iz odstavka 9 Oddelka III za vse kopije, ki krožijo znotraj EU.

8. Kot referenčno podlago Varnostni urad GSS vsem državam članicam in, kadar je tako primerno, zadevnim decentraliziranim agencijam EU v kroženje pošlje pregled, v katerem so povzete vrste in stopnje tajnosti podatkov ter seznam organizacij in držav, katerim se te lahko sporočajo glede na odločitev Sveta.

9. ONV držav članic, ki sporočajo podatke, ali Varnostni urad GSS sprejmejo vse potrebne ukrepe za lažjo ocenitev posledične škode in morebitno revizijo postopkov.

10. Ob vsakršni spremembi pogojev sodelovanja se je treba obrniti na Svet.

PREDPISI O VAROVANJU TAJNOSTI, KI JIH MORAJO SPOŠTOVATI UPORABNIKI

11. Odločitev Sveta glede dovoljenja za sporočanje tajnih podatkov EU državam uporabnicam ali mednarodnim organizacijam v vednost sporoči generalni sekretar/visoki predstavnik skupaj s podrobnimi pravili o varovanju, ki jih predlaga Varnostni odbor Sveta in ki jih potrdi Svet. Če je prošnjo podala država članica, ta država uporabnika uradno obvesti o dovoljenju za sporočanje.

Odločitev postane veljavna takrat, ko uporabnice pisno zagotovijo, da bodo:

— podatke uporabljale zgolj v namene sodelovanja, za katerega se je odločil Svet,

— podatke varovale, tako kot to zahteva Svet.

12. *Prenos dokumentov*

(a) O praktičnih postopkih za prenos dokumentov se dogovorijo Varnostni urad GSS in varnostni organi držav prejemnic ali mednarodnih organizacij. Zlasti morajo določiti točne naslove, na katere se pošiljajo dokumenti.

(b) Dokumenti na stopnji CONFIDENTIEL UE in višje, se pošiljajo v dvojnih ovojnicah. Na notranji ovojnici je poseben žig ali določeno kodirano ime ter navedena posebne razvrstitev, ki je bila odobrena za dokument. Vsakemu tajnemu dokumentu je priložen obrazec o prejemu. Obrazec o prejemu, ki sam ni varnostno razvrščen, vsebuje samo podatke o dokumentu (opravilna številka, datum, številka kopije) in jeziku dokumenta, ne pa naslova.

(c) Notranja ovojnica je položena v zunanjo ovojnico, ki je označena z odpremno številko za namene prejema. Zunanja ovojnica nima označene razvrstitve po stopnji tajnosti.

(d) Kurirjem se vedno izroči potrdilo o prejemu z navedeno odpremno številko pošiljke.

13. *Evidentiranje ob prejemu*

ONV države naslovnice ali njegov ekvivalent v državi, ki v imenu vlade sprejema tajne podatke, ki jih pošilja EU ali varnostni urad mednarodne organizacije kot prejemnice, odpre posebni vpisnik, v katerega ob prejemu vpiše tajne podatke EU. Vpisnik vsebuje stolpce za datum prejema, podatke o dokumentu (datum, opravilno številko in številko kopije), razvrstitev, naslov, ime ali delovni naslov naslovnika, datum povratnice in datum povratnice dokumenta EU ter datum njegovega uničenja.

14. *Uporaba in zaščita izmenjanih tajnih podatkov*

(a) Podatke na stopnji SECRET UE obdelujejo posebej določeni uslužbenci, ki so pooblaščeni za dostop do tako razvrščenih podatkov. Hranijo se v kakovostnih varnostnih omarah, ki jih lahko odpirajo samo osebe, pooblaščene za dostop do podatkov, ki se v njih nahajajo. Območja, na katerih so varnostne omare, so pod stalnim nadzorom; vzpostavi se sistem preverjanja, ki zagotavlja, da imajo vstop do njih samo ustrezno pooblaščene osebe. Podatki na stopnji SECRET UE se pošiljajo z diplomatsko pošto, varovano poštno službo in z varovanimi komunikacijami. Dokument na stopnji SECRET UE se lahko kopira samo ob pismenem pristanku organa izvora. Vse kopije se vpišejo v evidenco in so pod nadzorom. Za vsa ravnanja v zvezi z dokumenti SECRET UE se izdajo ustrezna potrdila.

(b) Podatke na stopnji CONFIDENTIEL UE obdelujejo ustrezno določeni uslužbenci, ki imajo pravico biti obveščeni o zadevnem vprašanju. Dokumenti se hranijo v zaklenjenih varnostnih omarah na območjih pod nadzorom.

Podatki na stopnji CONFIDENTIEL UE se pošiljajo z diplomatsko pošto, vojaško poštno službo in z varovanimi komunikacijami. Kopije lahko naredi prejemnik, njihovo število in razpošiljanje se vpiše v posebne vpisnike.

(c) Podatki na stopnji RESTREINT UE se obdelujejo v prostorih, kamor nepooblaščene osebe nimajo vstopa, in se hranijo v zaklenjenih vsebnikih. Dokumenti se lahko pošiljajo z javno poštno službo v dvojni ovojnici pod oznako priporočeno in, v nujnih primerih med operacijami, z nevarovanimi javnimi telekomunikacijskimi sistemi. Naslovniki lahko naredijo kopije.

(d) Netajni podatki ne zahtevajo posebnih varovalnih ukrepov in se lahko sporočajo po pošti in javnih telekomunikacijskih sistemih. Naslovniki lahko naredijo kopije.

15. *Uničenje*

Dokumente, po katerih ni več potrebe, je treba uničiti. Za dokumente na stopnji RESTREINT UE in CONFIDENTIEL UE se v posebne vpisnike vpiše ustrezna zabeležka. Za dokumente na stopnji SECRET UE se izdajo potrdila o uničenju, ki jih podpišeta dve osebi kot priči ob uničenju.

16. *Kršitve varovanja tajnosti*

Če pride do ogrožanja podatkov na stopnjah CONFIDENTIEL UE ali SECRET UE ali če se pojavi sum o ogrožanju, ONV zadevne države ali vodja, zadolžen za varnost v zadevni organizaciji, uvede preiskavo o okoliščinah ogrožanja. Če preiskava privede do potrditve ogrožanja, se o tem obvesti organ izvora podatkov. Sprejmejo se ustrezni koraki za odpravo neustreznih postopkov ali metod hranjenja, če so ti vzrok ogrožanja. Generalni sekretar Sveta/visoki predstavnik ali ONV države članice, ki je sporočila ogrožani podatek, lahko uporabnika zaprosi za podrobnosti v zvezi s preiskavo.