IV

(Informacije)

INFORMACIJE INSTITUCIJ, ORGANOV, URADOV IN AGENCIJ EVROPSKE UNIJE

EVROPSKA SLUŽBA ZA ZUNANJE DELOVANJE

Sklep visokega predstavnika Unije za zunanje zadeve in varnostno politiko z dne 19. septembra 2017 o varnostnih pravilih za Evropsko službo za zunanje delovanje

ADMIN(2017) 10

(2018/C 126/01)

VISOKI PREDSTAVNIK UNIJE ZA ZUNANJE ZADEVE IN VARNOSTNO POLITIKO JE –

ob upoštevanju Sklepa Sveta 2010/427/EU z dne 26. julija 2010 o organizaciji in delovanju Evropske službe za zunanje delovanje ([1]) (v nadaljnjem besedilu: ESZD),

ob upoštevanju mnenja odbora iz člena 9(6) Sklepa visokega predstavnika z dne 15. junija 2011 o varnostnih pravilih za Evropsko službo za zunanje delovanje ([2]),

ob upoštevanju naslednjega:

(1) ESZD bi morala kot samostojno delovno telo Evropske unije (EU) imeti varnostna pravila iz člena 10(1) Sklepa Sveta 2010/427/EU.

(2) Visoki predstavnik Unije za zunanje zadeve in varnostno politiko (v nadaljnjem besedilu: visoki predstavnik) mora odločiti o varnostnih pravilih za ESZD, ki zajemajo vse varnostne vidike v zvezi z delovanjem ESZD, da lahko ESZD učinkovito obvladuje tveganja za osebje v njeni pristojnosti, svoja materialna sredstva, podatke in obiskovalce ter da izpolnjuje svoje dolžnosti glede skrbnosti v zvezi s tem.

(3) Zlasti je treba zagotoviti stopnjo varovanja osebja v pristojnosti ESZD, materialnih sredstev ESZD, vključno s komunikacijskimi in informacijskimi sistemi, podatkov in obiskovalcev, ki je v skladu z najboljšo prakso v Svetu, Komisiji, državah članicah in po potrebi v mednarodnih organizacijah.

(4) Varnostna pravila za ESZD bi morala prispevati k skladnejšemu celovitemu splošnemu okviru znotraj EU za varovanje tajnih podatkov EU na podlagi varnostnih pravil Sveta Evropske unije (v nadaljnjem besedilu: Svet) in varnostnih določb Evropske komisije ter čim bolj skladno z njimi.

(5) ESZD, Svet in Komisija se zavzemajo za enakovredne standarde varovanja tajnih podatkov EU.

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

([1]) UL L 201, 3.8.2010, str. 30.
([2]) UL C 304, 15.10.2011, str. 7.

(7) Določiti je treba organizacijsko strukturo za zagotavljanje varnosti v ESZD in dodeliti naloge varovanja v okviru struktur ESZD.

(8) Visoki predstavnik bi se moral po potrebi opreti na ustrezno strokovno znanje iz držav članic, generalnega sekretariata Sveta in Komisije.

(9) Visoki predstavnik bi moral sprejeti vse ustrezne ukrepe za izvajanje teh pravil ob podpori držav članic, generalnega sekretariata Sveta in Komisije.

(10) Generalni sekretar ESZD je varnostni organ ESZD in člen 1 Sklepa ADMIN (2015)34 z dne 14. septembra 2015 generalnega sekretarja Evropske službe za zunanje delovanje določa, da varnostne naloge varnostnega organa, kot so določene v varnostnih pravilih ESZD, izvaja generalni direktor za proračun in upravo –

SPREJEL NASLEDNJI SKLEP:

Člen 1

Namen in področje uporabe

Ta sklep določa pravila za varnost Evropske službe za zunanje delovanje (v nadaljnjem besedilu: varnostna pravila ESZD).

V skladu s členom 10(1) Sklepa Sveta 2010/427/EU z dne 26. julija 2010 o organizaciji in delovanju Evropske službe za zunanje delovanje se uporablja za osebje ESZD in za vse osebje delegacij Unije ne glede na njihov upravni položaj ali poreklo ter določa splošni regulativni okvir za učinkovito obvladovanje tveganj za osebje v pristojnosti ESZD, kakor je določeno v členu 2, prostore ESZD, materialna sredstva, podatke in obiskovalce.

Člen 2

Opredelitev pojmov

V tem sklepu se uporabljajo naslednje opredelitve:

(a) „Osebje ESZD“ pomeni uradnike in druge uslužbence ESZD, vključno z osebjem diplomatskih služb držav članic, ki so imenovani za začasne uslužbence, ter napotene nacionalne strokovnjake, kakor je opredeljeno v členu 6 Sklepa Sveta 2010/427/EU z dne 26. julija 2010 o organizaciji in delovanju Evropske službe za zunanje delovanje.

(b) „Osebje v pristojnosti ESZD“ pomeni osebje ESZD na sedežu in v vseh delegacijah Unije ter vse osebje delegacij Unije ne glede na njihov upravni položaj ali poreklo ter, v okviru tega sklepa, tudi visokega predstavnika in po potrebi drugo osebje v prostorih sedeža ESZD.

(c) „Vzdrževanci“ pomenijo člane družine osebja v pristojnosti ESZD v delegacijah Unije, ki so del njihovega gospodinjstva, kakor je bilo priglašeno ministrstvu za zunanje zadeve države sprejemnice.

(d) „Prostori ESZD“ pomenijo vse poslovne enote ESZD, vključno z zgradbami, pisarnami, sobami in drugimi območji ter območji s komunikacijskimi in informacijskimi sistemi (vključno s tistimi za delo s tajnimi podatki EU), kjer ESZD izvaja stalne ali začasne dejavnosti.

(e) „Varnostni interesi ESZD“ pomenijo osebje v pristojnosti ESZD, prostore ESZD, vzdrževance, materialna sredstva, vključno s komunikacijskimi in informacijskimi sistemi, podatke in obiskovalce.

(f) „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.

(g) „Delegacija Unije“ pomeni delegacijo Unije v tretji državi in mednarodni organizaciji iz člena 1(4) Sklepa Sveta 2010/427/EU z dne 26. julija 2010 o organizaciji in delovanju Evropske službe za zunanje delovanje.

Druge opredelitve so naštete v ustreznih prilogah in Dodatku A.

Člen 3

Skrbnost

1. Cilj varnostnih pravil ESZD je izpolnjevanje dolžnosti glede skrbnosti ESZD.

2. Skrbnost ESZD zajema skrbno sprejemanje razumnih ukrepov za izvajanje varnostnih ukrepov, namenjenih preprečitvi škode za varnostne interese ESZD, ki jo je mogoče razumno predvideti.

Zajema elemente varnosti in zaščite, vključno s tistimi, ki so posledica izrednih razmer ali kriz, ne glede na njihovo naravo.

3. Ob upoštevanju dolžnosti glede skrbnosti držav članic, institucij ali organov EU ter drugih strani z osebjem v delegacijah Unije in/ali v prostorih delegacij Unije ali take dolžnosti, ki jo ima ESZD, kadar delegacije Unije gostujejo v zgoraj omenjenih prostorih drugih strani, ESZD sklene dogovore o izvajanju z vsakim od zgornjih subjektov, v katerih so določene njihove vloge in odgovornosti, naloge in mehanizmi sodelovanja.

Člen 4

Materialna varnost in varnost infrastrukture

1. ESZD sprejme vse ustrezne (stalne in začasne) ukrepe fizične varnosti, vključno z ureditvijo nadzora dostopa, za vse prostore ESZD, katerih namen je zaščita varnostnih interesov ESZD. Taki ukrepi se upoštevajo pri oblikovanju in načrtovanju novih prostorov ali pred najemanjem obstoječih prostorov.

2. Osebju v pristojnosti ESZD in vzdrževancem se lahko zaradi varnostnih razlogov za določeno obdobje in na določenih področjih naložijo posebne obveznosti ali omejitve.

3. Ukrepi iz odstavkov 1 in 2 so sorazmerni z ocenjenim tveganjem.

Člen 5

Stopnje pripravljenosti in obvladovanje kriznih razmer

1. Varnostni organ ESZD, kot je opredeljen v členu 13(1) oddelka I, je v pričakovanju groženj in incidentov, ki vplivajo na varnost v ESZD, ter kot odziv nanje odgovoren za uvedbo ustreznih ukrepov za stopnje pripravljenosti ter za ukrepe, potrebne za obvladovanje kriznih razmer.

2. Ukrepi za stopnje pripravljenosti iz odstavka 1 so sorazmerni z varnostno grožnjo. Stopnje pripravljenosti se opredelijo v tesnem sodelovanju s pristojnimi službami drugih institucij, agencij in organov Unije in z državami članicami ali z državami članicami, v katerih se nahajajo prostori ESZD.

3. Varnostni organ ESZD je kontaktna točka v zvezi s stopnjami pripravljenosti in obvladovanjem kriznih razmer.

Člen 6

Varovanje tajnih podatkov

1. Varovanje tajnih podatkov EU urejajo zahteve iz tega sklepa, zlasti Priloga A. Imetnik katerega koli tajnega podatka EU je odgovoren za njegovo ustrezno varovanje.

2. ESZD zagotavlja, da se dostop do tajnih podatkov dodeli le posameznikom, ki izpolnjujejo pogoje iz člena 5 Priloge A.

3. Pogoje, pod katerimi lahko lokalni uslužbenci dostopajo do tajnih podatkov EU, prav tako določi visoki predstavnik, in sicer v skladu s pravili za varovanje tajnih podatkov EU iz Priloge A k temu sklepu.

4. Direktorat ESZD, odgovoren za varnost, upravlja podatkovno zbirko s statusom dostopa do tajnih podatkov osebja v pristojnosti ESZD in izvajalcev ESZD.

5. Če države članice v strukture ali omrežja ESZD vnesejo tajne podatke z nacionalno oznako stopnje tajnosti, ESZD te podatke varuje v skladu z zahtevami, ki se uporabljajo za tajne podatke EU enakovredne stopnje, kakor je določeno v preglednici enakovrednih stopenj tajnosti v Dodatku B k temu sklepu.

6. Območja v ESZD, v katerih se hranijo podatki stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, se določijo kot varovana območja v skladu s pravili iz Priloge A II k temu sklepu in jih odobri varnostni organ ESZD.

7. Postopki za izpolnjevanje odgovornosti visokega predstavnika v okviru sporazumov ali dogovorov o izvajanju izmenjave tajnih podatkov EU s tretjimi državami ali mednarodnimi organizacijami so opisani v prilogah A in A VI k temu sklepu.

8. Generalni sekretar določi pogoje, pod katerimi lahko ESZD posreduje tajne podatke EU, ki jih poseduje, drugim institucijam, organom, uradom ali agencijam Unije. V ta namen se lahko vzpostavi ustrezen okvir, vključno s sklenitvijo medinstitucionalnih dogovorov ali drugih ureditev, kjer je to potrebno za ta namen.

9. Vsak tak okvir zagotovi, da so tajni podatki EU ustrezno zavarovani glede na njihovo stopnjo tajnosti in v skladu z osnovnimi načeli in minimalnimi standardi, ki so enakovredni tistim iz tega sklepa.

Člen 7

Varnostni incidenti in izredne razmere

1. ESZD za pravočasen in učinkovit odziv na varnostne incidente vzpostavi postopek poročanja o takih incidentih in izrednih razmerah, ki deluje štiriindvajset ur na dan, sedem dni v tednu in zajema vse vrste varnostnih incidentov ali nevarnosti za varnostne interese ESZD (npr. nesreče, spore, zlonamerne dejavnosti, kriminalne dejavnosti, ugrabitve in pridržanje talcev, krizne zdravstvene razmere, incidente v zvezi s komunikacijskimi in informacijskimi sistemi, kibernetske napade itd.).

2. Med sedežem ESZD, delegacijami Unije, Svetom, Komisijo, posebnimi predstavniki EU in državami članicami se vzpostavijo mehanizmi izredne povezave, ki omogočajo podporo pri obvladovanju varnostnih incidentov, ki vključujejo osebje, in njihovih posledic, vključno z oblikovanjem načrtov za izredne razmere.

3. To obvladovanje varnostnih incidentov med drugim vključuje:

— postopke za učinkovito podporo postopka odločanja v zvezi z varnostnim incidentom, ki vključuje osebje, tudi s sklepi o prekinitvi ali začasni prekinitvi misije, ter

— politiko in postopke umika osebja – npr. ob izginotju osebja, ugrabitvi ali zadržanju talcev – pri čemer se upoštevajo zlasti odgovornosti držav članic, institucij EU in ESZD. Pri potrebi po posebnih zmogljivostih v okviru upravljanja takih operacij se upoštevajo viri, ki jih lahko zagotovijo države članice.

4. ESZD sprejme ustrezne dogovore o izvajanju poročanja o varnostnih incidentih v delegacijah Unije. Kadar je to ustrezno, se o tem obvesti države članice, Komisijo, kateri koli drug pristojni organ in pristojne varnostne odbore.

5. Postopke obvladovanja incidentov bi bilo treba redno izvajati in pregledovati.

Člen 8

Varovanje komunikacijskih in informacijskih sistemov

1. ESZD varuje podatke, s katerimi poteka delo v komunikacijskih in informacijskih sistemih (v nadaljnjem besedilu: KIS), pred nevarnostmi, ki ogrožajo njihovo zaupnost, celovitost, razpoložljivost, avtentičnost in nezatajljivost.

2. Pravila, varnostne smernice in varnostni program za varovanje vseh KIS, ki jih ima v lasti ali upravljanju ESZD, odobri varnostni organ ESZD.

3. Pravila, politika in program so skladni, njihovo izvajanje pa dobro usklajeno s pravili, politiko in programom Sveta in Komisije ter, kjer je to ustrezno, z varnostnimi politikami, ki jih uporabljajo države članice.

4. Za vse komunikacijske in informacijske sisteme, v katerih poteka delo s tajnimi podatki, se opravi akreditacijski postopek. ESZD uporablja sistem za upravljanje varnostne akreditacije po posvetovanju z generalnim sekretariatom Sveta in Komisijo.

5. Kadar tajne podatke EU, s katerimi poteka delo v ESZD, varujejo šifrirni izdelki, take izdelke na priporočilo Varnostnega odbora Sveta odobri organ ESZD za odobritev šifrirnih metod in izdelkov.

6. Varnostni organ ESZD po potrebi določi naslednje funkcije za zagotavljanje informacijske varnosti:

(a) organ za zagotavljanje informacijske varnosti;

(b) organ TEMPEST;

(c) organ za odobritev šifrirnih metod iz izdelkov;

(d) organ za razpošiljanje šifrirnega materiala.

7. Varnostni organ ESZD za vsak sistem določi naslednje funkcije:

(a) organ za varnostno akreditacijo;

(b) operativni organ za zagotavljanje informacijske varnosti.

8. Določbe za izvajanje tega člena v zvezi z varovanjem tajnih podatkov EU so določene v prilogah A in A IV.

Člen 9

Kršitev varovanja tajnosti in nepooblaščeno razkritje tajnih podatkov

1. Kršitev varovanja tajnosti je posledica dejanja ali opustitve dejanja, ki je v nasprotju z varnostnimi pravili iz tega sklepa in/ali z varnostnimi politikami ali smernicami, ki določajo vse potrebne ukrepe za njegovo izvajanje, kot je potrjeno v skladu s členom 21(1).

2. Za nepooblaščeno razkritje tajnih podatkov gre, kadar so bili tajni podatki v celoti ali delno razkriti nepooblaščenim osebam ali subjektom.

3. O vseh kršitvah ali domnevnih kršitvah varovanja tajnosti ter o vseh nepooblaščenih razkritjih ali domnevnih razkritjih tajnih podatkov se nemudoma obvesti direktorat ESZD, odgovoren za varnost, ki sprejme ustrezne ukrepe, kot je določeno v členu 11 Priloge A.

4. Za vsakega posameznika, ki je odgovoren za kršitev varnostnih pravil iz tega sklepa ali za razkritje tajnih podatkov, se lahko uvede disciplinski ukrep in/ali se sproži pravni spor v skladu z zakoni, pravili in predpisi, ki se uporabljajo, kot je določeno v členu 11(3) Priloge A.

Člen 10

Preiskovanje varnostnih incidentov, kršitev in/ali razkritij ter popravni ukrepi

1. Brez poseganja v člen 86 (disciplinski ukrepi) in Prilogo IX h kadrovskim predpisom ([1]) lahko direktorat ESZD, odgovoren za varnost, izvaja varnostne preiskave:

(a) v primeru morebitnega uhajanja, neustreznega obravnavanja ali nepooblaščenega razkritja tajnih podatkov EU ter tajnih ali občutljivih podatkov, ki niso tajni, EURATOM;

(b) za preprečevanje napadov sovražnih obveščevalnih služb na ESZD in njeno osebje;

(c) za preprečevanje terorističnih napadov na ESZD in njeno osebje;

(d) v primeru kibernetskih incidentov;

(e) v primeru drugih incidentih, ki vplivajo ali lahko vplivajo na splošno varnost v ESZD, vključno s sumi kaznivih dejanj.

2. Direktorat ESZD, odgovoren za varnost, s pomočjo strokovnjakov iz držav članic in/ali po potrebi strokovnjakov iz drugih institucij EU po pooblastilu varnostnega organa ESZD, kadar je to potrebno, izvede vse potrebne popravljalne ukrepe na podlagi preiskav, kadar in če je to ustrezno.

Za izvajanje in usklajevanje varnostnih preiskav v ESZD je lahko pristojno le osebje, ki mu varnostni organ ESZD na podlagi njegovih trenutnih zadolžitev podeli poimensko pooblastilo.

3. Preiskovalci imajo dostop do vseh potrebnih podatkov za izvedbo takih preiskav in imajo pri tem popolno podporo služb in osebja ESZD.

Preiskovalci lahko ustrezno ukrepajo, da bi zaščitili dokaze, pri čemer mora biti njihovo ukrepanje sorazmerno z resnostjo primera, ki se preiskuje.

4. Kadar je dostop do podatkov povezan z osebnimi podatki, vključno s tistimi, ki so zajeti v komunikacijskih in informacijskih sistemih, je tak dostop urejen z Uredbo (ES) št. 45/2001 ([2]).

5. Kadar je treba ustvariti preiskovalno podatkovno zbirko, ki zajema osebne podatke, se o tem v skladu z zgornjo uredbo obvesti evropskega nadzornika za varstvo podatkov (ENVP).

Člen 11

Obvladovanje varnostnega tveganja

1. ESZD za opredelitev svojih potreb po varnosti v tesnem sodelovanju z Varnostnim direktoratom Komisije in po potrebi z Varnostnim uradom generalnega sekretariata Sveta razvije celovito metodologijo za oceno varnostnih tveganj.

2. Za obvladovanje tveganja, povezanega z varnostnimi interesi ESZD, je predviden postopek. Ta postopek je namenjen opredelitvi znanih varnostnih tveganj in varnostnih ukrepov za zmanjšanje takih tveganj na sprejemljivo raven ter izvajanju ukrepov v skladu s konceptom globinske obrambe. Učinkovitost teh ukrepov in raven tveganja se nenehno ocenjujeta.

([1]) Kadrovski predpisi za uradnike Evropske unije in Pogoji za zaposlitev drugih uslužbencev Evropske unije, določenih v Uredbi (EGS, Euratom, ESPJ) št. 259/68 Sveta (UL L 56, 4.3.1968, str. 1), v nadaljnjem besedilu: kadrovski predpisi.

([2]) Uredba (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, 12.1.2001, str. 1).

3. Vloge, odgovornosti in naloge iz tega sklepa ne vplivajo na odgovornost vsakega člana osebja v pristojnosti ESZD. Zlasti osebje EU na misijah v tretjih državah mora glede lastne varnosti in zaščite ravnati razumno in po ustrezni presoji ter pri tem upoštevati vsa veljavna varnostna pravila, predpise, postopke in navodila.

4. Za preprečevanje in obvladovanje varnostnih tveganj lahko pooblaščeno osebje opravi preverjanje zanesljivosti oseb, za katere velja ta sklep, da se ugotovi, ali dostop takih oseb do prostorov ali podatkov ESZD predstavlja grožnjo za varnost. V ta namen ter v skladu z Uredbo (ES) št. 45/2001 lahko zadevno pooblaščeno osebje: (a) uporabi vse vire informacij, ki so na voljo ESZD, pri čemer upošteva zanesljivost vira informacij; (b) dostopa do kadrovskih map ali podatkov, ki jih ima ESZD o posameznikih, ki jih zaposluje ali namerava zaposliti, ali o pogodbenem osebju, kadar je to ustrezno utemeljeno.

5. ESZD sprejme vse ustrezne ukrepe, da zagotovi zaščito svojih varnostnih interesov in prepreči škodo v zvezi z njimi, ki jo je mogoče razumno predvideti.

6. V okviru ESZD so varnostni ukrepi za varovanje tajnih podatkov EU v njihovem življenjskem ciklu, ko so označeni za tajne, sorazmerni zlasti s stopnjo tajnosti, obliko in količino podatkov ali materialnih sredstev, lokacijo in vrsto objektov, v katerih se tajni podatki EU hranijo, ter z nevarnostjo, zlasti z lokalno oceno nevarnosti, zlonamernih in/ali kriminalnih dejavnosti, vključno z vohunjenjem, sabotažo in terorizmom.

Člen 12

Ozaveščanje in usposabljanje na področju varnosti

1. Varnostni organ ESZD zagotovi, da se pripravijo in izvajajo ustrezni programi ozaveščanja in usposabljanja na področju varnosti ter da se članom osebja v pristojnosti ESZD in po potrebi njihovim vzdrževancem zagotovijo potrebna navodila in usposabljanje na področju varnosti, ki so sorazmerni s tveganji na njihovem delovnem mestu ali v njihovem stalnem prebivališču.

2. Preden se članom osebja dodeli dostop do tajnih podatkov EU ter nato v rednih presledkih, so vsi poučeni o svoji odgovornosti za varovanje tajnih podatkov EU v skladu s pravili po členu 6 in slednjo tudi potrdijo.

Člen 13

Organiziranost varovanja tajnosti v ESZD

Oddelek 1

Splošne določbe

1. Generalni sekretar je varnostni organ ESZD. Generalni sekretar v tej funkciji zagotovi, da:

(a) se varnostni ukrepi o vseh varnostnih zadevah, pomembnih za dejavnosti ESZD, tudi glede vrste tveganj za varnostne interese ESZD ter načinov zaščite pred njimi, po potrebi uskladijo s pristojnimi organi držav članic, generalnim sekretariatom Sveta in Komisijo ter po potrebi s tretjimi državami ali mednarodnimi organizacijami;

(b) se varnostni vidiki v celoti upoštevajo od začetka vseh dejavnosti ESZD;

(c) se dostop do tajnih podatkov dodeli le posameznikom, ki izpolnjujejo pogoje iz člena 5 Priloge A;

(d) se vzpostavi sistem registrov, ki zagotavlja, da poteka delo s podatki stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje v skladu s tem sklepom znotraj ESZD ali kadar se dajo državam članicam EU, institucijam, organom in agencijam EU ter drugim pooblaščenim prejemnikom. Vodi se posebna evidenca vseh tajnih podatkov EU, ki jih ESZD da tretjim državam ali mednarodnim organizacijam, ter vseh drugih tajnih podatkov, ki jih prejme od tretjih držav ali mednarodnih organizacij;

(e) se opravijo varnostne inšpekcije iz člena 16;

(f) se izvedejo preiskave vsake dejanske ali domnevne kršitve varovanja tajnosti, vključno z vsakim dejanskim ali domnevnim nepooblaščenim razkritjem ali izgubo tajnih podatkov, ki jih hrani ESZD ali z izvorom v ESZD, ter se ustrezni varnostni organi zaprosijo za pomoč pri takih preiskavah;

(g) se za pravočasen in učinkovit odziv na varnostne incidente vzpostavijo ustrezni načrti in mehanizmi upravljanja incidentov in posledic;

(h) se sprejmejo ustrezni ukrepi v primerih, ko posamezniki ne ravnajo v skladu s tem sklepom;

(i) da so za zaščito varnostnih interesov ESZD sprejeti ustrezni fizični in organizacijski ukrepi.

V zvezi s tem varnostni organ ESZD:

— po posvetovanju s Komisijo določi varnostno kategorijo delegacij Unije,

— po posvetovanju z visokim predstavnikom, kjer je ustrezno, določi, kdaj bi bilo treba evakuirati osebje delegacije, če to zahtevajo varnostne razmere,

— določi ukrepe, ki se bodo po potrebi uporabili za zaščito vzdrževancev ob upoštevanju dogovorov z institucijami EU iz člena 3(3),

— odobri politiko šifrirnega sporočanja, zlasti program namestitve šifrirnih izdelkov in mehanizma.

2. Varnostnemu organu ESZD pri tej nalogi pomagajo DGBA, direktor ESZD, odgovoren za varnost, in, če je primerno, namestnik generalnega sekretarja za SVOP in krizno odzivanje.

3. Generalni sekretar lahko kot varnostni organ ESZD po potrebi prenese s tem povezane naloge.

4. Vsak vodja oddelka/enote je odgovoren za izvajanje pravil za varovanje tajnih podatkov EU znotraj svojega oddelka/enote.

Poleg zgornjih odgovornosti vsak vodja oddelka/enote imenuje osebje za izvajanje funkcije oddelčnega varnostnega koordinatorja, katerega sredstva bodo sorazmerna s količino tajnih podatkov EU, s katerimi dela navedeni oddelek/navedena enota.

Oddelčni varnostni koordinatorji po potrebi in kadar je ustrezno pomagajo svoji vodji oddelka/enote pri izvajanju nalog na področju varnosti, kot so:

(a) razvoj vseh dodatnih varnostnih zahtev, prilagojenih posebnim potrebam oddelka/enote;

(b) redno poučevanje članov njihovega oddelka/enote glede varnosti;

(c) zagotavljanje spoštovanja načela potrebe po seznanitvi s podatki na njihovem oddelku/enoti;

(d) redno posodabljanje seznama varnih kod in ključev;

(e) vzdrževanje varnostnih postopkov in varnostnih ukrepov;

(f) obveščanje direktorja in direktorata, odgovornega za varnost, o vseh kršitvah varovanja tajnosti in/ali o nepooblaščenem razkritju tajnih podatkov EU;

(g) pridobivanje informacij od osebja, ki ni več zaposleno v ESZD;

(h) redno poročanje nadrejenim o varnostnih zadevah oddelka/enote;

(i) povezovanje z direktoratom ESZD, odgovornim za varnost, v zvezi z varnostnimi vprašanji.

Direktorat ESZD, odgovoren za varnost, se pravočasno obvesti o vsaki dejavnosti ali vprašanju, ki bi lahko vplivalo na varnost.

5. Vsak vodja delegacije je odgovoren za izvajanje vseh ukrepov v zvezi z varnostjo delegacije Unije.

Oddelek 2

Direktorat ESZD, odgovoren za varnost

1. ESZD ima direktorat, ki je odgovoren za varnost. Direktorat izvaja naslednje naloge:

(a) upravlja, koordinira, nadzira in/ali izvaja vse varnostne ukrepe v vseh prostorih v pristojnosti ESZD, na sedežu, znotraj EU in v tretjih državah;

(b) zagotavlja doslednost in usklajenost s tem sklepom ter z izvedbenimi določbami za vsako dejavnost, ki bi lahko vplivala na zaščito varnostnih interesov ESZD;

(c) je glavni svetovalec visokega predstavnika, varnostnega organa ESZD in namestnika generalnega sekretarja glede vseh zadev na področju varnosti;

(d) v skladu s členom 10(3) Sklepa Sveta 2010/427/EU o organizaciji in delovanju ESZD mu pomagajo ustrezne službe držav članic;

(e) podpira dejavnosti organa za varnostno akreditacijo ESZD z ocenjevanjem fizične varnosti splošnega varnostnega okolja in lokalnega varnostnega okolja komunikacijskih in informacijskih sistemov, v katerih poteka delo s tajnimi podatki EU, ter prostorov, ki bodo pooblaščeni za delo s tajnimi podatki EU in njihovo shranjevanje.

2. Direktor ESZD, odgovoren za varnost, je odgovoren za:

(a) zagotavljanje celostne zaščite varnostnih interesov ESZD;

(b) oblikovanje, pregledovanje in posodabljanje varnostnih pravil ter uskladitev varnostnih ukrepov s pristojnimi organi držav članic ter po potrebi s pristojnimi organi tretjih držav in mednarodnih organizacij, ki jih z EU povezujejo varnostni sporazumi in/ali druge varnostne ureditve;

(c) podporo v postopkih Varnostnega odbora ESZD, kakor je določeno v členu 15(1) tega sklepa;

(d) povezovanje s partnerji ali organi, ki se razlikujejo od tistih iz zgornje točke (b), glede varnostnih zadev, kadar je to ustrezno;

(e) določanje prednostnih nalog in oblikovanje predlogov za upravljanje proračuna za varnost na sedežu in v delegacijah Unije.

3. Vodja direktorata ESZD, odgovornega za varnost:

(a) zagotavlja, da se vodijo evidence kršitev varovanja tajnosti in nepooblaščenih razkritij, ter po potrebi začne ustrezne preiskave;

(b) se redno sestaja in, kadar je potrebno, razpravlja o področjih skupnega interesa z direktorjem za varnost generalnega sekretariata Sveta in direktorjem za varnost Varnostnega direktorata Komisije.

4. Direktorat ESZD, odgovoren za varnost, vzpostavi stik in ves čas tesno sodeluje z:

— oddelki za varnost na ministrstvih za zunanje zadeve držav članic,

— nacionalnimi varnostnimi organi in/ali drugimi pristojnimi varnostnimi organi držav članic, da bi prejel njihovo pomoč v zvezi s podatki, ki jih potrebuje za oceno takih nevarnosti in tveganj za ESZD, njeno osebje, dejavnosti, sredstva in vire ter tajne podatke na njenem običajnem sedežu,

— pristojnimi varnostnimi organi držav članic ali držav gostiteljic na ozemlju, na katerem lahko ESZD izvaja svoje dejavnosti, v zvezi z vsemi zadevami na področju varnosti njenega osebja, dejavnosti, sredstev in virov ter tajnih podatkov med bivanjem na njihovem ozemlju,

— Varnostnim uradom generalnega sekretariata Sveta in Varnostnim direktoratom Generalnega direktorata za človeške vire in varnost Komisije ter po potrebi z oddelki za varnost drugih institucij, organov in agencij EU,

— oddelki za varnost tretjih držav ali mednarodnih organizacij v zvezi s kakršnim koli uporabnim usklajevanjem ter

— nacionalnimi varnostnimi organi držav članic v zvezi z vsemi zadevami na področju varstva tajnih podatkov EU.

Oddelek 3

Delegacije Unije

1. Vsak vodja delegacije je odgovoren za lokalno izvajanje in upravljanje vseh ukrepov na področju zaščite varnostnih interesov ESZD v prostorih in pristojnosti delegacije Unije.

Po posvetovanju s pristojnimi organi države gostiteljice bo po potrebi sprejel vse smiselno izvedljive ukrepe, da bi zagotovil obstoj ustreznih fizičnih in organizacijskih ukrepov za doseganje tega cilja.

Vodja delegacije po potrebi oblikuje varnostne postopke za zaščito vzdrževancev, kakor so bili opredeljeni v členu 2(c), pri čemer upošteva kakršne koli dogovore o izvajanju iz člena 3(3). Vodja delegacije letno poroča vodji direktorata ESZD, odgovornega za varnost, o vseh vprašanjih na področju varnosti, ki so v njegovi pristojnosti.

Pri teh nalogah mu pomagajo direktorat ESZD, odgovoren za varnost, varnostna ekipa delegacije Unije, v kateri je osebje, ki opravlja varnostne naloge in funkcije, ter specializirano varnostno osebje, ki se razporedi po potrebi.

Delegacija Unije vzpostavi redne stike in tesno sodelovanje pri varnostnih vprašanjih z diplomatskimi misijami držav članic.

2. Vodja delegacije bo poleg tega:

— za delegacijo Unije oblikoval podroben varnostni načrt in načrt obvladovanja nepredvidljivih razmer na podlagi operativnih postopkov splošnega standarda,

— upravljal učinkovit sistem za obvladovanje varnostnih incidentov in izrednih razmer, ki deluje ves dan vse dni v tednu, znotraj obsega delovanja delegacije Unije,

— zagotavljal, da je vse osebje delegacije Unije zavarovano v skladu s pogoji s tega področja,

— zagotavljal, da je varnost del uvodnega usposabljanja v okviru delegacije Unije, ki se ga pred prihodom ali ob prihodu v delegacijo Unije udeleži vse osebje delegacije Unije, ter

— zagotavljal, da se izvajajo vsa priporočila na podlagi varnostnih ocen, ter predložil redna pisna poročila o njihovem izvajanju in drugih varnostnih vprašanjih varnostnemu organu ESZD.

3. Vodja delegacije lahko prenese izvajanje svojih varnostnih nalog na varnostnega koordinatorja delegacije, ki je namestnik vodje delegacije, kadar ta ni bil imenovan, pa na drugega ustreznega zaposlenega, pri tem pa je še vedno odgovoren za zaščito upravljanja varovanja in zagotavljanje prilagodljivosti organizacije.

Varnostnemu koordinatorju delegacije se lahko zaupajo zlasti naslednje odgovornosti:

— usklajevanje varnostnih funkcij v delegacijah Unije;

— povezovanje s pristojnimi organi države gostiteljice in ustreznimi organi na veleposlaništvih in v diplomatskih misijah držav članic v zvezi z varnostnimi vprašanji,

— izvajanje ustreznih postopkov upravljanja varovanja, povezanih z varnostnimi interesi ESZD, vključno z varovanjem tajnih podatkov EU,

— zagotavljanje upoštevanja varnostnih pravil in navodil;

— poučevanje osebja o varnostnih pravilih, ki se uporabljajo zanj, in o posebnih tveganjih v državi gostiteljici,

— predložitev zahtev direktoratu ESZD, odgovornemu za varnostno preverjanje, v zvezi s tistimi delovnimi mesti, ki zahtevajo varnostno preverjanje osebja, ter

— redno obveščanje vodje delegacije, regionalnega varnostnega uradnika in direktorata ESZD, odgovornega za varnost, glede incidentov ali sprememb na področju, ki vplivajo na zaščito varnostnih interesov ESZD.

4. Vodja delegacije lahko prenese varnostne naloge upravne ali tehnične narave na upravnega vodjo in druge člane osebja delegacije Unije.

5. Delegaciji Unije pomaga regionalni varnostni uradnik. Regionalni varnostni uradniki sprejmejo naloge, opredeljene v nadaljevanju, v delegacijah Unije znotraj posameznih zadevnih geografskih območij v njihovi pristojnosti.

Pod nekaterimi pogoji, kadar to zahteva prevladujoči varnostni položaj, je lahko specializirani regionalni varnostni uradnik napoten v posebno delegacijo Unije kot polnopravni rezident.

Regionalnega varnostnega uradnika se lahko na zahtevo premesti na območje zunaj njegovega področja pristojnosti, tudi na sedež, ali ob ustreznih varnostnih razmerah celo na delovno mesto z bivanjem v kateri koli državi, kakor zahteva direktorat ESZD, odgovoren za varnost.

6. Regionalni varnostni uradnik je pod neposrednim operativnim nadzorom službe na sedežu ESZD, ki je odgovorna za varnost na terenu, vendar pod skupnim upravnim nadzorom vodje delegacije Unije v kraju zaposlitve in službe na sedežu, odgovorne za varnost na terenu. Regionalni varnostni uradniki svetujejo in pomagajo vodji in osebju delegacije Unije pri urejanju in izvajanju vseh fizičnih, organizacijskih in postopkovnih ukrepov v zvezi z varnostjo delegacije Unije.

7. Regionalni varnostni uradniki z nasveti in podporo pomagajo vodji in osebju delegacije Unije. Po potrebi, zlasti kadar so regionalni varnostni uradniki polnopravni rezidenti, bi morali pomagati delegaciji Unije pri upravljanju in izvajanju na področju varnosti, vključno s pripravo varnostnih pogodb, upravljanjem varnostnih akreditacij in izdajanjem dovoljenj za dostop do tajnih podatkov.

Člen 14

Operacije skupne varnostne in obrambne politike ter posebni predstavniki EU

Direktorat ESZD, odgovoren za varnost, pomaga in svetuje direktorju direktorata za krizno upravljanje in načrtovanje, generalnemu direktorju Vojaškega štaba Evropske unije, civilnemu poveljniku operacije, ki vodi civilno zmogljivost za načrtovanje in izvajanje operacij, ter vojaškim poveljnikom operacije EU v zvezi z varnostnimi vidiki operacij skupne varnostne in obrambne politike (v nadaljnjem besedilu: SVOP), posebnim predstavnikom EU pa v zvezi z varnostnimi vidiki njihovega mandata, ki dopolnjujejo sedanje posebne določbe, določene z ustreznimi politikami, ki jih je sprejel Svet.

Člen 15

Varnostni odbor ESZD

1. Ustanovi se Varnostni odbor ESZD.

Odboru predseduje varnostni organ ESZD ali njegov imenovani namestnik, sestaja se po navodilih predsednika ali na zahtevo katerega koli od članov odbora. Direktorat ESZD, odgovoren za varnost, podpira funkcijo predsednika in po potrebi omogoča upravno pomoč pri postopkih odbora.

2. Varnostni odbor ESZD sestavljajo predstavniki:

— vsake države članice,

— Varnostnega urada generalnega sekretariata Sveta,

— Varnostnega direktorata Generalnega direktorata za človeške vire in varnost Komisije.

Delegacijo države članice v Varnostnem odboru ESZD lahko sestavljajo člani:

— nacionalnega varnostnega organa in/ali imenovanega varnostnega organa,

— oddelkov za varnost na ministrstvih za zunanje zadeve.

3. Predstavnike odbora lahko po potrebi spremljajo in jim svetujejo strokovnjaki. Predstavnike drugih institucij, agencij ali organov EU se lahko povabi, da se udeležijo razprave o vprašanjih, povezanih z njihovo varnostjo.

4. Varnostni odbor ESZD brez poseganja v odstavek 5 pomaga ESZD s svetovanjem o vseh varnostnih vprašanjih, povezanih z dejavnostmi ESZD, na sedežu in v delegacijah Unije.

Z varnostnim odborom ESZD se zlasti in brez poseganja v odstavek 5:

(a) posvetuje o:

— varnostnih politikah, smernicah, konceptih in drugih dokumentih o metodologiji na področju varnosti, zlasti v zvezi z varovanjem tajnih podatkov in ukrepi, ki jih je treba sprejeti, kadar osebje ESZD ne spoštuje varnostnih pravil,

— tehničnih vidikih varnosti, ki lahko vplivajo na odločitev visokega predstavnika, da Svetu predloži priporočilo za začetek pogajanj o sporazumih o varovanju tajnosti podatkov iz člena 10(1)(a) Priloge A,

— kakršni koli spremembi tega sklepa;

(b) posvetuje ali se ga po potrebi obvesti o vprašanjih na področju varnosti osebja in sredstev na sedežu ESZD ali v delegacijah Unije brez poseganja v člen 3(3);

(c) Varnostni odbor ESZD se obvesti o vseh nepooblaščenih razkritjih ali izgubi tajnih podatkov EU znotraj ESZD.

5. Vsaka sprememba pravil v zvezi z varovanjem tajnih podatkov EU, ki so zajeti v tem sklepu in Prilogi A k temu sklepu, zahteva soglasno pozitivno mnenje držav članic, kakor so zastopane v Varnostnem odboru ESZD. Tako soglasno pozitivno mnenje se zahteva pred:

— začetkom pogajanj o dogovorih o izvajanju iz člena 10(1)(b) Priloge A,

— dajanjem tajnih podatkov v izjemnih okoliščinah iz odstavkov 9, 11 in 12 Priloge A VI,

— prevzetjem odgovornosti organa izvora tajnih podatkov pod pogoji iz zadnjega stavka člena 10(6) Priloge A.

Kadar se zahteva soglasno pozitivno mnenje, je ta pogoj izpolnjen, ko delegacije držav članic med postopki odbora ne izrazijo nobenih pripomb.

6. Varnostni odbor ESZD v celoti upošteva varnostne politike in smernice, ki jih uporabljata Svet in Komisija.

7. Varnostni odbor ESZD prejme seznam letnih inšpekcij ESZD, po njihovem zaključku pa prejme poročila o inšpekcijskih pregledih.

8. Organizacija sestankov:

— Varnostni odbor ESZD se sestane vsaj dvakrat na leto. Dodatne sestanke v celotni sestavi ali v sestavi nacionalnih varnostnih organov/imenovanih varnostnih organov ali v obliki avtentikacije z več dejavniki organizira predsednik ali pa jih zahtevajo člani odbora,

— Varnostni odbor ESZD svoje dejavnosti organizira tako, da lahko daje priporočila o posebnih področjih varovanja tajnosti. Po potrebi lahko oblikuje druga strokovna podpodročja. Zanje določi naloge in pristojnosti, ta pa mu pošiljajo poročila o svoji dejavnosti,

— Direktorat ESZD, odgovoren za varnost, je odgovoren za pripravo tem za razpravo. Predsednik za vsak sestanek sestavi začasni dnevni red. Člani odbora lahko predlagajo dodatne teme za razpravo.

Člen 16

Varnostne inšpekcije

1. Varnostni organ ESZD zagotavlja redno izvajanje varnostnih inšpekcij na sedežu ESZD in v delegacijah Unije, da se oceni ustreznost varnostnih ukrepov in preveri njihova skladnost s tem sklepom. Direktorat ESZD, odgovoren za varnost, lahko po potrebi imenuje dodatne strokovnjake, ki bodo sodelovali pri varnostnih inšpekcijah agencij in organov EU, ustanovljenih v skladu s poglavjem 2 naslova V PEU.

2. Varnostne inšpekcije ESZD se izvajajo v pristojnosti Direktorata ESZD, odgovornega za varnost, in po potrebi s pomočjo varnostnih strokovnjakov, ki predstavljajo druge institucije EU ali države članice, zlasti v okviru dogovorov iz člena 3(3).

3. ESZD se lahko po potrebi opre na strokovno znanje iz držav članic, generalnega sekretariata Sveta in Komisije.

Po potrebi se lahko k sodelovanju pri varnostni inšpekciji delegacije Unije povabi tudi ustrezne varnostne strokovnjake na misijah držav članic v tretjih državah in/ali predstavnike diplomatskih oddelkov za varnost držav članic.

4. Določbe za izvajanje tega člena v zvezi z varovanjem tajnih podatkov EU so v prilogi A III.

Člen 17

Ocenjevalni obiski

Izvajajo se ocenjevalni obiski, da bi se ugotovilo, kako učinkoviti so varnostni ukrepi, ki se uporabljajo za varovanje tajnih podatkov EU v tretji državi ali mednarodni organizaciji v skladu z dogovori o izvajanju iz člena 10(1)(b) Priloge A.

Direktorat ESZD, odgovoren za varnost, lahko imenuje dodatne strokovnjake, ki bodo sodelovali pri ocenjevalnih obiskih v tretjih državah ali mednarodnih organizacijah, s katerimi je EU sklenila sporazum o varovanju tajnosti podatkov iz člena 10(1)(a) Priloge A.

Člen 18

Načrtovanje neprekinjenega poslovanja

Direktorat ESZD, odgovoren za varnost, pomaga operativnemu direktorju pri upravljanju varnostnih vidikov postopkov neprekinjenega poslovanja ESZD v okviru splošnega načrtovanja neprekinjenega poslovanja ESZD.

Člen 19

Napotki pred potovanjem za misije zunaj EU

Direktorat ESZD, odgovoren za varnost, zagotavlja dostopnost napotkov pred potovanjem za misije osebja v pristojnosti ESZD zunaj EU, ki jih črpa iz virov vseh ustreznih služb ESZD, zlasti virov SITROOM, INTCEN, geografskih oddelkov in delegacij Unije.

Direktorat ESZD, odgovoren za varnost, na zahtevo in na podlagi zgornjih virov omogoča tudi posebne napotke pred potovanjem za misije osebja v pristojnosti ESZD v tretje države, ki predstavljajo visoko tveganje ali povečano raven tveganja.

Člen 20

Zdravje in varnost

Varnostna pravila ESZD dopolnjujejo pravila ESZD za zaščito zdravja in varnosti, ki jih je sprejel visoki predstavnik.

Člen 21

Izvajanje in pregled

1. Varnostni organ ESZD, po potrebi po posvetovanju z Varnostnim odborom ESZD, odobri varnostne smernice, ki določajo vse potrebne ukrepe za izvajanje teh pravil v ESZD, ter vzpostavi potrebne zmogljivosti, ki zajemajo vse vidike varnosti, v tesnem sodelovanju s pristojnimi varnostnimi organi držav članic in s pomočjo ustreznih služb institucij EU.

2. V skladu s členom 4(5) Sklepa Sveta 2010/427/EU z dne 26. julija 2010 o organizaciji in delovanju Evropske službe za zunanje delovanje se lahko po potrebi uporabijo prehodne ureditve z dogovori na ravni služb z ustreznimi službami generalnega sekretariata Sveta in Komisije.

3. Visoki predstavnik zagotovi vsesplošno dosledno uporabo tega sklepa in redno pregleduje ta varnostna pravila.

4. Varnostna pravila ESZD se izvajajo v tesnem sodelovanju s pristojnimi varnostnimi organi držav članic.

5. ESZD zagotavlja, da se znotraj sistema ESZD za krizno odzivanje upoštevajo vsi varnostni vidiki.

6. Izvajanje tega sklepa zagotovita generalni sekretar kot varnostni organ in vodja direktorata ESZD, odgovornega za varnost.

Člen 22

Nadomestitev prejšnjih sklepov

Sklep visokega predstavnika Unije za zunanje zadeve in varnostno politiko z dne 19. aprila 2013 o varnostnih pravilih za Evropsko službo za zunanje delovanje ([1]) se razveljavi in nadomesti s tem sklepom.

Člen 23

Končne določbe

Ta sklep začne veljati na dan podpisa.

Objavi se v Uradnem listu Evropske unije.

Pristojni organi ESZD ustrezno in pravočasno obvestijo vse osebje, ki spada v področje uporabe tega sklepa in njegovih prilog, o vsebini, začetku veljavnosti in vseh nadaljnjih spremembah tega sklepa.

V Bruslju, 19. septembra 2017

Federica MOGHERINI

Visoka predstavnica Unije za zunanje zadeve in varnostno politiko

([1]) UL C 190, 29.6.2013, str. 1.

PRILOGA A

NAČELA IN STANDARDI VAROVANJA TAJNIH PODATKOV EU

Člen 1

Namen, področje uporabe in opredelitev pojmov

1. V tej prilogi so določena temeljna načela in minimalni standardi varovanja tajnih podatkov EU.

2. Ta temeljna načela in minimalni standardi se uporabljajo za ESZD in osebje v pristojnosti ESZD, na katera se sklicuje člen 1 in ki sta opredeljena v členu 2 tega sklepa.

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) stopnja tajnosti TRES 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) stopnja tajnosti 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) stopnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL: podatki in material, katerih nepooblaščeno razkritje bi lahko škodovalo vitalnim interesom Evropske unije ali ene ali več držav članic;

(d) stopnja tajnosti 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. Dodajo se lahko tudi oznake, iz katerih so razvidni področje dejavnosti, na katero se nanašajo, organ izvora, omejitve pri razpošiljanju, omejitve uporabe ali možnosti posredovanja.

Člen 3

Sistem določanja stopenj tajnosti

1. ESZD zagotovi, 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. Varnostni organ ESZD po posvetovanju z Varnostnim odborom ESZD v skladu s členom 15(5) tega sklepa odobri varnostne smernice 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 elementa tajnega podatka EU je odgovoren za njegovo varovanje v skladu s tem sklepom.

3. Če države članice v strukture ali omrežja ESZD vnesejo tajne podatke z nacionalno oznako stopnje tajnosti, ESZD te podatke varuje v skladu z zahtevami, ki se uporabljajo za tajne podatke EU enakovredne stopnje, kakor je določeno v preglednici enakovrednih stopenj tajnosti v Dodatku B.

ESZD vzpostavi ustrezne postopke za zagotavljanje natančnih evidenc v zvezi z organom izvora

— tajnih podatkov, ki jih prejme ESZD, ter

— izvornega materiala, vključenega v tajne podatke z izvorom v ESZD.

Varnostni odbor ESZD je obveščen o teh postopkih.

4. Pri velikih količinah ali zbirkah tajnih podatkov EU je morda upravičena raven zaščite, ki ustreza višji stopnji tajnosti, kot jo zahtevajo njihovi sestavni deli.

Člen 5

Varnost osebja pri delu s tajnimi podatki EU

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

— imajo potrebo po seznanitvi;

— so bili za dostop do podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje varnostno preverjeni na ustrezni stopnji ali drugače pravilno pooblaščeni zaradi svoje funkcije v skladu z nacionalnimi zakoni in predpisi, 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. Preden se posameznikom odobri dostop do tajnih podatkov EU ter nato v rednih presledkih, so vsi pisno poučeni o svoji odgovornosti za varovanje tajnih podatkov EU v skladu s tem sklepom ter to tudi potrdijo.

4. Določbe za izvajanje tega člena so v Prilogi A I.

Člen 6

Fizična varnost tajnih podatkov EU

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, zgradbah, 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 8(2) Priloge A.

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 A II, odobri pa jih varnostni organ ESZD.

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 A II.

Člen 7

Upravljanje tajnih podatkov

1. Upravljanje tajnih podatkov je uporaba upravnih ukrepov za nadzor nad tajnimi podatki EU v njihovem življenjskem ciklu, ki dopolnjujejo ukrepe iz členov 5, 6 in 8 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 ter delo z njimi.

2. Podatki stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje se iz varnostnih razlogov vpišejo pred razpošiljanjem in ob prejemu. Pristojni organi ESZD v ta namen vzpostavijo sistem registrov. Podatki stopnje TRES SECRET UE/EU TOP SECRET se vpišejo v za to namenjene registre.

3. Varnostni organ ESZD 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 7(5) tega sklepa in z jasno opredeljenimi varnostno-operativnimi postopki;

(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 8(5) tega sklepa; ali

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

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

Člen 8

Varovanje 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 ter bodo delovali tako, kot morajo in kadar morajo, pod nadzorom zakonitih uporabnikov. Učinkovito zagotavljanje informacijske varnosti zagotavlja ustrezno stopnjo tajnosti, celovitost, razpoložljivost, nezatajljivost in avtentičnost podatkov. Zagotavljanje informacijske varnosti temelji na postopku obvladovanja tveganja.

2. „Komunikacijski in informacijski sistem“ (KIS) pomeni sistem, ki omogoča delo s podatkov v elektronski obliki. Komunikacijski in informacijski sistem zajema vse sestavne dele, potrebne za njegovo delovanje, tudi infrastrukturo, organizacijo, osebje in informacijske vire. Ta priloga se uporablja za vse KIS ESZD, v katerih poteka delo s tajnimi podatki EU.

3. V KIS se tajni podatki EU obravnavajo v skladu z načelom zagotavljanja informacijske varnosti.

4. Za vse KIS, v katerih poteka delo s tajnimi podatki EU, se opravi akreditacijski postopek. Namen akreditacije je pridobiti zagotovilo, da so bili izvedeni vsi ustrezni varnostni ukrepi in da je bila dosežena zadostna stopnja varovanja 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 v skladu s členom 8(5) tega sklepa.

7. Med pošiljanjem 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 A IV, uporabijo posebni postopki.

8. V skladu s členom 8(6) tega sklepa se po potrebi ustanovijo naslednji organi 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. V skladu s členom 8(7) tega sklepa se za vsak sistem ustanovijo:

(a) organ za varnostno akreditacijo (SAA);

(b) operativni organ za zagotavljanje informacijske varnosti.

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

Člen 9

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. Praviloma te pogodbe ne vključujejo dostopa do podatkov stopnje TRES SECRET UE/EU TOP SECRET.

2. ESZD 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 o varovanju tajnosti podatkov ali dogovor o izvajanju iz člena 10(1) Priloge A.

3. Pri dodeljevanju pogodb s tajnimi podatki industrijskim ali drugim subjektom ESZD kot naročnik zagotovi, da so izpolnjeni minimalni standardi industrijske varnosti iz tega sklepa in pogodbe. Skladnost s temi minimalnimi standardi zagotavlja prek ustreznih nacionalnih varnostnih organov/imenovanih varnostnih organov.

4. Izvajalci ali podizvajalci, registrirani na ozemlju 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, imajo varnostno dovoljenje organizacije za zahtevano stopnjo tajnosti, ki jim ga odobri nacionalni varnostni organ, imenovani varnostni organ ali kateri koli drug pristojni varnostni organ zadevne države članice.

5. 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 A I.

6. Določbe za izvajanje tega člena so v Prilogi A V.

Člen 10

Izmenjava tajnih podatkov s tretjimi državami in mednarodnimi organizacijami

1. ESZD lahko izmenja tajne podatke EU s tretjo državo ali mednarodno organizacijo le, kadar:

(a) obstaja veljaven sporazum o varovanju tajnosti podatkov med EU in navedeno tretjo državo ali mednarodno organizacijo, ki je bil sklenjen v skladu s členom 37 PEU in členom 218 PDEU; ali

(b) je začel veljati dogovor o izvajanju med visokim predstavnikom in pristojnimi varnostnimi organi navedene tretje države ali mednarodne organizacije za izmenjavo tajnih podatkov, ki praviloma ne presegajo stopnje RESTREINT UE/EU RESTRICTED, ki je bil sklenjen v skladu s postopkom iz člena 15(5) tega sklepa; ali

(c) se v okviru operacij kriznega upravljanja SVOP uporablja okvirni ali *ad hoc* sporazum o sodelovanju med EU in navedeno tretjo državo, ki je bil sklenjen v skladu s členom 37 PEU in členom 218 PDEU,

in so izpolnjeni pogoji iz navedenega instrumenta.

Izjeme od zgornjega splošnega pravila so v oddelku V Priloge A VI.

2. Dogovori o izvajanju iz odstavka 1(b) 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.

Podatki, izmenjani na podlagi sporazumov iz odstavka 1(c), so omejeni na podatke v zvezi z operacijami SVOP, v katerih na podlagi teh sporazumov in v skladu z njihovimi določbami sodeluje zadevna tretja država.

3. Če Unija in sodelujoča tretja država ali mednarodna organizacija naknadno skleneta sporazum o varnosti podatkov, ta sporazum nadomesti določbe o izmenjavi tajnih podatkov iz vsakega okvirnega sporazuma o sodelovanju, *ad hoc* sporazuma o sodelovanju ali *ad hoc* dogovora o izvajanju, kar zadeva izmenjavo tajnih podatkov EU in delo z njimi.

4. Tajni podatki EU, ki nastanejo za namene operacije SVOP, se lahko v skladu z odstavki 1 do 3 in Prilogo A VI 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 komunikacijskem in informacijskem sistemu operacije SVOP 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.

5. Izvajajo se ocenjevalni obiski tretjih držav ali mednarodnih organizacij iz člena 17 tega sklepa, s katerimi se ugotovi učinkovitost ukrepov, uvedenih za varovanje vseh izmenjanih tajnih podatkov EU.

6. Odločitev o dajanju tajnih podatkov EU z izvorom v ESZD tretji državi ali mednarodni organizaciji se sprejme za vsak primer posebej glede na naravo in vsebino teh podatkov, potrebo prejemnika po seznanitvi ter koristi, ki jih bo imela EU.

ESZD zaprosi za pisno soglasje vse subjekte, ki so predložili tajne podatke kot izvorni material za tajne podatke EU z izvorom v ESZD, da bi potrdil, da ni nikakršnega nasprotovanja za dajanje tajnih podatkov.

Če organ izvora tajnega podatka, ki ga želi dati, ni ESZD, ESZD ta organ najprej zaprosi za pisno soglasje, da sme dati tajni podatek.

Če ESZD ne more določiti organa izvora, varnostni organ ESZD prevzame odgovornost organa izvora po pridobitvi soglasnega pozitivnega mnenja držav članic, kakor so zastopane v Varnostnem odboru ESZD.

7. Določbe za izvajanje tega člena so v Prilogi A VI.

Člen 11

Kršitev varovanja tajnosti in nepooblaščeno razkritje tajnih podatkov

1. O vseh kršitvah ali domnevnih kršitvah varovanja tajnosti ter o vseh nepooblaščenih razkritjih ali domnevnih razkritjih tajnih podatkov se nemudoma obvesti direktorat ESZD, odgovoren za varnost, ki obvesti zadevne države članice ali kateri koli drug zadevni subjekt, kot je ustrezno.

2. Če je bilo ugotovljeno ali če obstajajo utemeljeni razlogi za domnevo, da so bili tajni podatki nepooblaščeno razkriti ali izgubljeni, direktorat ESZD, odgovoren za varnost, po potrebi obvesti nacionalni varnostni organ zadevnih držav članic in sprejme vse primerne ukrepe v skladu z ustreznimi zakoni in predpisi, da:

(a) zavaruje dokaze;

(b) zagotovi, da zadevo preišče osebje, ki ni neposredno povezano s kršitvijo ali nepooblaščenim razkritjem, in ugotovi dejstva;

(c) nemudoma obvesti organ izvora ali kateri koli drug zadevni subjekt;

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

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

(f) obvesti ustrezne organe o posledicah dejanskega ali domnevnega nepooblaščenega razkritja in sprejetih ukrepih.

3. Zoper vsakega člana osebja v pristojnosti ESZD, ki je odgovoren za kršitev varnostnih pravil iz tega sklepa, se lahko uvede disciplinski postopek v skladu z veljavnimi pravili in predpisi.

Za vsakega posameznika, ki je odgovoren za razkritje ali izgubo tajnih podatkov, se lahko uvede disciplinski ukrep in/ali kazenski postopek v skladu z veljavnimi zakoni, pravili in predpisi.

4. Vodja direktorata ESZD, odgovoren za varnost, lahko med preiskavo kršitve in/ali razkritja začasno ustavi dostop posameznikov do tajnih podatkov EU in do prostorov ESZD. O tej odločitvi se nemudoma obvesti Varnostni direktorat Generalnega direktorata za človeške vire in varnost Komisije, Varnostni urad generalnega sekretariata Sveta ali nacionalni varnostni organ zadevnih držav članic ali drug zadevni subjekt.

PRILOGA A I

VARNOSTNO PREVERJANJE OSEBJA

I. UVOD

1. V tej prilogi so določbe za izvajanje člena 5 Priloge A. Zlasti določa merila, ki jih ESZD uporablja 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. „Dovoljenje za dostop do tajnih podatkov" 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".

3. „Potrdilo za dostop do tajnih podatkov" pomeni potrdilo, ki ga izda varnostni organ ESZD in dokazuje, da je posameznik varnostno preverjen, na njem pa so navedeni stopnja tajnosti podatkov EU, do katerih ima lahko posameznik dostop, datum veljavnosti ustreznega dovoljenja za dostop do tajnih podatkov in datum izteka veljavnosti samega potrdila.

4. „Pooblastilo za dostop do tajnih podatkov EU" je pooblastilo varnostnega organa ESZD, sprejeto v skladu s tem sklepom potem, ko so pristojni organi države članice izdali dovoljenje za dostop do tajnih podatkov, s katerim 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; ta posameznik je „varnostno preverjen".

II. POOBLASTILO ZA DOSTOP DO TAJNIH PODATKOV EU

5. Dostop do podatkov stopnje RESTREINT UE/EU RESTRICTED ne zahteva dovoljenja za dostop do tajnih podatkov in se odobri, potem ko:

   (a) je bilo med posameznikom in ESZD vzpostavljeno pravno ali pogodbeno razmerje;

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

   (c) je bil posameznik poučen o varnostnih pravilih in postopkih za varovanje tajnih podatkov EU ter je pisno potrdil odgovornosti za varovanje tajnih podatkov EU v skladu s tem sklepom.

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

   (a) je bilo med posameznikom in ESZD vzpostavljeno pravno ali pogodbeno razmerje;

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

   (c) 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; ter

   (d) je bil poučen o varnostnih pravilih in postopkih za varovanje tajnih podatkov EU ter je pisno potrdil odgovornosti za varovanje teh podatkov.

7. ESZD določi 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 iz zgornjega odstavka 4.

8. Osebje ESZD sporoči, kadar ima državljanstvo več kot ene države.

Postopki varnostnega preverjanja osebja v ESZD

9. Vprašalnike za varnostno preverjanje osebja, ki jih izpolni osebje ESZD, varnostni organ ESZD 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.

10. Kadar ima posameznik državljanstvo več kot ene države, se bo zahteva po varnostni preiskavi predložila nacionalnemu varnostnemu organu države, katere državljanstvo je oseba predložila pri zaposlitvi.

11. Če ESZD izve za podatke o prosilcu za dovoljenje 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.

12. Ustrezni nacionalni varnostni organ po zaključku varnostne preiskave obvesti direktorat ESZD, odgovoren za varnost, o izidu te preiskave.

    (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 varnostni organ ESZD zadevni osebi dodeli pooblastilo za dostop do tajnih podatkov EU do ustrezne stopnje in do določenega datuma;

    (b) ESZD sprejme vse ustrezne ukrepe za zagotovitev ustreznega izvajanja pogojev ali omejitev, ki jih nalaga nacionalni varnostni organ. Nacionalni varnostni organ je obveščen o izidu;

    (c) če z varnostno preiskavo tega ni mogoče zagotoviti, varnostni organ ESZD o tem uradno obvesti zadevnega posameznika, ki lahko zaprosi za zaslišanje pri varnostnem organu ESZD. 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 pooblastilo za dostop do tajnih podatkov EU ne izda. V tem primeru ESZD sprejme vse ustrezne ukrepe za zagotovitev, da bo prosilcu za dovoljenje onemogočen dostop do tajnih podatkov EU.

13. Za varnostno preiskavo skupaj z dobljenimi rezultati, na podlagi katere se ESZD odloči, ali bo dodelila pooblastilo za dostop do tajnih podatkov EU ali ne, se upoštevajo ustrezni zakoni in predpisi, ki veljajo v zadevni državi članici, vključno s tistimi, ki urejajo pritožbe. Na odločitve varnostnega organa ESZD se je mogoče pritožiti v skladu s kadrovskimi predpisi.

14. Zagotovila, na katerih temelji dovoljenje za dostop do tajnih podatkov, če je še veljavno, zajemajo vse zadolžitve zadevnega posameznika v ESZD ali generalnem sekretariatu Sveta ali Komisije.

15. ESZD sprejme pooblastilo za dostop do tajnih podatkov EU, ki ga je podelila katera koli druga institucija, organ ali agencija Evropske unije, pod pogojem, da je še veljavno. Pooblastilo pokriva vse zadolžitve zadevnega posameznika v ESZD. Institucija, organ ali agencija Evropske unije, kjer se posameznik zaposli, bo nacionalni varnostni organ uradno obvestila o spremembi delodajalca.

16. Če posameznik ne nastopi službe v roku 12 mesecev po uradnem obvestilu varnostnega organa ESZD o izidu varnostne preiskave ali če posameznik 12 ali več mesecev ne opravlja službe, med tem časom pa ni zaposlen na delovnem mestu v ESZD, v drugih institucijah, agencijah ali organih EU ali v državni upravi države članice, ki zahteva dostop do tajnih podatkov, se ta izid predloži zadevnemu nacionalnemu varnostnemu organu v potrditev, da je še vedno veljaven in ustrezen.

17. Če ESZD izve za informacije o varnostnem tveganju, ki ga predstavlja posameznik, ki ima pooblastilo za dostop do tajnih podatkov EU, o tem v skladu z ustreznimi pravili in predpisi obvesti ustrezni nacionalni varnostni organ ter lahko začasno prekine dostop do tajnih podatkov EU ali odvzame pooblastilo za dostop do tajnih podatkov EU. Če nacionalni varnostni organ obvesti ESZD o preklicu zagotovil, ki so bila v skladu z odstavkom 12(a) dana za posameznika, ki ima veljavno pooblastilo za dostop do tajnih podatkov EU, lahko varnostni organ ESZD 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 zgornje pooblastilo 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.

18. Vsaka odločitev o odvzemu pooblastila za dostop do tajnih podatkov EU uslužbencu ESZD in po potrebi razlogi zanjo se sporočijo zadevni osebi, ki lahko zaprosi za zaslišanje pri varnostnem organu ESZD. 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 odločitve varnostnega organa ESZD se je mogoče pritožiti v skladu s kadrovskimi predpisi.

19. Nacionalni strokovnjaki, ki so dodeljeni ESZD na delovno mesto, za katero je potreben dostop do tajnih podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, pred prevzemom svojih zadolžitev varnostnemu organu ESZD predložijo veljavno dovoljenje za dostop do tajnih podatkov. Zgornji postopek upravlja država članica pošiljateljica.

Evidence dovoljenj za dostop do tajnih podatkov

20. ESZD upravlja podatkovno zbirko s statusom dostopa do tajnih podatkov vsega osebja v pristojnosti ESZD in izvajalcev ESZD. Te evidence vključujejo stopnjo tajnosti podatkov EU, do katere ima lahko posameznik dostop (CONFIDENTIEL UE/EU CONFIDENTIAL ali višje), datum izdaje dovoljenja za dostop do tajnih podatkov in njegovo obdobje veljavnosti.

21. V državah članicah ter drugih institucijah, agencijah in organih EU se vzpostavijo ustrezni usklajevalni postopki, da se zagotovi natančna in celovita evidenca ESZD glede statusa dostopa do tajnih podatkov vsega osebja v pristojnosti ESZD in izvajalcev ESZD.

22. Varnostni organ ESZD lahko izda potrdilo za dostop do tajnih podatkov (PSCC), iz katerega so razvidni stopnja tajnosti podatkov EU, do katere ima lahko posameznik dostop (CONFIDENTIEL UE/EU CONFIDENTIAL ali višje), datum veljavnosti ustreznega dovoljenja ali pooblastila za dostop do tajnih podatkov in datum izteka veljavnosti samega potrdila.

Izjeme od zahteve glede dovoljenja za dostop do tajnih podatkov

23. Posameznike, ki so zaradi svoje funkcije v skladu z nacionalnimi zakoni in predpisi pooblaščeni za dostop do tajnih podatkov EU, direktorat ESZD, odgovoren za varnost, po potrebi pouči o njihovih obveznostih glede varovanja tajnih podatkov EU.

III. IZOBRAŽEVANJE IN OZAVEŠČANJE O VAROVANJU TAJNOSTI

24. Pred dodelitvijo pooblastila za dostop do tajnih podatkov EU vsi posamezniki pisno potrdijo, da razumejo svoje obveznosti glede varovanja tajnih podatkov EU in da se zavedajo posledic njihovega nepooblaščenega razkritja. ESZD vodi evidenco takšnih pisnih potrditev.

25. 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.

26. Za vse posameznike, ki imajo dostop do tajnih podatkov EU, se morajo v obdobju njihovega dela s tajnimi podatki EU stalno izvajati varnostni ukrepi, ki se uporabljajo za osebje (tj. varnostna obravnava po delu). Za stalno varnost osebja so odgovorni:

(a) posamezniki, ki imajo dostop do tajnih podatkov EU: posamezniki so osebno odgovorni za varno ravnanje in so ustrezne varnostne organe dolžni nemudoma obvestiti o vsakem poskusu približevanja ali ravnanju, ki se jim zdi sumljivo ali nenavadno, ter o vseh spremembah osebnih okoliščin, ki bi lahko vplivale na njihovo dovoljenje za dostop do tajnih podatkov ali pooblastilo za dostop do tajnih podatkov EU;

(b) nadrejeni vodje: njihova naloga je zagotoviti, da se njihovo osebje zaveda varnostnih ukrepov in odgovornosti za varovanje tajnih podatkov EU, spremljati varnostno ravnanje njihovega osebja in nadaljnje ukrepati v zvezi s težavami na področju varnosti ali obvestiti ustrezne varnostne organe o vseh negativnih informacijah, ki bi lahko vplivale na dovoljenje za dostop do tajnih podatkov ali pooblastilo za dostop do tajnih podatkov EU njihovega osebja;

(c) akterji na področju varovanja tajnosti varnostne organizacije ESZD iz člena 12 tega sklepa: njihova naloga je, da redno poučujejo osebje glede varnosti na njihovem področju, da na svojem področju pristojnosti vzdržujejo trdno varnostno kulturo, da določijo ukrepe za spremljanje varnostnega ravnanja osebja ter da ustrezne varnostne organe obvestijo o vseh negativnih informacijah, ki bi lahko vplivale na dovoljenje za dostop do tajnih podatkov katerega koli posameznika;

(d) ESZD in države članice: vzpostavijo potrebne poti za sporočanje podatkov, ki bi lahko vplivali na posameznikovo dovoljenje za dostop do podatkov ali pooblastilo za dostop do tajnih podatkov EU.

27. 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.

IV. IZJEMNE OKOLIŠČINE

28. V nujnih primerih, kadar je to ustrezno utemeljeno v interesu ESZD in do zaključka celovite varnostne preiskave, varnostni organ ESZD 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 ESZD izda začasno pooblastilo za dostop do tajnih podatkov EU za določeno funkcijo. Celovita varnostna preiskava se čim prej zaključi. Ta začasna pooblastila veljajo največ šest mesecev in ne dovoljujejo dostopa do podatkov stopnje TRES 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. ESZD vodi evidenco takšnih pisnih potrditev.

29. 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 dovoljenje 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 ESZD;

(g) po posvetovanju z ustreznim nacionalnim varnostnim organom/imenovanim varnostnim organom, ki je izdal posameznikovo dovoljenje za dostop do tajnih podatkov, niso bile prejete nobene pripombe; ter

(h) zapisnik o izjemi, ki vključuje opis podatkov, do katerih je bil odobren dostop, se hrani v pristojnem registru ali podregistru.

30. 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.

31. 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 visoki predstavnik, varnostni organ ESZD ali DGBA pisno, če je to mogoče, odobri 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. Dodelitev takega dovoljenja se evidentira z opisom podatkov, do katerih je bil odobren dostop.

32. Za podatke stopnje TRES 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 TRES SECRET UE/EU TOP SECRET na nacionalni ravni, bodisi do podatkov stopnje SECRET UE/EU SECRET.

33. Če se uporabi postopek iz odstavkov 31 in 32, se Varnostnemu odboru ESZD o tem pošlje obvestilo.

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

V. UDELEŽBA NA SESTANKIH NA SEDEŽU ESZD IN V DELEGACIJAH UNIJE

35. Posamezniki, ki naj bi se udeležili sestankov na sedežu ESZD ali v delegacijah Unije, 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. Za predstavnike držav članic, uradnike GSS in Komisije, ustrezni organi pošljejo potrdilo za dostop do tajnih podatkov ali drug dokaz o varnostnem preverjanju direktoratu ESZD, odgovornemu za varnost, in varnostnemu koordinatorju delegacije Unije, izjemoma pa ga lahko predloži zadevna oseba. Po potrebi se lahko uporabi zbirni seznam imen z ustreznimi dokazili o opravljenem varnostnem preverjanju.

36. Če je posamezniku, ki mora zaradi nalog, ki jih opravlja, sodelovati na sestankih na sedežu ESZD ali v delegaciji Uniji, na kateri se obravnavajo podatki stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, odvzeto dovoljenje za dostop do tajnih podatkov EU, pristojni organ o tem obvesti ESZD.

VI. MOREBITEN DOSTOP DO TAJNIH PODATKOV EU

37. 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.

38. 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; redno so poučeni o varnostnih postopkih za varovanje tajnih podatkov EU ter o dolžnosti, da varujejo podatke, ki so jim zaupani ali do katerih imajo morda nehote dostop.

PRILOGA A II

FIZIČNA VARNOST TAJNIH PODATKOV EU

I. UVOD

1. V tej prilogi so določbe za izvajanje člena 6 Priloge A. 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 zagavljanjem, da obravnavanje tajnih podatkov 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 dejavnosti ter

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

II. ZAHTEVE IN UKREPI GLEDE FIZIČNE VARNOSTI

3. ESZD v svojih prostorih uporablja 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 varnostne ukrepe;

   (c) okolica in struktura zgradb ali območij, kjer so tajni podatki EU;

   (d) ocena nevarnosti, ki jo predstavljajo tretje države, kot jo je razvil INTCEN na podlagi zlasti poročil delegacij Unije; in

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

4. Varnostni organ ESZD 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 ter

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

5. Direktorat ESZD, odgovoren za varnost, lahko opravlja 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 VAROVANJE 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 varnostni organ ESZD 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 ESZD.

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 VAROVANA OBMOČJA

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

(a) upravna območja in

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

13. Varnostni organ ESZD 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 direktorat ESZD, odgovoren za varnost, 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 zavarovan 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 na ustrezni stopnji 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 pooblastilo 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;

(c) elektronske naprave se pustijo zunaj območja.

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

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

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

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

(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 varnostni organ ESZD 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 nevarnost za tajne podatke EU ocenjena kot velika, to opremo najprej preveri, zato da zagotovi, da te naprave ne morejo nehoteno ali nezakonito pošiljati 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 zunaj običajnega delovnega časa, razen če je 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, ki se jih lahko obravnava in se lahko hranijo v tem območju;

(b) nadzorne in varnostne ukrepe, ki jih je treba izvajati;

(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 je drugim posameznikom dovoljen 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 varnostni organ ESZD, 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. Tajni podatki stopnje RESTREINT UE/EU RESTRICTED se lahko obravnavajo:

(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 30 do 42 Priloge A III in se je zavezal, da bo ravnal v skladu z nadomestnimi ukrepi iz varnostnih navodil varnostnega organa ESZD, 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 zaklenjenih pisarniških omarah 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 varnostnega organa ESZD.

25. Delo s tajnimi podatki stopnje tajnosti 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:

(i) imetnik prenaša tajne podatke EU v skladu z odstavki 30 do 42 Priloge A III;

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

(iii) ima imetnik 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 CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET se hranijo v varovanem območju, blagajni ali sobi trezorju.

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

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

(a) v blagajni, ki je 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 A III.

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

30. Varnostni organ ESZD 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) ob prejemu nove blagajne;

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

(c) ob vsakem nepooblaščenem razkritju ali sumu razkritja;

(d) ob vsakem vzdrževanju ali popravilu ključavnice; ter

(e) najmanj vsakih 12 mesecev.

PRILOGA A III

UPRAVLJANJE TAJNIH PODATKOV

I. UVOD

1. V tej prilogi so določbe za izvajanje člena 7 Priloge A. Določa upravne ukrepe 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. SISTEM DOLOČANJA STOPENJ 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 širjenje podatkov.

4. Stopnja tajnosti tajnih podatkov EU se določi v skladu s členom 2(2) Priloge A in ob upoštevanju varnostnih smernic, ki se odobrijo v skladu s členom 3(3) Priloge A.

5. Tajnim podatkom držav članic, ki so izmenjani z ESZD, se dodeli enaka stopnja varovanja kot tajnim podatkom EU z enakovredno stopnjo tajnosti. Preglednica enakovrednih stopenj je na voljo v Dodatku B k tej odločbi.

6. Stopnja tajnosti in po potrebi datum ali določen dogodek, po katerem se lahko stopnja tajnosti zniža ali se tajnost prekliče, je jasno in pravilno označena, ne glede na to, ali so tajni podatki EU v pisni, ustni, elektronski ali kateri drugi obliki.

7. Posamezni deli nekega dokumenta (tj. strani, odstavki, oddelki, priloge, dodatki ter dodani in priloženi deli) imajo lahko različne stopnje tajnosti in so temu ustrezno označeni, tudi če se hranijo v elektronski obliki.

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 ločiti.

9. 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.

10. Stopnja tajnosti pisma ali dopisa, ki vsebuje 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

11. Tajni podatki EU lahko poleg varnostnih oznak stopnje tajnosti iz člena 2(2) Priloge A nosijo dodatne oznake, kot so:

(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 omejitev pri uporabi;

(c) oznake pogojev za dajanje tajnih podatkov.

12. Po sprejetju odločitve o dajanju tajnih podatkov EU tretji državi ali mednarodni organizaciji ESZD, odgovoren za varnost, pošlje zadevne tajne podatke z oznako, da se dajo tretji državi ali mednarodni organizaciji.

13. Seznam dovoljenih oznak bo sprejel varnostni organ ESZD.

Okrajšane oznake stopnje tajnosti

14. Za navedbo stopnje tajnosti posameznih odstavkov besedila se lahko uporabijo standardizirane okrajšane oznake stopnje tajnosti. Okrajšave ne nadomestijo popolnih oznak tajnosti.

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

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

Ustvarjanje tajnih podatkov EU

16. Pri ustvarjanju 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 CONFIDENTIEL UE/EU CONFIDENTIAL ali višje je treba na vsaki strani navesti številko kopije, če se razpošiljajo v več kopijah.

17. Če za tajne podatke EU ni mogoče uporabljati odstavka 16, se sprejmejo drugi ustrezni ukrepi v skladu z varnostnimi smernicami, vzpostavljenimi v skladu s tem sklepom.

Znižanje stopnje tajnosti in njen preklic za tajne podatke EU

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

19. ESZD redno pregleduje svoje tajne podatke EU, da bi ugotovila, ali je stopnja tajnosti še ustrezna. ESZD vzpostavi sistem za pregledovanje stopnje tajnosti vpisanih tajnih podatkov EU, ki jih je ustvarila, vsaj vsakih pet let. Takšen pregled ni potreben, če je organ izvora že na začetku navedel določeno obdobje, ko bo stopnja tajnosti podatkov samodejno znižana ali preklicana, in če je podatek temu ustrezno označen.

III. VPIS TAJNIH PODATKOV EU IZ VARNOSTNIH RAZLOGOV

20. Na sedežu se vzpostavi centralni register. Za vsak organizacijski subjekt v ESZD, v katerem poteka delo s tajnimi podatki EU, se vzpostavi pristojni register, podrejen centralnemu registru, 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 A.

Vsaka delegacija Unije ustanovi lasten register tajnih podatkov EU.

Varnostni organ ESZD imenuje vodjo registra za te registre.

21. Za namene tega sklepa vpis iz varnostnih razlogov (v nadaljnjem besedilu: vpis) pomeni uporabo postopkov, ki beležijo življenjski cikel podatkov, vključno z njihovim razširjanjem in uničenjem. V primeru komunikacijskega in informacijskega sistema se vpisni postopki lahko opravijo v okviru procesov znotraj samega komunikacijskega in informacijskega sistema.

22. Ves material stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL in višje se vpiše ob prispetju v organizacijski subjekt, vključno z delegacijami Unije, ali pri odpošiljanju iz njega. Podatki stopnje TRES SECRET UE/EU TOP SECRET se vpišejo v za to namenjene registre.

23. Centralni register na sedežu ESZD je glavna točka vstopa in izstopa pri izmenjavi tajnih podatkov s tretjimi državami in mednarodnimi organizacijami. Vodi evidenco vseh teh izmenjav.

24. Varnostni organ ESZD odobri varnostne smernice glede vpisovanja tajnih podatkov EU iz varnostnih razlogov v skladu s členom 14 tega sklepa.

Registri za podatke stopnje tajnosti TRES SECRET UE/EU TOP SECRET

25. Na sedežu ESZD se določi centralni register, ki deluje kot centralni organ za prejemanje in razpošiljanje podatkov stopnje TRES SECRET UE/EU TOP SECRET. Po potrebi se lahko določijo podregistri, v katerih delajo s takšnimi podatki za potrebe vpisovanja.

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

IV. KOPIRANJE IN PREVAJANJE TAJNIH DOKUMENTOV EU

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

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

29. Varnostni ukrepi, ki veljajo za izvorni dokument, veljajo tudi za njegove kopije in prevode. Kopije dokumentov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje pripravi le ustrezni (pod)register z zaščitenim fotokopirnim strojem. Kopije je treba vpisati.

V. PRENAŠANJE TAJNIH PODATKOV EU

30. Za prenašanje tajnih podatkov EU veljajo varnostni ukrepi iz odstavkov 32 do 42. Pri prenašanju tajnih podatkov EU na elektronskih medijih se varnostni ukrepi, navedeni v nadaljevanju, ne glede na člen 7(4) Priloge A lahko dopolnijo z ustreznimi tehničnimi protiukrepi, ki jih predpiše varnostni organ ESZD, tako da se čim bolj zmanjša nevarnost izgube ali nepooblaščenega razkritja.

31. Varnostni organ ESZD izda navodila za prenašanje tajnih podatkov EU v skladu s tem sklepom.

Znotraj zgradbe ali samostojne skupine zgradb

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

33. Znotraj zgradbe ali samostojne skupine zgradb tajne podatke stopnje tajnosti TRES SECRET UE/EU TOP SECRET v zaščitenih ovojnicah, na katerih je samo ime naslovnika, prenašajo usposobljeni, nadzorovani in ustrezno varnostno preverjeni posamezniki.

Znotraj EU

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

35. Prenašanje podatkov do stopnje tajnosti 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 A II;

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

(iii) so posamezniki varnostno preverjeni na ustrezni stopnji in 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 ustrezni nacionalni varnostni organ v skladu z nacionalnimi zakoni in predpisi;

(ii) uporabljajo ustrezne varnostne ukrepe v skladu z minimalnimi zahtevami, ki se določijo v varnostnih smernicah iz člena 21(1) tega sklepa.

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

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

37. Podatki stopnje tajnosti TRES 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 ali med subjekti EU v tretjih državah

38. Tajni podatki EU, ki se prenašajo iz EU na ozemlje tretje države ali med subjekti EU v tretjih državah, so pakirani tako, da so zaščiteni pred nepooblaščenim razkritjem.

39. Prenašanje podatkov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET iz EU na ozemlje tretje države ter prenašanje katerih koli tajnih podatkov do stopnje tajnosti SECRET UE/EU SECRET med subjekti EU v tretjih državah 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 A II;

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

(v) so posamezniki varnostno preverjeni na ustrezni stopnji in poučeni o svoji odgovornosti v zvezi z varovanjem tajnosti.

40. Pri prenašanju podatkov stopnje tajnosti 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 10(2) Priloge A.

41. Podatki stopnje tajnosti RESTREINT UE/EU RESTRICTED se lahko prenašajo tudi iz EU na ozemlje tretje države prek poštnih služb ali komercialnih kurirskih služb.

42. Podatki stopnje tajnosti TRES SECRET UE/EU TOP SECRET se iz EU na ozemlje tretje države ali med subjekti EU v tretjih državah prenašajo po vojaškem ali diplomatskem kurirju.

VI. UNIČENJE TAJNIH PODATKOV EU

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

44. Dokumente, ki se vpisujejo v skladu s členom 7(2) Priloge A, po navodilu imetnika tajnih podatkov ali pristojnega organa uniči pristojni register. Vpisniki in drugi podatki o vpisu se ustrezno posodobijo.

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

46. Uradnik registra in priča, če je njena navzočnost obvezna, podpišeta potrdilo o uničenju, ki se shrani v registru. Register potrdila o uničenju dokumentov stopnje TRES 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.

47. 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.

48. Uničenje računalniških shranjevalnih nosilcev, ki se uporabljajo za tajne podatke EU, poteka v skladu s postopki, ki jih je odobril varnostni organ ESZD.

VII. VARNOSTNE INŠPEKCIJE

Varnostne inšpekcije ESZD

49. V skladu s členom 16 tega sklepa varnostne inšpekcije ESZD zajemajo:

(a) splošne varnostne inšpekcije, katerih cilj je oceniti splošno stopnjo varovanja sedeža ESZD, delegacij Unije in vseh odvisnih ali povezanih prostorov, predvsem za oceno učinkovitosti varnostnih ukrepov, ki se izvajajo za varovanje varnostnih interesov ESZD;

(b) varnostne inšpekcije tajnih podatkov EU, katerih cilj je na splošno v smislu akreditacije oceniti učinkovitost ukrepov, ki se izvajajo za varovanje tajnih podatkov EU na sedežu ESZD in delegacijah Unije.

Take inšpekcije pregledi se med drugim izvajajo z namenom:

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

(ii) izpostaviti pomen varnosti in učinkovitega obvladovanja tveganja v subjektih, kjer poteka inšpekcija;

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

(iv) okrepiti izobraževalne programe in programe ozaveščanja v teku, ki jih izvajajo varnostni organi.

Izvajanje varnostnih inšpekcij ESZD in poročanje o njih

50. Varnostne inšpekcije ESZD izvaja inšpekcijska ekipa direktorata ESZD, odgovornega za varnost, in po potrebi s pomočjo varnostnih strokovnjakov iz drugih institucij EU ali držav članic.

Inšpekcijska ekipa ima dostop do vseh lokacij, kjer poteka delo s tajnimi podatki EU, še zlasti pa do registrov in dostopovnih vozlišč KIS.

51. Varnostne inšpekcije ESZD v delegacijah Unije se lahko po potrebi izvajajo s pomočjo varnostnih uradnikov veleposlaništev držav članic v tretjih državah.

52. Pred koncem vsakega koledarskega leta varnostni organ ESZD sprejme program varnostnih inšpekcij za ESZD za naslednje leto.

53. Po potrebi varnostni organ ESZD organizira varnostne inšpekcije, ki niso predvidene v programu zgoraj.

54. Ob koncu varnostne inšpekcije se pregledanemu subjektu predložijo glavni zaključki in priporočila. Nato inšpekcijska ekipa pripravi poročilo o inšpekciji. Če so bili predlagani korektivni ukrepi in priporočila, se v poročilo vključi dovolj podrobnosti, da je mogoče dosežene zaključke utemeljiti. Poročilo se pošlje varnostnemu organu ESZD in vodji pregledanega subjekta.

V pristojnosti direktorata ESZD, odgovornega za varnost, se pripravi redno poročilo, v katerem se poudarijo dognanja inšpekcij, opravljenih v določenem obdobju v državah članicah; poročilo prouči Varnostni odbor ESZD.

Izvajanje varnostnih inšpekcij v agencijah in organih EU, ustanovljenih v skladu s poglavjem 2 naslova V PEU, in poročanje o njih

55. Direktorat ESZD, odgovoren za varnost, lahko po potrebi imenuje sodelujoče strokovnjake za sodelovanje v skupnih inšpekcijskih ekipah EU, ki izvajajo inšpekcije v agencijah in organih EU, ustanovljenih v skladu s poglavjem 2 naslova V PEU.

Kontrolni seznam varnostnih inšpekcij ESZD

56. Direktorat ESZD, odgovoren za varnost, pripravi in posodablja kontrolni seznam točk, ki jih je treba preveriti med varnostno inšpekcijo ESZD. Ta kontrolni seznam se pošlje Varnostnemu odboru ESZD.

57. Podatki za izpolnitev kontrolnega seznama se pridobijo zlasti med inšpekcijo 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 inšpekciji.

PRILOGA A 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 8 Priloge A.

2. Za varovanje tajnosti in pravilno delovanje operacij v komunikacijskih in informacijskih sistemih (KIS) 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 varnost vseh komunikacijskih in informacijskih sistemov, v katerih poteka delo s tajnimi podatki EU. Natančne zahteve za izvajanje teh določb so opredeljene v smernicah o zagotavljanju informacijske varnosti.

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 obvladovanja tveganja.

5. Pristojni organi ESZD proučijo 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 obvladovanja varnostnega tveganja je uporabiti sklop varnostnih ukrepov, s čimer se doseže zadovoljivo ravnovesje med zahtevami uporabnikov 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 se, vključno s tehničnimi in netehničnimi varnostnimi ukrepi, v okviru postopka akreditacije varnostno preskuša, da se zagotovi ustrezna stopnja izvajanih varnostnih ukrepov in preveri, ali se pravilno izvajajo ter ali so pravilno integrirani in konfigurirani.

11. Varnostne ocene, inšpekcije in pregledi se izvajajo med delovanjem in vzdrževanjem KIS 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. ESZD sodeluje z GSS, Komisijo in državami članicami 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 upravlja ESZD, ki dela 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 komunikacijske in informacijske sisteme;

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

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

Stopnja strogosti takšnih varnostnih ukrepov in njihova uporabnost se določita po oceni tveganja.

17. Pristojni organi ESZD zagotovijo, da se lahko odzovejo na incidente, ki lahko presegajo organizacijske in državne meje, da bi uskladili odzive in izmenjavo podatkov 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 funkcionalnosti, naprave in storitve, potrebne za delovanje, da ni izpostavljanja nepotrebnim tveganjem.

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

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

Ozaveščenost o zagotavljanju informacijske varnosti

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

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

(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 zagotavljanju informacijske varnosti in usposabljanje za krepitev ozaveščenosti o njej 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 8(5) tega sklepa takšni šifrirni izdelki priporočijo v odobritev organu za odobritev šifrirnih metod in izdelkov ESZD, 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 se jih s temi izdelki varuje.

27. Organ za odobritev šifrirnih metod in izdelkov ESZD lahko na priporočilo Varnostnega odbora Sveta zaradi posebnih operativnih razlogov opusti zahteve iz odstavka 25 ali 26 in za določen čas izda odobritev v skladu s členom 8(5) tega sklepa.

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. Visoki predstavnik odobri varnostno politiko glede ustreznosti in odobritve nešifrirnih varnostnih izdelkov IT.

Pošiljanje v varovanih območjih

30. Ne glede na določbe tega sklepa se v primerih, ko je pošiljanje tajnih podatkov EU omejeno na varovana območja ali upravna 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 komunikacijskih in informacijskih sistemov

31. V tem sklepu medsebojna povezava 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 varnostne ukrepe, s katerimi nadzoruje izmenjavo tajnih podatkov.

33. Vse medsebojne povezave KIS z drugim sistemom IT ustrezajo naslednjim osnovnim zahtevam:

    (a) pristojni organi določijo in odobrijo poslovne ali operativne zahteve za takšne medsebojne povezave;

    (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 (IAA), odobri pa jih pristojni organ za varnostno akreditacijo (SAA).

    Če se nezaščiteno ali javno omrežje uporablja izključno za prenos in so podatki šifrirani s šifrirnim izdelkom, odobrenim v skladu s členom 8(5) tega sklepa, se takšna povezava ne šteje za medsebojno povezavo.

35. Neposredna ali kaskadna medsebojna povezava KIS, akreditiranega za delo s podatki stopnje tajnosti TRES 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 varnostni organ ESZD.

37. Računalniški nosilci podatkov se lahko ponovno uporabijo, stopnja njihove tajnosti pa se lahko zniža ali prekliče v skladu z varnostnimi smernicami iz člena 8(2) tega sklepa.

Izredne razmere

38. Ne glede na določbe tega sklepa se lahko posebni postopki, opisani v nadaljevanju, za omejeno obdobje 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 prenašajo 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 gradiva, in če:

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

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

40. Tajni podatki, poslani pod pogoji iz odstavka 39, 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 39, se Varnostnemu direktoratu ESZD in Varnostnemu odboru ESZD naknadno pošlje poročilo. V tem poročilu bodo navedeni vsaj pošiljatelj, prejemnik in organ izvora vsakega tajnega podatka EU.

III. FUNKCIJE IN ORGANI ZA ZAGOTAVLJANJE INFORMACIJSKE VARNOSTI

42. V ESZD 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 (IAA)

43. Organ za zagotavljanje informacijske varnosti je odgovoren za:

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

(b) varovanje in upravljanje tehničnih informacij, povezanih s šifrirnimi izdelki;

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

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

(e) usklajevanje usposabljanja in ozaveščenosti o zagotavljanju informacijske varnosti;

(f) posvetovanje s ponudnikom sistema, akterji na področju varovanja tajnosti in predstavniki uporabnikov glede varnostnih smernic o zagotavljanju informacijske varnosti; ter

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

Organ TEMPEST

44. Organ TEMPEST je pristojen za zagotavljanje, da je KIS skladen s politikami in smernicami 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 (CAA)

45. Organ za odobritev šifrirnih metod in izdelkov zagotavlja, da šifrirni izdelki ustrezajo posameznim zadevnim šifrirnim smernicam. Šifrirni izdelek odobri za varovanje tajnih podatkov EU do določene stopnje tajnosti v njegovem operativnem okolju.

Organ za razpošiljanje šifrirnega materiala (CDA)

46. Organ za razpošiljanje šifrirnega materiala 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, ter

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

Organ za varnostno akreditacijo (SAA)

47. Organ za varnostno akreditacijo za vsak sistem je odgovoren za:

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

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

(c) določitev strategije za varnostno akreditacijo, ki določa stopnjo podrobnosti za postopek akreditacije, ki je sorazmerna z zahtevano stopnjo 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, dokumentacije o preverjanju varovanja tajnosti in varnostno-operativnih postopkov, ter zagotavljanje, da je skladna z varnostnimi pravili in smernicami ESZD;

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

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

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

Odbor za varnostno akreditacijo

49. Skupni odbor za varnostno akreditacijo je odgovoren za akreditacijo KIS, ki so v pristojnosti organa za varnostno akreditacijo ESZD 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 GSS in Komisije. K sodelovanju so povabljeni tudi drugi subjekti z vozlišči na KIS, če se razpravlja o tem sistemu.

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

Operativni organ za zagotavljanje informacijske varnosti

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

(a) pripravo varnostne dokumentacije v skladu z varnostnimi smernicami, zlasti izjav o posebnih varnostnih zahtevah, značilnih za sistem, vključno z izjavo o preostalem tveganju, varnostno-operativnimi postopki in načrtom za šifriranje v okviru postopka 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 varnostnih zahtevah, 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 A V

INDUSTRIJSKA VARNOST

I. UVOD

1. V tej prilogi so določbe za izvajanje člena 9 Priloge A. 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 ESZD.

2. Varnostni organ ESZD odobri smernice o industrijski varnosti, v kateri so podrobno opisane predvsem zahteve glede varnostnih dovoljenj organizacij, listin o varnostnih vidikih, obiskov, pošiljanja in prenašanja 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 ESZD kot naročnik določi stopnjo tajnosti podatkov, ki se posredujejo ponudnikom in izvajalcem, pa tudi stopnjo tajnosti podatkov, ki jih bo ustvaril izvajalec. ESZD za ta namen pripravi vodič po stopnjah tajnosti, ki se uporablja pri izvajanju pogodbe.

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

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

   (b) splošna stopnja tajnosti naročila ne sme biti nižja od najvišje stopnje tajnosti vsakega izmed njegovih elementov, ter

   (c) ESZD 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

5. Varnostne zahteve, povezane s posamezno pogodbo, so opisane v listini o varnostnih vidikih. Tej listini 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

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

8. Direktorat ESZD, odgovoren za varnost, zaprosi nacionalni varnostni organ ali imenovani varnostni organ ali kateri koli drug pristojni varnostni organ zadevne države članice za izdajo varnostnega dovoljenja organizacije, 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). Izvajalcu, podizvajalcu ali morebitnemu izvajalcu ali podizvajalcu se tajni podatki EU ne zagotovijo ali se mu dostop do njih ne odobri, dokler se ESZD ne predloži dokazilo o varnostnem dovoljenju organizacije.

9. Po potrebi ESZD kot naročnik nacionalni varnostni organ/imenovani varnostni organ ali kateri koli drug pristojni varnostni organ uradno obvesti, da se v fazi pred sklenitvijo pogodbe ali za izvajanje pogodbe zahteva varnostno dovoljenje organizacije. 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 tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET.

10. ESZD kot naročnik najustreznejšemu ponudniku ne sme dodeliti pogodbe s tajnimi podatki, dokler ji 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.

11. ESZD kot naročnik zaprosi nacionalni varnostni organ/imenovani varnostni organ ali kateri koli drug pristojni varnostni organ, ki je izdal varnostno dovoljenje organizacije, naj jo obvesti o vsakršnih negativnih informacijah, 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.

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

IV. DOVOLJENJA ZA DOSTOP DO TAJNIH PODATKOV ZA OSEBJE IZVAJALCEV

13. Vsi člani osebja, ki delajo za izvajalce, ki potrebujejo dostop do tajnih podatkov EU stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, so bili ustrezno varnostno preverjeni in imajo potrebo po seznanitvi za dostop do podatkov. Čeprav varnostno preverjanje osebja ni potrebno za dostop do tajnih podatkov EU stopnje RESTREINT UE/EU RESTRICTED, obstaja potreba po seznanitvi za takšen dostop.

14. Vloge za dovoljenja za dostop do tajnih podatkov za osebje izvajalcev se vložijo pri nacionalnem varnostnem organu/imenovanem varnostnem organu, pristojnem za subjekt.

15. ESZD opozori izvajalce, ki želijo zaposliti državljana tretje države na delovnem mestu, na katerem potrebujejo dostop do tajnih podatkov EU, da sta ugotovitev, ali se posamezniku lahko odobri dostop do takih podatkov, in potrditev, da mora biti pred dodelitvijo dostopa zagotovljeno soglasje organa izvora, v skladu s tem sklepom v pristojnosti nacionalnega varnostnega organa/imenovanega varnostnega organa države članice, v kateri je subjekt, ki zaposluje, registriran in ima sedež.

V. POGODBE IN PODIZVAJALSKE POGODBE S TAJNIMI PODATKI

16. 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.

17. Ko je pogodba ali podizvajalska pogodba s tajnimi podatki dodeljena, ESZD 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.

18. Ko se takšne pogodbe prekinejo ali prenehajo veljati, ESZD 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.

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

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

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

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

23. Izvajalec pred oddajo delov pogodbe s tajnimi podatki podizvajalcu pridobi dovoljenje ESZD 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.

24. 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.

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

VI. OBISKI V ZVEZI S POGODBAMI S TAJNIMI PODATKI

26. Če morajo ESZD, 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. To ne vpliva na posebno pravico nacionalnih varnostnih organov/imenovanih varnostnih organov v okviru posebnih projektov, da se sporazumejo o postopku, na podlagi katerega se je mogoče o takšnih obiskih dogovoriti neposredno.

27. 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 ESZD.

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

VII. POŠILJANJE IN PRENAŠANJE TAJNIH PODATKOV EU

29. Za pošiljanje tajnih podatkov EU z elektronskimi sredstvi se uporabljajo ustrezne določbe iz člena 8 Priloge A ter iz Priloge A IV.

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

31. Za prevoz tajnega materiala kot tovora se pri določanju varnostnega režima upoštevajo naslednja načela:

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

(b) stopnja varovanja pošiljke se določi na podlagi materiala z najvišjo stopnjo tajnosti, ki ga pošiljka vsebuje;

(c) za prevoznika se pridobi varnostno dovoljenje organizacije na ustrezni stopnji, če to pomeni tudi, da se tajni podatki hranijo v objektih izvajalcev. V vsakem primeru mora biti osebje, ki dela s pošiljko, ustrezno varnostno preverjeno v skladu s Prilogo A 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 ESZD po potrebi v sodelovanju z zadevnimi nacionalnimi varnostnimi organi/imenovanimi varnostnimi organi pošiljatelja in prejemnika ali katerim koli drugim pristojnim varnostnim organom;

(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 ESZD ali kateri koli drug pristojni varnostni organ države pošiljatelja in države prejemnika.

VIII. PRENOS TAJNIH PODATKOV EU IZVAJALCEM V TRETJIH DRŽAVAH

32. Prenos tajnih podatkov EU izvajalcem in podizvajalcem v tretjih državah, ki imajo sklenjen veljaven varnostni sporazum z EU, poteka v skladu z varnostnimi ukrepi, dogovorjenimi med ESZD kot naročnikom in nacionalnim varnostnim organom/imenovanim varnostnim organom zadevne tretje države, v kateri je registriran izvajalec.

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

33. ESZD kot naročnik sme po potrebi v sodelovanju 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.

34. Če to zahtevajo nacionalni zakoni in predpisi, ESZD 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.

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

36. ESZD kot naročnik prouči 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.

37. Izvajalec lahko sklene podizvajalsko pogodbo pod pogoji, ki so skladni z odstavki 22–24.

38. Če pogodba vključuje delo s tajnimi podatki stopnje RESTREINT UE/EU RESTRICTED v KIS, ki ga upravlja izvajalec, ESZD 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 A VI

IZMENJAVA TAJNIH PODATKOV S TRETJIMI DRŽAVAMI IN MEDNARODNIMI ORGANIZACIJAMI

I. UVOD

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

II. OKVIRI ZA IZMENJAVO TAJNIH PODATKOV

2. ESZD lahko izmenja tajne podatke EU s tretjimi državami ali mednarodnimi organizacijami v skladu s členom 10(1) Priloge A.

Za podporo visokemu predstavniku pri izvajanju odgovornosti iz člena 218 PDEU:

(a) ustrezni geografski ali tematski oddelek ESZD po posvetovanju z direktoratom ESZD, odgovornim za varnost, po potrebi določi potrebo po dolgoročni izmenjavi tajnih podatkov EU z zadevnimi tretjimi državami ali mednarodnimi organizacijami;

(b) direktorat ESZD, odgovoren za varnost, po posvetovanju z ustreznim geografskim oddelkom ESZD visokemu predstavniku po potrebi predloži osnutke besedil, ki se predlagajo Svetu v skladu s členom 218(3),(5) in (6) PDEU;

(c) Direktorat ESZD, odgovoren za varnost, podpira visokega predstavnika pri vodenju pogajanj v sodelovanju z ustreznimi službami Komisije in generalnega sekretariata Sveta;

(d) v zvezi s sporazumi ali dogovori s tretjimi državami glede njihovega sodelovanja v operacijah za krizno upravljanje SVOP, kakor je navedeno v členu 10(1)(c) Priloge A, direktorat za krizno upravljanje in načrtovanje ESZD po posvetovanju z ustreznimi službami ESZD visokemu predstavniku po potrebi predloži osnutke besedil, ki se predlagajo Svetu v skladu s členom 218(3),(5) in (6) PDEU ter visokega predstavnika podpira pri vodenju pogajanj v sodelovanju z ustreznimi službami ESZD in generalnega sekretariata Sveta.

3. Če sporazumi o varovanju tajnosti podatkov vsebujejo tehnične izvedbene določbe, o katerih se dogovorita direktorat ESZD, odgovoren za varnost, – v sodelovanju z Varnostnim direktoratom Generalnega direktorata Komisije za človeške vire in varnost ter varnostnim uradom generalnega sekretariata Sveta – in pristojni varnostni organ zadevne tretje države ali mednarodne organizacije, take določbe upoštevajo stopnjo varovanja, ki jo določajo veljavni varnostni predpisi, strukture in postopki v zadevni tretji državi ali mednarodni organizaciji.

4. Če obstaja dolgoročna potreba ESZD po izmenjavanju tajnih podatkov, ki načeloma ne presegajo stopnje RESTREINT UE/EU RESTRICTED, s tretjo državo ali mednarodno organizacijo in če je bilo ugotovljeno, da zadevna stran nima dovolj razvitega varnostnega sistema, da bi bila zmožna skleniti sporazum o varovanju tajnosti podatkov, lahko visoki predstavnik po pridobitvi soglasnega pozitivnega mnenja Varnostnega odbora ESZD v skladu s členom 15(5) tega sklepa sklene dogovor o izvajanju z ustreznimi varnostnimi organi zadevne tretje države ali mednarodne organizacije.

5. Tajni podatki EU se s tretjo državo ali mednarodno organizacijo ne izmenjujejo z elektronskimi sredstvi, razen če je to izrecno določeno v sporazumu o varovanju tajnosti podatkov ali dogovoru o izvajanju.

6. V skladu z dogovorom o izvajanju glede izmenjave tajnih podatkov ESZD in tretja država ali mednarodna organizacija vsaka posebej določijo register, ki je glavna točka vstopa in izstopa pri izmenjavi tajnih podatkov. Za ESZD bo to centralni register ESZD.

7. Dogovori o izvajanju so praviloma v obliki izmenjave pisem.

III. OCENJEVALNI OBISKI

8. Ocenjevalni obiski iz člena 17 tega sklepa se izvedejo v medsebojnem dogovoru z zadevno tretjo državo ali mednarodno organizacijo ter ocenijo:

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

(b) kakršne koli posebne značilnosti varnostnih zakonov, predpisov, politik ali postopkov tretje države ali mednarodne organizacije, ki lahko vplivajo na najvišjo stopnjo tajnosti podatkov, ki se lahko izmenjajo;

(c) varnostne ukrepe in postopke, ki se trenutno uporabljajo za varovanje tajnih podatkov, in ter

(d) postopke za pridobitev dovoljenja za dostop do stopnje tajnih podatkov EU, ki bodo posredovani.

9. Tajni podatki EU se ne izmenjajo dokler ni izveden ocenjevalni obisk in določena stopnja, na kateri se lahko med stranmi izmenjajo tajni podatki EU, in sicer na podlagi enakovrednosti stopnje varovanja, ki bo zagotovljena.

Če je visoki predstavnik pred takšnim ocenjevalnim obiskom obveščen o kakršnih koli izrednih ali nujnih razlogih za izmenjavo tajnih podatkov, ESZD:

(a) najprej zaprosi organ izvora za pisno soglasje, da ugotovi, da ni pripomb glede dajanja podatkov.

(b) prenese zadevo varnostnemu organu ESZD, ki lahko odloči o dajanju tajnih podatkov, pod pogojem, da je bilo pridobljeno soglasno pozitivno mnenje držav članic, kakor so zastopane v Varnostnem odboru ESZD.

Če ESZD ne more določiti organa izvora, varnostni organ ESZD prevzame odgovornost organa izvora po pridobitvi soglasnega pozitivnega mnenja Varnostnega odbora ESZD.

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

10. Če obstaja okvir za izmenjavo tajnih podatkov s tretjo državo ali mednarodno organizacijo v skladu s členom 10(1) Priloge A, odločitev ESZD za dajanje tajnih podatkov EU tretji državi ali mednarodni organizaciji sprejme varnostni organ ESZD, ki lahko takšno pooblastilo prenese na višje uradnike ESZD ali druge njim podrejene osebe.

11. Če organ izvora tajnih podatkov, ki bodo dani, vključno z organi izvora izvornega materiala, ki ga ti podatki lahko vsebujejo, ni ESZD, ESZD ta organ najprej zaprosi za pisno soglasje, da ugotovi, da ni pripomb glede dajanja podatkov. Če ESZD ne more določiti organa izvora, varnostni organ ESZD prevzame odgovornost organa izvora po pridobitvi soglasnega pozitivnega mnenja držav članic, kakor so zastopane v Varnostnem odboru ESZD.

V. *AD HOC* POSREDOVANJE TAJNIH PODATKOV EU V IZJEMNIH PRIMERIH

12. Če ni enega od okvirov iz člena 10(1) Priloge A in ko interesi EU ali ene ali več držav članic zahtevajo dajanje tajnih podatkov EU iz političnih, operativnih ali nujnih razlogov, se lahko tajni podatki EU izjemoma dajo tretji državi ali mednarodni organizaciji, potem ko so bili sprejeti naslednji ukrepi.

Potem ko zagotovi, da so izpolnjeni pogoji iz odstavka 11 zgoraj, direktorat ESZD, odgovoren za varnost:

(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 v skladu s standardi, ki niso manj strogi od standardov iz tega sklepa;

(b) pozove Varnostni odbor ESZD, naj na podlagi razpoložljivih podatkov oblikuje mnenje o tem, ali je mogoče zaupati varnostnim predpisom, strukturam in postopkom v tretji državi ali mednarodni organizaciji, ki naj bi prejela tajne podatke EU;

(c) prenese zadevo varnostnemu organu ESZD, ki lahko odloči o dajanju tajnih podatkov, pod pogojem, da je bilo pridobljeno soglasno pozitivno mnenje držav članic, kakor so zastopane v Varnostnem odboru ESZD.

13. Če ni enega od okvirov iz člena 10(1) Priloge A, se zadevna tretja stran pisno zaveže, da bo ustrezno varovala tajne podatke EU.

Dodatek A

Opredelitev pojmov

V tem sklepu se uporabljajo naslednje opredelitve pojmov:

„akreditacija“ pomeni postopek, ki se zaključi z uradno izjavo organa za varnostno akreditacijo o odobritvi sistema, da deluje z določeno stopnjo tajnosti v posebnem varnostnem načinu delovanja v svojem operativnem okolju in s sprejemljivo stopnjo tveganja, ob predpostavki, da je bila uvedena vrsta odobrenih tehničnih, fizičnih, organizacijskih in postopkovnih varnostnih ukrepov;

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

„pooblastilo za dostop do tajnih podatkov EU“ pomeni pooblastilo varnostnega organa ESZD, sprejeto v skladu s tem sklepom, potem ko so pristojni organi države članice izdali dovoljenje za dostop do tajnih podatkov, s katerim 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 – glej člen 2 Priloge A I;

„kršitev“ je posameznikovo dejanje ali opustitev dejanja v nasprotju z varnostnimi pravili iz tega sklepa in/ali varnostnimi politikami ali smernicami, ki določajo katere koli ukrepe, potrebne za njegovo izvajanje;

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

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

„podizvajalska pogodba s tajnimi podatki“ pomeni pogodbo, ki jo izvajalec ESZD 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;

„komunikacijski in informacijski sistem“ (KIS) 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 – glej člen 8(2) Priloge A;

„nepooblaščeno razkritje tajnih podatkov EU“ pomeni razkritje tajnih podatkov EU nepooblaščenim osebam ali subjektom v celoti ali delno – glej člen 9(2);

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

„šifrirni izdelki“ so šifrirni algoritmi, šifrirni moduli strojne in programske opreme ter izdelki, vključno s podrobnostmi izvajanja in s tem povezano dokumentacijo, ter šifrirni ključi;

„operacija SVOP“ pomeni vojaško ali civilno operacijo kriznega upravljanja iz naslova V poglavja 2 PEU;

„preklic stopenj tajnosti“ pomeni odpravo vseh stopenj tajnosti;

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

„imenovani varnostni organ“ 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.

„dokument“ pomeni vse zapisane podatke, ne glede na njihovo fizično obliko ali značilnosti;

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

„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 – glej člen 2(f);

„varnostno dovoljenje organizacije“ SC) 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;

„delo“ s tajnimi podatki EU pomeni vse možne dejavnosti, v katere so vključeni tajni podatki EU skozi njihov celotni obstoj. Zajema njihov nastanek, obdelavo, prenašanje, znižanje stopnje tajnosti, preklic stopenj tajnosti in uničenje. V zvezi s komunikacijskimi in informacijskimi sistemi zajema tudi njihovo zbiranje, prikaz, pošiljanje in hrambo;

„imetnik podatkov“ pomeni ustrezno pooblaščenega posameznika, za katerega je ugotovljeno, da mora biti seznanjen z zadevnimi podatki, in razpolaga z elementom tajnega podatka EU ter je zato odgovoren za njegovo varovanje;

„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 samozaposlen posameznik;

„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 – glej člen 9(1) Priloge A;

„zagotavljanje informacijske varnosti“ v komunikacijskih in informacijskih sistemih zagotovi, da bodo podatki v teh sistemih zaščiteni in bodo delovali tako, kot morajo, kadar morajo, pod nadzorom zakonitih uporabnikov. Učinkovito zagotavljanje informacijske varnosti zagotavlja ustrezno stopnjo tajnosti, celovitost, razpoložljivost, nezatajljivost in avtentičnost podatkov. Zagotavljanje informacijske varnosti temelji na postopku obvladovanja tveganja – glej člen 8(1) Priloge A;

„medsebojna povezava“ v tem sklepu pomeni neposredno povezavo dveh ali več sistemov IT za namen izmenjave podatkov in drugih informacijskih virov (npr. komunikacija) v eni ali več smereh – glej odstavek 31 Priloge A IV;

„upravljanje tajnih podatkov“ je uporaba upravnih ukrepov za nadzor nad tajnimi podatki EU v njihovem življenjskem ciklu, ki dopolnjujejo ukrepe iz členov 5, 6 in 8 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 ter delo z njimi – glej člen 7(1) Priloge A;

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

„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;

„varnost osebja“ je izvajanje ukrepov, s katerimi se zagotovi, da imajo dostop do tajnih podatkov EU samo posamezniki, ki:

— imajo potrebo po seznanitvi;

— so bili varnostno preverjeni na ustrezni stopnji za dostop do podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje ali drugače pravilno pooblaščeni zaradi svoje funkcije v skladu z nacionalnimi zakoni in predpisi, ter

— so bili poučeni o svoji odgovornosti –

glej člen 5(1) Priloge A;

„dovoljenje za dostop do tajnih podatkov“ (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; ta posameznik je „varnostno preverjen“; ta posameznik je „varnostno preverjen“;

„potrdilo za dostop do tajnih podatkov“ pomeni potrdilo, ki ga izda pristojni organ in ki dokazuje, da je posameznik varnostno preverjen in da ima veljavno dovoljenje za dostop do tajnih podatkov ali pooblastilo vodje direktorata, odgovornega za varnost, za dostop do tajnih podatkov EU, na katerem so navedeni stopnja tajnosti tajnih 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 dovoljenja;

„fizična varnost“ je uporaba fizičnih in tehničnih zaščitnih ukrepov za odvračanje nepooblaščenega dostopa do tajnih podatkov EU – glej člen 6 Priloge A;

„varnostna navodila za program/projekt“ pomenijo seznam varnostnih postopkov, ki se uporabljajo za specifičen program/projekt zaradi standardizacije varnostnih postopkov. Ta seznam je mogoče revidirati kadar koli v času trajanja programa/projekta;

„vpis“ pomeni uporabo postopkov, ki beležijo življenjski cikel podatkov, vključno z njihovim razširjanjem in uničenjem – glej odstavek 21 Priloge A III;

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

„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 se sprejme prisotnost preostalega tveganja, potem ko se je poskušalo tveganje obvladati;

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

„obveščanje o tveganju“ zajema ozaveščanje skupnosti uporabnikov komunikacijskih in informacijskih sistemov o tveganjih, obveščanje organov za odobritev o tveganjih in poročanje o tveganjih operativnim organom;

„postopek obvladovanja 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;

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

„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 – glej oddelek II Priloge A V;

„vodič po stopnjah tajnosti“ pomeni dokument, ki opisuje elemente programa ali naročila, ki so tajni, in določa ustrezne stopnje tajnosti. Vodič po stopnjah tajnosti se lahko tekom celotnega programa ali naročila razširi, elementi podatkov pa se lahko prerazvrstijo ali razvrstijo na nižjo stopnjo. Če obstaja vodič po stopnjah tajnosti, je del listine o varnostnih vidikih – glej oddelek II Priloge A V;

„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);

„varnostno-operativni postopki“ (SecOP) pomenijo opis izvajanja varnostne politike, ki jo je treba sprejeti, operativnih postopkov, ki jih je treba izvajati, in odgovornosti osebja;

„občutljivi netajni podatki“ pomenijo podatke in material, ki ga mora ESZD varovati na podlagi pravnih obveznosti, določenih s Pogodbama ali akti, sprejetimi za njuno izvajanje, in/ali zaradi njihove občutljive narave. Občutljivi netajni podatki med drugim vključujejo podatke ali gradivo, za katero velja obveznost varovanja poslovne skrivnosti iz člena 339 PDEU, podatke, ki se nanašajo na interese, zaščitene na podlagi člena 4 Uredbe Evropskega parlamenta in Sveta (ES) št. 1049/2001 ([1]) v povezavi z ustrezno sodno prakso Sodišča, ali osebne podatke v okviru področja uporabe Uredbe (ES) št. 45/2001.

„izjava o posebnih varnostnih zahtevah“ (SSRS) pomeni zavezujoč sklop načel varnosti, ki jih je treba upoštevati, in podrobnih varnostnih zahtev, ki jih je treba izvajati, pri čemer so osnova postopka certificiranja in akreditacije KIS;

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

„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;

„ranljiva točka“ pomeni kakršno koli pomanjkljivost, zaradi katere se lahko uresniči ena ali več groženj. 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.

([1]) Uredba Evropskega parlamenta in Sveta (ES) št. 1049/2001 z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije (UL L 145, 31.5.2001, str. 43).

Dodatek B

Enakovredne stopnje tajnosti

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
EURATOM	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Belgija	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	Opomba (1) spodaj
Bolgarija	Строго секретно	Секретно	Поверително	За служебно ползване
Češka	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
Irska	Top Secret	Secret	Confidential	Restricted
Grčija	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Španija	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Francija	Très Secret Défense	Secret Défense	Confidentiel Défense	Opomba (3) spodaj
Hrvaška	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italija	Segretissimo	Segreto	Riservatissimo	Riservato
Ciper	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης 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

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Romunija	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenija	Strogo tajno	Tajno	Zaupno	Interno
Slovaška	Prísne tajné	Tajné	Dôverné	Vyhradené
Finska	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Švedska ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Združeno kraljestvo	UK TOP SECRET	UK SECRET	Ni enakovredne stopnje ([5])	UK OFFICIAL – SENSITIVE

([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.
([5]) Združeno kraljestvo s tajnimi podatki „CONFIDENTIEL UE/EU CONFIDENTIAL“ dela in jih varuje v skladu z varnostnimi zahtevami za stopnjo „UK SECRET“.