II

*(Nezakonodajni akti)*

# SKLEPI

## SKLEP SVETA

## z dne 31. marca 2011

## o varnostnih predpisih za varovanje tajnih podatkov EU

(2011/292/EU)

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o delovanju Evropske unije, zlasti člena 240(3) Pogodbe,

ob upoštevanju Sklepa Sveta 2009/937/EU z dne 1. decembra 2009 o sprejetju poslovnika Sveta ([1]), zlasti člena 24 Sklepa,

ob upoštevanju naslednjega:

(1) Za razvoj dejavnosti Sveta na vseh področjih, na katerih je potrebno delo s tajnimi podatki, je primerno vzpostaviti celovit varnostni sistem za varovanje tajnih podatkov, ki bo vključeval Svet, njegov generalni sekretariat in države članice.

(2) Ta sklep bi bilo treba uporabljati, ko Svet, njegova pripravljalna telesa in generalni sekretariat Sveta (GSS) delajo s tajnimi podatki EU.

(3) Države članice bi morale v skladu z nacionalnimi zakoni in predpisi ter v obsegu, ki zagotavlja delovanje Sveta, spoštovati ta sklep, kadar njihovi pristojni organi, osebje ali izvajalci delajo s tajnimi podatki EU, tako da bodo vsi lahko prepričani, da so tajni podatki EU deležni enakovredne stopnje varovanja.

(4) Svet in Komisija se zavzemata za enakovredne standarde varovanja tajnih podatkov EU.

(5) Svet poudarja, da je treba v načela, standarde in pravila za varovanje tajnih podatkov, potrebna za zaščito interesov Unije in njenih držav članic, ustrezno vključiti Evropski parlament in druge institucije, agencije, organe ali urade EU.

(6) Agencije in organi EU, ki so bili ustanovljeni v skladu z naslovom V, poglavje 2 Pogodbe o Evropski uniji (PEU), Europol in Eurojust v okviru svoje notranje organiziranosti uporabljajo za varovanje tajnih podatkov EU temeljna načela in minimalne standarde iz tega sklepa, kakor je določeno v njihovih ustanovnih aktih.

(7) V operacijah kriznega upravljanja, ki so bile vzpostavljene v skladu z naslovom V, poglavje 2 PEU, se uporabljajo varnostni predpisi, ki jih je sprejel Svet za varovanje tajnih podatkov EU; te predpise uporablja tudi osebje, ki sodeluje v operacijah.

(8) Posebni predstavniki EU in člani njihovega osebja uporabljajo varnostne predpise, ki jih je za varovanje tajnih podatkov EU sprejel Svet.

(9) Ta sklep ne vpliva na člena 15 in 16 Pogodbe o delovanju Evropske unije (PDEU) in ustrezne izvedbene instrumente.

(10) Ta sklep ne vpliva na običajne postopke v državah članicah glede obveščanja nacionalnih parlamentov o dejavnostih Unije –

SPREJEL NASLEDNJI SKLEP:

*Člen 1*

**Namen, področje uporabe in opredelitev pojmov**

1. V tem sklepu so določena temeljna načela in minimalni standardi varovanja tajnih podatkov EU.

([1]) UL L 325, 11.12. 2009, str. 35.

2. Ta temeljna načela in minimalni standardi veljajo za Svet in GSS, države članice pa jih morajo spoštovati v skladu s svojimi nacionalnimi zakoni in predpisi, tako da so vsi lahko prepričani, da je zagotovljena enakovredna stopnja varovanja tajnih podatkov EU.

3. Pojmi, ki se uporabljajo v tem sklepu, so opredeljeni v dodatku A.

*Člen 2*

**Opredelitev tajnih podatkov EU, stopenj tajnosti in oznak**

1. „Tajni podatek EU" pomeni vsak podatek ali material z oznako stopnje tajnosti EU, katerega nepooblaščeno razkritje bi lahko zelo ali manj škodovalo interesom Evropske unije ali eni ali več državam članicam.

2. Tajni podatki EU imajo naslednje stopnje tajnosti:

(a) TRÈS SECRET UE/EU TOP SECRET: podatki in material, katerih nepooblaščeno razkritje bi lahko imelo izjemno težke posledice za vitalne interese Evropske unije ali ene ali več držav članic.

(b) SECRET UE/EU SECRET: podatki in material, katerih nepooblaščeno razkritje bi lahko resno škodovalo vitalnim interesom Evropske unije ali ene ali več držav članic.

(c) CONFIDENTIEL UE/EU CONFIDENTIAL: podatki in material, katerih nepooblaščeno razkritje bi lahko škodovalo vitalnim interesom Evropske unije ali ene ali več držav članic.

(d) RESTREINT UE/EU RESTRICTED: podatki in material, katerih nepooblaščeno razkritje bi lahko bilo škodljivo za interese Evropske unije ali ene ali več držav članic.

3. Tajni podatki EU so označeni s stopnjo tajnosti v skladu z odstavkom 2. Iz njihovih oznak je poleg tega lahko razvidno področje dejavnosti, na katero se nanašajo, organ izvora, omejitev pri razpošiljanju, omejitev uporabe ali dajanja.

*Člen 3*

**Sistem določanja stopenj tajnosti**

1. Pristojni organi zagotovijo, da so tajni podatki EU označeni z ustrezno stopnjo tajnosti, da je jasno razvidno, da so tajni, in da stopnjo tajnosti obdržijo le, dokler je to potrebno.

2. Brez predhodnega pisnega soglasja organa izvora se stopnja tajnosti tajnih podatkov EU ne zniža ali prekliče, niti se ne spremenijo ali odstranijo oznake iz člena 2(3).

3. Svet odobri varnostno politiko o nastajanju tajnih podatkov EU, ki vključuje praktični vodič po stopnjah tajnosti.

*Člen 4*

**Varovanje tajnih podatkov**

1. Tajni podatki EU se varujejo v skladu s tem sklepom.

2. Imetnik katerega koli tajnega podatka EU je odgovoren za njegovo varovanje v skladu s tem sklepom.

3. Če države članice v strukture ali omrežja Evropske unije vnesejo tajne podatke z oznako nacionalne stopnje tajnosti, Svet in GSS te podatke varujeta v skladu z zahtevami, ki se uporabljajo za tajne podatke EU enakovredne stopnje, kakor je določeno v preglednici enakovrednih stopenj tajnosti v dodatku B.

4. Pri velikih količinah ali zbirkah tajnih podatkov EU je morda upravičena raven zaščite, ki ustreza višji stopnji tajnosti.

*Člen 5*

**Obvladovanje varnostnega tveganja**

1. Za obvladovanje tveganja, povezanega s tajnimi podatki EU, je predviden postopek. Njegov cilj je opredeliti znana varnostna tveganja, določiti varnostne ukrepe za zmanjšanje teh tveganj na sprejemljivo raven v skladu s temeljnimi načeli in minimalnimi standardi iz tega sklepa ter uporabljati te ukrepe ob upoštevanju koncepta globinske obrambe, kakor je opredeljena v Dodatku A. Učinkovitost teh ukrepov se nenehno ocenjuje.

2. Varnostni ukrepi za varovanje tajnih podatkov EU v njihovem življenjskem ciklu so sorazmerni zlasti s stopnjo tajnosti, obliko in obsegom podatkov ali materiala, krajem in strukturo objektov, kjer se hranijo tajni podatki EU, ter lokalno oceno nevarnosti zlonamernih in/ali kriminalnih dejavnosti, vključno z nevarnostjo vohunstva, sabotaže in terorizma.

3. V načrtih za izredne razmere je upoštevana potreba po varovanju tajnih podatkov EU v izrednih razmerah, da se prepreči nepooblaščen dostop, razkritje ali izguba celovitosti podatkov ali nedostopnost.

4. V načrte za zagotovitev neprekinjenega poslovanja so vključeni preventivni in obnovitveni ukrepi, tako da so posledice velikih napak ali incidentov pri delu s tajnimi podatki EU in njihovi hrambi čim manjše.

*Člen 6*

**Izvajanje tega sklepa**

1. Po potrebi Svet na priporočilo varnostnega odbora odobri varnostno politiko, ki določa ukrepe za izvajanje tega sklepa.

2. Varnostni odbor se lahko na svoji ravni dogovori o varnostnih smernicah, ki bodo dopolnjevale ali podpirale ta sklep in varnostno politiko, ki jo odobri Svet.

*Člen 7*

**Osebna varnost**

1. Osebna varnost je izvajanje ukrepov, s katerimi se zagotovi, da imajo dostop do tajnih podatkov EU samo posamezniki, ki:

— imajo potrebo po seznanitvi,

— so bili po potrebi varnostno preverjeni na ustrezni stopnji, ter

— so bili poučeni o svoji odgovornosti.

2. Namen postopkov varnostnega preverjanja osebja je ugotoviti, ali je posameznik dovolj lojalen, vreden zaupanja in zanesljiv, da ga je mogoče pooblastiti za dostop do tajnih podatkov EU.

3. Vsi posamezniki v GSS, ki morajo zaradi svojih dolžnosti morda imeti dostop do tajnih podatkov EU stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, so varnostno preverjeni na ustrezni stopnji, preden se jim odobri dostop do takih tajnih podatkov EU. Postopek varnostnega preverjanja uradnikov in drugega osebja GSS je opisan v Prilogi I.

4. Osebje držav članic iz člena 14(3), ki mora zaradi svojih dolžnosti morda imeti dostop do tajnih podatkov EU stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, je varnostno preverjeno na ustrezni stopnji ali drugače pravilno pooblaščeno zaradi svoje funkcije v skladu z nacionalnimi zakoni in predpisi, preden se mu odobri dostop do takih tajnih podatkov EU.

5. Preden se posameznikom odobri dostop do tajnih podatkov EU ter nato v rednih presledkih, so vsi poučeni o svoji odgovornosti za varovanje tajnih podatkov EU v skladu s tem sklepom ter to tudi potrdijo.

6. Določbe za izvajanje tega člena so v Prilogi I.

*Člen 8*

**Fizična varnost**

1. Fizična varnost je uporaba fizičnih in tehničnih zaščitnih ukrepov za preprečitev nepooblaščenega dostopa do tajnih podatkov EU.

2. Namen ukrepov fizične varnosti je preprečiti nedovoljen ali nasilen vstop vsiljivcem, odvrniti, ovirati in odkriti nedovoljena dejanja ter omogočiti ločevanje osebja pri dostopu do tajnih podatkov EU glede na potrebo po seznanitvi. Takšni ukrepi se določijo na osnovi postopka obvladovanja tveganja.

3. Fizična varnost se uvede v vseh prostorih, stavbah, pisarnah, sobah in drugih območjih, v katerih se dela s tajnimi podatki EU ali v katerih se tajne podatke EU shranjuje, vključno z območji, kjer so nameščeni komunikacijski in informacijski sistemi, kakor je določeno v členu 10(2).

4. Območja, na katerih se hranijo tajni podatki EU stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, so določena kot varovana območja v skladu s Prilogo II, odobri pa jih pristojni varnostni organ.

5. Za varovanje tajnih podatkov EU stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje se uporablja le odobrena oprema ali naprave.

6. Določbe za izvajanje tega člena so v Prilogi II.

*Člen 9*

**Obravnavanje tajnih podatkov**

1. Obravnavanje tajnih podatkov je uporaba upravnih ukrepov za nadzor nad tajnimi podatki EU v njihovem življenjskem ciklu, ki dopolnjujejo ukrepe iz členov 7, 8 in 10 ter tako prispevajo k odvračanju, odkrivanju in obnovitvi takih podatkov po naključnem ali namernem nepooblaščenem razkritju ali izgubi. Ti ukrepi se nanašajo predvsem na nastajanje, vpisovanje, kopiranje, prevajanje, prenašanje in uničenje tajnih podatkov EU.

2. Podatki stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje se iz varnostnih razlogov vpišejo pred razpošiljanjem in ob prejemu. Pristojni organi GSS in držav članic v ta namen vzpostavijo sistem registrov. Podatki stopnje TRÈS SECRET UE/EU TOP SECRET se vpišejo v za to namenjenih registrih.

3. Pristojni varnostni organ redno pregleduje službe in prostore, v katerih poteka delo s tajnimi podatki EU ali v katerih se ti hranijo.

4. Tajni podatki EU se med službami in prostori zunaj fizično zaščitenih območij prenašajo:

(a) praviloma se tajni podatki EU prenašajo z elektronskimi sredstvi, ki so zaščiteni s šifrirnimi izdelki, odobrenimi v skladu s členom 10(6);

(b) če se sredstva iz točke (a) ne uporabijo, se tajni podatki EU prenašajo:

(i) na elektronskih nosilcih (tj. ključi USB, zgoščenke, trdi diski), ki so zaščiteni s šifrirnimi izdelki, odobrenimi v skladu s členom 10(6); ali

(ii) v vseh drugih primerih, kakor določi pristojni varnostni organ v skladu z ustreznimi zaščitnimi ukrepi iz Priloge III.

5. Določbe za izvajanje tega člena so navedene v Prilogi III.

*Člen 10*

**Zaščita tajnih podatkov EU s katerimi poteka delo v komunikacijskih in informacijskih sistemih**

1. Z zagotavljanjem informacijske varnosti (IA) v komunikacijskih in informacijskih sistemih je mogoče zagotoviti, da bodo podatki v teh sistemih zaščiteni, in bodo delovali tako, kot morajo, kadar morajo, pod nadzorom zakonitih uporabnikov. Pri učinkovitem zagotavljanju varnosti podatkov se poskrbi za ustrezno stopnjo tajnosti, celovitost, razpoložljivost, nezatajljivost in avtentičnost. Zagotavljanje informacijske varnosti temelji na postopku obvladovanja tveganja.

2. „Komunikacijski in informacijski sistem“ pomeni sistem, ki omogoča delo s podatki v elektronski obliki. Komunikacijski in informacijski sistem zajema vse elemente, potrebne za svoje delovanje, tudi infrastrukturo, organizacijo, osebje in informacijske vire. Ta sklep se uporablja za komunikacijske in informacijske sisteme, v katerih poteka delo s tajnimi podatki EU (KIS).

3. V KIS delo s tajnimi podatki EU poteka v skladu z načelom zagotavljanja informacijske varnosti.

4. Za vse KIS se opravi postopek akreditacije. Cilj akreditacije je pridobiti zagotovilo, da so bili izvedeni vsi ustrezni varnostni ukrepi in da je bila dosežena zadostna stopnja zaščite tajnih podatkov EU ter KIS v skladu s tem sklepom. V izjavi o akreditaciji so določeni najvišja stopnja tajnosti podatkov, s katerimi se lahko dela v KIS, in ustrezni pogoji.

5. KIS, v okviru katerih poteka delo s podatki stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, so zaščiteni tako, da podatki ne morejo biti nepooblaščeno razkriti zaradi nenamernega elektromagnetnega oddajanja („varnostni ukrepi TEMPEST“).

6. Kjer se zaščita tajnih podatkov EU zagotavlja s šifrirnimi izdelki, se ti izdelki odobrijo, kot sledi:

(a) zaupnost podatkov stopnje SECRET UE/EU SECRET in višje se zaščiti s šifrirnimi izdelki, ki jih odobri Svet v vlogi organa za odobritev šifrirnih metod in izdelkov na priporočilo varnostnega odbora;

(b) zaupnost podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali RESTREINT UE/EU RESTRICTED se zaščiti s šifrirnimi izdelki, ki jih odobri generalni sekretar Sveta (v nadaljnjem besedilu: „generalni sekretar“) v vlogi organa za odobritev šifrirnih metod in izdelkov na priporočilo varnostnega odbora.

Ne glede na točko (b) se lahko zaupnost tajnih podatkov EU stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali RESTREINT UE/EU RESTRICTED v nacionalnih sistemih držav članic zaščiti s šifrirnimi izdelki, ki jih odobri organ države članice za odobritev šifrirnih metod in izdelkov.

7. Med prenašanjem tajnih podatkov EU z elektronskimi sredstvi se uporabljajo odobreni šifrirni izdelki. Ne glede na navedeno zahtevo se lahko v izrednih razmerah ali specifičnih tehničnih konfiguracijah, določenih v Prilogi IV, uporabijo posebni postopki.

8. Pristojni organi GSS in posameznih držav članic ustanovijo naslednje organe za zagotavljanje informacijske varnosti:

(a) organ za zagotavljanje informacijske varnosti (IAA),

(b) organ TEMPEST (TA),

(c) organ za odobritev šifrirnih metod in izdelkov (CAA),

(d) organ za razpošiljanje šifrirnega materiala (CDA).

9. Pristojni organi GSS in posameznih držav članic za vsak sistem ustanovijo:

(a) organ za varnostno akreditacijo (SAA); in

(b) operativni organ za zagotavljanje informacijske varnosti (IA).

10. Določbe za izvajanje tega člena so v Prilogi IV.

*Člen 11*

**Industrijska varnost**

1. Industrijska varnost je uporaba ukrepov, s katerimi se zagotovi, da izvajalci ali podizvajalci varujejo tajne podatke EU med pogajanji za sklenitev pogodbe in v življenjskem ciklu pogodb s tajnimi podatki. Te pogodbe ne vključujejo dostopa do podatkov stopnje TRÈS SECRET UE/EU TOP SECRET.

2. GSS lahko naloge, ki vključujejo dostop do tajnih podatkov EU ali delo z njimi ali njihovo hrambo, s pogodbo prenese na industrijske ali druge subjekte, registrirane v državi članici ali tretji državi, ki je sklenila sporazum ali dogovor o izvajanju v skladu s členom 12(2)(a) ali (b).

3. Pri dodeljevanju pogodb s tajnimi podatki industrijskim ali drugim subjektom GSS kot naročnik zagotovi, da so izpolnjeni minimalni standardi industrijske varnosti iz tega sklepa in pogodbe.

4. Nacionalni varnostni organ, imenovani varnostni organ ali kateri koli drug pristojni organ vsake države članice zagotovi, kolikor to omogočajo nacionalni zakoni in predpisi, da izvajalci ali podizvajalci, registrirani na ozemlju njegove države članice, v pogajanjih za sklenitev pogodbe ali pri izvajanju pogodbe s tajnimi podatki sprejmejo vse ustrezne ukrepe za varovanje tajnih podatkov EU.

5. Nacionalni varnostni organ, imenovani varnostni organ ali kateri koli drug pristojni organ vsake države članice v skladu z nacionalnimi zakoni in predpisi zagotovi, da imajo izvajalci ali podizvajalci, registrirani na ozemlju njegove države članice, ki sodelujejo pri pogodbah ali podizvajalskih pogodbah s tajnimi podatki, zaradi katerih morajo v svojih prostorih imeti dostop do podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET, bodisi pri izvajanju takšnih pogodb ali v pogajanjih za njihovo sklenitev, varnostno dovoljenje organizacije za zahtevano stopnjo tajnosti.

6. Nacionalni varnostni organ, imenovani varnostni organ ali kateri koli drug pristojni varnostni organ odobri dovoljenje za dostop do tajnih podatkov osebju izvajalca ali podizvajalca, ki mora zaradi izvajanja pogodbe s tajnimi podatki imeti dostop do podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET, in sicer v skladu z nacionalnimi zakoni in predpisi ter minimalnimi standardi iz Priloge I.

7. Določbe za izvajanje tega člena so v Prilogi V.

*Člen 12*

**Izmenjava tajnih podatkov s tretjimi državami in mednarodnimi organizacijami**

1. Ko Svet sprejme odločitev o potrebi po izmenjavi tajnih podatkov s tretjo državo ali mednarodno organizacijo, se v ta namen vzpostavi ustrezen okvir.

2. Da bi vzpostavili tak okvir in določili vzajemna pravila za varovanje izmenjanih tajnih podatkov,

(a) Svet sklene sporazume o varnostnih postopkih za izmenjavo in varovanje tajnih podatkov (v nadaljnjem besedilu: „sporazumi o varovanju tajnosti podatkov“); ali

(b) pa lahko generalni sekretar sklene dogovore o izvajanju v skladu z odstavkom 17 Priloge VI, če stopnja tajnih podatkov EU, ki bodo dani, praviloma ni višja od RESTREINT UE/EU RESTRICTED.

3. Sporazumi o varovanju tajnosti podatkov ali dogovori o izvajanju iz odstavka 2 vsebujejo določbe, s katerimi se tajnim podatkom EU, ki jih prejmejo tretje države ali mednarodne organizacije, zagotovi varovanje, ustrezno njihovi stopnji tajnosti v skladu z minimalnimi standardi, ki niso manj strogi od standardov iz tega sklepa.

4. Odločitev o dajanju tajnih podatkov EU z izvorom v Svetu tretji državi ali mednarodni organizaciji sprejme Svet za vsak primer posebej glede na naravo in vsebino teh podatkov, potrebo prejemnika po seznanitvi ter koristi, ki jih bo imela EU. Če organ izvora tajnega podatka, ki ga želi dati, ni Svet, GSS ta organ najprej zaprosi za pisno soglasje, da sme dati tajni podatek. Če organa izvora ni mogoče ugotoviti, Svet prevzame to odgovornost.

5. Organizirajo se ocenjevalni obiski, s katerimi se ugotovi učinkovitost varnostnih ukrepov, ki se v tretji državi ali mednarodni organizaciji uporabljajo za varovanje zagotovljenih ali izmenjanih tajnih podatkov EU.

6. Določbe za izvajanje tega člena so v Prilogi VI.

*Člen 13*

**Kršitev varovanja tajnosti in nepooblaščeno razkritje tajnih podatkov EU**

1. Kršitev varovanja tajnosti je posledica posameznikovega dejanja ali opustitve dejanja v nasprotju z varnostnimi predpisi iz tega sklepa.

2. Do nepooblaščenega razkritja tajnih podatkov EU pride, če so ti kot posledica kršitve varovanja tajnosti v celoti ali delno razkriti nepooblaščenim osebam.

3. O vseh kršitvah ali domnevnih kršitvah varovanja tajnosti se nemudoma obvesti pristojni varnostni organ.

4. Če je bilo ugotovljeno ali če obstajajo utemeljeni razlogi za domnevo, da so bili tajni podatki EU nepooblaščeno razkriti ali izgubljeni, pristojni varnostni organ sprejme vse primerne ukrepe v skladu z ustreznimi zakoni in predpisi ter:

(a) obvesti organ izvora;

(b) zagotovi, da bo zadevo preiskalo osebje, ki ni neposredno povezano s kršitvijo, in ugotovilo, kakšna so dejstva;

(c) oceni morebitno škodo za interese EU ali držav članic;

(d) sprejme vse primerne ukrepe, da se kršitev ne bi ponovila, ter

(e) o sprejetih ukrepih obvesti ustrezne organe.

5. Zoper vsakega posameznika, ki je odgovoren za kršitev varnostnih predpisov iz tega sklepa, se lahko uvede disciplinski postopek v skladu z veljavnimi pravili in predpisi. Zoper vsakega posameznika, ki je odgovoren za nepooblaščeno razkritje ali izgubo tajnih podatkov EU, se lahko uvede disciplinski in/ali kazenski postopek v skladu z veljavnimi zakoni, pravili in predpisi.

*Člen 14*

**Odgovornost za izvrševanje**

1. Svet sprejme vse ustrezne ukrepe, s katerimi zagotovi vsesplošno dosledno uporabo tega sklepa.

2. Generalni sekretar sprejme vse ustrezne ukrepe, s katerimi zagotovi, da v prostorih, ki jih uporablja Svet, in v GSS ter njegovih uradih za zvezo v tretjih državah uradniki in drugi uslužbenci sekretariata, osebje, ki mu je dodeljeno, in njegovi izvajalci pri delu s tajnimi podatki EU ali kakršnimi koli drugimi tajnimi podatki ali njihovi hrambi uporabljajo ta sklep.

3. Države članice sprejmejo vse ustrezne ukrepe v skladu s svojo nacionalno zakonodajo in predpisi, s katerimi zagotovijo, da pri delu s tajnimi podatki EU in njihovi hrambi naslednje osebe spoštujejo ta sklep:

(a) osebje stalnih predstavništev držav članic pri Evropski uniji in nacionalni delegati, ki se udeležujejo sestankov Sveta ali njegovih pripravljalnih teles ali pa sodelujejo pri drugih dejavnostih Sveta;

(b) drugo osebje državnih uprav držav članic, vključno z osebjem, dodeljenim tem upravam, nameščeno bodisi na ozemlju držav članic ali v tujini;

(c) druge osebe v državah članicah, ki so zaradi svoje funkcije pravilno pooblaščene za dostop do tajnih podatkov EU, ter

(d) izvajalci držav članic na ozemlju držav članic ali v tujini.

*Člen 15*

**Organiziranost varovanja tajnosti v Svetu**

1. Svet v okviru odgovornosti za zagotavljanje vsesplošne dosledne uporabe tega sklepa potrdi:

(a) sporazume iz člena 12(2)(a);

(b) sklepe o odobritvi dajanja tajnih podatkov EU tretjim državam in mednarodnim organizacijam;

(c) letni program inšpekcijskih pregledov, ki ga predlaga generalni sekretar in priporoči Varnostni odbor, za inšpekcijske preglede služb in prostorov držav članic in agencij in organov EU, ustanovljenih v skladu z naslovom V, poglavjem 2 PEU kakor tudi Europol in Eurojust ter ocenjevalne obiske v tretjih državah in mednarodnih organizacijah, da bi ugotovili učinkovitost ukrepov, ki se izvajajo za zaščito tajnih podatkov EU, ter

(d) varnostno politiko, kot je predvideno v členu 6(1).

2. Varnostni organ GSS je generalni sekretar. Generalni sekretar v tej funkciji:

(a) izvaja in preverja varnostno politiko Sveta;

(b) z nacionalnimi varnostnimi organi držav članic usklajuje vse varnostne zadeve v zvezi z varovanjem tajnih podatkov, ki se nanašajo na delovanje Sveta;

(c) preden se lahko uradnikom in drugim uslužbencem GSS odobri dostop do podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, temu osebju v skladu s členom 7(3) dodeli dovoljenje EU za dostop do tajnih podatkov;

(d) po potrebi naroča preiskave dejanskega nepooblaščenega razkritja ali izgube tajnih podatkov EU ali suma takega razkritja ali izgube, ki jih hrani Svet ali z izvorom v Svetu, ter ustrezne varnostne organe prosi za pomoč pri taki preiskavi;

(e) izvaja redne inšpekcijske preglede varnostne ureditve za varovanje tajnih podatkov EU v prostorih GSS;

(f) izvaja redne inšpekcijske preglede varnostne ureditve za varovanje tajnih podatkov EU v agencijah in organih EU ustanovljenih v skladu z naslovom V, poglavjem 2 PEU kakor tudi Europol in Eurojust, operacijah za krizno upravljanje, vzpostavljenih v skladu z naslovom V, poglavjem 2 PEU, ter s strani posebnih predstavnikov EU (PPEU) in članov njihovega osebja;

(g) skupaj in usklajeno z zadevnimi nacionalnimi varnostnimi organi izvaja redne inšpekcijske preglede varnostne ureditve za varovanje tajnih podatkov EU v službah in prostorih držav članic;

(h) usklajuje varnostne ukrepe s pristojnimi organi držav članic, ki so odgovorni za varovanje tajnih podatkov, oziroma tretjih držav ali mednarodnih organizacij, tudi glede vrste nevarnosti, ki ogroža tajne podatke EU in zaščite pred njimi;

(i) sklepa dogovore o izvajanju iz člena 12(2)(b); ter

(j) izvaja začetne in redne ocenjevalne obiske tretjih držav in mednarodnih organizacij, da bi ugotovil, kako učinkoviti so ukrepi za varovanje tajnih podatkov EU, ki so jim bili zagotovljeni ali so bili z njimi izmenjani.

Varnostni urad GSS je generalnemu sekretarju na razpolago in mu pomaga pri teh nalogah.

3. Države članice morajo za izvajanje člena 14(3):

(a) imenovati nacionalni varnostni organ, ki je odgovoren za varnostno ureditev za varovanje tajnih podatkov EU, da:

(i) se tajni podatki EU, ki jih ima katero koli državno ministrstvo, javni ali zasebni organ ali agencija, doma ali v tujini varujejo v skladu s tem sklepom;

(ii) se izvajajo redni inšpekcijski pregledi varnostne ureditve za varovanje tajnih podatkov EU;

(iii) so vse osebe, zaposlene v državni upravi ali pri izvajalcu, ki se jim lahko odobri dostop do podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, ustrezno varnostno preverjene ali so zaradi svoje funkcije za to pravilno pooblaščene v skladu z nacionalnimi zakoni in predpisi;

(iv) so po potrebi vzpostavljeni varnostni programi, da se tveganje nepooblaščenega razkritja ali izgube tajnih podatkov EU čim bolj zniža;

(v) so varnostne zadeve, ki se nanašajo na varovanje tajnih podatkov EU, usklajene z drugimi pristojnimi nacionalnimi organi, tudi s tistimi iz tega sklepa, ter

(vi) se zagotovi odziv na zahteve agencij in organov EU, operacij za krizno upravljanje, vzpostavljenih v skladu z naslovom V, poglavjem 2 PEU, Europol, Eurojust, ter posebnih predstavnikov EU in njihovega osebja po varnostnem preverjanju.

Nacionalni varnostni organi so navedeni v Dodatku C;

(b) zagotoviti, da njihovi pristojni organi preskrbijo podatke ter svetujejo svojim vladam in tako tudi Svetu o vrsti nevarnosti, ki ogroža tajne podatke EU, in načinih zaščite pred njimi.

*Člen 16*

**Varnostni odbor**

1. Ustanovi se Varnostni odbor. Preučuje in ocenjuje vse zadeve v zvezi z varovanjem tajnosti v okviru področja uporabe tega sklepa ter po potrebi za Svet pripravi priporočila.

2. Sestavljen je iz predstavnikov nacionalnih varnostnih organov držav članic, njegovih sestankov pa se udeležuje tudi predstavnik Komisije in Evropske službe za zunanje delovanje. Predseduje mu generalni sekretar ali njegov namestnik. Sestaja se po navodilih Sveta ali na zahtevo generalnega sekretarja ali enega od nacionalnih varnostnih organov.

Na sestanke odbora so lahko vabljeni in jim prisostvujejo tudi predstavniki agencij in organov EU, ustanovljenih v skladu z naslovom V, poglavjem 2 PEU, kakor tudi Europol in Eurojust, kadar se obravnavajo vprašanja v zvezi z njimi.

3. Varnostni odbor svoje dejavnosti organizira tako, da lahko daje priporočila o posebnih področjih varovanja tajnosti. Ustanovi strokovno podobmočje za vprašanja zagotavljanja informacijske varnosti, po potrebi pa tudi druga strokovna podobmočja. Zanje določi naloge in pristojnosti, oni pa mu pošiljajo poročila o svoji dejavnosti, ki po potrebi vključujejo tudi priporočila za Svet.

*Člen 17*

**Razveljavitev in nadomestitev prejšnjega sklepa**

1. Sklep Sveta 2001/264/ES z dne 19. marca 2001 o sprejetju predpisov Sveta o varovanju tajnosti [1] se razveljavi in nadomesti s tem sklepom.

2. Varovanje vseh podatkov EU, ki so v skladu s Sklepom 2001/264/ES imeli oznako tajnosti, se nadaljuje v skladu z ustreznimi določbami tega sklepa.

*Člen 18*

**Začetek veljavnosti**

Ta sklep začne veljati na dan objave v *Uradnem listu Evropske unije*.

V Bruslju, 31. marca 2011

*Za Svet*

*Predsednik*

VÖLNER P.

[1] UL L 101, 11.4.2001, str. 1.

*PRILOGE*

*PRILOGA I*

Varnost osebja

*PRILOGA II*

Fizična varnost

*PRILOGA III*

Obravnavanje tajnih podatkov

*PRILOGA IV*

Varovanje tajnih podatkov EU, s katerimi poteka delo v KIS

*PRILOGA V*

Industrijska varnost

*PRILOGA VI*

Izmenjava tajnih podatkov s tretjimi državami in mednarodnimi organizacijami

*PRILOGA I*

**VARNOST OSEBJA**

I. UVOD

1. V tej prilogi so določbe za izvajanje člena 7. Zlasti določa merila za ugotavljanje, ali je posameznik dovolj lojalen, vreden zaupanja in zanesljiv, da je lahko pooblaščen za dostop do tajnih podatkov EU, ter za preiskovalne in upravne postopke, ki jih je treba izvesti v ta namen.

2. Če razlikovanje ni pomembno, izraz „dovoljenje za dostop do tajnih podatkov" v tej prilogi pomeni nacionalno dovoljenje za dostop do tajnih podatkov in/ali dovoljenje EU za dostop do tajnih podatkov, kot sta opredeljeni v Dodatku A.

II. POOBLASTILO ZA DOSTOP DO TAJNIH PODATKOV EU

3. Posameznik je za dostop do podatkov EU stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje pooblaščen šele potem, ko:

(a) je bilo ugotovljeno, da ima potrebo po seznanitvi;

(b) je dobil dovoljenje za dostop do tajnih podatkov ustrezne stopnje ali je zaradi svoje funkcije drugače pravilno pooblaščen v skladu z nacionalnimi zakoni in predpisi; in

(c) je bil poučen o varnostnih pravilih in postopkih za varovanje tajnih podatkov EU ter je sprejel odgovornost za varovanje teh podatkov.

4. Vse države članice in GSS določijo delovna mesta v svoji strukturi, na katerih je potreben dostop do podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje in zato dovoljenje za dostop do tajnih podatkov ustrezne stopnje.

III. ZAHTEVE ZA DOVOLJENJE ZA DOSTOP DO TAJNIH PODATKOV

5. Po prejemu pravilno odobrene prošnje so nacionalni varnostni organi ali drugi pristojni nacionalni organi odgovorni za varnostne preiskave svojih državljanov, ki morajo imeti dostop do podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje. Standardi za preiskavo so skladni z nacionalnimi zakoni in predpisi.

6. Če zadevni posameznik prebiva na ozemlju druge države članice ali tretje države, pristojni nacionalni organi za pomoč zaprosijo pristojni organ države prebivališča v skladu z nacionalnimi zakoni in predpisi. Države članice si medsebojno pomagajo pri varnostnih preiskavah v skladu z nacionalnimi zakoni in predpisi.

7. Če to dovoljujejo nacionalni zakoni in predpisi, lahko nacionalni varnostni organi ali drugi pristojni nacionalni organi opravijo preiskavo tujih državljanov, ki morajo imeti dostop do podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje. Standardi za preiskavo so skladni z nacionalnimi zakoni in predpisi.

**Merila za varnostno preiskavo**

8. Za ugotavljanje, ali je posameznik dovolj lojalen, vreden zaupanja in zanesljiv, da se mu lahko dodeli dovoljenje za dostop do tajnih podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, se uporabi varnostna preiskava. Pristojni nacionalni organ na podlagi ugotovitev take varnostne preiskave pripravi splošno oceno. Nobena posamezna negativna ugotovitev ni nujno razlog za zavrnitev dovoljenja za dostop do tajnih podatkov. Med osnovnimi merili za takšno ugotavljanje bi moralo biti, kolikor to dopuščajo nacionalni zakoni in predpisi, preverjanje ali je posameznik:

(a) storil ali poskušal storiti kaznivo dejanje vohunjenja, terorizma, sabotaže, izdajstva ali upora oziroma sodeloval ali pomagal in nudil podporo pri izvedbi takega kaznivega dejanja;

(b) sodeloval ali še sodeluje z vohuni, teroristi, saboterji ali posamezniki, za katere se upravičeno sumi, da to so, oziroma s predstavniki organizacij tujih držav, vključno s tujimi obveščevalnimi službami, ki lahko ogrozijo varnost EU in/ali držav članic, razen če je bilo tako sodelovanje odobreno v okviru uradne dolžnosti;

(c) bil ali je še vedno član kakršne koli organizacije, ki skuša z nasilnimi, uničevalnimi ali drugimi nezakonitimi sredstvi med drugim zrušiti vlado določene države članice, spremeniti ustavni red države članice ali zamenjati obliko ali politike njene vlade;

(d) bil ali je še vedno pristaš kakšne izmed organizacij iz točke (c) ali sodeluje oziroma je tesno sodeloval s člani takih organizacij;

(e) namerno zadrževal, napačno razlagal ali potvarjal pomembne podatke, predvsem tajne podatke, ali je namerno lagal pri izpolnjevanju vprašalnika za varnostno preverjanje osebja oziroma pri razgovoru za varnostno preverjanje;

(f) bil obsojen zaradi kaznivega dejanja ali več dejanj;

(g) bil odvisen od alkohola, je uporabljal nedovoljene droge in/ali je kdaj zlorabljal dovoljene droge;

(h) bil ali je še vpleten v dejavnost, ki bi lahko povzročila izpostavljenost izsiljevanju ali pritiskom;

(i) se z dejanji ali besedami izkazal za nepoštenega, nelojalnega, nezanesljivega ali nevrednega zaupanja;

(j) resno ali večkrat kršil varnostne predpise; ali je poskušal izvesti oziroma je uspešno izvedel nepooblaščeno dejavnost v zvezi s komunikacijskimi in informacijskimi sistemi;

(k) podvržen pritiskom (npr. ker je državljan ene ali več držav, ki niso članice EU) sorodnikov ali ožjih znancev, ki bi lahko bili dovzetni za sodelovanje s tujimi obveščevalnimi službami, terorističnimi skupinami ali drugimi uničevalnimi organizacijami ali posamezniki, katerih nameni lahko ogrozijo varnostne interese EU in/ali držav članic.

9. Kadar je to primerno in v skladu z nacionalnimi zakoni in predpisi, je lahko pri varnostni preiskavi pomembno tudi finančno in zdravstveno stanje posameznika.

10. Kadar je to primerno in v skladu z nacionalnimi zakoni in predpisi, so lahko osebnostne lastnosti, vedenje in okoliščine v zvezi z zakonskim partnerjem, izvenzakonskim partnerjem ali ožjim družinskim članom prav tako pomembni pri varnostni preiskavi.

**Preiskovalne zahteve za dostop do tajnih podatkov EU**

*Izdaja prvega dovoljenja za dostop do tajnih podatkov*

11. Varnostno preverjanje osebja za prvo dovoljenje za dostop do podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET temelji na varnostni preiskavi iz obdobja najmanj zadnjih petih let ali od 18. leta starosti do sedaj, pri čemer se upošteva krajše obdobje, in vključuje naslednje:

(a) izpolnitev nacionalnega vprašalnika za varnostno preverjanje osebja glede dostopa do tajnih podatkov EU tiste stopnje tajnosti, ki jo bo posameznik morda potreboval. Izpolnjeni vprašalnik se pošlje pristojnemu varnostnemu organu;

(b) preverjanje identitete/državljanstva/državljanskega statusa – preverijo se datum in kraj rojstva ter identiteta posameznika. Dokazati je treba pretekli in sedanji državljanski status in/ali državljanstvo posameznika, vključno z oceno kakršne koli izpostavljenosti pritiskom iz zunanjih virov, npr. zaradi prejšnjega prebivališča ali zvez iz preteklosti, ter

(c) preverjanje državnih in lokalnih evidenc – preverijo se državne varnostne in centralne kazenske evidence, če slednje obstajajo, in/ali druge primerljive vladne in policijske evidence. Preverijo se evidence organov pregona, ki imajo sodno pristojnost na območju, kjer je imel posameznik prebivališče ali zaposlitev.

12. Varnostno preverjanje osebja za prvo dovoljenje za dostop do podatkov stopnje SECRET UE/EU TOP SECRET temelji na varnostni preiskavi obdobja najmanj zadnjih desetih let, ali od 18. leta starosti do sedaj, pri čemer se upošteva krajše obdobje. Če razgovori potekajo, kakor je določeno v točki (e) v nadaljevanju besedila, preiskave zajemajo najmanj obdobje zadnjih sedmih let ali od 18. leta do sedaj, pri čemer se upošteva krajše obdobje. Pred izdajo dovoljenja za dostop do tajnih podatkov stopnje TRÈS SECRET UE/EU TOP SECRET, ali če to zahtevajo nacionalni zakoni in predpisi, tudi za dostop do tajnih podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET, se ob upoštevanju meril iz prej navedenega odstavka 8 preveri tudi naslednje, če to zahtevajo nacionalni zakoni in predpisi:

(a) finančni status – pridobijo se informacije o posameznikovem finančnem stanju, da se oceni izpostavljenost tujim ali domačim pritiskom zaradi resnih finančnih težav ali zato, da se odkrije nepojasnjen priliv kapitala;

(b) izobrazba – pridobijo se informacije za potrditev izobraževanja posameznika na šolah, univerzah in drugih izobraževalnih ustanovah od dopolnjenega 18. leta starosti ali v ustreznem časovnem obdobju po presoji preiskovalnega varnostnega organa;

(c) zaposlitev – pridobijo se informacije o sedanji zaposlitvi in zaposlitvah v preteklosti, s sklicevanjem na vire, kot so evidence o zaposlitvi, poročila o uspešnosti in učinkovitosti, pa tudi na delodajalce ali nadrejene;

(d) služenje vojaškega roka – kjer je to primerno, se preveri služenje posameznika v oboroženih silah in način odpusta, in

(e) razgovori – s posameznikom se opravi razgovor, če to določa in dovoljuje nacionalna zakonodaja. Razgovori se opravijo tudi z osebami, ki lahko podajo nepristransko oceno o posameznikovi preteklosti, dejavnostih, lojalnosti, ter o tem, ali je vreden zaupanja in zanesljiv. Če je v nacionalni praksi običajno, da preiskovana oseba navede reference, se izvedejo razgovori z referenčnimi osebami, razen če obstajajo upravičeni razlogi, da se tega ne stori.

13. Po potrebi in v skladu z nacionalnimi zakoni in predpisi se lahko opravijo dodatne preiskave za pridobitev vseh ustreznih informacij o posamezniku in za utemeljitev ali ovržbo negativnih informacij.

*Podaljšanje veljavnosti dovoljenja za dostop do tajnih podatkov*

14. Po izdaji prvega dovoljenja za dostop do tajnih podatkov in pod pogojem, da je posameznik nepretrgoma služboval v državni upravi ali v GSS in še vedno potrebuje dostop do tajnih podatkov EU, se dovoljenje pregleda zaradi podaljšanja veljavnosti v največ petletnih presledkih za dovoljenje za stopnjo tajnosti TRÈS SECRET UE/EU TOP SECRET in v največ desetletnih presledkih za dovoljenje za stopnjo tajnosti SECRET UE/EU SECRET in CONFIDENTIEL UE/EU CONFIDENTIAL, in sicer z začetkom veljavnosti od datuma uradnega obvestila o zadnji varnostni preiskavi, na podlagi katere je bilo izdano. Vse varnostne preiskave za podaljšanje veljavnosti dovoljenja za dostop do tajnih podatkov zajemajo obdobje od zaključka predhodne tovrstne preiskave.

15. Za podaljšanje veljavnosti dovoljenj za dostop do tajnih podatkov se preiščejo elementi iz odstavkov 11 in 12.

16. Zahteve za podaljšanje veljavnosti se predložijo pravočasno ob upoštevanju časa, ki je potreben za varnostne preiskave. Če pa je zadevni nacionalni varnostni organ ali drug pristojni nacionalni organ prejel zadevno zahtevo za podaljšanje veljavnosti in ustrezni vprašalnik za varnostno preverjanje osebja pred iztekom veljavnosti dovoljenja za dostop do tajnih podatkov in če potrebna varnostna preiskava v tem času še ni zaključena, lahko pristojni nacionalni organ, če to dopuščajo nacionalni zakoni in predpisi, podaljša veljavnost trenutnega dovoljenja za največ 12 mesecev. Če ob izteku teh 12 mesecev varnostna preiskava še vedno ni zaključena, se posamezniku dodeli take naloge, za katere ne potrebuje dovoljenja za dostop do tajnih podatkov.

*Postopki varnostnega preverjanja osebja v GSS*

17. Vprašalnike za varnostno preverjanje osebja, ki jih izpolnijo uradniki in drugi uslužbenci v GSS, varnostni organ GSS pošlje nacionalnemu varnostnemu organu države članice, katere državljan je zadevni posameznik, z zahtevkom, da se izvede varnostna preiskava glede dostopa do tajnih podatkov EU tiste stopnje tajnosti, ki jih bo ta posameznik potreboval.

18. Če GSS izve za podatke o prosilcu za dovoljenje EU za dostop do tajnih podatkov, ki se nanašajo na varnostno preiskavo, o tem v skladu z ustreznimi pravili in predpisi obvesti ustrezni nacionalni varnostni organ.

19. Zadevni nacionalni varnostni organ po opravljeni varnostni preiskavi obvesti varnostni organ GSS o njenem izidu, s standardnim obrazcem, ki ga predpiše Varnostni odbor.

(a) Če se z varnostno preiskavo zagotovi, da ni nobenih negativnih informacij, ki bi vzbudile dvome o tem, ali je posameznik lojalen, vreden zaupanja in zanesljiv, lahko organ GSS za imenovanje zadevni osebi podeli dovoljenje EU za dostop do tajnih podatkov in dovoli dostop do tajnih podatkov EU do ustrezne stopnje in do določenega datuma;

(b) če z varnostno preiskavo tega ni mogoče zagotoviti, organ GSS za imenovanje o tem uradno obvesti zadevnega posameznika, ki lahko zaprosi za zaslišanje pri organu za imenovanje. Slednji lahko zaprosi pristojni nacionalni varnostni organ za vsa dodatna pojasnila, ki jih ta lahko priskrbi skladno z nacionalnimi zakoni in predpisi. Če je izid potrjen, se dovoljenja EU za dostop do tajnih podatkov ne izda.

20. Za varnostno preiskavo skupaj z dobljenimi rezultati se upoštevajo ustrezni zakoni in predpisi, ki veljajo v zadevni državi članici, vključno s tistimi, ki urejajo pritožbe. Na odločbe organa GSS za imenovanje se je mogoče pritožiti v skladu s kadrovskimi predpisi za uradnike Evropske unije in pogoji za zaposlitev drugih uslužbencev Evropske unije iz Uredbe (EGS, EURATOM, ESPJ) št. 259/68 ([1]) (v nadaljnjem besedilu: Kadrovski predpisi in pogoji za zaposlitev).

21. Zagotovila, na katerih temelji dovoljenje EU za dostop do tajnih podatkov – pod pogojem, da so še vedno v veljavi –, zajemajo vse zadolžitve zadevnega posameznika v GSS ali Komisiji.

22. Če posameznik ne nastopi službe v roku 12 mesecev po uradnem obvestilu organa GSS za imenovanje o izidu varnostne preiskave, ali če posameznik 12 mesecev ne opravlja službe, med tem časom pa ni zaposlen na delovnem mestu v GSS ali v državni upravi države članice, se ta izid predloži zadevnemu nacionalnemu varnostnemu organu v potrditev, da je še vedno veljaven in ustrezen.

23. Če GSS izve za informacije o nevarnosti, povezani s posameznikom, ki ima veljavno dovoljenje EU za dostop do tajnih podatkov, o tem v skladu z ustreznimi pravili in predpisi obvesti ustrezni nacionalni varnostni organ. Če nacionalni varnostni organ obvesti GSS o preklicu zagotovil, ki so bila v skladu z odstavkom 19(a) dana za posameznika, ki ima veljavno dovoljenje EU za dostop do tajnih podatkov, lahko organ GSS za imenovanje zaprosi nacionalni varnostni organ za vsa pojasnila, ki jih slednji lahko zagotovi skladno z nacionalnimi zakoni in predpisi. Če se izkaže, da so negativne informacije resnične, se posamezniku odvzame dovoljenje EU za dostop do tajnih podatkov in se mu onemogoči dostop do tajnih podatkov EU ter se ga umakne z delovnega mesta, na katerem je takšen dostop mogoč ali na katerem bi lahko ogrozil varnost.

24. Vsaka odločitev o odvzemu dovoljenja EU za dostop do tajnih podatkov uradniku ali drugemu uslužbencu GSS in po potrebi razlogi zanjo se sporočijo zadevni osebi, ki lahko zaprosi za zaslišanje pri organu za imenovanje. Za informacije, ki jih predloži nacionalni varnostni organ, veljajo ustrezni zakoni in predpisi, ki veljajo v zadevni državi članici, vključno s pravili in predpisi, ki urejajo pritožbe. Na odločbe organa GSS za imenovanje se je mogoče pritožiti v skladu s Kadrovskimi predpisi in pogoji za zaposlitev.

25. Nacionalni strokovnjaki, ki so dodeljeni GSS na delovno mesto, za katero je potrebno dovoljenje EU za dostop do tajnih podatkov, pred prevzemom svojih zadolžitev varnostnemu organu GSS predložijo veljavno nacionalno dovoljenje za dostop do tajnih podatkov.

*Evidence dovoljenj za dostop do tajnih podatkov*

26. Evidence nacionalnih in EU dovoljenj za dostop do tajnih podatkov EU vodijo posamezne države članice in GSS. Te evidence vsebujejo najmanj stopnjo tajnosti podatkov EU, do katerih ima lahko posameznik dostop (CONFIDENTIEL UE/EU CONFIDENTIAL ali višje), datum izdaje dovoljenja za dostop do tajnih podatkov in njegovo obdobje veljavnosti.

27. Pristojni varnostni organ lahko izda potrdilo za dostop do tajnih podatkov (PSCC), iz katerega so razvidni stopnja tajnosti podatkov EU, do katerih ima lahko posameznik dostop (CONFIDENTIEL UE/EU CONFIDENTIAL ali višje), datum veljavnosti zadevnega nacionalnega ali EU dovoljenja za dostop do tajnih podatkov in datum izteka veljavnosti samega potrdila.

**Izjeme od zahteve glede dovoljenja za dostop do tajnih podatkov**

28. V državah članicah je dostop do tajnih podatkov EU za posameznike, ki so zaradi svoje funkcije za to pravilno pooblaščeni, urejen z nacionalnimi zakoni in predpisi; ti posamezniki so poučeni o svojih obveznostih pri varovanju tajnih podatkov EU.

IV. IZOBRAŽEVANJE IN OSVEŠČANJE O VAROVANJU TAJNOSTI

29. Vsi posamezniki, ki prejmejo dovoljenje za dostop do tajnih podatkov, pisno potrdijo, da razumejo svoje obveznosti glede varovanja tajnih podatkov EU in da se zavedajo posledic, če pride do nepooblaščenega razkritja tajnih podatkov EU. Za vodenje evidence o takih pisnih potrditvah sta odgovorna država članica in GSS, kakor je ustrezno.

30. Vse posameznike, ki imajo pooblastilo za dostop do tajnih podatkov EU ali se od njih zahteva delo s temi podatki, je treba na začetku opozoriti in jih nato redno poučevati glede nevarnosti za varovanje tajnosti; ustrezne varnostne organe so dolžni nemudoma obvestiti o vsakem poskusu približevanja ali ravnanju, ki se jim zdi sumljivo ali nenavadno.

31. Vsi posamezniki, ki prenehajo opravljati naloge, za katere potrebujejo dostop do tajnih podatkov EU, se seznanijo s svojo obveznostjo, da morajo te podatke varovati tudi v prihodnje, in to po potrebi tudi pisno potrdijo.

([1]) UL L 56. 4.3. 1968, str. 1.

V. IZJEMNE OKOLIŠČINE

32. Če to dovoljujejo nacionalni zakoni in predpisi, imajo lahko nacionalni uradniki z dovoljenjem pristojnega nacionalnega organa države članice za dostop do nacionalnih tajnih podatkov začasno dostop do tajnih podatkov EU do ustrezne stopnje, določene v preglednici enakovrednih stopenj tajnosti v dodatku B, dokler jim ne izdajo nacionalnega dovoljenja za dostop do tajnih podatkov EU, če je tak začasen dostop v interesu EU. Če nacionalna zakonodaja in predpisi ne dovoljujejo takega začasnega dostopa do tajnih podatkov EU, nacionalni varnostni organ o tem obvesti Varnostni odbor.

33. V nujnih primerih, kadar je to ustrezno utemeljeno v interesu službe in do zaključka celovite varnostne preiskave, organ GSS za imenovanje po posvetovanju z nacionalnim varnostnim organom države članice, katere državljan je posameznik, in ob upoštevanju izida predhodnih pregledov, s katerimi se preveri, da ni nobenih negativnih informacij, uradnikom in drugim uslužbencem GSS izda začasno pooblastilo za dostop do tajnih podatkov EU za določeno funkcijo. Ta začasna pooblastila veljajo največ šest mesecev in ne dovoljujejo dostopa do podatkov stopnje TRÈS SECRET UE/EU TOP SECRET. Vsi posamezniki, ki prejmejo začasno pooblastilo, pisno potrdijo, da razumejo svoje obveznosti glede varovanja tajnih podatkov EU in da se zavedajo posledic njihovega nepooblaščenega razkritja. GSS vodi evidenco takšnih pisnih potrditev.

34. Če je posameznik dodeljen na delovno mesto, za katerega je potrebno dovoljenje za dostop do tajnih podatkov, ki je za eno stopnjo višji od stopnje dovoljenja, ki ga trenutno ima, se lahko na to mesto začasno imenuje pod naslednjimi pogoji:

(a) posameznikov nadrejeni mora pisno upravičiti nujno potrebo po dostopu do tajnih podatkov EU na višji stopnji tajnosti;

(b) dostop se omeji na določene podrobnosti iz tajnih podatkov EU, ki so potrebne za izvajanje nalog na tem delovnem mestu;

(c) posameznik ima veljavno nacionalno dovoljenje ali dovoljenje EU za dostop do tajnih podatkov;

(d) ukrepi za pridobitev pooblastila za stopnjo dostopa za novo delovno mesto so že v teku;

(e) pristojni organ je dobro preveril, ali ni posameznik kdaj resno ali večkrat kršil varnostnih predpisov;

(f) imenovanje posameznika je odobril pristojni organ; ter

(g) zapisnik o taki izjemi, ki vključuje opis podatkov, do katerih je bil odobren dostop, se hrani v pristojnem registru ali pod-registru.

35. Opisani postopek se uporabi za enkraten dostop do tajnih podatkov EU, ki so za eno stopnjo tajnosti višji od tistih, za katere je bil posameznik varnostno preverjen. Ta postopek se ne uporablja prepogosto.

36. V zares izjemnih okoliščinah, kot so misije v sovražnem okolju ali v obdobju naraščajoče mednarodne napetosti, ko je to potrebno zaradi izrednih ukrepov, zlasti če gre za vprašanje življenja ali smrti, lahko države članice in generalni sekretar pisno, če je to mogoče, odobrijo dostop do tajnih podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET posameznikom, ki nimajo ustreznega dovoljenja za dostop do tajnih podatkov, če je tako dovoljenje zares nujno in ni nikakršnih dvomov, da je zadevni posameznik lojalen, vreden zaupanja in zanesljiv. Dodelitev takega dovoljenja se evidentira z opisom podatkov, do katerih je bil odobren dostop.

37. Za podatke stopnje TRÈS SECRET UE/EU TOP SECRET se tak nujni dostop omeji na državljane EU, ki so že pooblaščeni za dostop do bodisi podatkov stopnje, ki je enakovredna TRÈS SECRET UE/EU TOP SECRET na nacionalni ravni, bodisi do podatkov stopnje SECRET UE/EU SECRET.

38. Če se uporabi postopek iz odstavkov 36 in 37, se Varnostnemu odboru o tem pošlje obvestilo.

39. Če so glede začasnih pooblastil, začasnega imenovanja posameznikov, njihovega enkratnega dostopa oziroma dostopa do tajnih podatkov v nujnih primerih v nacionalni zakonodaji in predpisih države članice določena strožja pravila, se postopki, predvideni v tem oddelku, izvajajo samo v okviru omejitev iz zadevnih nacionalnih zakonov in predpisov.

40. Varnostni odbor prejme letno poročilo o uporabi postopkov iz tega oddelka.

VI. UDELEŽBA NA SESTANKIH V SVETU

41. Posamezniki, ki naj bi se udeležili sestankov Sveta ali pripravljalnih teles Sveta, na katerih se obravnavajo podatki stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, lahko to storijo šele potem, ko je odobren status njihovega dovoljenja za dostop do tajnih podatkov in ob upoštevanju odstavka 28. Za delegate ustrezni organi pošljejo Varnostnemu uradu GSS potrdilo za dostop do tajnih podatkov ali drug dokaz o varnostnem preverjanju, izjemoma pa ga lahko predloži zadevni delegat. Po potrebi se lahko uporabi zbirni seznam imen z ustreznimi dokazili o opravljenem varnostnem preverjanju.

42. Če je posamezniku, ki mora zaradi nalog, ki jih opravlja, sodelovati na sestankih Sveta ali pripravljalnih teles Sveta, iz varnostnih razlogov odvzeto nacionalno dovoljenje za dostop do tajnih podatkov EU, pristojni organ o tem obvesti GSS.

VII. MOREBITEN DOSTOP DO TAJNIH PODATKOV EU

43. Če se bodo posamezniki zaposlili v okoliščinah, v katerih bi lahko imeli dostop do tajnih podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, morajo biti za to ustrezno varnostno preverjeni ali pri tem imeti ves čas spremstvo.

44. Kurirji, varnostniki in spremljevalci se varnostno preverijo do ustrezne stopnje ali se o njih opravi drugačna ustrezna preiskava v skladu z nacionalnimi zakoni in predpisi; obveščeni so o varnostnih postopkih za varovanje tajnih podatkov EU ter poučeni o dolžnosti, da varujejo podatke, ki so jim zaupani.

*PRILOGA II*

**FIZIČNA VARNOST**

I. UVOD

1. V tej prilogi so določbe za izvajanje člena 8. Določa minimalne zahteve za fizično varovanje prostorov, zgradb, pisarn, sob in drugih območij, kjer poteka delo s tajnimi podatki EU in kjer se ti hranijo, vključno z območji, kjer so nameščeni komunikacijski in informacijski sistemi.

2. Namen ukrepov fizične varnosti je preprečiti nepooblaščen dostop do tajnih podatkov EU:

(a) z zagotovitvijo, da delo s tajnimi podatki EU poteka na ustrezen način in da se ti podatki ustrezno hranijo;

(b) z omogočanjem ločevanja osebja glede na njihov dostop do tajnih podatkov EU na podlagi načela potrebe po seznanitvi in, kjer je to ustrezno, glede na njihovo varnostno preverjenost;

(c) z odvračanjem, oviranjem in odkrivanjem nedovoljenih dejanj, in

(d) s preprečevanjem ali zadrževanjem skrivnih ali nasilnih vdorov vsiljivcev.

II. ZAHTEVE IN UKREPI GLEDE FIZIČNE VARNOSTI

3. Ukrepi fizične varnosti se izberejo na podlagi ocene nevarnosti, ki jo opravijo pristojni organi. GSS in države članice v svojih prostorih uporabljajo postopek obvladovanja tveganja za varovanje tajnih podatkov EU, s čimer se zagotovi, da je stopnja fizične varnosti sorazmerna ocenjenemu tveganju. V okviru postopka obvladovanja tveganja se upoštevajo vsi ustrezni dejavniki, zlasti:

(a) stopnja tajnosti tajnih podatkov EU;

(b) oblika in obseg tajnih podatkov EU, ob upoštevanju, da je treba zaradi velike količine ali zbirke tajnih podatkov EU morda uporabiti strožje ukrepe varovanja;

(c) okolico in strukturo zgradb ali območij, kjer so tajni podatki EU, in

(d) oceno nevarnosti, ki jo za EU ali države članice pomenijo obveščevalne službe, ter nevarnosti zaradi sabotaže, terorizma, uničevalnih ali drugih kriminalnih dejavnosti.

4. Pristojni varnostni organ na podlagi koncepta globinske obrambe določi ustrezno kombinacijo ukrepov fizične varnosti, ki naj bi se izvedli. Vključujejo lahko enega ali več od naslednjih ukrepov:

(a) pregrada varnostnega perimetra: fizična pregrada, ki varuje mejo območja, na katerem je potrebno varovanje;

(b) sistem odkrivanja vdorov (IDS): IDS se lahko uporablja za izboljšanje stopnje varovanja, ki jo nudi pregrada varnostnega perimetra, ali v sobah in zgradbah namesto varnostnega osebja ali v pomoč temu osebju;

(c) nadzor dostopa: nadzor dostopa se lahko izvaja na lokaciji, v zgradbi ali zgradbah na lokaciji ali na območjih ali v sobah v zgradbi. Nadzor se lahko izvaja z elektronskimi ali elektromehanskimi sredstvi, izvaja ga lahko varnostno osebje in/ali receptor ali pa se izvaja z drugimi fizičnimi sredstvi;

(d) varnostno osebje: tudi za odvračanje posameznikov, ki načrtujejo prikrit vdor, se lahko zaposli usposobljeno, nadzorovano in ustrezno varnostno preverjeno varnostno osebje;

(e) sistem televizije zaprtega kroga (CCTV): CCTV lahko varnostno osebje uporablja za preverjanje incidentov ter alarmov sistema odkrivanja vsiljivcev na obsežnih lokacijah ali v varnostnih perimetrih;

(f) varnostna razsvetljava: varnostna razsvetljava se lahko uporabi za odvračanje morebitnih vsiljivcev ter za zagotavljanje osvetlitve, ki jo za učinkovit nadzor neposredno potrebuje varnostno osebje ali posredno sistem CCTV, in

(g) vsi drugi ustrezni fizični ukrepi, s katerimi naj bi odvračali ali odkrivali nepooblaščen dostop ali preprečili izgubo ali poškodovanje tajnih podatkov EU.

5. Pristojni organ je lahko pooblaščen za preglede na vhodih in izhodih, kar naj bi odvračalo od nedovoljenega vnosa materiala v prostore ali zgradbe ali od nedovoljene odstranitve tajnih podatkov EU iz njih.

6. Če obstaja tveganje vpogleda v tajne podatke EU, tudi po naključju, se sprejmejo ustrezni ukrepi za preprečitev tega tveganja.

7. Za nove objekte se zahteve glede fizične varnosti in njihove funkcijske specifikacije določijo v sklopu načrtovanja in zasnove objektov. Pri obstoječih objektih se zahteve glede fizične varnosti izvajajo v največji možni meri.

III. OPREMA ZA FIZIČNO ZAŠČITO TAJNIH PODATKOV EU

8. Pri nabavi opreme (kot so blagajne, uničevalci papirja, vratne ključavnice, elektronski sistemi nadzora dostopa, sistemi odkrivanja vsiljivcev, alarmni sistemi) za fizično varovanje tajnih podatkov EU pristojni varnostni organ zagotovi, da oprema izpolnjuje potrjene tehnične standarde in minimalne zahteve.

9. Tehnične specifikacije opreme, ki se bo uporabljala za fizično varovanje tajnih podatkov EU, se določijo v varnostnih smernicah, ki jih odobri Varnostni odbor.

10. Varnosti sistemi se redno inšpekcijsko pregledujejo, oprema pa se redno vzdržuje. Vzdrževalna dela upoštevajo izid inšpekcijskih pregledov, da se zagotovi, da oprema še naprej deluje optimalno.

11. Učinkovitost posameznih varnostnih ukrepov in celotnega varnostnega sistema se med vsakim inšpekcijskim pregledom ponovno oceni.

IV. FIZIČNO ZAŠČITENA OBMOČJA

12. Za fizično zaščito tajnih podatkov EU se vzpostavi dvoje vrst fizično zaščitenih območij ali enakovredna območja na državni ravni:

(a) upravna območja; in

(b) varovana območja (vključno s tehnično varovanimi območji).

Vsako sklicevanje na upravna območja in varovana območja, vključno s tehnično varovanimi območji, v tem sklepu pomeni tudi sklicevanje na enakovredna območja na državni ravni.

13. Pristojni varnostni organ ugotovi, da območje izpolnjuje zahteve in ga je zato mogoče določiti za upravno območje, varovano območje ali tehnično varovano območje.

14. Na upravnih območjih:

(a) se vzpostavi vidno določen varnostni perimeter, ki omogoča preverjanje posameznikov in po možnosti vozil;

(b) se vstop brez spremstva odobri le posameznikom, ki jih je pristojni organ za to pravilno pooblastil, ter

(c) imajo vsi drugi posamezniki ves čas spremstvo ali so pod enakovrednim nadzorom.

15. Na varovanih območjih:

(a) se vzpostavi vidno določen in zaščiten varnostni perimeter, preko katerega se vsi vhodi in izhodi nadzorujejo z uporabo prepustnic ali s sistemom prepoznavanja oseb;

(b) vstop brez spremstva se odobri le posameznikom, ki so varnostno preverjeni in posebej pooblaščeni za vstop na območje na podlagi njihove potrebe po seznanitvi;

(c) imajo vsi drugi posamezniki ves čas spremstvo ali so pod enakovrednim nadzorom.

16. Če vstop na varovano območje praktično pomeni neposreden dostop do tajnih podatkov na tem območju, veljajo naslednje dodatne zahteve:

(a) najvišja stopnja tajnosti podatkov, ki so običajno na območju, mora biti jasno označena;

(b) vsi obiskovalci potrebujejo posebno dovoljenje za vstop na območje, imajo ves čas spremstvo in so ustrezno varnostno preverjeni, razen če je z ustreznimi ukrepi zagotovljeno, da dostop do tajnih podatkov EU ni mogoč.

17. Varovana območja, zaščitena pred prisluškovanjem, se določijo za tehnično varovana območja. Veljajo naslednje dodatne zahteve:

(a) ta območja so opremljena s sistemom odkrivanja vsiljivcev in, kadar v prostorih ni nikogar, zaklenjena, sicer pa varovana. Vsi ključi so pod nadzorom skladno z delom VI;

(b) vstop vseh oseb in vnos vsega materiala na ta območja se nadzoruje;

(c) ta območja se redno fizično in/ali tehnično inšpekcijsko pregledujejo, kakor to zahteva pristojni varnostni organ. Ti inšpekcijski pregledi se lahko izvajajo tudi po vsakem nepooblaščenem vstopu ali sumu takšnega vstopa, in

(d) na teh območjih ni nedovoljenih komunikacijskih vodov, nedovoljenih telefonov ali drugih nedovoljenih komunikacijskih naprav ter električne in elektronske opreme.

18. Ne glede na točko (d) odstavka 17 pristojni varnostni organ pred uporabo komunikacijskih naprav ter električne ali elektronske opreme na območjih, kjer potekajo sestanki ali se opravlja delo s podatki stopnje SECRET UE/EU SECRET in višje, ter je ocena nevarnosti za tajne podatke EU velika, to opremo najprej preveri, zato da zagotovi, da te naprave ne morejo nehoteno ali nezakonito prenašati uporabnih podatkov zunaj varnostnega perimetra varovanega območja.

19. Varovana območja, na katerih dežurno osebje ni prisotno 24 ur na dan, se, kjer je to ustrezno, inšpekcijsko pregledajo po zaključku običajnega delovnega časa in v naključnih presledkih pred ali po običajnem delovnem času, razen če ni nameščen sistem za odkrivanje vsiljivcev.

20. V upravnem območju se lahko zaradi tajnega sestanka ali za podobne namene začasno vzpostavijo varovana območja in tehnično varovana območja.

21. Za vsako varovano območje se oblikujejo varnostno-operativni postopki, ki določajo:

(a) stopnjo tajnih podatkov EU, s katerimi lahko poteka delo in se lahko hranijo v tem območju;

(b) uporabljene nadzorne in zaščitne ukrepe;

(c) posameznike, ki so zaradi svoje potrebe po seznanitvi in varnostne preverjenosti pooblaščeni za dostop na območje brez spremstva;

(d) kjer je to ustrezno, postopke v zvezi s spremljanjem ali postopke za varovanje tajnih podatkov EU, ko drugi posamezniki dobijo dovoljenje za dostop na območje;

(e) vse druge ustrezne ukrepe in postopke.

22. V varovanih območjih se zgradijo sobe-trezorji. Stene, tla, strope, okna in vrata, ki jih je mogoče zakleniti, odobri pristojni varnostni organ, zagotavljajo pa zaščito, enakovredno blagajni, odobreni za hrambo tajnih podatkov EU enake stopnje tajnosti.

V. FIZIČNI ZAŠČITNI UKREPI ZA DELO S TAJNIMI PODATKI EU IN NJIHOVO HRAMBO

23. Delo s tajnimi podatki stopnje RESTREINT UE/EU RESTRICTED lahko poteka:

(a) v varovanem območju;

(b) v upravnem območju, če so tajni podatki EU zaščiteni pred dostopom nepooblaščenih posameznikov, ali

(c) zunaj varovanega ali upravnega območja, če imetnik podatkov prenaša tajne podatke EU v skladu z odstavki 28 do 40 Priloge III in se je zavezal, da bo ravnal v skladu z nadomestnimi ukrepi iz varnostnih navodil pristojnega varnostnega organa, s čimer se zagotovi, da so tajni podatki EU zaščiteni pred dostopom nepooblaščenih oseb.

24. Tajni podatki EU stopnje RESTREINT UE/EU RESTRICTED se hranijo v ustrezno zaklenjenem pisarniškem pohištvu v upravnem območju ali v varovanem območju. Začasno se lahko hranijo zunaj varovanega ali upravnega območja, če se je imetnik podatkov zavezal, da bo ravnal v skladu z nadomestnimi ukrepi iz varnostnih navodil pristojnega varnostnega organa.

25. Delo s tajnimi podatki stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET lahko poteka:

(a) v varovanem območju;

(b) v upravnem območju, če so tajni podatki EU zaščiteni pred dostopom nepooblaščenih posameznikov, ali

(c) zunaj varovanega ali upravnega območja, če imetnik podatkov:

(i) prenaša tajne podatke EU v skladu z odstavki 28 do 40 Priloge III;

(ii) se je zavezal, da bo ravnal v skladu z nadomestnimi ukrepi iz varnostnih navodil pristojnega varnostnega organa, s čimer se zagotovi, da so tajni podatki EU varovani pred dostopom nepooblaščenih oseb, ter

(iii) ima tajne podatke EU ves čas pod osebnim nadzorom, ter

(iv) v primeru dokumentov na papirju o tem obvesti pristojni register.

26. Tajni podatki EU stopnje UE/EU CONFIDENTIAL in SECRET UE/EU SECRET se hranijo v varovanem območju v blagajni ali sobi-trezorju.

27. Delo s tajnimi podatki stopnje TRÈS SECRET UE/EU TOP SECRET poteka v varovanem območju.

28. Tajni podatki EU stopnje SECRET UE/EU TOP SECRET se hranijo v varovanem območju pod enim od naslednjih pogojev:

(a) v blagajni v skladu z odstavkom 8 z eno ali več vrstami dodatnega nadzora:

(i) neprekinjeno varovanje ali preverjanje, ki ga izvaja varnostno osebje ali dežurno osebje, ki je bilo ustrezno varnostno preverjeno;

(ii) odobren sistem odkrivanja vsiljivcev v kombinaciji z varnostnim osebjem za odzivanje;

ali

(b) v sobi-trezorju, opremljeni s sistemom odkrivanja vsiljivcev, v kombinaciji z varnostnim osebjem za odzivanje.

29. Pravila o prenašanju tajnih podatkov EU zunaj fizično varovanih območij so navedena v Prilogi III.

VI. NADZOR NAD KLJUČI IN KOMBINACIJAMI, KI SE UPORABLJAJO ZA VAROVANJE TAJNIH PODATKOV EU

30. Pristojni varnostni organ določi postopke za ravnanje s ključi in nastavitvami kombinacij za pisarne, sobe, sobe-trezorje in blagajne. Takšni postopki varujejo pred nepooblaščenim dostopom.

31. Nastavitve kombinacij si na pamet zapomni najmanjše možno število oseb, ki jih morajo poznati. Nastavitve kombinacij za blagajne in sobe-trezorje, kjer se hranijo tajni podatki EU, se spremenijo:

(a) vedno ko se zamenja osebje, ki pozna kombinacijo;

(b) ob vsakem nepooblaščenem razkritju ali sumu razkritja;

(c) ob vsakem vzdrževanju ali popravilu ključavnice; in

(d) najmanj vsakih 12 mesecev.

*PRILOGA III*

## UPRAVLJANJE TAJNIH PODATKOV

I. UVOD

1. V tej prilogi so določbe za izvajanje člena 9. V njej so določeni upravni ukrepi za nadzor nad tajnimi podatki EU ves čas njihovega življenjskega cikla, ki so namenjeni odvračanju, odkrivanju in obnovitvi takšnih podatkov po naključnem ali namernem nepooblaščenem razkritju ali izgubi.

II. STOPNJE TAJNOSTI

**Stopnje tajnosti in oznake**

2. Podatkom se stopnja tajnosti določi takrat, kadar jih je treba varovati zaradi njihove tajnosti.

3. Organ izvora tajnih podatkov EU je v skladu z ustreznimi smernicami za razvrstitev pristojen za določanje stopnje tajnosti in za začetno širjenje podatkov.

4. Stopnja tajnosti podatkov EU se določi v skladu s členom 2(2) in ob upoštevanju varnostne politike, ki se odobri v skladu s členom 3(3).

5. Stopnja tajnosti je jasno in pravilno označena, ne glede na to, ali so tajni podatki EU v pisni, ustni, elektronski ali kateri drugi obliki.

6. Posamezni deli nekega dokumenta (tj. strani, odstavki, oddelki, priloge, dodatki ter dodani in priloženi deli) so lahko različnih stopenj tajnosti in se jih ustrezno temu označi, tudi če se hranijo v elektronski obliki.

7. Splošna stopnja tajnosti dokumenta ali datoteke je vsaj tako visoka, kot del istega dokumenta z najvišjo stopnjo tajnosti. Če so podatki zbrani iz različnih virov, se končni izdelek pregleda zaradi dodelitve splošne stopnje tajnosti, saj mu bo morda treba določiti višjo stopnjo tajnosti kot jo imajo njegovi sestavni deli.

8. Dokumenti z deli, ki so označeni z različnimi stopnjami tajnosti, se, kolikor je to mogoče, oblikujejo tako, da je mogoče dele z različnimi stopnjami tajnosti brez težav najti in po potrebi izločiti.

9. Stopnja tajnosti pisma ali dopisa, ki se nanaša na priloge, je enaka najvišji stopnji tajnosti prilog. Organ izvora mora, če je tak dokument ločen od prilog, jasno navesti njegovo stopnjo tajnosti, in sicer z ustreznimi oznakami, npr.:

CONFIDENTIEL UE/EU CONFIDENTIAL

brez prilog(-e) RESTREINT UE/EU RESTRICTED

**Oznake**

10. Tajni podatki EU lahko poleg varnostnih oznak stopnje tajnosti iz člena 2(2) nosijo dodatne oznake, kot na primer:

(a) označba, ki določa organ izvora;

(b) kakršna koli opozorila, kode ali kratice za določitev področja dejavnosti, na katerega se nanaša dokument, ali za posebno razpošiljanje na podlagi potrebe po seznanitvi ali omejitve pri uporabi;

(c) oznake pogojev za dajanje tajnih podatkov;

(d) po potrebi datum ali določen dogodek, po katerem se lahko stopnja tajnosti zniža ali se tajnost prekliče.

**Okrajšane oznake stopnje tajnosti**

11. Standardizirane okrajšane oznake stopnje tajnosti se lahko uporabijo za navedbo stopnje tajnosti posameznih odstavkov besedila. Okrajšave ne nadomestijo popolnih oznak tajnosti.

12. Spodaj navedene standardizirane okrajšave se tako lahko uporabljajo v tajnih dokumentih EU za označevanje stopnje tajnosti delov ali segmentov besedila, krajših od ene strani:

| | |
|---|---|
| TRÈS SECRET UE/EU TOP SECRET | TS-UE/EU-TS |
| SECRET UE/EU SECRET | S-UE/EU-S |
| CONFIDENTIEL UE/EU CONFIDENTIAL | C-UE/EU-C |
| RESTREINT UE/EU RESTRICTED | R-UE/EU-R |

**Priprava tajnih podatkov EU**

13. Pri pripravi tajnega dokumenta EU:

(a) se vsaka stran jasno označi s stopnjo tajnosti;

(b) se vsaka stran oštevilči;

(c) dokument nosi opravilno številko in ime zadeve, ki pa sama po sebi nista tajni podatek, razen če ni tako označeno;

(d) se dokument datira;

(e) pri dokumentih stopnje SECRET UE/EU SECRET ali višje je treba na vsaki strani navesti številko kopije, če se razpošiljajo v več izvodih.

14. Če za tajne podatke EU ni mogoče uporabljati odstavka 13, se sprejmejo drugi ustrezni ukrepi v skladu z varnostnimi smernicami iz člena 6(2).

**Znižanje stopnje tajnosti in njen preklic za tajne podatke EU**

15. Organ izvora ob nastanku tajnih podatkov EU po možnosti in zlasti za podatke stopnje RESTREINT UE/EU RESTRICTED navede, ali se stopnja tajnosti lahko zniža ali prekliče na določen datum ali po določenem dogodku.

16. GSS redno pregleduje svoje tajne podatke EU, da bi ugotovil, ali je stopnja tajnosti še ustrezna. GSS vzpostavi sistem pregledovanja stopnje tajnosti vpisanih tajnih podatkov EU, ki jih je ustvaril, vsaj vsakih pet let. Takšen pregled ni potreben, če je organ izvora že na začetku navedel, da bo stopnja tajnosti podatkov samodejno znižana ali preklicana, in če je podatek temu ustrezno označen.

III. VPIS TAJNIH PODATKOV EU IZ VARNOSTNIH RAZLOGOV

17. Za vsak organizacijski subjekt v GSS in državnih upravah držav članic, v katerem poteka delo s tajnimi podatki EU, se določi pristojni register, ki zagotovi, da delo s tajnimi podatki EU poteka v skladu s tem sklepom. Registri se uredijo kot varovana območja, kakor so opredeljena v Prilogi II.

18. Za namene tega sklepa vpis iz varnostnih razlogov (v nadaljnjem besedilu: „vpis“) pomeni uporabo postopkov, ki evidentirajo življenjski cikel materiala, vključno z njegovim razširjanjem in uničenjem.

19. Ves material stopnje CONFIDENTIEL UE/EU CONFIDENTIAL in višje se ob prispetju v organizacijski subjekt ali pri odpošiljanju iz njega vpiše pri za to namenjenem registru.

20. Centralni register v GSS vodi evidenco vseh tajnih podatkov, ki jih Svet in GSS dasta tretjim državam in mednarodnim organizacijam, ter vseh tajnih podatkov, ki jih prejmeta od tretjih držav ali mednarodnih organizacij.

21. V primeru komunikacijskega in informacijskega sistema se vpisni postopki lahko opravijo v okviru procesov znotraj samega komunikacijskega in informacijskega sistema.

22. Svet odobri varnostno politiko glede vpisovanja tajnih podatkov EU iz varnostnih razlogov.

**Arhivski uradi za podatke stopnje TRÈS SECRET UE/EU TOP SECRET**

23. V državah članicah in GSS se določi register, ki deluje kot centralni organ za prejemanje in razpošiljanje podatkov stopnje tajnosti TRÈS SECRET UE/EU TOP SECRET. Po potrebi se lahko določijo podregistri, v katerih delajo s takšnimi podatki za potrebe vpisovanja.

24. Takšni podregistri ne smejo pošiljati dokumentov TRÈS SECRET UE/EU TOP SECRET neposredno drugim podregistrom v sklopu istega centralnega registra za podatke stopnje TRÈS SECRET UE/EU TOP SECRET ali zunaj njega brez njegovega izrecnega pisnega dovoljenja.

IV. KOPIRANJE IN PREVAJANJE TAJNIH DOKUMENTOV EU

25. Dokumenti stopnje TRÈS SECRET UE/EU TOP SECRET se lahko kopirajo ali prevajajo le s predhodnim pisnim soglasjem organa izvora.

26. Če organ izvora dokumentov stopnje SECRET UE/EU SECRET in nižje ni navedel opozoril glede kopiranja ali prevajanja, se lahko po navodilu imetnika takšni dokumenti kopirajo ali prevajajo.

27. Varnostni ukrepi, ki veljajo za izvorni dokument, veljajo tudi za njegove kopije in prevode.

V. PRENAŠANJE TAJNIH PODATKOV EU

28. Za prenašanje tajnih podatkov EU veljajo varnostni ukrepi iz odstavkov 30 do 40. Pri prenašanju tajnih podatkov EU na elektronskih medijih se ukrepi varovanja, navedeni v nadaljevanju, ne glede na člen 9(4) lahko dopolnijo z ustreznimi tehničnimi protiukrepi, ki jih predpiše pristojni varnostni organ, tako da se čim bolj zmanjša nevarnost izgube ali nepooblaščenega razkritja.

29. Pristojni varnostni organi v GSS in državah članicah izdajo navodila za prenašanje tajnih podatkov EU v skladu s tem sklepom.

**Znotraj zgradbe ali samostojne skupine zgradb**

30. Tajni podatki EU, ki se prenašajo znotraj zgradbe ali samostojne skupine zgradb, se zakrijejo zaradi preprečitve razkritja njihove vsebine.

31. Znotraj zgradbe ali samostojne skupine zgradb se tajni podatki stopnje TRÈS SECRET UE/EU TOP SECRET prenašajo v zaščitenih ovojnicah, na katerih je samo ime naslovnika.

**Znotraj EU**

32. Tajni podatki EU, ki se prenašajo med zgradbami ali prostori v EU, so pakirani tako, da so zaščiteni pred nepooblaščenim razkritjem.

33. Prenašanje podatkov do stopnje SECRET UE/EU SECRET znotraj EU poteka na enega izmed naslednjih načinov:

(a) po vojaškem, vladnem ali diplomatskem kurirju, kakor je ustrezno;

(b) ročno, pod pogojem da:

(i) se tajni podatki EU ne dajo iz rok prenašalca, razen če se hranijo v skladu z zahtevami iz Priloge II;

(ii) se tajni podatki EU ne odprejo na poti ali berejo na javnih mestih;

(iii) so posamezniki poučeni o svoji odgovornosti v zvezi z varovanjem tajnosti;

(iv) se posameznikom po potrebi zagotovi kurirsko potrdilo;

(c) z uporabo poštnih služb ali komercialnih kurirskih služb, če:

(i) jih je odobril nacionalni varnostni organ v skladu z nacionalnimi zakoni in predpisi;

(ii) uporabljajo ustrezne ukrepe varovanja v skladu z minimalnimi zahtevami, ki se določijo v varnostnih smernicah iz člena 6(2).

V primeru prenosa iz ene države članice v drugo se določbe iz točke (c) omejijo na podatke do stopnje CONFIDENTIEL UE/EU CONFIDENTIAL.

34. Material stopnje CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET (npr. oprema ali stroji), ki se ne more prenašati na načine iz odstavka 33, kot tovor prepeljejo komercialne prevozne družbe v skladu s Prilogo V.

35. Podatki stopnje TRÈS SECRET UE/EU TOP SECRET se med zgradbami ali prostori v EU prenašajo po vojaškem, vladnem ali diplomatskem kurirju, kakor je ustrezno.

**Iz EU na ozemlje tretje države**

36. Tajni podatki EU, ki se prenašajo iz EU na ozemlje tretje države, so pakirani tako, da so zaščiteni pred nepooblaščenim razkritjem.

37. Prenašanje podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET iz EU na ozemlje tretje države poteka na enega izmed naslednjih načinov:

(a) po vojaškem ali diplomatskem kurirju;

(b) ročno, pod pogojem da:

(i) je na paketu uradna plomba ali je pakiran tako, da nakazuje, da gre za uradno pošiljko, ki ne gre skozi carinski in varnostni pregled;

(ii) imajo posamezniki pri sebi kurirsko potrdilo, ki opredeljuje paket in jih pooblašča za njegov prenos;

(iii) se tajni podatki EU ne dajo iz rok prenašalca, razen če se hranijo v skladu z zahtevami iz Priloge II;

(iv) se tajni podatki EU ne odprejo na poti ali berejo na javnih mestih; in

(v) so posamezniki poučeni o svoji odgovornosti v zvezi z varovanjem tajnosti.

38. Pri prenosu podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET, ki jih EU da tretji državi ali mednarodni organizaciji, se upoštevajo ustrezne določbe iz sporazuma o varovanju tajnosti podatkov ali dogovora o izvajanju v skladu s členom 12(2)(a) ali (b).

39. Podatki stopnje RESTREINT UE/EU RESTRICTED se lahko prenašajo tudi prek poštnih služb ali komercialnih kurirskih služb.

40. Podatki stopnje TRÈS SECRET UE/EU TOP SECRET se iz EU na ozemlje tretje države prenašajo po vojaškem ali diplomatskem kurirju.

VI. UNIČENJE TAJNIH PODATKOV EU

41. Tajni dokumenti EU, ki niso več potrebni, se lahko uničijo, brez poseganja v ustrezna pravila in predpise o arhiviranju.

42. Dokumente, ki se vpisujejo v skladu s členom 9(2), po navodilu imetnika tajnih podatkov ali pristojnega organa uniči pristojni register. Vpisniki in drugi podatki o vpisu se ustrezno posodobijo.

43. Dokumenti stopnje SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET se uničijo v prisotnosti priče, ki je varnostno preverjena vsaj do stopnje tajnosti dokumenta, ki se uničuje.

44. Uradnik registra in priča, če je njena navzočnost obvezna, podpišeta potrdilo o uničenju, ki se shrani v registru. Register potrdila o uničenju dokumentov stopnje TRÈS SECRET UE/EU TOP SECRET hrani vsaj deset let, potrdila o uničenju dokumentov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET pa vsaj pet let.

45. Tajni dokumenti, vključno z dokumenti stopnje RESTREINT UE/EU RESTRICTED, se uničijo po metodah, ki so skladne z ustreznimi EU ali enakovrednimi standardi ali so jih odobrile države članice v skladu z nacionalnimi tehničnimi standardi, da se prepreči popolna ali delna obnova.

46. Uničenje računalniških shranjevalnih nosilcev, ki se uporabljajo za tajne podatke EU, poteka v skladu z odstavkom 36 Priloge IV.

VII. INŠPEKCIJSKI PREGLEDI IN OCENJEVALNI OBISKI

47. Izraz „inšpekcijski pregled“ v nadaljevanju pomeni:

(a) inšpekcijo v skladu s členom 9(3) ter členom 15(2)(e), (f) in (g); ali

(b) ocenjevalni obisk v skladu s členom 12(5),

s katerimi se ovrednoti učinkovitost ukrepov, ki se izvajajo za varovanje tajnih podatkov EU.

48. Namen inšpekcijskih pregledov je, med drugim,:

(a) zagotoviti spoštovanje zahtevanih minimalnih standardov za varovanje tajnih podatkov EU, določenih v tem sklepu;

(b) izpostaviti pomen varnosti in učinkovitega obvladovanja tveganja v subjektih, kjer poteka inšpekcijski pregled;

(c) priporočiti protiukrepe za blažitev specifičnih posledic izgube zaupnosti, celovitosti ali razpoložljivosti tajnih podatkov; ter

(d) okrepiti izobraževalne programe in programe osveščanja v teku, ki jih izvajajo varnostni organi.

49. Pred koncem vsakega koledarskega leta Svet sprejme program inšpekcijskih pregledov iz točke (c) člena 15(1) za naslednje leto. Dejanski datum vsakega inšpekcijskega pregleda se določi v dogovoru z zadevno agencijo ali organom EU, državo članico, tretjo državo ali mednarodno organizacijo.

**Izvajanje inšpekcijskih pregledov**

50. Z inšpekcijskimi pregledi se pri subjektu preverijo ustrezna pravila, predpisi in postopki, preveri se tudi, ali prakse subjekta ustrezajo temeljnim načelom in minimalnim standardom iz tega sklepa in določbam o izmenjavi tajnih podatkov s tem subjektom.

51. Inšpekcijski pregledi se izvajajo v dveh fazah. Pred samim inšpekcijskim pregledom se po potrebi organizira pripravljalni sestanek z zadevnim subjektom, nato pa inšpekcijska ekipa v dogovoru z zadevnim subjektom pripravi podroben program inšpekcije, ki zajema vsa področja varovanja tajnosti. Inšpekcijska ekipa ima dostop do vseh lokacij, kjer poteka delo s tajnimi podatki EU, še zlasti pa do registrov in dostopovnih vozlišč KIS.

52. Izvajanje inšpekcijskih pregledov v državnih upravah držav članic poteka v pristojnosti skupne inšpekcijske ekipe GSS/Komisije, pri čemer sodelujejo tudi uradniki subjekta, v katerem se inšpekcijski pregled izvaja.

53. Izvajanje inšpekcijskih pregledov v tretjih državah in mednarodnih organizacijah poteka v pristojnosti skupne inšpekcijske ekipe GSS/Komisije, pri čemer sodelujejo tudi uradniki tretje države ali mednarodne organizacije, v kateri se inšpekcijski pregled izvaja.

54. Inšpekcijske preglede agencij in organov EU ustanovljenih v skladu z naslovom V, poglavjem 2 PEU, kakor tudi Europola in Eurojusta, opravi Varnostni urad GSS s pomočjo strokovnjakov nacionalnega varnostnega organa države, na ozemlju katere je agencija ali organ. Varnostni direktorat Evropske komisije (ECSD) se lahko vključi, če z zadevno agencijo ali organom redno izmenjuje tajne podatke EU.

55. V primeru inšpekcijskih pregledov v agencijah in organih EU, ustanovljenih v skladu z naslovom V, poglavjem 2 PEU, kakor tudi Europola in Eurojusta, ter tretjih državah in mednarodnih organizacijah se zahtevajo pomoč in prispevki strokovnjakov nacionalnega varnostnega organa v skladu z natančnimi načrti, o katerih se dogovori Varnostni odbor.

**Poročila o inšpekcijskih pregledih**

56. Ob koncu inšpekcijskega pregleda se pregledanemu subjektu predložijo glavni zaključki in priporočila. Nato se pripravi poročilo o inšpekcijskem pregledu v pristojnosti Varnostnega organa GSS (Varnostnega urada). Če so bili predlagani korektivni ukrepi in priporočila, se v poročilo vključi dovolj podrobnosti, da je mogoče dosežene zaključke utemeljiti. Poročilo se pošlje ustreznemu organu pregledanega subjekta.

57. Pri inšpekcijskih pregledih, opravljenih v državnih upravah držav članic:

(a) se osnutek poročila o inšpekcijskem pregledu pošlje zadevnemu nacionalnemu varnostnemu organu, ki preveri, da so dejstva v njem pravilna in da ne vsebuje podatkov višje stopnje od RESTREINT UE/EU RESTRICTED;

(b) razen če nacionalni varnostni organ zadevne države članice ne prepove splošnega razpošiljanja, se poročila o inšpekcijskih pregledih pošljejo članom Varnostnega odbora in Varnostnemu direktoratu Evropske komisije; stopnja tajnosti poročila je RESTREINT UE/EU RESTRICTED.

V pristojnosti Varnostnega organa GSS (Varnostnega urada) se pripravi redno poročilo, v katerem se poudarijo dognanja inšpekcijskih pregledov, opravljenih v določenem obdobju v državah članicah; Varnostni odbor to poročilo preuči.

58. Poročila o ocenjevalnih obiskih tretjih držav in mednarodnih organizacij se pošljejo Varnostnemu odboru in Varnostnemu direktoratu Evropske komisije. Stopnja tajnosti poročila je vsaj RESTREINT UE/EU RESTRICTED. Ob naslednjem obisku se preverijo vsi korektivni ukrepi; o njih se poroča varnostnemu odboru.

59. Poročila o inšpekcijskih pregledih agencij in organov EU ustanovljenih v skladu z naslovom V, poglavjem 2 PEU, kakor tudi Europola in Eurojusta, se pošljejo članom Varnostnega odbora in Varnostnemu direktoratu Evropske komisije. Osnutek poročila o inšpekcijskem pregledu se pošlje zadevni agenciji ali organu, da preveri, ali so dejstva v njem pravilna in ne vsebuje podatkov višje stopnje od RESTREINT UE/EU RESTRICTED. Ob naslednjem obisku se preverijo vsi korektivni ukrepi; o njih se poroča Varnostnemu odboru.

60. Varnostni organ GSS izvaja redne inšpekcijske preglede organizacijskih subjektov v GSS za namene iz odstavka 48.

**Inšpekcijski kontrolni seznam**

61. Varnostni organ GSS (Varnostni urad) pripravi in posodablja inšpekcijski kontrolni seznam točk, ki jih je treba preveriti med inšpekcijskim pregledom. Ta kontrolni seznam se pošlje Varnostnemu odboru.

62. Informacije za izpolnitev kontrolnega seznama se pridobijo zlasti med inšpekcijskim pregledom pri osebju za upravljanje varovanja tajnosti subjekta, v katerem se izvaja inšpekcijski pregled. Ko je kontrolni seznam izpolnjen s podrobnimi odgovori, se mu v dogovoru s pregledanim subjektom določi stopnja tajnosti. Ni del poročila o inšpekcijskem pregledu.

*PRILOGA IV*

## VAROVANJE TAJNIH PODATKOV EU, S KATERIMI POTEKA DELO V KOMUNIKACIJSKIH IN INFORMACIJSKIH SISTEMIH

I. UVOD

1. V tej prilogi so določbe za izvajanje člena 10.

2. Za varovanje tajnosti in pravilno delovanje operacij v komunikacijskih in informacijskih sistemih so ključne naslednje lastnosti in pojmi v zvezi z zagotavljanjem informacijske varnosti:

avtentičnost: zagotovilo, da so podatki pravi in iz zaupanja vrednih virov;

razpoložljivost: podatki so dostopni ter na voljo za uporabo na zahtevo pooblaščenega subjekta;

tajnost: podatki se ne razkrijejo nepooblaščenim posameznikom in subjektom ali ne uporabijo v postopkih, kjer to ni dovoljeno;

celovitost: zagotavljanje točnosti in popolnosti podatkov in sestavnih delov;

nezatajljivost: zmožnost dokazati, da se je dejanje zgodilo ali da je prišlo do dogodka, tako da tega kasneje ni mogoče zanikati.

II. NAČELA ZA ZAGOTAVLJANJE INFORMACIJSKE VARNOSTI

3. Določbe v nadaljevanju predstavljajo osnovo za varovanje vseh KIS, v katerih poteka delo s tajnimi podatki EU. Natančne zahteve za izvajanje teh določb so opredeljene v politikah o zagotavljanju informacijske varnosti in varnostnih smernicah.

**Obvladovanje varnostnega tveganja**

4. Obvladovanje varnostnega tveganja je sestavni del določanja, razvijanja, delovanja in vzdrževanja KIS. Postopek obvladovanja tveganja (ocena, obravnava, sprejemanje in obveščanje) kot ponavljajoč se postopek skupaj izvajajo predstavniki lastnikov sistema, projektni organi, operativni organi in varnostni organi za odobritev, ki uporabljajo preverjen, pregleden ter popolnoma razumljiv postopek ocene tveganja. Področje uporabe KIS ter njegovih sestavnih delov je jasno določeno na začetku izvajanja postopka za obvladovanje tveganja.

5. Pristojni organi preučijo morebitne nevarnosti za KIS in poskrbijo za posodobljene in natančne ocene nevarnosti, ki odražajo trenutno operativno okolje. Stalno posodabljajo znanje o vprašanjih glede izpostavljenosti in redno pregledujejo ocene ranljivih točk ter tako sledijo spremembam na področju informacijske tehnologije (IT).

6. Namen obravnave varnostnega tveganja je uporabiti sklop varnostnih ukrepov, s čimer se doseže zadovoljivo ravnovesje med zahtevami uporabnikov, stroški in preostalim varnostnim tveganjem.

7. Konkretne zahteve, obseg in stopnja natančnosti, ki jih za akreditacijo KIS določi pristojni organ za varnostno akreditacijo, morajo biti sorazmerni z ocenjenim tveganjem ob upoštevanju vseh pomembnih dejavnikov, med drugim stopnje tajnosti podatkov EU v KIS. Akreditacija vključuje uradno izjavo pristojnega organa o preostalem tveganju in sprejemanju tega tveganja.

**Varnost ves čas življenjskega cikla KIS**

8. Zagotovitev varnosti je ena od zahtev, ki velja ves čas življenjskega cikla KIS od njegove uvedbe do prenehanja delovanja.

9. Za vsako fazo življenjskega cikla KIS se določita vloga in interakcija, ki jo ima v zvezi z varnostjo sistema vsak akter, ki je vanj vključen.

10. KIS, vključno s tehničnimi in netehničnimi varnostnimi ukrepi, se v okviru akreditacijskega postopka varnostno preskušajo, da se zagotovi ustrezna stopnja jamstva in preveri, ali se pravilno izvajajo, ter ali so pravilno integrirani in konfigurirani.

11. Varnostne ocene, inšpekcijski pregledi in pregledi se med obratovanjem KIS in v času njegovega vzdrževanja izvajajo v rednih časovnih presledkih, pa tudi v izjemnih okoliščinah.

12. Varnostna dokumentacija za KIS se razvija ves čas njegovega življenjskega cikla v sklopu spreminjanja in upravljanja konfiguracije.

**Najboljša praksa**

13. GSS in države članice sodelujejo pri oblikovanju najboljših praks za varovanje tajnih podatkov EU, s katerimi poteka delo v KIS. Smernice glede najboljših praks določajo tehnične, fizične, organizacijske in postopkovne varnostne ukrepe za KIS, katerih učinkovitost pri preprečevanju določenih nevarnosti in ranljivih točk je dokazana.

14. K varovanju tajnih podatkov EU, s katerimi poteka delo v KIS, prispevajo tudi izkušnje subjektov, ki delujejo na področju zagotavljanja informacijske varnosti v EU in drugod.

15. Razširjanje najboljše prakse in nato njeno izvajanje prispeva k doseganju enakovredne ravni jamstva pri različnih KIS, s katerimi upravljajo GSS in države članice, ki delajo s tajnimi podatki EU.

**Globinska obramba**

16. Za ublažitev tveganja za KIS se izvaja vrsta tehničnih in netehničnih varnostnih ukrepov, ki so organizirani kot večplastna obramba. Te plasti zajemajo:

(a) *odvračanje:* varnostni ukrepi za odvrnitev od načrtovanja sovražnih napadov na KIS;

(b) *preprečevanje:* varnostni ukrepi za oviranje ali zaustavitev napadov na KIS;

(c) *odkrivanje:* varnostni ukrepi za odkrivanje napadov na KIS;

(d) *odpornost:* varnostni ukrepi za omejitev učinka napadov na najmanjši možen sklop podatkov ali sestavnih delov KIS ter preprečevanje nadaljnje škode ter

(e) *ponovna vzpostavitev:* varnostni ukrepi za ponovno vzpostavitev varnosti v okviru KIS.

Stopnja strogosti takšnih varnostnih ukrepov se določi po oceni tveganja.

17. Pristojni organi zagotovijo, da se lahko odzovejo na incidente, ki lahko presegajo organizacijske in državne meje, da bi uskladili odzive in izmenjavo informacij o teh dogodkih in z njimi povezanih tveganjih (zmogljivosti odzivanja na izredne razmere na področju informatike).

**Načelo minimalnosti in najmanjšega privilegija**

18. Izvajajo se le ključne funkcionalnosti, naprave in storitve, potrebne za obratovanje, da ni izpostavljanja nepotrebnim tveganjem.

19. Uporabniki KIS ter avtomatizirani postopki dobijo le takšen dostop, privilegije in pooblastila, ki jih potrebujejo za opravljanje svojih nalog, da se omeji škoda, ki bi nastala zaradi nesreč, napak ali nepooblaščene uporabe virov KIS.

20. Vpisni postopki, ki se po potrebi opravijo v KIS, se preverijo kot del postopka akreditacije.

**Osveščenost o zagotavljanju informacijske varnosti**

21. Za varnost KIS je v prvi vrsti pomembno poznavanje tveganj in razpoložljivih varnostnih ukrepov. Zlasti vsi člani osebja, vključeni v življenjski cikel KIS, vključno z uporabniki, se morajo zavedati:

(a) da lahko kršitve varnosti povzročijo znatno škodo v KIS;

(b) morebitne škode za druge, ki lahko nastane zaradi medsebojne povezanosti in soodvisnosti, ter

(c) svojih individualnih obveznosti in odgovornosti v zvezi z varnostjo KIS glede na vlogo, ki jo imajo v sistemih in postopkih.

22. Da bi zagotovili ustrezno razumevanje odgovornosti glede varovanja tajnosti, mora biti izobraževanje o informacijski varnosti in usposabljanje za krepitev osveščenosti obvezno za vse ustrezno osebje, vključno z višjim vodstvom in uporabniki KIS.

**Ocena in odobritev varnostnih izdelkov IT**

23. Potrebna stopnja zaupanja v varnostne ukrepe, opredeljena kot stopnja jamstva, se določi glede na rezultat postopka obvladovanja tveganja in v skladu z ustreznimi varnostnimi politikami in varnostnimi smernicami.

24. Stopnja jamstva se preveri z mednarodno priznanimi postopki in metodologijami ali postopki in metodologijami, ki so odobreni na nacionalni ravni. To so predvsem ocena, nadzor in presoja.

25. Šifrirne izdelke za varovanje tajnih podatkov EU oceni in odobri nacionalni organ države članice za odobritev šifrirnih metod in izdelkov (CAA).

26. Preden se v skladu s členom 10(6) takšni šifrirni izdelki priporočijo v odobritev Svetu in/ali generalnemu sekretarju, jih mora pozitivno oceniti še drug ustrezno usposobljen organ države članice (AQUA ), ki ni vključen v načrtovanje ali izdelovanje opreme. Kako natančna mora biti druga ocena, je odvisno od predvidene najvišje stopnje tajnosti tajnih podatkov EU, ki naj bi jih s temi izdelki varovali. Varnostno politiko glede ocene in odobritve šifrirnih izdelkov odobri Svet.

27. Svet oziroma generalni sekretar lahko na priporočilo Varnostnega odbora zaradi posebnih operativnih razlogov opusti zahtevo iz odstavka 25 ali 26 in za določen čas izda odobritev v skladu s postopkom iz člena 10(6).

28. Ustrezno usposobljen organ je organ države članice za odobritev šifrirnih metod in izdelkov, ki je bil za izvedbo druge ocene šifrirnih izdelkov za varovanje tajnih podatkov EU akreditiran na podlagi meril, ki jih je določil Svet.

29. Svet odobri varnostno politiko glede ustreznosti in odobritve nešifrirnih varnostnih izdelkov IT.

**Prenos v varovanih območjih**

30. Ne glede na določbe tega sklepa se v primerih, ko je prenos tajnih podatkov EU omejen na varovana območja, lahko uporabi nešifrirano pošiljanje ali šifriranje na nižji stopnji, in sicer na podlagi rezultata postopka obvladovanja tveganja in odobritve organa za varnostno akreditacijo.

**Varne medsebojne povezave KIS**

31. V tem sklepu medsebojna povezanost sistemov pomeni neposredno povezavo dveh ali več sistemov IT za namen izmenjave podatkov in drugih informacijskih virov (npr. komunikacija) v eni ali več smereh.

32. KIS vsak sistem IT, povezan z njim, samodejno obravnava kot nezanesljiv in izvede ukrepe varovanja, s katerimi nadzoruje izmenjavo tajnih podatkov.

33. Povezave KIS z drugim sistemom IT ustrezajo naslednjim osnovnim zahtevam:

(a) pristojni organi določijo in odobrijo poslovne ali operativne zahteve za takšne povezane sisteme;

(b) za povezane sisteme se izvedeta postopek obvladovanja tveganja in akreditacijski postopek, odobriti pa jih morajo pristojni organi za varnostno akreditacijo, ter

(c) na varnostnem perimetru vseh KIS se izvajajo storitve v zvezi z zaščito razmejitve (BPS).

34. Akreditiran KIS ter nezavarovano ali javno omrežje ne smeta biti med seboj povezana, razen če ima KIS v ta namen med KIS ter nezavarovanim ali javnim omrežjem nameščene odobrene storitve v zvezi z zaščito razmejitve. Varnostne ukrepe za takšne medsebojne povezave pregleda pristojni organ za zagotavljanje informacijske varnosti, odobri pa jih pristojni organ za varnostno akreditacijo.

Če se nezaščiteno ali javno omrežje uporablja izključno za prenos in so podatki šifrirani s šifrirnim izdelkom, odobrenim v skladu s členom 10, se takšna povezava ne šteje za medsebojno povezavo.

35. Neposredna ali kaskadna medsebojna povezava KIS, akreditiranega za delo s podatki stopnje TRÈS SECRET UE/EU TOP SECRET, z nezavarovanim ali javnim omrežjem, je prepovedana.

**Računalniški nosilci podatkov**

36. Računalniški nosilci podatkov se uničijo v skladu s postopki, ki jih odobri pristojni varnostni organ.

37. Računalniški nosilci podatkov se lahko ponovno uporabijo, stopnja njihove tajnosti pa se lahko zniža ali prekliče v skladu z varnostno politiko iz člena 6(1).

**Izredne razmere**

38. Ne glede na določbe tega sklepa se posebni postopki, opisani v nadaljevanju, lahko uporabijo v izrednih razmerah, kot na primer v času preteče ali dejanske krize, spopada, vojnih razmer ali v izjemnih operativnih okoliščinah.

39. Tajni podatki EU se lahko razpošiljajo z uporabo šifrirnih izdelkov, ki so bili odobreni za nižjo stopnjo tajnosti, ali brez šifriranja s soglasjem pristojnega organa, če bi kakršna koli zamuda povzročila škodo, ki bi bila nedvomno večja od škode zaradi razkritja tajnega materiala, in če:

(a) pošiljatelj in prejemnik nimata potrebnih naprav za šifriranje ali nimata nobenih takih naprav; in

(b) tajnega materiala ni mogoče pravočasno poslati na drug način.

40. Tajni podatki, preneseni pod pogoji iz odstavka 38, nimajo nikakršnih oznak ali navedb, na podlagi katerih bi jih bilo mogoče ločiti od podatkov, ki niso tajni ali ki se lahko zaščitijo z razpoložljivim šifrirnim izdelkom. Prejemniki so o stopnji tajnosti nemudoma obveščeni, vendar na drugačen način.

41. Če se uporabi odstavek 38, se pristojnemu organu in Varnostnemu odboru naknadno pošlje poročilo.

III. FUNKCIJE IN ORGANI ZA ZAGOTAVLJANJE INFORMACIJSKE VARNOSTI

42. V državah članicah in GSS se določijo naslednje funkcije na področju zagotavljanja informacijske varnosti. Te funkcije ne potrebujejo enotnih organizacijskih subjektov. Imajo ločene naloge. Vendar se lahko te funkcije in odgovornosti združujejo ali vključujejo v isti organizacijski subjekt ali porazdeljujejo po različnih organizacijskih subjektih pod pogojem, da ne pride do notranjih nasprotij interesov ali nalog.

**Organ za zagotavljanje informacijske varnosti**

43. Organ za zagotavljanje informacijske varnosti je odgovoren za:

(a) razvijanje varnostnih politik in varnostnih smernic za zagotavljanje informacijske varnosti ter spremljanje njihove učinkovitosti in ustreznosti;

(b) varovanje tehničnih informacij, povezanih s šifrirnimi izdelki, ter ravnanje z njimi;

(c) zagotavljanje, da so ukrepi za zagotavljanje informacijske varnosti, izbrani za varovanje tajnih podatkov EU, v skladu z ustreznimi politikami, ki določajo njihovo upravičenost in urejajo njihov izbor;

(d) zagotavljanje, da so šifrirni izdelki izbrani v skladu s politikami, ki določajo njihovo upravičenost in urejajo njihov izbor;

(e) usklajevanje usposabljanja in osveščenosti o zagotavljanju varnosti podatkov;

(f) posvetovanje s ponudnikom sistema, akterji na področju varovanja tajnosti in predstavniki uporabnikov glede varnostnih politik in varnostnih smernic za zagotavljanje informacijske varnosti, in

(g) zagotavljanje razpoložljivosti ustreznega strokovnega znanja v strokovnem podpodročju Varnostnega odbora za vprašanja zagotavljanja informacijske varnosti.

**Organ TEMPEST**

44. Organ TEMPEST (TA) je pristojen za zagotavljanje, da KIS ustreza politikam in smernicam TEMPEST. Organ odobri protiukrepe TEMPEST za namestitev in izdelke za varovanje tajnih podatkov EU do določene stopnje tajnosti v njegovem operativnem okolju.

**Organ za odobritev šifrirnih metod in izdelkov**

45. Organ za odobritev šifrirnih metod in izdelkov (CAA) zagotavlja, da šifrirni izdelki ustrezajo nacionalni šifrirni politiki oziroma šifrirni politiki Sveta. Šifrirni izdelek odobri za varovanje tajnih podatkov EU do določene stopnje tajnosti v njegovem operativnem okolju. V državah članicah je organ za odobritev šifrirnih metod in izdelkov poleg tega pristojen za ocenjevanje šifrirnih izdelkov.

**Organ za razpošiljanje šifrirnega materiala**

46. Organ za razpošiljanje šifrirnega materiala (CDA) je odgovoren za:

(a) upravljanje šifrirnega materiala EU ter vodenje evidenc o tem materialu;

(b) zagotavljanje, da se uporabljajo ustrezni postopki in da so vzpostavljeni ustrezni mehanizmi za vodenje evidenc, varno delo z vsem šifrirnim materialom EU, shranjevanje in razpošiljanje tega materiala, in

(c) zagotavljanje prenosa šifrirnega materiala EU do in od posameznikov ali služb, ki ga uporabljajo.

**Organ za varnostno akreditacijo**

47. Organ za varnostno akreditacijo (SAA) za vsak sistem je odgovoren za:

(a) zagotavljanje, da je KIS v skladu z ustreznimi varnostnimi politikami in varnostnimi smernicami, dajanje izjave o odobritvi KIS za delo s tajnimi podatki EU do določene stopnje tajnosti v njegovem operativnem okolju, navajanje pogojev za akreditacijo in meril, v skladu s katerimi je potrebna ponovna odobritev;

(b) vzpostavitev postopka varnostne akreditacije v skladu z ustreznimi politikami, pri čemer jasno določi pogoje za odobritev KIS v svoji pristojnosti;

(c) določitev strategije za varnostno akreditacijo, ki določa stopnjo natančnosti za akreditacijski postopek, ki ustreza zahtevani stopnji jamstva;

(d) pregledovanje in odobritev dokumentacije, povezane z varovanjem tajnosti, tudi izjav o obvladovanju tveganja in preostalem tveganju, izjav o posebnih varnostnih zahtevah, značilnih za sistem (SSRS), dokumentacije o preverjanju varovanja tajnosti in varnostno-operativnih postopkov (SecOPs), ter zagotavljanje, da je skladna z varnostnimi pravili in politikami Sveta;

(e) preverjanje izvajanja varnostnih ukrepov v zvezi s KIS z izvedbo ali naročilom varnostnih ocen, inšpekcijskih pregledov ali pregledov;

(f) določitev varnostnih zahtev (npr. stopnje varnostnega preverjanja osebja) za občutljiva delovna mesta, povezana s KIS;

(g) potrditev izbora odobrenih šifrirnih izdelkov in izdelkov TEMPEST, ki se uporabljajo za zagotovitev varnosti KIS;

(h) odobritev medsebojne povezave KIS z drugimi KIS ali, kjer je to ustrezno, sodelovanje pri skupni odobritvi; in

(i) posvetovanje s ponudnikom sistema, akterji na področju varovanja tajnosti in predstavniki uporabnikov o obvladovanju varnostnega tveganja, zlasti preostalega tveganja, in pogojih za izjavo o odobritvi.

48. Organ za varnostno akreditacijo GSS je odgovoren za akreditiranje vseh KIS, ki delujejo v pristojnosti GSS.

49. Pristojni organ za varnostno akreditacijo države članice je odgovoren za akreditiranje KIS in komponent teh sistemov, ki delujejo v pristojnosti države članice.

50. Skupni odbor za varnostno akreditacijo je odgovoren za akreditacijo KIS, ki so v pristojnosti organa GSS za varnostno akreditacijo in organov držav članic za varnostno akreditacijo. Sestavljajo ga po en predstavnik organa za varnostno akreditacijo iz vsake države članice, v njem pa sodeluje tudi predstavnik organa za varnostno akreditacijo Komisije. K sodelovanju se povabijo tudi drugi subjekti z vozlišči na KIS, če se razpravlja o tem sistemu.

Odboru za varnostno akreditacijo predseduje predstavnik organa za varnostno akreditacijo GSS. Odločitve sprejema v soglasju s predstavniki organov za varnostno akreditacijo institucij, držav članic in drugih subjektov z vozlišči na zadevnem KIS. O svojih dejavnostih redno poroča Varnostnemu odboru in ga obvesti o vseh izjavah o akreditaciji.

**Operativni organ za zagotavljanje informacijske varnosti**

51. Operativni organ za zagotavljanje informacijske varnosti za vsak sistem je odgovoren za:

(a) pripravo varnostne dokumentacije v skladu z varnostnimi politikami in varnostnimi smernicami, zlasti izjav o posebnih varnostnih zahtevah sistema, vključno z izjavo o preostalem tveganju, varnostno-operativnimi postopki in načrtom za šifriranje v okviru postopku akreditacije KIS;

(b) sodelovanje pri izboru in preskušanju tehničnih varnostnih ukrepov, naprav in programske opreme, značilnih za sistem, zaradi nadzora nad njihovim izvajanjem in zagotovitve, da so varno nameščeni, konfigurirani in vzdrževani v skladu z ustrezno varnostno dokumentacijo;

(c) sodelovanje pri izboru varnostnih ukrepov in naprav TEMPEST, če tako zahteva izjava o posebnih zahtevah za varovanje tajnosti, značilnih za sistem, in zagotavljanje, da so varno nameščeni in vzdrževani, v sodelovanju z organom TEMPEST;

(d) spremljanje izvajanja in uporabe varnostno-operativnih postopkov; po potrebi lahko odgovornost v zvezi z varnostjo delovanja prenese na lastnika sistema;

(e) upravljanje šifrirnih izdelkov in delo z njimi, zagotavljanje hrambe šifrirnih in nadzorovanih predmetov ter po potrebi zagotavljanje oblikovanja šifrirnih spremenljivk;

(f) izvedbo pregledov in preskusov varnostnih analiz, zlasti za pripravo ustreznih poročil o tveganju, kakor zahteva organ za varnostno akreditacijo;

(g) pripravo usposabljanja o zagotavljanju varnosti podatkov v KIS;

(h) izvajanje in vodenje varnostnih ukrepov za KIS.

*PRILOGA V*

## INDUSTRIJSKA VARNOST

I. UVOD

1. V tej prilogi so določbe za izvajanje člena 11. Opredeljene so splošne varnostne določbe, ki veljajo za industrijske ali druge subjekte v pogajanjih pred sklenitvijo pogodbe in ves čas življenjskega cikla pogodb s tajnimi podatki, ki jih sklene GSS.

2. Svet odobri politiko o industrijski varnosti, v kateri so podrobno opisane predvsem zahteve glede varnostnih dovoljenj organizacij, listin o varnostnih vidikih, obiskih, razpošiljanju in prenašanju tajnih podatkov EU.

II. VARNOSTNI ELEMENTI V POGODBAH S TAJNIMI PODATKI

**Vodič po stopnjah tajnosti**

3. Pred objavo razpisa ali sklenitvijo pogodbe s tajnimi podatki GSS kot naročnik določi stopnjo tajnosti podatkov, ki se posredujejo ponudnikom in izvajalcem, pa tudi stopnjo tajnosti podatkov, ki jih bo ustvaril izvajalec. GSS za ta namen pripravi vodič po stopnjah tajnosti, ki se uporablja pri izvajanju pogodbe.

4. Za določitev stopnje tajnosti različnih delov pogodbe s tajnimi podatki veljajo naslednja načela:

(a) GSS pri pripravi vodiča po stopnjah tajnosti upošteva vse pomembne varnostne vidike, tudi stopnjo tajnosti, določeno za zagotovljene in odobrene podatke, ki jih organ izvora potrebuje za namene pogodbe;

(b) splošna stopnja tajnosti posamezne pogodbe ne sme biti nižja od najvišje stopnje tajnosti katerega koli izmed njenih elementov; ter

(c) GSS se, če pride do kakršnih koli sprememb v zvezi s stopnjo tajnosti podatkov, ki so nastali pri izvajalcih ali so jim bili predloženi pri izvajanju pogodbe, ali ob kakršni koli naknadni spremembi vodiča po stopnjah tajnosti, po potrebi poveže z zadevnimi nacionalnimi varnostnimi organi/imenovanimi varnostnimi organi države članice ali katerim koli drugim pristojnim varnostnim organom.

**Listina o varnostnih vidikih (Security Aspects Letter – SAL)**

5. Varnostne zahteve, povezane s posamezno pogodbo, so opisane v listini o varnostnih vidikih. Temu je po potrebi dodan vodič po stopnjah tajnosti in je sestavni del pogodbe s tajnimi podatki ali podizvajalske pogodbe s tajnimi podatki.

6. V listini o varnostnih vidikih so določbe, ki od izvajalca in/ali podizvajalca zahtevajo spoštovanje minimalnih standardov iz tega sklepa. Nespoštovanje teh minimalnih standardov je lahko zadosten razlog za prekinitev pogodbe.

**Varnostna navodila za program/projekt (PSI)**

7. Odvisno od obsega programov ali projektov, ki vključujejo dostop do tajnih podatkov EU ali delo z njimi ali njihovo hrambo, lahko naročnik, imenovan za vodenje programa ali projekta, pripravi posebna varnostna navodila za program/projekt. Varnostna navodila za program/projekt, ki lahko vsebujejo dodatne varnostne zahteve, morajo odobriti nacionalni varnostni organi/imenovani varnostni organi držav članic ali kateri koli drug pristojni varnostni organ, ki sodeluje pri programu/projektu.

III. VARNOSTNO DOVOLJENJE ORGANIZACIJE (FSC)

8. Varnostno dovoljenje organizacije izda nacionalni varnostni organ ali imenovani varnostni organ ali kateri koli drug pristojni varnostni organ države članice, kar skladno z nacionalnimi zakoni in predpisi pomeni, da je industrijski ali drugi subjekt v svojih prostorih zmožen varovati tajne podatke EU ustrezne stopnje tajnosti (CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET). Dovoljenje se predloži GSS kot naročniku, še preden se izvajalcu ali podizvajalcu ali morebitnemu izvajalcu ali podizvajalcu zagotovijo tajni podatki EU ali se mu odobri dostop do njih.

9. Pri izdajanju varnostnega dovoljenja organizacije ustrezni nacionalni varnostni organ ali imenovani varnostni organ vsaj:

(a) oceni celovitost industrijskega ali drugega subjekta;

(b) oceni lastništvo, nadzor ali morebitno nedovoljeno vplivanje, ki lahko predstavlja varnostno tveganje;

(c) preveri, da ima industrijski ali drug subjekt v svojih prostorih vzpostavljen varnostni sistem z vsemi ustreznimi varnostnimi ukrepi, potrebnimi za varovanje podatkov ali materiala stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET v skladu z zahtevami iz tega sklepa;

(d) preveri, da so člani uprave, lastniki in zaposleni, ki naj bi imeli dostop do podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET, varnostno preverjeni v skladu z zahtevami iz tega sklepa;

(e) preveri, da je industrijski ali drug subjekt imenoval svojega varnostnega uradnika, ki vodstvu odgovarja za izvajanje varnostnih obveznosti v subjektu.

10. Po potrebi GSS kot naročnik nacionalni varnostni organ/imenovani varnostni organ ali kateri koli drug pristojni varnostni organ uradno obvesti, da se varnostno dovoljenje organizacije zahteva v fazi pred sklenitvijo pogodbe ali za izvajanje pogodbe. Varnostno dovoljenje organizacije ali dovoljenje za dostop do tajnih podatkov se v fazi pred sklenitvijo pogodbe zahteva, če je treba v postopku priprave ponudb predložiti tajne podatke EU stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET.

11. Naročnik najustreznejšemu ponudniku ne sme dodeliti pogodbe s tajnimi podatki, dokler mu nacionalni varnostni organ/imenovani varnostni organ ali kateri koli drug pristojni varnostni organ države članice, v kateri je izvajalec ali podizvajalec registriran, ne potrdi, da je bilo, kjer je to potrebno, ponudniku izdano ustrezno varnostno dovoljenje organizacije.

12. Nacionalni varnostni organ/imenovani varnostni organ ali kateri koli drug pristojni varnostni organ, ki je izdal varnostno dovoljenje organizacije, uradno obvesti GSS kot naročnika o spremembah, ki zadevajo varnostno dovoljenje organizacije. V primeru podizvajalske pogodbe se ustrezno obvesti nacionalni varnostni organ/imenovani varnostni organ ali kateri koli drug pristojni varnostni organ.

13. Če nacionalni varnostni organ/imenovani varnostni organ ali kateri koli drug pristojni varnostni organ odvzame varnostno dovoljenje organizacije, ima GSS kot naročnik zadosten razlog za prekinitev pogodbe s tajnimi podatki ali izključitev ponudnika iz natečaja.

IV. POGODBE IN PODIZVAJALSKE POGODBE S TAJNIMI PODATKI

14. Če se tajni podatki EU ponudniku zagotovijo v fazi pred sklenitvijo pogodbe, razpis vsebuje določbo, v skladu s katero mora ponudnik, ki ne predloži ponudbe ali ki ni izbran, v določenem roku vrniti vse tajne dokumente.

15. Ko je pogodba ali podizvajalska pogodba s tajnimi podatki dodeljena, GSS kot naročnik obvesti nacionalni varnostni organ/imenovani varnostni organ ali kateri koli drug pristojni varnostni organ izvajalca ali podizvajalca o varnostnih določbah pogodbe s tajnimi podatki.

16. Ko takšne pogodbe prenehajo veljati, GSS kot naročnik (in/ali nacionalni varnostni organ/imenovani varnostni organ ali po potrebi kateri koli drug pristojni varnostni organ v primeru podizvajalske pogodbe) nemudoma obvesti nacionalni varnostni organ/imenovani varnostni organ ali kateri koli drug pristojni varnostni organ države članice, v kateri je izvajalec ali podizvajalec registriran.

17. Na splošno velja, da mora izvajalec ali podizvajalec naročniku ob prenehanju veljavnosti pogodbe ali podpogodbe s tajnimi podatki vrniti vse tajne podatke EU, ki jih ima.

18. V listini o varnostnih vidikih se zapišejo posebne določbe o razpolaganju s tajnimi podatki EU v času izvajanja pogodbe ali po prenehanju njene veljavnosti.

19. Če smeta izvajalec ali podizvajalec tajne podatke EU obdržati tudi po prenehanju veljavnosti pogodbe, morata še naprej ravnati skladno z minimalnimi standardi iz tega sklepa in varovati tajnost podatkov EU.

20. Pogoji, v skladu s katerimi lahko izvajalec sklene podizvajalsko pogodbo, so določeni v razpisu in v pogodbi.

21. Izvajalec pred oddajo delov pogodbe s tajnimi podatki podizvajalcu pridobi dovoljenje GSS kot naročnika. Podizvajalska pogodba se ne sme dodeliti industrijskim ali drugim subjektom, registriranim v državi, ki ni članica EU in z EU ni sklenila sporazuma o varovanju tajnosti podatkov.

22. Izvajalec mora zagotoviti, da se vse podizvajalske dejavnosti opravljajo v skladu z minimalnimi standardi iz tega sklepa in podizvajalcu ne zagotovi tajnih podatkov EU brez predhodnega pisnega soglasja naročnika.

23. Kar zadeva tajne podatke, ki nastanejo pri izvajalcu ali podizvajalcu ali izvajalec ali podizvajalec z njimi dela, pravice organa izvora uveljavlja naročnik.

V. OBISKI V ZVEZI S POGODBAMI S TAJNIMI PODATKI

24. Če morajo GSS, izvajalci ali podizvajalci za izvajanje pogodbe s tajnimi podatki imeti dostop do podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET v prostorih enih ali drugih, se v sodelovanju z zadevnimi nacionalnimi varnostnimi organi/imenovanimi varnostnimi organi ali katerim koli drugim pristojnim varnostnim organom organizirajo obiski. Nacionalni varnostni organi/imenovani varnostni organi pa se lahko za posebne projekte tudi sporazumejo o postopku, na podlagi katerega se je mogoče o takšnih obiskih dogovoriti neposredno.

25. Vsi obiskovalci imajo ustrezno dovoljenje za dostop do tajnih podatkov in imajo potrebo po seznanitvi za dostop do tajnih podatkov EU, povezanih s pogodbo z GSS.

26. Obiskovalci imajo dostop le do tajnih podatkov EU, povezanih z namenom obiska.

VI. POŠILJANJE IN PRENAŠANJE TAJNIH PODATKOV EU

27. Za pošiljanje tajnih podatkov EU z elektronskimi sredstvi se uporabljajo ustrezne določbe iz člena 10 in Priloge IV.

28. Za prenašanje tajnih podatkov EU se v skladu z nacionalnimi zakoni in predpisi uporabljajo ustrezne določbe iz Priloge III.

29. Za prevoz tajnega gradiva kot tovora se pri določanju varnostnega režima upoštevajo naslednja načela:

(a) varnost je zagotovljena v vseh fazah prevoza, od odhodnega kraja do namembnega kraja;

(b) stopnja zaščite se za pošiljko določi na podlagi gradiva z najvišjo stopnjo tajnosti, ki ga pošiljka vsebuje;

(c) za prevoznika se pridobi varnostno dovoljenje organizacije na ustrezni stopnji. V teh primerih mora biti osebje, ki dela s pošiljko, varnostno preverjeno v skladu s Prilogo I;

(d) pošiljatelj pred vsakim premikom materiala stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET čez mejo pripravi načrt prevoza, ki ga odobri zadevni nacionalni varnostni organ/imenovani varnostni organ ali kateri koli drug pristojni varnostni organ;

(e) prevozi so, če je le mogoče, brez postanka in se opravijo v najhitrejšem možnem času, ki ga dovoljujejo okoliščine;

(f) če je le mogoče, se uporabljajo izključno poti skozi države članice EU. Poti prek držav, ki niso države članice, se uporabijo le, če to odobri nacionalni varnostni organ/imenovani varnostni organ ali kateri koli drug pristojni varnostni organ države pošiljatelja in države prejemnika.

VII. POŠILJANJE TAJNIH PODATKOV EU IZVAJALCEM V TRETJIH DRŽAVAH

30. Pošiljanje tajnih podatkov EU izvajalcem in podizvajalcem v tretjih državah poteka v skladu z varnostnimi ukrepi, dogovorjenimi med GSS kot naročnikom in nacionalnim varnostnim organom/imenovanim varnostnim organom zadevne tretje države, v kateri je registriran izvajalec.

VIII. DELO S PODATKI STOPNJE TAJNOSTI RESTREINT UE/EU RESTRICTED IN NJIHOVA HRAMBA

31. GSS kot naročnik sme po potrebi v navezi z nacionalnim varnostnim organom/imenovanim varnostnim organom države članice na podlagi pogodbenih določb obiskovati prostore izvajalca/podizvajalca in preverjati, ali so bili skladno s pogodbo uvedeni vsi ustrezni ukrepi za varovanje tajnih podatkov EU stopnje RESTREINT UE/EU RESTRICTED.

32. Če to zahtevajo nacionalni zakoni in predpisi, GSS kot naročnik uradno obvesti nacionalne varnostne organe/imenovane varnostne organe ali kateri koli drug pristojni varnostni organ o pogodbah ali podizvajalskih pogodbah s tajnimi podatki stopnje RESTREINT UE/EU RESTRICTED.

33. Izvajalci ali podizvajalci in njihovo osebje za pogodbe s podatki stopnje RESTREINT UE/EU RESTRICTED, ki jih sklene GSS, ne potrebujejo varnostnega dovoljenja organizacije ali dovoljenja za dostop do tajnih podatkov.

34. GSS kot naročnik preuči ponudbe na razpisu za pogodbe, za katere je treba imeti dostop do podatkov stopnje RESTREINT UE/EU RESTRICTED, ne glede na kakršne koli zahteve v zvezi z varnostnim dovoljenjem organizacije ali dovoljenjem za dostop do tajnih podatkov v okviru nacionalnih zakonov in predpisov.

35. Izvajalec lahko sklene podizvajalsko pogodbo pod pogoji, ki so skladni z odstavkom 21.

36. Če pogodba vključuje delo s tajnimi podatki stopnje RESTREINT UE/EU RESTRICTED v KIS, ki ga upravlja izvajalec, GSS kot naročnik zagotovi, da se v pogodbi ali kakršni koli podizvajalski pogodbi določijo potrebne tehnične in upravne zahteve glede akreditacije KIS, ki so v sorazmerju z ocenjenim tveganjem ob upoštevanju vseh ustreznih dejavnikov. Naročnik in ustrezni nacionalni varnostni organ/imenovani varnostni organ se dogovorita o obsegu akreditacije takšnega KIS.

*PRILOGA VI*

## IZMENJAVA TAJNIH PODATKOV S TRETJIMI DRŽAVAMI IN MEDNARODNIMI ORGANIZACIJAMI

I. UVOD

1. V tej prilogi so določbe za izvajanje člena 12.

II. OKVIRI ZA IZMENJAVO TAJNIH PODATKOV

2. Če Svet ugotovi, da obstaja dolgoročna potreba po izmenjavi tajnih podatkov, se sklene

— sporazum o varovanju tajnosti podatkov, ali

— dogovor o izvajanju

v skladu s členom 12(2) ter oddelkoma III in IV ter na podlagi priporočila Varnostnega odbora.

3. Če je treba tajne podatke EU, ki nastanejo za namene operacije CSDP, zagotoviti tretjim državam ali mednarodnim organizacijam, ki sodelujejo pri tej operaciji, in če ni nobenega okvira iz odstavka 2, izmenjavo tajnih podatkov EU s sodelujočo tretjo državo ali mednarodno organizacijo v skladu z oddelkom V ureja:

— okvirni sporazum o sodelovanju;

— *ad hoc* sporazum o sodelovanju; ali

— če ni nobenega od teh sporazumov, *ad hoc* dogovor o izvajanju.

4. Če okvira iz odstavkov 2 in 3 ni in je sprejeta odločitev o dajanju tajnih podatkov EU tretji državi ali mednarodni organizaciji izjemoma na *ad hoc* podlagi, se v skladu z oddelkom VI od zadevne tretje države ali mednarodne organizacije zahteva pisno jamstvo o tem, da varuje prejete tajne podatke EU v skladu s temeljnimi načeli in minimalnimi standardi iz tega sklepa.

III. SPORAZUMI O VAROVANJU TAJNOSTI PODATKOV

5. Sporazumi o varovanju tajnosti podatkov določajo temeljna načela in minimalne standarde, ki urejajo izmenjavo tajnih podatkov med EU in tretjo državo ali mednarodno organizacijo.

6. Sporazumi o varovanju tajnosti podatkov vsebujejo tehnične izvedbene določbe, o katerih se dogovorijo Varnostni urad GSS, Varnostni direktorat Evropske komisije in pristojni varnostni organ zadevne tretje države ali mednarodne organizacije. Te določbe upoštevajo stopnjo varovanja, ki jo določajo veljavni varnostni predpisi, strukture in postopki v zadevni tretji državi ali mednarodni organizaciji. Odobriti jih mora Varnostni odbor.

7. Tajni podatki EU se ne izmenjujejo z elektronskimi sredstvi, razen če ni to izrecno določeno v sporazumu o varovanju tajnosti podatkov in/ali tehničnih izvedbenih določbah.

8. V sporazumih o varovanju tajnih podatkov je določeno, da Varnostni urad GSS in Varnostni direktorat Evropske komisije pred izmenjavo tajnih podatkov v skladu z zadevnim sporazumom soglašata, da je stran prejemnica sposobna ustrezno zaščititi in varovati prejete podatke.

9. Kadar Svet sklene sporazum o varovanju tajnosti podatkov, vsaka stran določi register, ki je glavna točka vstopa in izstopa pri izmenjavi tajnih podatkov.

10. Za oceno učinkovitosti varnostnih predpisov, struktur in postopkov v zadevni tretji državi ali mednarodni organizaciji Varnostni urad GSS skupaj z Varnostnim direktoratom Evropske komisije v soglasju z zadevno tretjo državo ali mednarodno organizacijo opravi ocenjevalne obiske. Takšni ocenjevalni obiski se izvedejo v skladu z ustreznimi določbami iz Priloge III in ocenijo:

(a) regulativni okvir, ki se uporablja za varovanje tajnih podatkov;

(b) kakršne koli posebne značilnosti varnostne politike in načina organizacije varovanja tajnosti v tretji državi ali mednarodni organizaciji, ki lahko vplivajo na stopnjo tajnosti podatkov, ki se lahko izmenjajo;

(c) dejanske varnostne ukrepe in postopke; ter

(d) postopke varnostnega preverjanja za stopnjo tajnih podatkov EU, ki bodo dani.

11. Skupina, ki opravlja ocenjevalni obisk v imenu EU, oceni, ali so varnostni predpisi in postopki v zadevni tretji državi ali mednarodni organizaciji ustrezni za varovanje tajnih podatkov EU določene stopnje.

12. O ugotovitvah teh obiskov se pripravi poročilo, na podlagi katerega Varnostni odbor določi najvišjo stopnjo tajnih podatkov EU, ki se lahko z zadevno tretjo stranjo izmenjujejo v papirnati in, če je to primerno, v elektronski obliki, ter kakršne koli posebne pogoje za izmenjavo tajnih podatkov s to stranjo.

13. Prizadevati si je treba, da se obisk, namenjen celoviti oceni varovanja tajnosti v zadevni tretji državi ali mednarodni organizaciji, opravi preden Varnostni odbor odobri izvedbene določbe, da se določita vrsta in učinkovitost obstoječega varnostnega sistema. Če to ni mogoče, Varnostni urad GSS predloži Varnostnemu odboru čim bolj popolno poročilo, v katerem ga na podlagi razpoložljivih informacij obvesti o veljavnih varnostnih predpisih in načinu organizacije varovanja tajnosti v zadevni tretji državi ali mednarodni organizaciji.

14. Varnostni odbor lahko odloči, da se pred preučitvijo rezultatov ocenjevalnega obiska ne sme sporočati nobenih tajnih podatkov EU, ali da se smejo dati samo tajni podatki do navedene stopnje, ali lahko določi druge posebne pogoje, ki urejajo dajanje tajnih podatkov EU zadevnim tretjim državam ali mednarodnim organizacijam. Varnostni urad GSS o tem obvesti zadevno tretjo državo ali mednarodno organizacijo.

15. V medsebojnem dogovoru z zadevno tretjo državo ali mednarodno organizacijo Varnostni urad GSS redno opravlja nadaljnje ocenjevalne obiske, da preveri, ali so veljavne ureditve še vedno v skladu z dogovorjenimi minimalnimi standardi.

16. Ko začne veljati sporazum o varovanju tajnih podatkov in se tajni podatki izmenjujejo z zadevno tretjo državo ali mednarodno organizacijo, lahko Varnostni odbor sklene, da bo spremenil najvišjo stopnjo tajnih podatkov EU, ki se lahko izmenjujejo v papirnati ali elektronski obliki, zlasti na podlagi nadaljnjih ocenjevalnih obiskov.

IV. DOGOVORI O IZVAJANJU

17. Če obstaja dolgoročna potreba po izmenjavanju tajnih podatkov, ki praviloma ne presegajo stopnje RESTREINT UE/EU RESTRICTED, s tretjo državo ali mednarodno organizacijo, in je Varnostni odbor ugotovil, da zadevna stran nima dovolj razvitega varnostnega sistema, da bi bila zmožna skleniti sporazum o varovanju tajnosti podatkov, lahko generalni sekretar z odobritvijo Sveta z ustreznimi organi zadevne tretje države ali mednarodne organizacije sklene dogovor o izvajanju.

18. Če pa je treba iz nujnih operativnih razlogov hitro vzpostaviti okvir za izmenjavo tajnih podatkov, lahko Svet izjemoma odloči, da se sklene dogovor o izvajanju za izmenjavo tajnih podatkov višje stopnje.

19. Praviloma imajo dogovori o izvajanju obliko izmenjave pisem.

20. Preden se tajni podatki EU dejansko dajo zadevni tretji državi ali mednarodni organizaciji, se opravi ocenjevalni obisk iz odstavka 10, poročilo pa se pošlje Varnostnemu odboru, ki mora o njem podati pozitivno mnenje. Če pa je Svet obveščen o izrednih razlogih za nujno izmenjavo tajnih podatkov, se lahko tajni podatki EU vseeno dajo, pod pogojem, da se stori vse, da se takšen ocenjevalni obisk opravi čim prej.

21. Tajni podatki EU se ne izmenjujejo z elektronskimi sredstvi, razen če ni to izrecno določeno v dogovoru o izvajanju.

V. IZMENJAVA TAJNIH PODATKOV V OKVIRU OPERACIJ CSDP

22. Sodelovanje tretjih držav ali mednarodnih organizacij v operacijah CSDP urejajo okvirni sporazumi o sodelovanju. Ti sporazumi vključujejo določbe o dajanju tajnih podatkov EU, ki nastanejo za namene operacij CSDP, sodelujočim tretjim državam ali mednarodnim organizacijam. Najvišja stopnja tajnosti tajnih podatkov EU, ki se lahko izmenjujejo, je RESTREINT UE/EU RESTRICTED za civilne operacije CSDP in CONFIDENTIEL UE/EU CONFIDENTIAL za vojaške operacije CSDP, razen če je drugače določeno v sklepu o vzpostavitvi posamezne operacije CSDP.

23. *Ad hoc* sporazumi o sodelovanju, sklenjeni za določeno operacijo CSDP, vključujejo določbe o dajanju tajnih podatkov EU, ki nastanejo za namene te operacije, sodelujoči tretji državi ali mednarodni organizaciji. Najvišja stopnja tajnosti tajnih podatkov EU, ki se lahko izmenjujejo, je RESTREINT UE/EU RESTRICTED za civilne operacije CSDP in CONFIDENTIEL UE/EU CONFIDENTIAL za vojaške operacije CSDP, razen če je drugače določeno v sklepu o vzpostavitvi posamezne operacije CSDP.

24. *Ad hoc* dogovori o izvajanju glede sodelovanja tretje države ali mednarodne organizacije v določeni operaciji CSDP lahko med drugim vključujejo dajanje tajnih podatkov EU, ki nastanejo za namene operacije, tej tretji državi ali mednarodni organizaciji. Takšni *ad hoc* dogovori o izvajanju se sklenejo v skladu s postopkom iz odstavkov 17 in 18 oddelka IV. Najvišja stopnja tajnosti tajnih podatkov EU, ki se lahko izmenjujejo, je RESTREINT UE/EU RESTRICTED za civilne operacije CSDP in CONFIDENTIEL UE/EU CONFIDENTIAL za vojaške operacije CSDP, razen če je drugače določeno v sklepu o vzpostavitvi posamezne operacije CSDP.

25. Pred izvajanjem odločb o dajanju tajnih podatkov EU v skladu z odstavki 22, 23 in 24 niso potrebne nobene izvedbene ureditve ali ocenjevalni obiski.

26. Če država gostiteljica, na ozemlju katere se izvaja operacija CSDP, z EU nima sklenjenega sporazuma o varovanju tajnosti podatkov ali dogovora o izvajanju za izmenjavo tajnih podatkov, se v primeru posebne in nujne operativne potrebe lahko sprejme *ad hoc* dogovor o izvajanju. Ta možnost je določena v sklepu o vzpostavitvi operacije CSDP. Pod temi pogoji se dajejo samo tajni podatki, ki nastanejo za namene operacije CSDP in so največ stopnje RESTREINT UE/EU RESTRICTED. V skladu s takšnim *ad hoc* dogovorom o izvajanju se država gostiteljica zaveže, da bo varovala tajne podatke EU v skladu z minimalnimi standardi, ki niso manj strogi od standardov iz tega sklepa.

27. V določbah o tajnih podatkih, ki se vključijo v okvirne sporazume o sodelovanju, *ad hoc* sporazume o sodelovanju in *ad hoc* dogovore o izvajanju iz odstavkov 22 do 24, je predvideno, da zadevna tretja država ali mednarodna organizacija zagotovi, da bo njeno osebje, dodeljeno kateri koli operaciji, varovalo tajne podatke EU v skladu z varnostnimi pravili Sveta in nadaljnjimi smernicami, ki jih izdajo pristojni organi, vključno s strukturo poveljevanja operacije.

28. Če EU in sodelujoča tretja država ali mednarodna organizacija naknadno skleneta sporazum o varovanju tajnosti podatkov, ta sporazum nadomesti vsak okvirni sporazum o sodelovanju, *ad hoc* sporazum o sodelovanju ali *ad hoc* dogovor o izvajanju, kar zadeva izmenjavo tajnih podatkov EU in delo z njimi.

29. Izmenjava tajnih podatkov EU z elektronskimi sredstvi ni dovoljena v okvirnem sporazumu o sodelovanju, *ad hoc* sporazumu o sodelovanju ali *ad hoc* dogovoru o izvajanju s tretjo državo ali mednarodno organizacijo, razen če je to izrecno določeno v zadevnem sporazumu ali dogovoru.

30. Tajni podatki EU, ki nastanejo za namene operacije CSDP, se lahko v skladu z odstavki 22 do 29 razkrijejo osebju, ki ga tej operaciji dodelijo tretje države ali mednarodne organizacije. Pri odobritvi dostopa temu osebju do tajnih podatkov EU v prostorih ali v KIS operacije CSDP je treba uporabiti ukrepe (vključno z evidenco razkritih tajnih podatkov EU), da se zmanjša nevarnost izgube ali nepooblaščenega razkritja. Takšni ukrepi so določeni v ustreznih načrtih ali dokumentih misije.

VI. *AD HOC* DAJANJE TAJNIH PODATKOV EU V IZJEMNIH PRIMERIH

31. Če ni okvira v skladu s prej navedenimi oddelki III do V in če Svet ali eno izmed njegovih pripravljalnih teles ugotovi, da obstaja izjemna potreba po dajanju tajnih podatkov EU tretji državi ali mednarodni organizaciji, GSS:

(a) pri varnostnih organih zadevne tretje države ali mednarodne organizacije, kolikor je to mogoče, preveri, ali njeni varnostni predpisi, strukture in postopki zagotavljajo, da se tajni podatki EU, ki ji bodo dani, varujejo po standardih, ki niso manj strogi od standardov iz tega sklepa;

(b) pozove Varnostni odbor, naj na podlagi razpoložljivih informacij izda priporočilo o tem, ali je mogoče zaupati varnostnim predpisom, strukturam in postopkom v tretji državi ali mednarodni organizaciji, ki naj bi prejela tajne podatke EU.

32. Če Varnostni odbor izda pozitivno priporočilo glede dajanja tajnih podatkov EU, zadevo obravnava Odbor stalnih predstavnikov (COREPER), ki o tem sprejme odločitev.

33. Če je priporočilo varnostnega odbora glede dajanja tajnih podatkov EU negativno:

(a) v zadevah v zvezi s SZVP/CSDP o tem vprašanju razpravlja Politični in varnostni odbor, ki oblikuje priporočilo za odločitev COREPER-ja;

(b) v vseh drugih zadevah o tem razpravlja COREPER, ki sprejme odločitev.

34. Po potrebi in ob predhodnem pisnem soglasju organa izvora lahko COREPER odloči, da se lahko da le del tajnih podatkov, ali le, če se najprej zniža ali prekliče njihova stopnja tajnosti, ali če se podatki, ki naj bi jih dali, pripravijo brez navedbe vira ali prvotne stopnje tajnosti EU.

35. GSS po sprejetju odločitve o dajanju tajnih podatkov EU pošlje zadevni dokument z oznako, da se dajo tretji državi ali mednarodni organizaciji. Preden se tajni podatki dejansko dajo ali ob njihovi predaji se zadevna tretja stran pisno zaveže, da bo varovala prejete tajne podatke EU v skladu s temeljnimi načeli in minimalnimi standardi iz tega sklepa.

VII. POOBLASTILO ZA DAJANJE TAJNIH PODATKOV EU TRETJIM DRŽAVAM ALI MEDNARODNIM ORGANIZACIJAM

36. Če obstaja okvir za izmenjavo tajnih podatkov s tretjo državo ali mednarodno organizacijo v skladu z odstavkom 2, Svet sprejme odločitev, da se generalni sekretar pooblasti za dajanje tajnih podatkov EU zadevni tretji državi ali mednarodni organizaciji v skladu z načelom soglasja organa izvora.

37. Če obstaja okvir za izmenjavo tajnih podatkov s tretjo državo ali mednarodno organizacijo v skladu z odstavkom 3, se generalni sekretar pooblasti za dajanje tajnih podatkov EU v skladu s sklepom o vzpostavitvi operacije CSDP in načelom o soglasju organa izvora.

38. Generalni sekretar lahko takšno pooblastilo prenese na višje uradnike GSS ali druge podrejene osebe.

*Dodatki*

*Dodatek A*

Opredelitev pojmov

*Dodatek B*

Enakovrednost stopenj tajnosti

*Dodatek C*

Seznam nacionalnih varnostnih organov

*Dodatek D*

Seznam kratic

*Dodatek A*

OPREDELITEV POJMOV

V tem sklepu se uporabljajo naslednje opredelitve:

„akreditacija“ pomeni postopek, ki se zaključi z uradno izjavo organa za varnostno akreditacijo, da lahko sistem deluje z določeno stopnjo tajnosti v posebnem varnostnem načinu delovanja v svojem operativnem okolju in s sprejemljivo stopnjo tveganja, ob predpostavki, da je bil izveden odobren sklop tehničnih, fizičnih, organizacijskih in postopkovnih varnostnih ukrepov;

„delo“ s tajnimi podatki EU pomeni vsa možna dejanja, v katera so vključeni tajni podatki EU v njihovem življenjskem ciklu. Zajema njihov nastanek, obdelavo, prenos, znižanje stopnje tajnosti, preklic tajnosti in uničenje. V zvezi s komunikacijskimi in informacijskimi sistemi zajema tudi njihovo zbiranje, prikaz, prenos in hrambo;

„dokument“ pomeni vse zabeležene informacije, ne glede na njihovo fizično obliko ali značilnosti;

„dovoljenje za dostop do tajnih podatkov“ (PSC) pomeni eno ali oboje od naslednjega:

— „dovoljenje EU za dostop do tajnih podatkov“ (*EU PSC*) za dostop do tajnih podatkov EU pomeni pooblastilo organa GSS za imenovanje, sprejeto v skladu s tem sklepom po končani varnostni preiskavi, ki jo opravijo pristojni organi države članice, s katero je potrjeno, da se posameznik lahko pooblasti za dostop do tajnih podatkov EU do določene stopnje (CONFIDENTIEL UE/EU CONFIDENTIAL ali višje) in do določenega datuma, če je bila ugotovljena potreba po seznanitvi zadevnega posameznika; ta posameznik je „varnostno preverjen“;

— „nacionalno dovoljenje za dostop do tajnih podatkov“ (*national PSC*) za dostop do tajnih podatkov EU pomeni izjavo pristojnega organa države članice, sprejeto po končani varnostni preiskavi, ki jo opravijo pristojni organi države članice in s katero je potrjeno, da se posameznik lahko pooblasti za dostop do tajnih podatkov EU do določene stopnje (CONFIDENTIEL UE/EU CONFIDENTIAL ali višje) in do določenega datuma, če je bila ugotovljena potreba po seznanitvi zadevnega posameznika; ta posameznik je „varnostno preverjen“;

„fizična varnost“ – glej člen 8(1);

„globinska obramba“ pomeni uporabo več vrst varnostnih ukrepov, ki so urejeni kot večslojna obramba;

„imenovani varnostni organ“ (DSA) pomeni organ, odgovoren nacionalnemu varnostnemu organu države članice, ki je zadolžen, da industrijske ali druge subjekte obvešča o nacionalni politiki glede vseh zadev v zvezi z industrijsko varnostjo ter da zagotavlja usmeritve in pomoč pri njenem izvajanju. Funkcijo imenovanega varnostnega organa lahko opravlja nacionalni varnostni organ ali kateri koli drug pristojni organ;

„imetnik podatkov“ pomeni pravilno pooblaščeno osebo, za katero je ugotovljena potreba po seznanitvi in ki razpolaga s tajnim podatkom EU ter je zato odgovorna za njegovo varovanje;

„industrijska varnost“ – glej člen 11(1);

„industrijski ali drug subjekt“ pomeni subjekt, ki sodeluje pri dobavi blaga, izvedbi del ali opravljanju storitev; to je lahko industrijski, trgovski, storitveni, znanstveni, raziskovalni, izobraževalni ali razvojni subjekt ali samozaposlena oseba;

„izvajalec“ pomeni posameznika ali pravni subjekt, ki je pravno sposoben za izvajanje pogodb;

„komunikacijski in informacijski sistem (KIS)“ – glej člen 10(2);

„listina o varnostnih vidikih“ (SAL) pomeni sklop posebnih pogodbenih pogojev, ki jih objavi naročnik in so sestavni del vsake pogodbe s tajnimi podatki, ki vključuje dostop do tajnih podatkov EU ali njihov nastanek. Listina o varnostnih vidikih določa varnostne zahteve ali tiste elemente pogodbe, ki zahtevajo varovanje;

„material“ pomeni vsak dokument ali del stroja ali opreme, ki je že bil izdelan ali je v postopku izdelave;

„medsebojna povezanost“ – glej odstavek 31 v Prilogi IV;

„nevarnost“ pomeni morebiten vzrok neželenega dogodka, ki bi lahko škodil organizaciji ali kateremu od sistemov, ki jih uporablja; takšne nevarnosti so lahko naključne ali namerne (zlonamerne), zanje pa so značilni grozilni elementi, morebitni cilji in načini napada;

„obravnavanje tajnih podatkov“ – glej člen 9(1);

„operacija CSDP“ pomeni vojaško ali civilno operacijo kriznega upravljanja, vzpostavljeno na podlagi naslova V, poglavja 2 Pogodbe EU;

„organ izvora“ pomeni institucijo EU, agencijo ali organ, državo članico, tretjo državo ali mednarodno organizacijo, v pristojnosti katere so nastali tajni podatki in/ali so bili uvedeni v strukture EU;

„osebna varnost“ – glej člen 7(1);

„podizvajalska pogodba s tajnimi podatki“ pomeni pogodbo, ki jo izvajalec GSS sklene z drugim izvajalcem (tj. podizvajalcem) za dobavo blaga, izvedbo del ali opravljanje storitev, katere izpolnitev zahteva ali vključuje dostop do tajnih podatkov EU ali njihovo nastajanje;

„pogodba s tajnimi podatki“ pomeni pogodbo, ki jo GSS sklene z izvajalcem za dobavo blaga, izvedbo del ali opravljanje storitev, katere izpolnitev zahteva ali vključuje dostop do tajnih podatkov EU ali njihovo nastajanje;

„postopek za obvladovanje varnostnega tveganja“ pomeni celoten postopek opredelitve, nadzorovanja in čim večje omejitve negotovih dogodkov, ki bi lahko vplivali na varnost organizacije ali katerega od sistemov, ki jih uporablja. Zajema vse dejavnosti, povezane s tveganjem, vključno z njegovo oceno, obravnavo, sprejemanjem in obveščanjem o tveganju;

„potrdilo za dostop do tajnih podatkov“ (PSCC) pomeni potrdilo, ki ga izda pristojni organ in dokazuje, da je posameznik varnostno preverjen in ima veljavno nacionalno ali dovoljenje EU za dostop do tajnih podatkov. Na potrdilu so navedeni stopnja tajnosti podatkov EU, do katerih ima lahko posameznik dostop (CONFIDENTIEL UE/EU CONFIDENTIAL ali višje), datum veljavnosti ustreznega dovoljenja za dostop do tajnih podatkov in datum izteka veljavnosti samega potrdila;

„preklic stopnje tajnosti“ pomeni odstranitev vsakršne stopnje tajnosti;

„preostalo tveganje“ pomeni tveganje, ki je še vedno prisotno, potem ko so bili izvedeni varnostni ukrepi, saj vseh nevarnosti ni mogoče preprečiti in vseh ranljivih točk ni mogoče odpraviti;

„ranljiva točka“ pomeni kakršno koli pomanjkljivost, zaradi katere se lahko uresniči ena ali več nevarnosti. Ranljiva točka lahko pomeni opustitev dejanja ali pa se nanaša na pomanjkljivost v nadzoru – ta morda ni dovolj strog, popoln ali dosleden –, ki je lahko tehnične, postopkovne, fizične, organizacijske ali operativne narave.

„sredstvo“ pomeni vse, kar je pomembno za organizacijo, njene poslovne dejavnosti in njihovo kontinuiteto, vključno z informacijskimi viri, ki podpirajo naloge organizacije;

„šifrirni material“ pomeni šifrirne algoritme, šifrirne module strojne in programske opreme ter izdelke, vključno s podrobnostmi izvajanja in s tem povezano dokumentacijo, ter šifrirne ključe;

„tajni podatki EU“ – glej člen 2(1);

„TEMPEST“ pomeni preiskavo, preučevanje in nadzor škodljivega elektromagnetnega oddajanja ter ukrepe za njegovo preprečevanje;

„tveganje“ pomeni možnost, da se zaradi notranje ali zunanje ranljive točke organizacije ali katerega koli sistema, ki ga uporablja, uresniči določena grožnja, kar lahko škodi organizaciji in njenim opredmetenim ali neopredmetenim sredstvom. Meri se kot kombinacija verjetnosti pojava nevarnosti in njihovega učinka.

— „sprejemanje tveganja“ je odločitev, da je preostalo tveganje še naprej prisotno potem, ko se je poskušalo tveganje obvladati;

— „ocena tveganja“ zajema opredelitev nevarnosti in ranljivih točk ter izvedbo s tem povezane analize tveganja, tj. analize verjetnosti in učinka;

— „obveščanje o tveganju“ zajema osveščanje skupnosti uporabnikov KIS o tveganjih, obveščanje organov za odobritev o tveganjih in poročanje o tveganjih operativnim organom;

— „obravnava tveganja“ zajema ublažitev tveganja, njegovo odpravo, zmanjšanje (z ustrezno kombinacijo tehničnih, fizičnih, organizacijskih ali postopkovnih ukrepov), prenos ali spremljanje;

„varnostna navodila za program/projekt“ (Programme/Project Security Instructions – PSI) pomenijo seznam varnostnih postopkov, ki se uporabljajo za določen program/projekt zaradi standardizacije varnostnih postopkov. Ta seznam je mogoče revidirati kadar koli v času trajanja programa/projekta;

„varnostna preiskava“ pomeni preiskovalne postopke, ki jih izvede pristojni organ države članice v skladu z njenimi nacionalnimi zakoni in predpisi z namenom pridobiti jamstvo, da niso znane nobene negativne informacije, zaradi katerih osebi ne bi odobrili nacionalnega dovoljenja ali dovoljenja EU za dostop do tajnih podatkov EU do določene stopnje (CONFIDENTIEL UE/EU CONFIDENTIAL ali višje);

„varnostni način delovanja“ pomeni opredelitev pogojev za delovanje KIS na podlagi stopnje tajnosti podatkov, s katerimi poteka delo v sistemu, in stopenj varnostnega preverjanja, uradnih odobritev dostopa in potrebe njegovih uporabnikov po seznanitvi. Za delo s tajnimi podatki ali njihov prenos obstajajo štirje načini delovanja: „namenski način“, „način po sistemu visoke varnosti“, „oddelčni način“ in „večstopenjski način“;

— „namenski način“ pomeni način delovanja, pri katerem so VSI posamezniki, ki imajo dostop do KIS, varnostno preverjeni do najvišje stopnje tajnosti podatkov, s katerimi poteka delo v KIS, in za katere velja splošna potreba po seznanitvi z VSEMI podatki, s katerimi poteka delo v okviru KIS;

— „način po sistemu visoke varnosti“ pomeni način delovanja, pri katerem so VSI posamezniki, ki imajo dostop do KIS, varnostno preverjeni do najvišje stopnje tajnosti podatkov, s katerimi poteka delo v KIS, splošna potreba po seznanitvi s podatki, s katerimi poteka delo v KIS, pa NI enaka za VSE posameznike, ki imajo dostop do KIS; dostop do podatkov lahko odobri posameznik;

— „oddelčni način“ pomeni način delovanja, pri katerem so vsi posamezniki, ki imajo dostop do KIS, varnostno preverjeni do najvišje stopnje tajnosti podatkov, s katerimi poteka delo v KIS, vsi posamezniki, ki imajo dostop do KIS, pa niso uradno pooblaščeni za dostop do vseh podatkov, s katerimi poteka delo v okviru KIS; uradno pooblastilo pomeni, da dostopa ne more odobriti posameznik, pač pa je nadzor urejen formalno in centralizirano;

— „večstopenjski način“ pomeni način delovanja, pri katerem VSI posamezniki, ki imajo dostop do KIS, niso varnostno preverjeni do najvišje stopnje tajnosti podatkov, s katerimi poteka delo v KIS, splošna potreba po seznanitvi s podatki, s katerimi poteka delo v okviru KIS, pa ni enaka za vse posameznike, ki imajo dostop do KIS;

„varnostno dovoljenje organizacije“ (FSC) pomeni upravno ugotovitev nacionalnega varnostnega organa ali imenovanega varnostnega organa, da lahko določena organizacija z varnostnega vidika nudi ustrezno stopnjo varovanja tajnih podatkov EU določene stopnje tajnosti ter da je njeno osebje, ki mora imeti dostop do tajnih podatkov EU, primerno varnostno preverjeno in poučeno o ustreznih varnostnih zahtevah, ki so potrebne za dostop do tajnih podatkov EU in njihovo varovanje;

„vodič po stopnjah tajnosti“ (SCG) pomeni dokument, ki opisuje elemente programa ali pogodbe, ki so tajni, in določa ustrezne stopnje tajnosti. Vodič po stopnjah tajnosti se lahko v času trajanja programa ali pogodbe razširi, stopnja tajnosti elementov podatkov pa se lahko spremeni ali zniža. Če obstaja vodič po stopnjah tajnosti, je del listine o varnostnih vidikih;

„vpis“ – glej odstavek 18 v Prilogi III;

„zagotavljanje informacijske varnosti“ – glej člen 10(1);

„znižanje stopnje tajnosti“ pomeni razvrstitev v nižjo stopnjo tajnosti;

„življenjski cikel KIS“ pomeni celoten čas obstoja komunikacijskega in informacijskega sistema, ki zajema začetek, zasnovo, načrtovanje, analizo zahtev, projektiranje, razvoj, testiranje, izvajanje, delovanje, vzdrževanje in razgradnjo;

*Dodatek B*

ENAKOVREDNE STOPNJE TAJNOSTI

| EU | TRÈS SECRET UE/EU TOP SECRET | SECRET UE/EU SECRET | CONFIDENTIEL UE/EU CONFIDENTIAL | RESTREINT UE/EU RESTRICTED |
|---|---|---|---|---|
| Belgija | Très Secret (Loi 11.12.1998)<br>Zeer Geheim (Wet 11.12.1998) | Secret (Loi 11.12.1998)<br>Geheim (Wet 11.12.1998) | Confidentiel (Loi 11.12.1998)<br>Vertrouwelijk (Wet 11.12.1998) | opomba [1] spodaj |
| Bolgarija | Строго секретно | Секретно | Поверително | За служебно ползване |
| Češka republika | Přísně tajné | Tajné | Důvěrné | Vyhrazené |
| Danska | Yderst hemmeligt | Hemmeligt | Fortroligt | Til tjenestebrug |
| Nemčija | STRENG GEHEIM | GEHEIM | VS [2]— VERTRAULICH | VS — NUR FÜR DEN DIENSTGEBRAUCH |
| Estonija | Täiesti salajane | Salajane | Konfidentsiaalne | Piiratud |
| Grčija | Άκρως Απόρρητο<br>Abr: ΑΑΠ | Απόρρητο<br>Abr: (ΑΠ) | Εμπιστευτικό<br>Abr: (ΕΜ) | Περιορισμένης Χρήσης<br>Abr: (ΠΧ) |
| Španija | SECRETO | RESERVADO | CONFIDENCIAL | DIFUSIÓN LIMITADA |
| Francija | Très Secret Défense | Secret Défense | Confidentiel Défense | opomba [3] spodaj |
| Irska | Top Secret | Secret | Confidential | Restricted |
| Italija | Segretissimo | Segreto | Riservatissimo | Riservato |
| Ciper | Άκρως Απόρρητο<br>Abr: (ΑΑΠ) | Απόρρητο<br>Abr: (ΑΠ) | Εμπιστευτικό<br>Abr: (ΕΜ) | Περιορισμένης Χρήσης<br>Abr: (ΠΧ) |
| Latvija | Sevišķi slepeni | Slepeni | Konfidenciāli | Dienesta vajadzībām |
| Litva | Visiškai slaptai | Slaptai | Konfidencialiai | Riboto naudojimo |
| Luksemburg | Très Secret Lux | Secret Lux | Confidentiel Lux | Restreint Lux |
| Madžarska | Szigorúan titkos! | Titkos! | Bizalmas! | Korlátozott terjesztésű! |
| Malta | L-Ogħla Segretezza | Sigriet | Kunfidenzjali | Ristrett |
| Nizozemska | Stg ZEER GEHEIM | Stg GEHEIM | Stg CONFIDENTIEEL | Dep VERTROUWELIJK |
| Avstrija | Streng Geheim | Geheim | Vertraulich | Eingeschränkt |
| Poljska | Ściśle Tajne | Tajne | Poufne | Zastrzeżone |
| Portugalska | Muito Secreto | Secreto | Confidencial | Reservado |
| Romunija | Strict secret de importanță deosebită | Strict secret | Secret | Secret de serviciu |

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

([1]) Diffusion Restreinte/Beperkte Verspreiding ni stopnja tajnosti v Belgiji. Belgija s podatki stopnje „RESTREINT UE/EU RESTRICTED“ dela in jih varuje na način, ki ni manj strog od standardov in postopkov, opisanih v varnostnih predpisih Sveta Evropske unije.
([2]) Nemčija: VS = Verschlusssache.
([3]) Francija v svojem nacionalnem sistemu ne uporablja stopnje „RESTREINT“. Francija s podatki stopnje „RESTREINT UE/EU RESTRICTED“ dela in jih varuje na način, ki ni manj strog od standardov in postopkov iz varnostnih predpisov Sveta Evropske unije.
([4]) Švedska: oznake stopenj tajnosti v zgornji vrstici uporabljajo obrambni organi, tiste iz spodnje vrstice pa drugi organi.

*Dodatek C*

SEZNAM NACIONALNIH VARNOSTNIH ORGANOV

**BELGIJA**
Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
B-1000 Bruxelles

Telefon sekretariata: + 32/2/501 45 42
Faks: + 32/2/501 45 96
E-pošta: nvo-ans@diplobel.fed.be

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

Telefon: + 45/33/14 88 88
Faks: + 45/33/43 01 90

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

Telefon: + 45/33/32 55 66
Faks: + 45/33/93 13 20

**BOLGARIJA**
State Commission on Information Security
90 Cherkovna Str.
BG-1505 Sofia

Telefon: + 359/2/921 5911
Faks: + 359/2/987 3750
E-pošta: dksi@government.bg
Spletno mesto: www.dksi.bg

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

Telefon: + 49/30/18 681 0
Faks: + 49/30/18 681 1441
E-pošta: oesIII3@bmi.bund.de

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

Telefon: + 420/257 28 33 35
Faks: + 420/257 28 31 10
E-pošta: czech.nsa@nbu.cz
Spletno mesto: www.nbu.cz

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

Telefon: +372/7170 113, +372/7170 117
Faks: +372/7170 213
E-pošta: nsa@kmin.ee

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

Telefon: + 353/1/ 478 08 22
Faks: + 353/1/ 408 29 59

**ŠPANIJA**
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
E-28023 Madrid

Telefon: + 34/91/372 50 00
Faks: + 34/91/372 58 08
E-pošta: nsa-sp@areatec.com

**GRČIJA**
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα

Τηλέφωνα: + 30/210/657 20 45 (ώρες γραφείου)
+ 30/210/657 20 09 (ώρες γραφείου)
Φαξ: + 30/210/653 62 79
+ 30/210/657 76 12

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos – Athens

Telefon: + 30/210/657 20 45
+ 30/210/657 20 09
Faks: + 30/210/653 62 79
+ 30/210/657 76 12

**FRANCIJA**
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
F-75700 Paris 07 SP

Telefon: + 33/1/71 75 81 77
Faks: + 33/1/71 75 82 00

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

Telefon: + 39/06/611 742 66
Faks: + 39/06/488 52 73

**CIPER**
ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος

Τηλέφωνα: + 357/22/80 75 69, + 357/22/80 76 43,
+ 357/22/80 77 64
Τηλεομοιότυπο: + 357/22/30 23 51

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
CY-1432 Nicosia

Telefon: + 357/22/80 75 69, + 357/22/80 76 43,
+357 /22/80 77 64
Faks: + 357/22/30 23 51
E-pošta: cynsa@mod.gov.cy

**LUKSEMBURG**
Autorité nationale de Sécurité
Boîte postale 2379
L-1023 Luxembourg

Telefon: + 352/2478 22 10 centrala
+ 352/2478 22 53 neposredna številka
Faks: + 352/2478 22 43

**MADŽARSKA**
Nemzeti Biztonsági Felügyelet
(National Security Authority)
P.O. Box 2
HU-1357 Budapest

Telefon: + 361/346 96 52
Faks: + 361/346 96 58
E-pošta: nbf@nbf.hu
Spletno mesto: www.nbf.hu

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

Telefon: + 356/21 24 98 44
Faks: + 356/25 69 53 21

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

Telefon: +371/6702 54 18
Faks: +371/6702 54 54
E-pošta: ndi@sab.gov.lv

**LITVA**
Lietuvos Respublikos paslapciu apsaugos koordinavimo komisija
The Commission for Secrets Protection Coordination of the Republic of Lithuania
National Security Authority
Gedimino 40/1
LT-01110 Vilnius

Telefon: + 370/5/266 32 01,
+ 370/5/266 32 02
Faks: + 370/5/266 32 00
E-pošta: nsa@vsd.lt

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

Telefon: + 31/70/320 44 00
Faks: + 31/70/320 07 33

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
NL-2500 ES Den Haag

Telefon: + 31/70/318 70 60
Faks: + 31/70/318 75 22

**AVSTRIJA**
Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
A-1014

Wien
Telefon: + 43/1/531 15 25 94
Faks: + 43/1/531 15 26 15

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

Telefon: + 48/22/585 73 60
Faks: + 48/22/585 85 09
E-pošta: nsa@abw.gov.pl
Spletno mesto: www.abw.gov.pl

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

Telefon: + 48/22/684 12 47
Faks: + 48/22/684 10 76
E-pošta: skw@skw.gov.pl

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

Telefon: 00 4 021 224 58 30
Faks: 00 4 021 224 07 14
E-pošta: nsa.romania@nsa.ro
Spletno mesto: www.orniss.ro

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

Telefon: +351/ 213 031 710
Faks: +351/ 213 031 711

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

Telefon: + 386 14781390
Faks: + 386 14781399

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

Telefon: + 421/2/68 69 23 14
Faks: + 421/2/63 82 40 05
Spletno mesto: www.nbusr.sk

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

Telefon: + 46/8/405 54 44
Faks: + 46/8/723 11 76
E-pošta: ud-nsa@foreign.ministry.se

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

Telefon 1: + 358/9/160 56487
Telefon 2: + 358/9/160 56484
Faks: + 358/9/160 55140
E-pošta: NSA@formin.fi

**ZDRUŽENO KRALJESTVO**
UK National Security Authority
Room 335, 3rd floor
70 Whitehall
PO Box 60628 London
SW1A 2AS

Telefon 1: + 44/20/7276 5649
Telefon 2: +44/20/7276 5497
Faks: + 44/20/7276 5651
E-pošta: UK-NSA@cabinet-office.x.gsi.gov.uk

*Dodatek D*

SEZNAM KRATIC

| Kratica | Pomen |
|---|---|
| AQUA | ustrezno usposobljen organ (Appropriately Qualified Authority) |
| BPS | storitve v zvezi z zaščito razmejitve (Boundary Protection Services) |
| CAA | organ za odobritev šifrirnih metod in izdelkov (Crypto Approval Authority) |
| CCTV | sistem televizije zaprtega kroga (Closed Circuit Television) |
| CDA | organ za razpošiljanje šifriranega materiala (Crypto Distribution Authority) |
| CFSP | skupna zunanja in varnostna politika (Common Foreign and Security Policy) |
| KIS | komunikacijski in informacijski sistemi (Communication and Information Systems (CIS)) |
| COREPER | Odbor stalnih predstavnikov (Commitee of Permanent Representatives) |
| CSDP | skupna varnostna in obrambna politika (Common Security and Defence Policy) |
| DSA | imenovani varnostni organ (Designated Security Authority) |
| ECSD | Varnostni direktorat Evropske komisije (European Commission Security Directorate) |
| EUCI | tajni podatki EU (EU Classified Information) |
| EUSR | posebni predstavnik EU (EU Special Representative) |
| FSC | varnostno dovoljenje organizacije (Facility Security Clearance) |
| GSS | generalni sekretariat Sveta (General Secretariat of the Council (GSC)) |
| IA | informacijska varnost (Information Assurance) |
| IAA | organ za zagotavljanje informacijske varnosti (Information Assurance Authority) |
| IDS | sistem odkrivanja vdorov (Intrusion Detection System) |
| IT | informacijska tehnologija (Information Technology) |
| NSA | nacionalni varnostni organ (National Security Authority) |
| PSC | pooblastilo za dostop do tajnih podatkov (Personnel Security Clearance) |
| PSCC | potrdilo za dostop do tajnih podatkov (Personnel Security Clearance Certificate) |
| PSI | varnostna navodila za program/projekt (Programme/Project Security Instructions) |
| SAA | organ za varnostno akreditacijo (Security Accreditation Authority) |
| SAB | odbor za varnostno akreditacijo (Security Accreditation Board) |
| SAL | listina o varnostnih vidikih (Security Aspects Letter) |
| SecOPs | varnostno-operativni postopki (Security Operating Procedures) |
| SCG | vodič po stopnjah tajnosti (Security Classification Guide) |
| SSRS | izjava o posebnih varnostnih zahtevah, značilnih za sistem (System-Specific Security Requirement Statement) |
| TA | organ TEMPEST (TEMPEST Authority) |