SKLEP KOMISIJE (EU, Euratom) 2015/444

z dne 13. marca 2015

o varnostnih predpisih za varovanje tajnih podatkov EU

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 249 Pogodbe,

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti za atomsko energijo in zlasti člena 106 Pogodbe,

ob upoštevanju Protokola št. 7 o privilegijih in imunitetah Evropske unije, priloženega k pogodbama, in zlasti člena 18 Protokola,

ob upoštevanju naslednjega:

(1) Varnostne določbe Komisije za varovanje tajnih podatkov Evropske unije (EUCI) je treba pregledati in posodobiti ob upoštevanju institucionalnih, organizacijskih, operativnih in tehnoloških dosežkov.

(2) Evropska komisija je pogodbenica instrumentov na področju varnosti na njenih glavnih lokacijah z vladami Belgije, Luksemburga in Italije ([1]).

(3) Komisija, Svet in Evropska služba za zunanje delovanje se zavzemajo za enakovredne standarde varovanja tajnih podatkov EU.

(4) Pomembno je, da se, kadar je to ustrezno, v načela, standarde in pravila za varovanje tajnih podatkov, potrebna za zaščito interesov Unije in njenih držav članic, vključijo Evropski parlament in druge institucije, agencije, organi ali uradi Unije.

(5) Za obvladovanje tveganja, povezanega s tajnimi podatki EU, je predviden poseben postopek. Cilj tega postopka je opredeliti znana varnostna tveganja, določiti varnostne ukrepe za zmanjšanje teh tveganj na sprejemljivo raven v skladu s temeljnimi načeli in minimalnimi standardi iz tega sklepa ter uporabljati te ukrepe ob upoštevanju koncepta globinske obrambe. Učinkovitost takšnih ukrepov se nenehno ocenjuje.

(6) Fizična varnost, namenjena varovanju tajnih podatkov, znotraj Komisije pomeni uporabo fizičnih in tehničnih zaščitnih ukrepov za preprečitev nepooblaščenega dostopa do tajnih podatkov EU.

(7) Upravljanje tajnih podatkov EU pomeni uporabo upravnih ukrepov za nadzor nad tajnimi podatki EU v njihovem življenjskem ciklu, ti ukrepi pa dopolnjujejo ukrepe iz poglavij 2, 3 in 5 tega sklepa ter tako prispevajo k odvračanju, odkrivanju in obnovitvi takih podatkov po naključnem ali namernem razkritju ali izgubi. Ti ukrepi se nanašajo predvsem na ustvarjanje, hrambo, vpisovanje, kopiranje, prevajanje, znižanje stopnje tajnosti, preklic tajnosti, prenašanje in uničenje tajnih podatkov EU ter dopolnjujejo splošna pravila o upravljanju dokumentov Komisije (sklepa 2002/47/ES ([2]), ESPJ, Euratom in 2004/563/ES, Euratom ([3])).

([1]) Glej „Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité“ z dne 31. decembra 2004, „Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois“ z dne 20. januarja 2007 in „Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale“ z dne 22. julija 1959.

([2]) Sklep Komisije 2002/47/ES, ESPJ, Euratom z dne 23. januarja 2002 o spremembi njenega poslovnika (UL L 21, 24.1.2002, str. 23).

([3]) Sklep Komisije 2004/563/ES, Euratom z dne 7. julija 2004 o spremembi poslovnika (UL L 251, 27.7.2004, str. 9).

(8) Določba tega sklepa ne vpliva na:

(a) Uredbo (Euratom) št. 3 ([1]);

(b) Uredbo (ES) št. 1049/2001 Evropskega parlamenta in Sveta ([2]);

(c) Uredbo (ES) 45/2001 Evropskega parlamenta in Sveta ([3]);

(d) Uredbo Sveta (EGS, Euratom) št. 354/83 ([4]) –

SPREJELA NASLEDNJI SKLEP:

POGLAVJE 1

OSNOVNA NAČELA IN MINIMALNI STANDARDI

Člen 1

Opredelitev pojmov

V tem sklepu se uporabljajo naslednje opredelitve pojmov:

1. „služba Komisije“ pomeni kateri koli generalni direktorat ali službo Komisije ali kateri koli kabinet člana Komisije;

2. „kriptografski material“ pomeni kriptografske algoritme, kriptografske module strojne in programske opreme ter produkte, vključno s podrobnostmi izvajanja in s tem povezano dokumentacijo, ter šifrirni material;

3. „preklic stopnje tajnosti“ pomeni odstranitev vsakršne stopnje tajnosti;

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

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

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

7. „obravnavanje“ tajnih podatkov EU pomeni vse možne dejavnosti, v katere so vključeni tajni podatki EU skozi celotni življenjski cikel. Zajema njihov ustvarjanje, vpis, obdelavo, prenašanje, znižanje stopnje tajnosti, preklic tajnosti in uničenje. V zvezi s komunikacijskimi in informacijskimi sistemi zajema tudi njihovo zbiranje, prikaz, razpošiljanje in hrambo;

8. „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;

9. „izvedbena pravila“ pomeni kakršen koli sklop pravil ali varnostnih obvestil, sprejetih v skladu s poglavjem 5 Sklepa Komisije (EU, Euratom) 2015/443 ([5]);

10. „gradivo“ pomeni vsak medij, nosilec podatkov ali del strojev ali opreme, ki je že bil izdelan ali je v postopku izdelave;

11. „tvorec“ pomeni institucijo, agencijo ali organ Unije, državo članico, tretjo državo ali mednarodno organizacijo, v pristojnosti katere so bili ustvarjeni tajni podatki in/ali so bili uvedeni v strukture Unije;

12. „prostori“ so vse nepremičnine in pritikline v lasti ali posesti Komisije;

([1]) Uredba (Euratom) št. 3 z dne 31. julija 1958 o izvajanju člena 24 Pogodbe o ustanovitvi Evropske skupnosti za atomsko energijo (UL 17, 6.10.1958, str. 406/58).
([2]) 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).
([3]) 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).
([4]) Uredba Sveta (EGS, Euratom) št. 354/83 z dne 1. februarja 1983 o odpiranju za javnost arhivskega gradiva Evropske gospodarske skupnosti in Evropske skupnosti za atomsko energijo (UL L 43, 15.2.1983, str. 1).
([5]) Sklep Komisije (EU, Euratom) 2015/443 z dne 13. marca 2015 o varnosti v Komisiji (glej stran 41 tega uradnega lista).

13. „postopek za obvladovanje varnostnega tveganja“ pomeni celoten postopek opredelitve, nadzorovanja in čim večje omejitve negotovih dogodkov, ki bi lahko negativno 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;

14. „kadrovski predpisi“ pomeni kadrovske predpise za uradnike Evropske unije in pogoje za zaposlitev drugih uslužbencev Evropske unije, določene v Uredbi Sveta (EGS, Euratom, ESPJ) št. 259/68 ([1]);

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

16. „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.

Člen 2

Predmet urejanja in področje uporabe

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

2. Ta sklep se uporablja za vse službe Komisije in v vseh prostorih Komisije.

3. Ne glede na kakršne koli posebne določbe v zvezi z določenimi skupinami osebja se ta sklep uporablja za člane Komisije, za osebje Komisije, ki spada v področje uporabe kadrovskih predpisov in pogojev za zaposlitev drugih uslužbencev Evropskih skupnosti za napotene nacionalne strokovnjake, dodeljene Komisiji, za ponudnike storitev in njihovo osebje, za pripravnike in za vse posameznike, ki imajo dostop do zgradb Komisije ali drugih sredstev ali do informacij, ki jih obravnava Komisija.

4. Določbe iz tega sklepa se uporabljajo brez poseganja v Sklep 2002/47/ES, ESPJ, Euratom in Sklep 2004/563/ES, Euratom.

Člen 3

Opredelitev tajnih podatkov EU, stopenj tajnosti in oznak

1. „Tajni podatek EU“ pomeni vsak podatek ali gradivo z oznako stopnje tajnosti EU, katerega nepooblaščeno razkritje bi lahko v različni meri škodovalo interesom Evropske unije ali eni ali več državam članicam.

2. Tajni podatki EU imajo naslednje stopnje tajnosti:

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

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

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

(d) RESTREINT UE/EU RESTRICTED: podatki in gradivo, 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. Nosijo lahko dodatne oznake, ki sicer niso oznake tajnosti, je pa njihov namen navesti področje dejavnosti, na katero se nanašajo, tvorca, omejitev pri razpošiljanju, omejitev uporabe ali možnosti pošiljanja.

([1]) Uredba Sveta (EGS, Euratom, ESPJ) št. 259/68 z dne 29. februarja 1968 o določitvi Kadrovskih predpisov za uradnike in Pogojev za zaposlitev drugih uslužbencev Evropskih skupnosti ter o uvedbi posebnih ukrepov, ki se začasno uporabljajo za uradnike Komisije (Pogoji za zaposlitev drugih uslužbencev) (UL L 56, 4.3.1968, str. 1).

Člen 4

Sistem določanja stopenj tajnosti

1. Vsak član Komisije ali služba Komisije zagotovi, da so tajni podatki EU, ki jih ustvari, označeni z ustrezno stopnjo tajnosti, da je jasno razvidno, da gre za tajne podatke EU, in da stopnjo tajnosti obdržijo le, dokler je potrebno.

2. Ne glede na člen 26 tega sklepa se brez predhodnega pisnega soglasja tvorca stopnja tajnosti tajnih podatkov EU ne zniža ali prekliče niti se ne spremenijo ali odstranijo oznake stopnje tajnosti iz člena 3(2).

3. Po potrebi se v skladu s členom 60 spodaj sprejmejo izvedbena pravila za obravnavanje tajnih podatkov EU, vključno s praktičnim vodičem o določanju stopenj tajnosti.

Člen 5

Varovanje tajnih podatkov

1. Tajni podatki EU se varujejo v skladu s tem sklepom in njegovimi izvedbenimi pravili.

2. Imetnik katerega koli tajnega podatka EU je odgovoren za njegovo varovanje v skladu s tem sklepom in njegovimi izvedbenimi pravili v skladu s pravili iz poglavja 4 spodaj.

3. Če države članice v strukture ali omrežja Komisije vnesejo tajne podatke z nacionalno oznako stopnje tajnosti, Komisija 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 Prilogi I.

4. Za skupek tajnih podatkov EU je morda upravičena raven varovanja, ki ustreza višji stopnji tajnosti, kot je stopnja za njihove posamezne sestavne dele.

Člen 6

Obvladovanje varnostnega tveganja

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

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

3. V načrte za zagotovitev neprekinjenega poslovanja vseh služb so vključeni preventivni in obnovitveni ukrepi, tako da so posledice velikih napak ali incidentov pri obravnavanju tajnih podatkov EU in njihovi hrambi čim manjše.

Člen 7

Izvajanje tega sklepa

1. Po potrebi se v skladu s členom 60 spodaj sprejmejo izvedbena pravila za dopolnitev tega sklepa ali v njegovo podporo.

2. Službe Komisije sprejmejo vse potrebne ukrepe, ki so v njihovi pristojnosti, da bi zagotovile, da se pri obravnavanju tajnih podatkov EU oziroma kakršnih koli drugih tajnih podatkov ali njihovi hrambi uporablja ta sklep in zadevna izvedbena pravila.

3. Varnostni ukrepi, ki so bili sprejeti za izvajanje tega sklepa, morajo biti v skladu z načeli za varnost v Komisiji iz člena 3 Sklepa (EU, Euratom) 2015/443.

4. Generalni direktor Generalnega direktorata za človeške vire in varnost vzpostavi varnostni organ Komisije v Generalnem direktoratu za človeške vire in varnost. Varnostni organ Komisije ima pristojnosti, ki so mu dodeljene s tem sklepom in njegovimi izvedbenimi pravili.

5. V vsaki službi Komisije ima lokalni uradnik za varnost, kakor je navedeno v členu 20 Sklepa Sveta (EU, Euratom) 2015/443, naslednje skupne odgovornosti za varovanje tajnih podatkov EU v skladu s tem sklepom, v tesnem sodelovanju z GD za človeške vire in varnost:

(a) obdelava zahtevkov za pooblastila za dostop do tajnih podatkov za osebje;

(b) prispevanje k usposabljanju na področju varnosti in sestankom za ozaveščanje;

(c) nadziranje nadzornega uradnika registra službe;

(d) poročanje o kršitvah varovanja tajnosti in nepooblaščenem razkritju tajnih podatkov EU;

(e) hranjenje nadomestnih ključev in pisnih zapisov vseh nastavitev kombinacij;

(f) druge naloge v zvezi z varovanjem tajnih podatkov EU ali naloge, ki so opredeljene z izvedbenimi pravili.

Člen 8

Kršitev varovanja tajnosti in nepooblaščeno razkritje tajnih podatkov EU

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

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

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

4. Če je bilo ugotovljeno ali če obstajajo utemeljeni razlogi za domnevo, da so bili tajni podatki EU nepooblaščeno razkriti ali izgubljeni, se opravi varnostna poizvedba v skladu s členom 13 Sklepa (EU, Euratom) 2015/443.

5. Izvedejo se vsi ustrezni ukrepi, da se:

(a) obvesti tvorca;

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

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

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

(e) o sprejetih ukrepih obvesti ustrezne organe.

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

POGLAVJE 2

VARNOSTNO PREVERJANJE OSEBJA

Člen 9

Opredelitev pojmov

V tem poglavju se uporabljajo naslednje opredelitve:

1. „pooblastilo za dostop do tajnih podatkov EU“ pomeni odločitev varnostnega organa Komisije, sprejeto v skladu z zagotovitvijo pristojnega organa države članice, da se uradnik Komisije, drugi uslužbenec ali napoten nacionalni strokovnjak lahko pooblasti za dostop do tajnih podatkov EU do določene stopnje tajnosti (CONFIDENTIEL UE/EU CONFIDENTIAL ali višje) in do določenega datuma, če je bila ugotovljena njegova potreba po vedenju in če je bil ustrezno poučen o svoji odgovornosti; ta posameznik je „varnostno preverjen“.

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

   (a) imajo potrebo po vedenju;

   (b) so bili po potrebi varnostno preverjeni na ustrezni stopnji in

   (c) so bili poučeni o svoji odgovornosti.

3. „dovoljenje za dostop do tajnih podatkov“ (PSC) 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 njegovi seznanitvi in če je bil ustrezno poučen o svoji odgovornosti;

4. „potrdilo za dostop do tajnih podatkov“ pomeni potrdilo, ki ga izda pristojni organ in ki dokazuje, da je posameznik imetnik veljavnega dovoljenja ali pooblastila za dostop do tajnih podatkov varnostnega organa Komisije, na katerem je navedena stopnja tajnosti podatkov EU, do katere se lahko posamezniku odobri dostop (CONFIDENTIEL UE/EU CONFIDENTIAL ali višje), obdobje veljavnosti ustreznega dovoljenja ali pooblastila za dostop do tajnih podatkov in datum izteka veljavnosti samega potrdila;

5. „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 dovoljenja za dostop do tajnih podatkov do določene stopnje (CONFIDENTIEL UE/EU CONFIDENTIAL ali višje).

Člen 10

Osnovna načela

1. Posamezniku se odobri dostop do tajnih podatkov EU šele, ko:

1. je bilo ugotovljeno, da ima potrebo po vedenju;

2. je bil poučen o varnostnih pravilih za varovanje tajnih podatkov EU ter relevantnih varnostnih standardih in smernicah ter je sprejel odgovornost za varovanje teh podatkov;

3. je bil za dostop do podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje varnostno pooblaščen na ustrezni stopnji ali drugače pravilno pooblaščen zaradi svoje funkcije v skladu z nacionalnimi zakoni in predpisi.

2. Vsi posamezniki, ki morajo zaradi svojih dolžnosti morda imeti dostop do tajnih podatkov EU stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, so varnostno preverjeni na ustrezni stopnji, preden se jim odobri dostop do takih tajnih podatkov EU. Zadevna oseba da pisno soglasje, da se zanjo opravi postopek za pridobitev dovoljenja za dostop do tajnih podatkov. Brez takšnega soglasja posamezniku ne more biti dodeljeno delovno mesto, funkcija ali naloga, ki vključuje dostop do podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje.

3. Namen postopkov za pridobitev dovoljenja za dostop do tajnih podatkov za osebje je ugotoviti, ali je posameznik dovolj lojalen, vreden zaupanja in zanesljiv, da ga je mogoče pooblastiti za dostop do tajnih podatkov EU.

4. Za namene postopka za pridobitev dovoljenja za dostop do tajnih podatkov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje se prek varnostne preiskave, ki jo izvedejo pristojni organi države članice v skladu z njenimi nacionalnimi zakoni in predpisi, ugotavlja, ali je posameznik lojalen, vreden zaupanja in zanesljiv.

5. Varnostni organ Komisije je edini odgovoren za stike z nacionalnimi varnostnimi organi (v nadaljnjem besedilu: NSA) ali drugimi pristojnimi nacionalnimi organi glede vseh vprašanj v zvezi s postopkom za pridobitev dovoljenja za dostop do tajnih podatkov. Vsi stiki med službami Komisije in njihovim osebjem ter NSA in drugimi pristojnimi organi morajo potekati prek varnostnega organa Komisije.

Člen 11

Postopek za pridobitev pooblastila za dostop do tajnih podatkov

1. Vsak generalni direktor ali vodja službe v okviru Komisije določi delovna mesta v svoji službi, na katerih zaposleni za opravljanje svojih nalog potrebujejo dostop do tajnih podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje in morajo zato biti varnostno preverjeni.

2. Takoj, ko je znano, da bo posameznik imenovan na delovno mesto, za katero je potreben dostop do tajnih podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, lokalni uradnik za varnost zadevne službe Komisije obvesti varnostni organ Komisije, ki posamezniku pošlje vprašalnik za dostop do tajnih podatkov, ki ga izda NSA države članice, katere državljan je posameznik, ki je imenovan za člana osebja evropskih institucij. Posameznik se s pisnim soglasjem strinja, da se zanj opravi postopek za pridobitev dovoljenja za dostop do tajnih podatkov, in izpolnjeni vprašalnik vrne varnostnemu organu Komisije v najkrajšem možnem roku.

3. Varnostni organ Komisije izpolnjeni vprašalnik za dostop do tajnih podatkov pošlje NSA države članice, katere državljan je posameznik, ki je imenovan za člana osebja evropskih institucij, z zahtevkom, da se izvede varnostna preiskava glede dostopa do tajnih podatkov EU tiste stopnje tajnosti, ki jih bo ta posameznik potreboval.

4. Če varnostni organ Komisije ve 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 pristojni nacionalni varnostni organ.

5. Po končani varnostni preiskavi in čim prej po tem, ko ga je zadevni NSA obvestil o svoji končni oceni ugotovitev v okviru varnostne preiskave, varnostni organ Komisije:

(a) lahko izda pooblastilo za dostop do tajnih podatkov EU za zadevnega posameznika in dovoli dostop do tajnih podatkov EU do ustrezne stopnje in do določenega datuma, ki ga določi, vendar za največ 5 let, če se z varnostno preiskavo zagotovi, da ni nobenih negativnih informacij, ki bi vzbudile dvome o lojalnosti, vrednosti zaupanja in zanesljivosti posameznika;

(b) če z varnostno preiskavo tega ni mogoče zagotoviti, v skladu z ustreznimi pravili in predpisi obvesti zadevnega posameznika, ki lahko zaprosi za zaslišanje pri varnostnem organu Komisije, ki lahko zaprosi pristojni NSA za vsa dodatna pojasnila, ki jih ta lahko priskrbi skladno z nacionalnimi zakoni in predpisi. Če se izid varnostne preiskave potrdi, se pooblastila za dostop do tajnih podatkov EU ne izda.

6. Za varnostno preiskavo skupaj s pridobljenimi rezultati veljajo ustrezni zakoni in predpisi, ki veljajo v zadevni državi članici, vključno s tistimi, ki urejajo pritožbe. Na odločitve varnostnega organa Komisije se je mogoče pritožiti v skladu s kadrovskimi predpisi.

7. Komisija sprejme pooblastilo za dostop do tajnih podatkov EU, ki ga je podelila katera koli druga institucija, organ ali agencija Unije, pod pogojem, da je še veljavno. Pooblastilo pokriva vse zadolžitve zadevnega posameznika v Komisiji. Institucija, organ ali agencija Unije, kjer se posameznik zaposli, bo uradno obvestila zadevni NSA o spremembi delodajalca.

8. Če posameznik ne nastopi službe v roku 12 mesecev po uradnem obvestilu varnostnemu organu Komisije o izidu varnostne preiskave ali če posameznik 12 mesecev ne opravlja službe, med tem časom pa ni zaposlen na delovnem mestu v Komisiji ali kateri koli drugi instituciji, organu ali agenciji Unije ali v državni upravi države članice, varnostni organ Komisije zadevo predloži zadevnemu NSA v potrditev, da je dovoljenje za dostop do tajnih podatkov EU še vedno veljavno in ustrezno.

9. Če varnostni organ Komisije izve za informacije o varnostnem tveganju, povezanem s posameznikom, ki ima veljavno pooblastilo za dostop do tajnih podatkov, o tem v skladu z ustreznimi pravili in predpisi obvesti pristojni nacionalni varnostni organ.

10. Če NSA obvesti varnostni organ Komisije o preklicu zagotovil, ki so bila v skladu z odstavkom 5(a) dana za posameznika, ki ima veljavno pooblastilo za dostop do tajnih podatkov EU, lahko varnostni organ Komisije zaprosi NSA za vsa pojasnila, ki jih slednji lahko zagotovi skladno z nacionalnimi zakoni in predpisi. Če zadevni NSA negativne informacije potrdi kot resnične, se posamezniku odvzame pooblastilo za dostop do tajnih podatkov in se mu onemogoči dostop do tajnih podatkov EU ter se ga umakne z delovnega mesta, na katerem je takšen dostop mogoč ali na katerem bi lahko ogrozil varnost.

11. Vsaka odločitev o odvzemu ali začasnem odvzemu pooblastila za dostop do tajnih podatkov EU kateremu koli posamezniku, ki spada v področje uporabe tega sklepa, in po potrebi razlogi zanjo se sporočijo zadevnemu posamezniku, ki lahko zaprosi za zaslišanje pri varnostnem organu Komisije. Za informacije, ki jih predloži NSA, veljajo ustrezni zakoni in predpisi, ki veljajo v zadevni državi članici. Na odločitve varnostnega organa Komisije v zvezi s tem se je mogoče pritožiti v skladu s kadrovskimi predpisi.

12. Službe Komisije zagotovijo, da nacionalni strokovnjaki, ki so dodeljeni na delovno mesto, za katero je potrebno pooblastilo za dostop do tajnih podatkov EU, pred prevzemom svojih zadolžitev varnostnemu organu Komisije predložijo veljavno dovoljenje za dostop do tajnih podatkov ali potrdilo za dostop do tajnih podatkov v skladu z nacionalno zakonodajo in predpisi, na podlagi katerega varnostni organ Komisije odobri pooblastilo za dostop do tajnih podatkov EU do stopnje, ki je enakovredna tisti iz nacionalnega dovoljenja za dostop do tajnih podatkov, z veljavnostjo največ za čas njihove napotitve.

Dostop do tajnih podatkov EU za posameznike, ki so zaradi svoje funkcije za to ustrezno pooblaščeni

13. Člani Komisije, ki imajo dostop do tajnih podatkov EU zaradi svoje funkcije na podlagi Pogodbe, se seznanijo s svojimi varnostnimi obveznostmi v zvezi z zaščito teh podatkov.

Evidence dovoljenj in pooblastil za dostop do tajnih podatkov

14. Evidence dovoljenj in pooblastil, podeljenih za dostop do tajnih podatkov EU, vodi varnostni organ Komisije v skladu s tem sklepom. Te evidence vsebujejo najmanj stopnjo tajnosti podatkov EU, do katerih ima lahko posameznik dostop, datum izdaje dovoljenja za dostop do tajnih podatkov in njegovo obdobje veljavnosti.

15. Varnostni organ Komisije lahko izda potrdilo za dostop do tajnih podatkov, iz katerega so razvidni stopnja tajnih podatkov EU, do katerih ima lahko posameznik dostop (CONFIDENTIEL UE/EU CONFIDENTIAL ali višje), datum veljavnosti zadevnega pooblastila za dostop do tajnih podatkov EU in datum izteka veljavnosti samega potrdila.

Podaljšanje pooblastil za dostop do tajnih podatkov

16. Po prvotni dodelitvi pooblastila za dostop do tajnih podatkov in pod pogojem, da je posameznik neprekinjeno delal na Evropski komisiji ali drugi instituciji, organu ali agenciji Unije in še vedno potrebuje dostop do tajnih podatkov EU, se pooblastilo za dostop do tajnih podatkov EU pregleda za podaljšanje praviloma vsakih pet let od datuma uradnega obvestila o rezultatih zadnje varnostne preiskave, na katerih temelji.

17. Varnostni organ Komisije lahko podaljša veljavnost trenutnega pooblastila za dostop do tajnih podatkov za največ 12 mesecev, če ni prejel nobene negativne informacije od ustreznega NSA ali drugega pristojnega nacionalnega organa v roku dveh mesecev od datuma predložitve zahteve za podaljšanje veljavnosti in ustreznega vprašalnika za dostop do tajnih podatkov. Če ob izteku teh 12 mesecev ustrezni NSA ali drug pristojni nacionalni organ varnostnemu organu Komisije ni podal svojega mnenja, se posamezniku dodelijo take naloge, za katere ne potrebuje pooblastila za dostop do tajnih podatkov.

Člen 12

Seznanjanje posameznikov za pridobitev pooblastila za dostop do tajnih podatkov

1. Po opravljeni fazi seznanja za pridobitev pooblastila za dostop do tajnih podatkov, ki ga organizira varnostni organ Komisije, vsi posamezniki, ki so dobili varnostno pooblastilo, pisno potrdijo, da so razumeli svoje obveznosti glede varovanja tajnih podatkov EU in da se zavedajo posledic, če pride do nepooblaščenega razkritja tajnih podatkov EU. Varnostni organ Komisije vodi evidenco takšnih pisnih potrditev.

2. Vse posameznike, ki imajo pooblastilo za dostop do tajnih podatkov EU ali se od njih zahteva obravnavanje teh podatkov, je treba na začetku opozoriti in jih nato redno seznanjati z ogrožanjem varnosti; varnostni organ Komisije so dolžni nemudoma obvestiti o vsakem poskusu približevanja ali ravnanju, ki se jim zdi sumljivo ali nenavadno.

3. 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.

Člen 13

Začasna pooblastila za dostop do tajnih podatkov

1. V izrednih okoliščinah, kadar je to ustrezno utemeljeno v interesu službe in do zaključka celovite varnostne preiskave, lahko varnostni organ Komisije po posvetovanju z NSA države članice, katere državljan je posameznik, in ob upoštevanju izida predhodnih pregledov, s katerimi se preveri, da ni nobenih negativnih informacij, posameznikom izda začasno pooblastilo za dostop do tajnih podatkov EU za določeno funkcijo, brez poseganja v določbe v zvezi s podaljšanjem dovoljenj za dostop do tajnih podatkov. Ta začasna pooblastila za dostop do tajnih podatkov EU veljajo največ šest mesecev in ne dovoljujejo dostopa do podatkov stopnje TRÈS SECRET UE/EU TOP SECRET.

2. Po tem, ko so bili seznanjeni v skladu s členom 12(1), 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. Varnostni organ Komisije vodi evidenco takšnih pisnih potrditev.

Člen 14

Udeležba na zaupnih sestankih, ki jih organizira Komisija

1. Službe Komisije, odgovorne za organizacijo sestankov, na katerih se razpravlja o podatkih stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, prek svojih lokalnih uradnikov za varnost ali organizatorjev sestankov, dovolj zgodaj obvestijo varnostni organ Komisije o datumih, času, krajih in udeležencih teh sestankov.

2. Ob upoštevanju določb člena 11(13) posamezniki, ki naj bi se udeležili sestankov, ki jih organizira Komisija in na katerih se razpravlja o podatkih stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, lahko na sestankih prisostvujejo šele po potrditvi statusa njihovega dovoljenja ali pooblastila za dostop do tajnih podatkov. Dostop do takih zaupnih sestankov se zavrne osebam, za katere varnostni organ Komisije ni prejel potrdila za dostop do tajnih podatkov ali drugega dokaza o imetju dovoljenja za dostop do tajnih podatkov, ali udeležencem, ki niso imetniki pooblastila za dostop do tajnih podatkov.

3. Odgovorni organizator zaupnega sestanka ali lokalni uradnik za varnost službe Komisije, ki sestanek organizira, pred pripravo zaupnega sestanka od zunanjih udeležencev zahteva, naj varnostnemu organu Komisije predložijo potrdilo za dostop do tajnih podatkov ali drug dokaz o imetju dovoljenja za dostop do tajnih podatkov. Varnostni organ Komisije obvesti lokalnega uradnika za varnost ali organizatorja sestanka o prejetih potrdilih za dostop do tajnih podatkov ali drugih dokazih o varnostnem dovoljenju. Po potrebi se lahko uporabi zbirni seznam imen z ustreznimi dokazi o imetju dovoljenja za dostop do tajnih podatkov.

4. Če pristojni organi obvestijo varnostni organ Komisije, da je bilo dovoljenje za dostop do tajnih podatkov odvzeto posamezniku, čigar naloge zahtevajo udeležbo na sestankih, ki jih organizira Komisija, varnostni organ Komisije o tem obvesti lokalnega uradnika za varnost službe Komisije, ki je pristojna za organizacijo sestanka.

Člen 15

Morebiten dostop do tajnih podatkov EU

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

POGLAVJE 3

FIZIČNA VARNOST ZA ZAŠČITO TAJNIH PODATKOV

Člen 16

Osnovna načela

1. Namen ukrepov za zagotavljanje 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 vedenju. Takšni ukrepi se določijo na osnovi postopka obvladovanja tveganja, v skladu s tem sklepom in njegovimi izvedbenimi pravili.

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

(a) z zagotovitvijo, 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 vedenju in, kjer je to ustrezno, glede na njihovo pooblastilo za dostop do tajnih podatkov;

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

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

3. Ukrepi fizične varnosti se uvedejo v vseh prostorih, stavbah, pisarnah, sobah in drugih območjih, v katerih se obravnavajo tajni podatki EU ali v katerih se tajne podatke EU hrani, vključno z območji, kjer so nameščeni komunikacijski in informacijski sistemi, kakor je navedeno v poglavju 5.

4. Območja, na katerih se hranijo tajni podatki EU stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, so določena kot varovana območja v skladu s tem poglavjem, odobri pa jih Organ Komisije za varnostno akreditacijo.

5. Za varovanje tajnih podatkov EU stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje se uporablja le oprema ali naprave, ki jih odobri varnostni organ Komisije.

Člen 17

Zahteve in ukrepi glede fizične varnosti

1. Ukrepi fizične varnosti se izberejo na podlagi ocene grožnje, ki jo opravi varnostni organ Komisije, po potrebi ob posvetovanju z drugimi službami Komisije, drugimi institucijami, agencijami ali organi Evropske unije in/ali pristojnimi organi v državah članicah. Komisija 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; ter

(d) ocena grožnje, ki jo za Unijo, njene institucije, organe ali agencije ali države članice pomenijo obveščevalne službe, ter nevarnosti zaradi sabotaže, terorizma, uničevalnih ali drugih kriminalnih dejavnosti.

2. Varnostni organ Komisije na podlagi koncepta globinske obrambe določi ustrezno kombinacijo ukrepov fizične varnosti, ki naj bi se izvedli. V ta namen varnostni organ Komisije razvije minimalne standarde, norme in merila, določene v izvedbenih pravilih.

3. Varnostni organ Komisije je pooblaščen za preglede na vhodih in izhodih, kar naj bi odvračalo od nedovoljenega vnosa gradiva v prostore ali zgradbe ali od nedovoljene odstranitve tajnih podatkov EU iz njih.

4. Če obstaja tveganje, da se tajni podatki EU spregledajo, tudi po naključju, zadevne službe Komisije sprejmejo ustrezne ukrepe, ki jih je za preprečitev tega tveganja določil varnostni organ Komisije.

5. Za nove objekte se zahteve glede fizične varnosti in njihove funkcijske specifikacije določijo s soglasjem varnostnega organa Komisije v sklopu načrtovanja in zasnove objektov. Pri obstoječih objektih se zahteve glede fizične varnosti izvajajo v skladu z minimalnimi standardi, normami in merili, določenimi v izvedbenih pravilih.

Člen 18

Oprema za fizično varovanje tajnih podatkov EU

1. Za fizično varovanje tajnih podatkov EU se vzpostavi dvoje vrst fizično varovanih območij:

(a) upravna območja; in

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

2. Organ Komisije za varnostno akreditacijo ugotovi, da območje izpolnjuje zahteve in ga je zato mogoče določiti za upravno območje, varnostno območje ali tehnično varovano območje.

3. 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 varnostni organ Komisije ali kateri koli drugi pristojni organ za to ustrezno pooblastil, in

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

4. Na varnostnih območjih:

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

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

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

5. Če vstop na varnostno 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.

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

(a) ta območja so opremljena s sistemom odkrivanja vsiljivcev („IDS“) in, kadar v prostorih ni nikogar, zaklenjena, sicer pa varovana. Z vsemi ključi se ravna skladno s členom 20;

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

(c) Varnostni organ Komisije ta območja redno fizično in/ali tehnično inšpekcijsko pregleduje. Ti inšpekcijski pregledi se lahko izvajajo tudi po vsakem nepooblaščenem vstopu ali sumu takšnega vstopa; in

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

7. Ne glede na točko (d) odstavka 6 varnostni organ Komisije pred uporabo komunikacijskih naprav ter električne ali elektronske opreme na območjih, kjer potekajo sestanki ali se opravlja delo s podatki stopnje tajnosti SECRET UE/EU SECRET in višje, ter je ocena grožnje za tajne podatke EU velika, te naprave in opremo najprej preveri, zato da zagotovi, da te naprave ne morejo nehoteno ali nezakonito pošiljati uporabnih podatkov zunaj varnostnega perimetra varovanega območja.

8. Varnostna 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 ni nameščen sistem za odkrivanje vsiljivcev.

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

10. Lokalni uradnik za varnost zadevne službe Komisije pripravi Varnostni postopek delovanja (SecOPs) za vsako varnostno območje pod njegovo odgovornostjo, v katerem so v skladu z določbami tega sklepa in njegovimi izvedbenimi pravili določeni:

(a) stopnja tajnih podatkov EU, ki se jih lahko obravnava in se lahko hranijo v tem območju;

(b) nadzorni in varnostni ukrepi, ki jih je treba izvajati;

(c) posamezniki, ki so zaradi svoje potrebe po vedenju in pooblastila za dostop do tajnih podatkov pooblaščeni za dostop na območje brez spremstva;

(d) kjer je to ustrezno, postopki v zvezi s spremljanjem ali postopki za varovanje tajnih podatkov EU, ko je drugim posameznikom dovoljen dostop na območje;

(e) vsi drugi ustrezni ukrepi in postopki.

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

Člen 19

Fizični zaščitni ukrepi za obravnavanje tajnih podatkov EU in njihovo hrambo

1. Tajni podatki stopnje RESTREINT UE/EU RESTRICTED se lahko obravnavajo:

(a) v varnostnem območju;

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

(c) zunaj varnostnega ali upravnega območja, če imetnik podatkov prenaša tajne podatke EU v skladu s členom 31 in se je zavezal, da bo ravnal v skladu z izravnalnimi ukrepi iz izvedbenih ukrepov, s čimer se zagotovi, da so tajni podatki EU zaščiteni pred dostopom nepooblaščenih oseb.

2. Tajni podatki EU stopnje RESTREINT UE/EU RESTRICTED se hranijo v ustrezno zaklenjenih pisarniških omarah v upravnem območju ali v varnostnem območju. Začasno se lahko hranijo zunaj upravnega ali varnostnega območja, če se je imetnik podatkov zavezal, da bo ravnal v skladu z izravnalnimi ukrepi iz izvedbenih pravil.

3. Tajni podatki stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET se lahko obravnavajo:

(a) v varnostnem območju;

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

(c) zunaj varnostnega ali upravnega območja, če::

(i) se je imetnik podatkov zavezal, da bo ravnal v skladu z izravnalnimi ukrepi iz izvedbenih pravil, s čimer se zagotovi, da so tajni podatki EU zaščiteni pred dostopom nepooblaščenih oseb;

(ii) ima imetnik podatkov tajne podatke EU ves čas pod osebnim nadzorom; in

(iii) imetnik podatkov v primeru dokumentov na papirju o tem obvesti pristojni register.

4. Tajni podatki EU stopnje UE/EU CONFIDENTIAL in SECRET UE/EU SECRET se hranijo v varnostnem območju v blagajni ali sobi trezorju.

5. Tajni podatki stopnje TRES SECRET UE/EU TOP SECRET se obravnavajo v varnostnem območju, ki ga je vzpostavil in ga vzdržuje varnostni organ Komisije, Organ Komisije za varnostno akreditacijo pa ga je do te stopnje akreditiral.

6. Tajni podatki EU stopnje TRÈS SECRET UE/EU TOP SECRET se hranijo v varnostnem območju, ki ga je do te stopnje akreditiral Organ Komisije za varnostno akreditacijo, in sicer pod enim od naslednjih pogojev:

(a) v blagajni v skladu z določbami člena 18 z eno ali več vrstami dodatnega nadzora:

1. neprekinjeno varovanje ali preverjanje, ki ga izvaja varnostno osebje ali dežurno osebje, ki je bilo ustrezno varnostno preverjeno;

2. 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.

Člen 20

Nadzor nad ključi in kombinacijami, ki se uporabljajo za varovanje tajnih podatkov EU

1. Postopki za ravnanje s ključi in nastavitvami kombinacij za pisarne, sobe, sobe- trezorje in blagajne se določijo v izvedbenih pravilih v skladu s členom 60 spodaj. Namen takšnih postopkov je varovanje pred nepooblaščenim dostopom.

2. 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; in

(e) najmanj vsakih 12 mesecev.

POGLAVJE 4

UPRAVLJANJE TAJNIH PODATKOV EU

Člen 21

Osnovna načela

1. Z vsemi dokumenti s tajnimi podatki EU je treba upravljati v skladu s politiko Komisije o upravljanju dokumentov in zato jih je treba vpisati, ustrezno uvrstiti, hraniti in nazadnje odstraniti, vzorčiti ali prenesti v zgodovinski arhiv v skladu s skupnim seznamom hrambe na ravni Komisije za datoteke Evropske komisije.

2. Podatki stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali višje se iz varnostnih razlogov vpišejo pred razpošiljanjem in ob prejemu. Podatki stopnje TRÈS SECRET UE/EU TOP SECRET se vpišejo v za to namenjenih registrih.

3. Znotraj Komisije se vzpostavi registrski sistem tajnih podatkov EU v skladu z določbami člena 27.

4. Varnostni organ Komisije redno pregleduje službe Komisije in prostore, v katerih se obravnavajo ali hranijo tajni podatki EU.

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

(a) praviloma z elektronskimi sredstvi, ki so zaščiteni s šifrirnimi izdelki, odobrenimi v skladu s poglavjem 5;

(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 poglavjem 5; ali

(ii) v vseh drugih primerih, kakor je določeno v izvedbenih pravilih.

Člen 22

Stopnje tajnosti in oznake

1. Podatkom se stopnja tajnosti določi takrat, kadar jih je treba varovati zaradi njihove tajnosti v skladu s členom 3(1).

2. Tvorec tajnih podatkov EU je v skladu z ustreznimi izvedbenimi pravili, standardi in smernicami za razvrstitev pristojen za določanje stopnje tajnosti in za začetno širjenje podatkov.

3. Stopnja tajnosti podatkov EU se določi v skladu s členom 3(2) in ustreznimi izvedbenimi pravili.

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

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

6. 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.

7. 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.

8. Stopnja tajnosti pisma ali dopisa, ki vsebuje priloge, je enaka najvišji stopnji tajnosti prilog. Tvorec 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

Člen 23

Oznake

Tajni podatki EU lahko poleg varnostnih oznak stopnje tajnosti iz člena 3(2) nosijo dodatne oznake, kot na primer:

(a) označba, ki določa tvorca;

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

(c) oznake pogojev za dajanje tajnih podatkov;

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

Člen 24

Okrajšane oznake stopnje tajnosti

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

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

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

Člen 25

Ustvarjanje tajnih podatkov EU

1. Pri ustvarjanju tajnega dokumenta EU:

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

(b) se vsaka stran oštevilči;

(c) dokument nosi registrsko 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 tajnosti SECRET UE/EU SECRET ali višje je treba na vsaki strani navesti številko kopije, če se razpošiljajo v več izvodih.

2. Če za tajne podatke EU ni mogoče uporabljati odstavka 1, se sprejmejo drugi ustrezni ukrepi v skladu z izvedbenimi pravili.

Člen 26

Znižanje stopnje tajnosti in njen preklic za tajne podatke EU

1. Tvorec ob ustvarjanju tajnih podatkov EU po možnosti navede, ali se stopnja tajnosti podatkov EU lahko zniža ali prekliče na določen datum ali po določenem dogodku.

2. Vsaka služba Komisije redno pregleduje tajne podatke EU, katerih tvorec je, da bi ugotovila, ali je stopnja tajnosti še ustrezna. Sistem pregledovanja stopnje tajnosti vpisanih tajnih podatkov EU, ki so nastali v Komisiji, najmanj vsakih pet let, se določi z izvedbenimi pravili. Takšen pregled ni potreben, če je tvorec že na začetku navedel, da bo stopnja tajnosti podatkov samodejno znižana ali da bodo preklicane stopnje tajnosti, in če je podatek temu ustrezno označen.

3. Za tajne podatke stopnje RESTREINT UE/EU RESTRICTED, ki izvirajo iz Komisije, šteje, da bo njihova stopnja tajnosti samodejno odpravljena po tridesetih letih, v skladu z Uredbo (EGS, Euratom) št. 354/83, kakor je bila spremenjena z Uredbo Sveta (ES, Euratom) št. 1700/2003 ([1]).

Člen 27

Registrski sistem tajnih podatkov EU v Komisiji

1. Brez poseganja v člen 52(5) spodaj se v vsaki službi Komisije, v kateri se obravnavajo ali hranijo tajni podatki EU na stopnji CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET, določi odgovorni lokalni register tajnih podatkov EU, ki zagotovi, da se tajni podatki EU obravnavajo v skladu s tem sklepom.

2. Register tajnih podatkov EU, ki ga upravlja generalni sekretariat Komisije, je centralni register tajnih podatkov EU v Komisiji. Deluje kot:

— lokalni register tajnih podatkov EU za generalni sekretariat Komisije;

— register tajnih podatkov EU za zasebne kabinete članov Komisije, razen če ti že imajo določen lokalni register tajnih podatkov EU;

— register tajnih podatkov EU za generalne direktorate ali službe, ki nimajo lokalnega registra tajnih podatkov EU;

— glavna vstopna in izstopna točka za vse tajne podatke stopnje RESTREINT UE/EU RESTRICTED in do vključno stopnje SECRET UE/EU SECRET, ki so bili izmenjani med Komisijo in njenimi službami ter tretjimi državami in mednarodnimi organizacijami, ter, če je tako določeno v posebnih dogovorih, glavna vstopna in izstopna točka za druge institucije, agencije in organe Unije.

3. Varnostni organ Komisije znotraj Komisije določi register, ki deluje kot centralni organ za prejemanje in razpošiljanje podatkov stopnje TRÈS SECRET UE/EU TOP SECRET. Po potrebi se lahko določijo podregistri, v katerih se obravnavajo takšni podatki za potrebe vpisovanja.

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

5. Registri tajnih podatki EU se določijo kot varnostna območja, kakor so opredeljena v poglavju 3, akreditira pa jih Organ Komisije za varnostno akreditacijo.

Člen 28

Nadzorni uradnik registra

1. Vsak register tajnih podatkov EU upravlja nadzorni uradnik registra.

2. Nadzorni uradnik registra je ustrezno varnostno preverjen.

3. Pri uporabi določb v zvezi z obravnavanjem dokumentom, ki vsebujejo tajne podatke EU, in skladnostjo z zadevnimi varnostnimi predpisi, standardi in smernicami nadzornega uradnika registra nadzoruje lokalni uradnik za varnost znotraj službe Komisije.

4. Nadzorni uradnik registra v okviru svoje odgovornosti za upravljanje registra tajnih podatkov EU, ki mu je bila zaupana, prevzame naslednje splošne naloge v skladu s tem sklepom in zadevnimi izvedbenimi pravili, standardi in smernicami:

— vodenje postopkov v zvezi z vpisom, ohranjanjem, razmnoževanjem, prevajanjem, razpošiljanjem, odpremljanjem in uničevanjem ali prenosom v zgodovinski arhiv tajnih podatkov EU;

— redno preverjanje potrebe po ohranjanju stopenj tajnosti podatkov;

— vse druge naloge v zvezi z varovanjem tajnih podatkov EU, opredeljene v izvedbenih pravilih.

Člen 29

Vpis tajnih podatkov EU iz varnostnih razlogov

1. Za namene tega sklepa vpis iz varnostnih razlogov (v nadaljnjem besedilu: „vpis“) pomeni uporabo postopkov, ki zapišejo življenjski cikel tajnih podatkov EU, vključno z njihovim razširjanjem.

([1]) Uredba Sveta (ES, Euratom) št. 1700/2003 z dne 22. septembra 2003 o spremembah Uredbe (EGS, Euratom) št. 354/83 v zvezi z odprtjem zgodovinskih arhivov Evropske gospodarske skupnosti in Evropske skupnosti za atomsko energijo za javnost (UL L 243, 27.9.2003, str. 1).

2. Vsi podatki oziroma vse gradivo stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL in višje se ob prejetju v organizacijski subjekt ali pri odpošiljanju iz njega vpišejo v za to namenjene registre.

3. Če se tajni podatki EU obravnavajo ali hranijo z uporabo komunikacijskega in informacijskega sistema, se vpisni postopki lahko opravijo v okviru procesov znotraj samega komunikacijskega in informacijskega sistema.

4. Podrobnejše določbe, ki se nanašajo na vpis tajnih podatkov EU iz varnostnih razlogov, se določijo v izvedbenih pravilih.

Člen 30

Kopiranje in prevajanje tajnih dokumentov EU

1. Dokumenti stopnje TRÈS SECRET UE/EU TOP SECRET se lahko kopirajo ali prevajajo le s predhodnim pisnim soglasjem tvorca.

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

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

Člen 31

Prenašanje tajnih podatkov EU

1. Tajni podatki EU se prenašajo na takšen način, da se jih med njihovim prenosom zavaruje pred nepooblaščenim razkritjem.

2. Za prenašanje tajnih podatkov EU veljajo varnostni ukrepi, ki

— so sorazmerni s stopnjo tajnosti tajnih podatkov EU, ki se prenašajo; in

— so prilagojeni posebnim pogojem njihovega prenosa, zlasti glede na to, ali se tajni podatki EU prenašajo:

  — znotraj zgradbe Komisije ali samostojne skupine zgradb Komisije;

  — med zgradbami Komisije v isti državi članici;

  — znotraj Unije;

  — iz Unije na ozemlje tretje države; ter

  — so prilagojeni naravi in obliki tajnih podatkov EU.

3. Ti varnostni ukrepi so podrobneje določeni v izvedbenih pravilih, v primeru projektov in programov iz člena 42 pa so sestavni del zadevnih varnostnih navodil za program ali projekt.

4. Izvedbena pravila ali varnostna navodila za program ali projekt vključujejo določbe, ki so sorazmerne s stopnjo tajnih podatkov EU v zvezi z:

— vrsto prenosa, kot je ročni prenos, prenos po diplomatski ali vojaški kurirski službi, prenos prek poštnih služb ali komercialnih kurirskih služb;

— pakiranjem tajnih podatkov EU;

— tehničnimi protiukrepi za tajne podatke EU, prenesene prek elektronskih medijev;

— vsemi drugimi postopkovnimi, fizičnimi ali elektronskimi ukrepi;

— postopki vpisa;

— uporabo varnostno pooblaščenega osebja.

5. Pri prenašanju tajnih podatkov EU prek elektronskih medijev se varnostni ukrepi, navedeni v zadevnih izvedbenih pravilih, ne glede na člen 21(5) lahko dopolnijo z ustreznimi tehničnimi protiukrepi, ki jih odobri varnostni organ Komisije, tako da se čim bolj zmanjša nevarnost izgube ali nepooblaščenega razkritja.

Člen 32

Uničenje tajnih podatkov EU

1. Tajni dokumenti EU, ki niso več potrebni, se lahko uničijo, pri čemer je treba upoštevati predpise o arhivih ter pravila in predpise Komisije o upravljanju dokumentov in arhiviranju, ter zlasti skupni seznam hrambe na ravni Komisije.

2. Tajne podatke EU stopnje CONFIDENTIEL UE/EU CONFIDENTIAL in višje uniči nadzorni uradnik registra, odgovoren za register tajnih podatkov EU, in sicer po navodilu imetnika tajnih podatkov ali pristojnega organa. Nadzorni uradnik registra ustrezno posodobi vpisnike in druge podatke o vpisu.

3. Dokumente stopnje SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET uniči nadzorni uradnik registra v prisotnosti priče, ki je varnostno preverjena vsaj do stopnje tajnosti dokumenta, ki se uničuje.

4. Uradnik registra in priča, če je njena navzočnost obvezna, podpišeta potrdilo o uničenju, ki se shrani v registru. Nadzorni uradnik registra, odgovoren za register tajnih podatkov EU, potrdila o uničenju dokumentov stopnje TRÈS SECRET UE/EU TOP SECRET hrani vsaj deset let, potrdila o uničenju dokumentov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET pa vsaj pet let.

5. Tajni dokumenti, vključno z dokumenti stopnje tajnosti RESTREINT UE/EU RESTRICTED, se uničijo po metodah, ki se določijo v izvedbenih pravilih in ki so skladne z ustreznimi standardi EU ali enakovrednimi standardi.

6. Računalniški shranjevalni nosilci, ki se uporabljajo za tajne podatke EU, se uničijo v skladu s postopki, določenimi v izvedbenih pravilih.

Člen 33

Uničenje tajnih podatkov EU v izrednih razmerah

1. Službe Komisije, ki imajo v lasti tajni podatke EU, ob upoštevanju lokalnih pogojev pripravijo načrte za varovanje tajnih podatkov EU v kriznih razmerah, vključno, če je to potrebno, z načrti za uničenje in evakuacijo v nujnih primerih. Razdelijo potrebna navodila za preprečevanje prehajanja tajnih podatkov EU v roke nepooblaščenim osebam.

2. Režim varovanja in/ali uničenja gradiva CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET UE/EU SECRET v kriznih razmerah ne sme biti v ničemer na škodo varovanju ali uničenju gradiva TRES SECRET UE/EU TOP SECRET, vključno z (de)šifrirno opremo, katere obravnava ima prednost pred vsemi drugimi nalogami.

3. V primeru izrednih razmer, če obstaja neposredno tveganje za nepooblaščeno razkritje, tajne podatke EU imetnik uniči, tako da jih ni mogoče v celoti ali delno ponovno sestaviti. Tvorec in izvorni register se obvestita o nujnem uničenju vpisanih tajnih podatkov EU.

4. Podrobnejše določbe za uničenje tajnih podatkov EU se določijo v izvedbenih pravilih.

POGLAVJE 5

VAROVANJE TAJNIH PODATKOV EU V KOMUNIKACIJSKIH IN INFORMACIJSKIH SISTEMIH (KIS)

Člen 34

Osnovna načela informacijske varnosti

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.

2. Učinkovita informacijska varnost zagotavlja ustrezno stopnjo:

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

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

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

celovitosti: zagotavljanje točnosti in popolnosti sestavnih delov in podatkov;

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

3. Zagotavljanje informacijske varnosti temelji na postopku obvladovanja tveganja.

Člen 35

Opredelitev pojmov

V tem poglavju se uporabljajo naslednje opredelitve pojmov:

(a) „akreditacija“ pomeni uradno dovoljenje in odobritev komunikacijskega in informacijskega sistema s strani Organa Komisije za varnostno akreditacijo za obdelavo tajnih podatkov EU v njegovem operativnem okolju, po uradni potrditvi varnostnega načrta in njegovega pravilnega izvajanja;

(b) „akreditacijski postopek“ pomeni vse potrebne ukrepe in naloge, ki so potrebne, preden Organ Komisije za varnostno akreditacijo dodeli akreditacijo. Ti ukrepi in naloge se natančno opredelijo v standardu za akreditacijski postopek;

(c) „komunikacijski in informacijski sistem“ (KIS) pomeni sistem, ki omogoča obravnavanje podatkov v elektronski obliki. Komunikacijski in informacijski sistem zajema vse sestavne dele, potrebne za njegovo delovanje, tudi infrastrukturo, organizacijo, osebje in informacijske vire;

(d) „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;

(e) „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 groženj in njihovega učinka;

(f) „sprejemanje tveganja“ je odločitev, da se sprejme prisotnost preostalega tveganja, potem ko se je poskušalo tveganje obvladati;

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

(h) „obveščanje o tveganju“ zajema ozaveščanje skupnosti uporabnikov KIS o tveganjih, obveščanje organov za odobritev o tveganjih in poročanje o tveganjih operativnim organom;

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

Člen 36

Komunikacijski in informacijski sistemi (KIS) za obravnavanje tajnih podatkov EU

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

2. Kar zadeva komunikacijske in informacijske sisteme za obravnavanje tajnih podatkov EU, njihova skladnost z varnostno politiko Komisije glede informacijskih sistemov, kot je navedeno v Sklepu Komisije C(2006)3602 ([1]), pomeni, da:

(a) se za izvajanje varnostne politike glede informacijskih sistemov skozi celotni življenjski cikel informacijskega sistema uporablja cikel PDCA (Plan-Do-Check-Act);

(b) je varnostne potrebe treba opredeliti v okviru ocene učinka na poslovanje;

(c) je za informacijski sistem in podatke v njem potrebna formalna razvrstitev sestavnih delov;

([1]) C(2006) 3602 z dne 16. avgusta 2006 o varnosti informacijskih sistemov, ki jih uporablja Evropska komisija.

(d) je treba izvesti vse obvezne varnostne ukrepe, kot jih določi politika za varnost informacijskih sistemov;

(e) se mora uporabljati postopek obvladovanja tveganja, ki vključuje naslednje stopnje: prepoznavanje groženj in ranljivosti, oceno tveganja, poskus obvladanja tveganja, prevzemanje tveganja in obveščanje o tveganju;

(f) se opredeli, izvaja, preveri in revidira varnostni načrt, vključno z varnostno politiko in varnostno-operativnimi postopki.

3. Vsi zaposleni, ki so vključeni v oblikovanje, razvoj, preskušanje, obratovanje, upravljanje ali uporabo komunikacijskih in informacijskih sistemov za obravnavanje tajnih podatkov EU, Organ Komisije za varnostno akreditacijo obvestijo o vseh morebitnih varnostnih pomanjkljivostih, incidentih in kršitvah v zvezi z varnostjo ali nepooblaščenim razkritjem, ki bi lahko vplivali na varovanje komunikacijskih in informacijskih sistemov in/ali tajnih podatkov EU v njih.

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

(a) prednost se da izdelkom, ki jih je odobril Svet ali generalni sekretar Sveta v svoji funkciji kot organ Sveta za odobritev šifrirnih metod in izdelkov po priporočilu strokovne skupine Komisije za varnost;

(b) če obstajajo posebni operativni razlogi, lahko organ Komisije za odobritev šifrirnih metod in izdelkov po priporočilu strokovne skupine Komisije za varnost opusti zahteve iz točke a) in izda odobritev za določeno obdobje.

5. Med razpošiljanjem, predelavo in hrambo 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 uporabijo posebni postopki, če jih je odobril organ Komisije za odobritev šifrirnih metod in izdelkov.

6. Izvajajo se varnostni ukrepi za zaščito komunikacijskih in informacijskih sistemov, v okviru katerih se obravnavajo podatki stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, tako da taki podatki ne morejo biti nepooblaščeno razkriti zaradi nenamernega elektromagnetnega oddajanja (v nadaljnjem besedilu: varnostni ukrepi TEMPEST). Takšni varnostni ukrepi so sorazmerni s tveganjem zlorabe in stopnje tajnosti podatkov.

7. Varnostni organ Komisije prevzame naslednje funkcije:

— organ za zagotavljanje informacijske varnosti;

— organ za varnostno akreditacijo;

— organ TEMPEST;

— organ za odobritev šifrirnih metod in izdelkov;

— organ za razpošiljanje šifrirnega materiala.

8. Varnostni organ Komisije za vsak sistem imenuje operativni organ za zagotavljanje informacijske varnosti.

9. Odgovornosti funkcij, opisanih v odstavkih 7 in 8, bodo opredeljene v izvedbenih pravilih.

Člen 37

Akreditacija komunikacijskih in informacijskih sistemov (KIS) za obravnavanje tajnih podatkov EU

1. Za vse KIS, v katerih se obravnavajo tajni podatki EU, se opravi akreditacijski postopek, ki temelji na načelih informacijske varnosti in katerega stopnja podrobnosti mora biti sorazmerna z zahtevano ravnjo varovanja.

2. Postopek akreditacije vključuje uradno potrditev varnostnega načrta v okviru komunikacijskega in informacijskega sistema s strani organa Komisije za varnostno akreditacijo, da se zagotovi, da:

(a) je bil postopek upravljanja s tveganji, kot je naveden v členu 36(2), ustrezno izveden;

(b) je lastnik sistema zavestno sprejel preostalo tveganje ter

(c) je bila dosežena zadostna stopnja zaščite KIS in varovanja tajnih podatkov EU, ki se v njih obravnavajo, v skladu s tem sklepom.

3. Organ Komisije za varnostno akreditacijo izda izjavo o akreditaciji, s katero določi najvišjo stopnjo tajnosti podatkov EU, ki se lahko obravnavajo v KIS, in ustrezne pogoje za delo. To ne posega v naloge, ki so dodeljene svetu za varnostno akreditacijo in opredeljene v členu 11 Uredbe (EU) št. 512/2014 Evropskega parlamenta in Sveta ([1]).

4. Skupni svet za varnostno akreditacijo je odgovoren za akreditacijo komunikacijskih in informacijskih sistemov Komisije, ki vključujejo več udeleženih strani. Sestavljajo ga po en predstavnik organa za varnostno akreditacijo iz vsake udeležene strani, predseduje pa mu predstavnik organa za varnostno akreditacijo Komisije.

5. Postopek akreditacije zajema številne naloge, ki jih prevzamejo udeležene strani. Odgovornost za pripravo akreditacijskih datotek in dokumentacije ostane v domeni lastnika sistema KIS.

6. Za akreditacijo je odgovoren organ Komisije za varnostno akreditacijo, ki ima v katerem koli trenutku v življenjskem ciklu KIS pravico:

(a) zahtevati, da se uporabi postopek akreditacije;

(b) opraviti revizijo ali pregled v komunikacijskih in informacijskih sistemih;

(c) kadar pogoji za uporabo niso več izpolnjeni, zahtevati opredelitev in učinkovito izvajanje načrta za izboljšanje varnosti v točno določenem časovnem okviru, pri čemer lahko odvzame dovoljenje za uporabo KIS, dokler pogoji za uporabo niso ponovno izpolnjeni.

7. Postopek akreditacije se določi v standardu za postopek akreditacije za komunikacijske in informacijske sisteme, v katerih se obravnavajo tajni podatki EU, ki se sprejme v skladu s členom 10(3) Sklepa C(2006) 3602.

Člen 38

Izredne razmere

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

2. 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 ter

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

3. Tajni podatki, poslani pod pogoji iz odstavka 1, 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.

4. Pristojnemu organu in strokovni skupini Komisije za varnost se nato pošlje poročilo.

POGLAVJE 6

INDUSTRIJSKA VARNOST

Člen 39

Osnovna načela

1. Industrijska varnost je uporaba ukrepov, s katerimi se zagotovi varovanje tajnih podatkov EU

(a) v okviru pogodb s tajnimi podatki in ki jih izvajajo:

(i) kandidati ali ponudniki med postopkom zbiranja ponudb in sklepanja pogodb;

(ii) izvajalci ali podizvajalci v celotnem življenjskem ciklu pogodb s tajnimi podatki;

([1]) Uredba (EU) št. 512/2014 Evropskega parlamenta in Sveta z dne 16. aprila 2014 o spremembi Uredbe (EU) št. 912/2010 o ustanovitvi Agencije za evropski GNSS (UL L 150, 20.5.2014, str. 72).

(b) v okviru tajnih sporazumov o donacijah in ki jih izvajajo:

(i) prosilci v postopkih za dodelitev donacij;

(ii) upravičenci v celotnem življenjskem ciklu tajnih sporazumov o donacijah.

2. Te pogodbe ali sporazumi o donacijah ne vključujejo podatkov stopnje TRÈS SECRET UE/EU TOP SECRET.

3. Če ni določeno drugače, se določbe iz tega poglavja, ki se nanašajo na pogodbe s tajnimi podatki ali izvajalce, uporabljajo tudi za podizvajalske pogodbe s tajnimi podatki ali podizvajalce.

Člen 40

Opredelitev pojmov

V tem poglavju se uporabljajo naslednje opredelitve pojmov:

(a) „pogodba s tajnimi podatki“ pomeni okvirno pogodbo ali pogodbo, kot je navedeno v Uredbi Sveta (ES, Euratom) št. 1605/2002 ([1]), ki jo je sklenila Komisija ali ena od njenih služb z izvajalcem za dobavo premičnin ali nepremičnin, izvedbo del ali opravljanje storitev, katere izpolnitev zahteva ali vključuje ustvarjanje tajnih podatkov EU, njihovo obravnavo ali hrambo;

(b) „podizvajalska pogodba s tajnimi podatki“ pomeni pogodbo, ki jo izvajalec Komisije ali ene od njenih služb sklene z drugim izvajalcem (tj. podizvajalcem) za dobavo premičnin ali nepremičnin, izvedbo del ali opravljanje storitev, katere izpolnitev zahteva ali vključuje ustvarjanje tajnih podatkov EU, njihovo obravnavo ali hrambo;

(c) „tajni sporazum o donacijah“ pomeni sporazum, v skladu s katerim Komisija dodeli donacije iz naslova VI dela I Uredbe (ES, Euratom) št. 1605/2002, katerega izpolnitev zahteva ali vključuje ustvarjanje tajnih podatkov EU, njihovo obravnavo ali hrambo;

(d) „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.

Člen 41

Postopek za pogodbe s tajnimi podatki ali tajne sporazume o donacijah

1. Vsaka služba Komisije kot javni organ naročnik zagotovi, da so v pogodbi navedeni ali vključeni minimalni standardi industrijske varnosti iz tega poglavja ter da so ti standardi izpolnjeni pri dodeljevanju pogodb s tajnimi podatki ali sklepanju tajnih sporazumov o donacijah.

2. Za namene odstavka 1 pristojne službe Komisije Generalni direktorat za človeške vire in varnost, ter zlasti njegov direktorat za varnost, zaprosijo za nasvet in zagotovijo, da vzorci pogodb in podizvajalskih pogodb ter vzorci sporazumov o donacijah vsebujejo določbe, ki odražajo osnovna načela in minimalne standarde za varovanje tajnih podatkov EU, ki jih morajo izpolnjevati izvajalci in podizvajalci ter upravičenci po sporazumih o donacijah.

3. Komisija tesno sodeluje z nacionalnim varnostnim organom, imenovanim varnostnim organom ali katerim koli drugim pristojnim organom zadevne države članice.

4. Kadar javni organ naročnik namerava začeti postopek za sklenitev pogodbe s tajnimi podatki ali sporazuma o donacijah, zaprosi za mnenje varnostnega organa Komisije o vprašanjih v zvezi s tajnostjo in elementi postopka v vseh fazah.

5. Vzorci in modeli pogodb s tajnimi podatki in podizvajalskih pogodb, sporazumov o donacijah, obvestil o sklenitvi pogodb, smernic o okoliščinah, v katerih se zahteva varnostno dovoljenje organizacij, varnostnih navodil za program ali projekt, listin o varnostnih vidikih, obiskih ter razpošiljanju in prenašanju tajnih podatkov EU na podlagi pogodb s tajnimi podatki ali sporazumov o donacijah se po posvetovanju s strokovno skupino Komisije za varnost določijo v izvedbenih pravilih o industrijski varnosti.

([1]) Uredba Sveta (ES, Euratom) št. 1605/2002 z dne 25. junija 2002 o finančni uredbi, ki se uporablja za splošni proračun Evropskih skupnosti (UL L 248, 16.9.2002, str. 1).

6. Komisija lahko sklepa pogodbe s tajnimi podatki ali sporazume o donacijah, ki nalagajo naloge, ki vključujejo dostop do tajnih podatkov EU ali njihovo obravnavo ali hrambo in ki jih izvedejo gospodarski subjekti, registrirani v državi članici ali tretji državi, s katero je sklenila sporazum ali upravni dogovor v skladu s poglavjem 7 tega sklepa.

Člen 42

Varnostni elementi pogodb s tajnimi podatki ali sporazumov o donacijah

1. Pogodbe s tajnimi podatki ali sporazumi o donacijah vključujejo naslednje varnostne elemente:

Varnostna navodila za program ali projekt

(a) „Varnostna navodila za program ali projekt“ (Programme or Project Security Instruction – PSI) pomeni seznam varnostnih postopkov, ki se uporabljajo za določen program ali projekt zaradi standardizacije varnostnih postopkov. Ta seznam je mogoče revidirati kadar koli v času trajanja programa ali projekta.

(b) Generalni direktorat za človeške vire in varnost oblikuje splošne PSI, ki jih lahko razvijejo službe Komisije, pristojne za programe ali projekte, ki vključujejo obravnavanje tajnih podatkov EU ali njihovo hrambo, ter, kadar je to ustrezno, posebne PSI, ki temeljijo na splošnih PSI.

(c) Posebni PSI se razvijejo zlasti za programe in projekte, za katere so značilni širok obseg, razsežnost ali kompleksnost ali veliko število in/ali raznolikost pogodbenikov, upravičencev ter drugih partnerjev in deležnikov, na primer glede njihovega pravnega statusa. Posebne PSI razvijejo službe Komisije, ki upravljajo zadevni program ali projekt, v tesnem sodelovanju z GD za človeške vire in varnost.

(d) Generalni direktorat za človeške vire in varnost strokovni skupini Komisije za varnost predloži splošne in specifične PSIS ter prosi za njeno mnenje.

Listina o varnostnih vidikih

(a) „Listina o varnostnih vidikih“ (Security Aspects Letter – SAL) pomeni sklop posebnih pogodbenih pogojev, ki jih objavi javni organ naročnik, in je sestavni del vsake pogodbe s tajnimi podatki, ki se nanaša na ustvarjanje tajnih podatkov EU, ter določa varnostne zahteve in tiste elemente pogodbe, ki zahtevajo varnostno zaščito.

(b) Varnostne zahteve, povezane s posamezno pogodbo, so opisane v SAL. Tej listini je po potrebi dodan vodič po stopnjah tajnosti in je sestavni del pogodbe s tajnimi podatki, podizvajalske pogodbe s tajnimi podatki ali sporazuma o donacijah.

(c) SAL vsebuje določbe, ki od izvajalca ali upravičenca zahtevajo spoštovanje minimalnih standardov iz tega sklepa. Javni organ naročnik zagotovi navedbo v SAL, da je nespoštovanje teh minimalnih standardov lahko zadosten razlog za prekinitev pogodbe ali sporazuma o donacijah.

2. Tako PSI kot tudi SAL vsebujeta vodič po stopnjah tajnosti kot obvezni varnostni element:

(a) „Vodič po stopnjah tajnosti“ je dokument, ki opisuje elemente programa, projekta, pogodbe ali sporazuma o donacijah, ki so tajni, in določa ustrezne stopnje tajnosti. Vodič po stopnjah tajnosti se lahko med trajanjem celotnega programa, projekta, pogodbe ali sporazuma o donacijah razširi, stopnja tajnosti elementov podatkov pa se lahko spremeni ali zniža; če obstaja vodič po stopnjah tajnosti, mora biti del listine o varnostnih vidikih.

(b) Pred objavo razpisa ali sklenitvijo pogodbe s tajnimi podatki služba Komisije kot javni organ naročnik določi stopnjo tajnosti vseh podatkov, ki se posredujejo kandidatom in ponudnikom ali izvajalcem, pa tudi stopnjo tajnosti podatkov, ki jih bo ustvaril izvajalec. Za ta namen po posvetovanju z varnostnim organom Komisije pripravi vodič po stopnjah tajnosti, ki se uporablja pri izvedbi pogodbe, v skladu s tem sklepom in njegovimi izvedbenimi pravili.

(c) Za določitev stopnje tajnosti različnih elementov pogodbe s tajnimi podatki veljajo naslednja načela:

(i) služba Komisije kot javni organ naročnik pri pripravi vodiča po stopnjah tajnosti upošteva vse pomembne varnostne vidike, vključno s stopnjo tajnosti, določeno za zagotovljene in odobrene podatke, ki jih tvorec uporablja za namene pogodbe;

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

(iii) javni organ naročnik se, če pride do kakršnih koli sprememb v zvezi s stopnjo tajnosti podatkov, ki so bili ustvarjeni pri izvajalcih ali so jim bili predloženi pri izvajanju pogodbe, ali ob kakršni koli naknadni spremembi vodiča po stopnjah tajnosti, po potrebi poveže prek varnostnega organa Komisije z zadevnimi nacionalnimi varnostnimi organi, imenovanimi varnostnimi organi ali katerim koli drugim pristojnim varnostnim organom države članice.

Člen 43

Dostop do tajnih podatkov EU za osebje izvajalcev in upravičencev

Javni organ naročnik ali organ, ki dodeljuje donacije, zagotovi, da pogodba s tajnimi podatki ali tajni sporazum o donacijah vsebuje določbe, ki navajajo, da se osebju izvajalca, podizvajalca ali upravičenca, ki za izvajanje pogodbe ali podizvajalske pogodbe s tajnimi podatki ali sporazuma o donacijah potrebuje dostop do tajnih podatkov EU, tak dostop odobri le, če:

(a) je bilo varnostno preverjeno na ustrezni stopnji ali je kako drugače ustrezno pooblaščeno, ker je bila ugotovljena njegova potreba po vedenju;

(b) je bilo poučeno o varnostnih pravilih za varovanje tajnih podatkov EU, ki se uporabljajo, ter je sprejelo odgovornost za varovanje teh podatkov;

(c) je bilo varnostno preverjeno na ustrezni ravni za podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET s strani ustreznega nacionalnega varnostnega organa, imenovanega varnostnega organa ali katerega koli drugega pristojnega organa.

Člen 44

Varnostno dovoljenje organizacije

1. „Varnostno dovoljenje organizacije“ je uradna izjava nacionalnega varnostnega organa, imenovanega varnostnega organa ali katerega koli drugega pristojnega varnostnega organa, da lahko določena organizacija iz varnostnega vidika nudi ustrezno stopnjo varovanja tajnih podatkov EU do določene stopnje tajnosti.

2. Varnostno dovoljenje organizacije, ki ga izda nacionalni varnostni organ, imenovani varnostni organ ali kateri koli drug pristojni varnostni organ države članice, s katerim skladno z nacionalnimi zakoni in predpisi navede, da je gospodarski subjekt zmožen varovati tajne podatke EU ustrezne stopnje tajnosti (CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET) v svojih prostorih, je treba predložiti varnostnemu organu Komisije, ki ga bo posredoval službi Komisije, ki deluje kot javni organ naročnik ali organ, odgovoren za dodelitev donacij, preden se kandidatu, ponudniku ali izvajalcu oziroma prosilcu za donacije ali upravičencu do njih omogoči ali odobri dostop do tajnih podatkov EU.

3. Po potrebi javni organ naročnik prek varnostnega organa Komisije uradno obvesti nacionalni varnostni organ, imenovani varnostni organ ali kateri koli drug pristojni varnostni organ, da se za izvajanje pogodbe zahteva varnostno dovoljenje organizacije. Varnostno dovoljenje organizacije ali dovoljenje za dostop do tajnih podatkov EU stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET se predloži v času teka postopka javnega naročanja ali postopka dodeljevanja donacij.

4. Javni organ naročnik ali organ, ki dodeljuje donacije, najustreznejšemu ponudniku ali prosilcu ne sme dodeliti pogodbe s tajnimi podatki ali tajnega sporazuma o donacijah, dokler mu nacionalni varnostni organ, imenovani varnostni organ ali kateri koli drug pristojni varnostni organ države članice, v kateri je izvajalec ali podizvajalec registriran, ne potrdi, da je bilo, kjer je to potrebno, ponudniku ali prosilcu izdano ustrezno varnostno dovoljenje organizacije.

5. Kadar nacionalni varnostni organ, imenovani varnostni organ ali kateri koli drug pristojni varnostni organ, ki je izdal varnostno dovoljenje organizacije, uradno obvesti varnostni organ Komisije o spremembah, ki zadevajo varnostno dovoljenje organizacije, ta nato obvesti službo Komisije, ki deluje kot javni organ naročnik ali organ, ki dodeljuje donacije. V primeru podizvajalske pogodbe se ustrezno obvesti nacionalni varnostni organ, imenovani varnostni organ ali kateri koli drug pristojni varnostni organ.

6. Če ustrezni nacionalni varnostni organ, imenovani varnostni organ ali kateri koli drug pristojni varnostni organ odvzame varnostno dovoljenje organizacije, je to zadosten razlog, da lahko javni organ naročnik ali organ, ki dodeljuje donacije, prekine pogodbo s tajnimi podatki ali kandidata, ponudnika ali prosilca izključi iz natečaja. Določbe v ta namen se vključijo v vzorce pogodb in sporazumov o donacijah, ki jih je treba izdelati.

Člen 45

Določbe za pogodbe s tajnimi podatki ali tajne sporazume o donacijah

1. Če se tajni podatki EU kandidatu, ponudniku ali prosilcu zagotovijo med postopkom javnega naročanja, razpis za zbiranje ponudb ali predlogov vsebuje določbo, v skladu s katero mora kandidat, ponudnik ali prosilec, ki ne predloži ponudbe ali predloga ali ki ni izbran, v določenem roku vrniti vse tajne dokumente.

2. Javni organ naročnik ali organ, ki dodeljuje donacije, prek varnostnega organa Komisije uradno obvesti pristojni nacionalni varnostni organ, imenovani varnostni organ ali kateri koli drug pristojni varnostni organ o tem, da je bila sklenjena pogodba s tajnimi podatki ali sporazum o donacijah in o relevantnih podatkih, kot so ime izvajalcev ali upravičencev, trajanje pogodbe in najvišje stopnje tajnosti.

3. Kadar takšne pogodbe ali sporazumi o donacijah prenehajo veljati, javni organ naročnik ali organ, ki dodeljuje donacije, o tem prek varnostnega organa Komisije nemudoma uradno obvesti nacionalni varnostni organ, imenovani varnostni organ ali kateri koli drug pristojni varnostni organ države članice, v kateri je izvajalec ali upravičenec do donacij registriran.

4. Na splošno velja, da mora izvajalec ali upravičenec do donacij ob prenehanju veljavnosti pogodbe s tajnimi podatki ali tajnega sporazuma o donacijah ali ob prenehanju sodelovanja s strani upravičenca do donacij javnemu organu naročniku ali organu, ki donacije dodeljuje, vrniti vse tajne podatke EU, ki jih ima.

5. V SAL se zapišejo posebne določbe o razpolaganju s tajnimi podatki EU v času izvajanja pogodbe s tajnimi podatki ali tajnega sporazuma o donacijah oziroma po prenehanju veljavnosti pogodbe ali sporazuma.

6. Če smeta izvajalec ali upravičenec do donacij tajne podatke EU obdržati tudi po prenehanju veljavnosti pogodbe s tajnimi podatki ali tajnega sporazuma o donacijah, morata še naprej ravnati skladno z minimalnimi standardi iz tega sklepa in varovati tajnost podatkov EU.

Člen 46

Posebne določbe za pogodbe s tajnimi podatki

1. Pogoji, povezani z varovanjem tajnih podatkov EU in v skladu s katerimi lahko izvajalec sklene podizvajalsko pogodbo, so določeni v razpisu in v pogodbi s tajnimi podatki.

2. Izvajalec pred oddajo delov pogodbe s tajnimi podatki podizvajalcu pridobi dovoljenje javnega organa naročnika. S podizvajalci, registriranimi v tretji državi, ni dovoljeno sklepati podizvajalskih pogodb, ki vključujejo dostop do tajnih podatkov EU, razen če obstaja regulativni okvir za varnost podatkov, kot je določeno v poglavju 7.

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

4. Kar zadeva tajne podatke, ki jih izvajalec ustvari ali obravnava, za tvorca šteje Komisija, pravice tvorca pa uveljavlja javni organ naročnik.

Člen 47

Obiski v zvezi s pogodbami s tajnimi podatki

1. Če mora član osebja Komisije, naročnika ali upravičenca do donacij za izvajanje pogodbe s tajnimi podatki ali sporazuma o donacijah imeti dostop do podatkov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET v prostorih drugih udeležencev, se v sodelovanju z zadevnimi nacionalnimi varnostnimi organi, imenovanimi varnostnimi organi ali katerim koli drugim pristojnim varnostnim organom organizirajo obiski. O takšnih obiskih se obvesti varnostni organ Komisije. Nacionalni varnostni organi, imenovani varnostni organi ali kateri koli drugi pristojni varnostni organi pa se lahko za posebne programe ali projekte tudi sporazumejo o postopku, na podlagi katerega se je mogoče o takšnih obiskih dogovoriti neposredno.

2. Vsi obiskovalci imajo ustrezno dovoljenje za dostop do tajnih podatkov in imajo potrebo po vedenju za dostop do tajnih podatkov EU, povezanih s pogodbo s tajnimi podatki.

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

4. Podrobnejše določbe so določene v izvedbenih pravilih.

5. Spoštovanje določb v zvezi z obiski v okviru pogodb s tajnimi podatki, določenimi v tem sklepu in v izvedbenih pravilih iz odstavka 4, je obvezno.

Člen 48

Razpošiljanje in prenos tajnih podatkov EU v zvezi s pogodbami s tajnimi podatki ali tajnimi sporazumi o donacijah

1. Za razpošiljanje tajnih podatkov EU z elektronskimi sredstvi se uporabljajo ustrezne določbe iz poglavja 5 tega sklepa.

2. Za prenašanje tajnih podatkov EU se v skladu z nacionalnimi zakoni in predpisi uporabljajo ustrezne določbe iz poglavja 4 tega sklepa in njegovih izvedbenih pravil.

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

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

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

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

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

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

Člen 49

Posredovanje tajnih podatkov EU izvajalcem ali upravičencem do donacij v tretjih državah

Prenos tajnih podatkov EU izvajalcem ali upravičencem do donacij v tretjih državah poteka v skladu z varnostnimi ukrepi, dogovorjenimi med varnostnim organom Komisije ali službo Komisije kot javnim organom naročnikom ali organom, ki dodeljuje donacije, in nacionalnim varnostnim organom, imenovanim varnostnim organom ali katerim koli drugim pristojnim varnostnim organom zadevne tretje države, v kateri je registriran izvajalec ali upravičenec do donacij.

Člen 50

Obravnavanje tajnih podatkov stopnje RESTREINT UE/EU RESTRICTED v okviru pogodb s tajnimi podatki ali tajnih sporazumov o donacijah

1. Varovanje podatkov stopnje RESTREINT UE/EU RESTRICTED, ki se jih obravnava ali hrani v okviru pogodb s tajnimi podatki ali sporazumov o donacijah, temelji na načelih sorazmernosti in stroškovne učinkovitosti.

2. V okviru pogodb s tajnimi podatki ali tajnimi sporazumi o donacijah se za obravnavanje tajnih podatkov s stopnjo tajnosti RESTREINT UE/EU RESTRICTED ne zahteva varnostno dovoljenje organizacije ali dovoljenje za dostop do tajnih podatkov.

3. Če pogodba ali sporazum o donacijah vključuje obravnavanje tajnih podatkov stopnje RESTREINT UE/EU RESTRICTED v KIS, ki ga upravlja izvajalec ali upravičenec do donacij, javni organ naročnik ali organ, ki dodeljuje donacije, po posvetovanju z varnostnim organom Komisije zagotovi, da se v pogodbi ali sporazumu o donacijah določijo potrebne tehnične in upravne zahteve glede akreditacije ali odobritve KIS, ki so v sorazmerju z ocenjenim tveganjem ob upoštevanju vseh ustreznih dejavnikov. Varnostni organ Komisije in ustrezni nacionalni varnostni organ ali imenovani varnostni organ se dogovorita o obsegu akreditacije ali odobritve takšnega KIS.

POGLAVJE 7

IZMENJAVA TAJNIH PODATKOV Z DRUGIMI INSTITUCIJAMI AGENCIJAMI, ORGANI IN URADI UNIJE, Z DRŽAVAMI ČLANICAMI TER S TRETJIMI DRŽAVAMI IN MEDNARODNIMI ORGANIZACIJAMI

Člen 51

Osnovna načela

1. Kadar Komisija ali ena od njenih služb sprejme odločitev o potrebi po izmenjavi tajnih podatkov z drugo institucijo, agencijo, organom ali uradom Unije ali s tretjo državo ali mednarodno organizacijo, se sprejmejo potrebni ukrepi, da se v ta namen vzpostavi ustrezen pravni ali upravni okvir, kar pa lahko vključuje sporazume o varovanju tajnosti podatkov ali upravne dogovore, sklenjene v skladu z ustreznimi predpisi.

2. Ne glede na člen 57 se tajni podatki EU z drugo institucijo, agencijo, organom ali uradom Unije ali s tretjo državo ali mednarodno organizacijo izmenjajo samo pod pogojem, da je na voljo ustrezen pravni ali upravni okvir in da obstaja dovolj jamstev, da institucija, agencija, organ ali urad Unije ali zadevna tretja država ali mednarodna organizacija uporablja enakovredna osnovna načela in minimalne standarde za varovanje tajnih podatkov.

Člen 52

Izmenjava tajnih podatkov EU z drugimi institucijami, agencijami, organi in uradi Unije

1. Pred sklenitvijo upravnega dogovora za izmenjavo tajnih podatkov EU z drugo institucijo, agencijo, organom ali uradom Unije Komisija zahteva zagotovilo, da zadevna institucija, agencija, organ ali urad Unije:

(a) ima vzpostavljen regulativni okvir za varovanje tajnih podatkov EU, ki določa temeljna načela in minimalne standarde, ki so enakovredni tistim iz tega sklepa in njegovih izvedbenih pravil;

(b) uporablja varnostne standarde in smernice glede varnosti osebja, fizične varnosti, ravnanja s tajnimi podatki EU ter varnosti komunikacijskih in informacijskih sistemov (KIS), ki zagotavljajo enakovredno raven varovanja tajnih podatkov EU, kot je zagotovljena na Komisiji;

(c) tajne podatke, ki jih ustvari, označi kot tajne podatke EU.

2. Generalni direktorat za človeške vire in varnost je ob tesnem sodelovanju z drugimi pristojnimi službami Komisije glavna služba znotraj Komisije za sklenitev upravnih dogovorov v zvezi z izmenjavo tajnih podatkov EU z drugimi institucijami, agencijami, organi ali uradi Unije.

3. Upravni dogovori praviloma potekajo v obliki izmenjave pisem, ki jih v imenu Komisije podpiše generalni direktor za človeške vire in varnost.

4. Pred sklenitvijo upravnega dogovora za izmenjavo tajnih podatkov EU varnostni organ Komisije opravi ocenjevalni obisk, da oceni regulativni okvir za varovanje tajnih podatkov EU in ugotovi učinkovitost ukrepov, ki se izvajajo za varovanje tajnih podatkov EU. Upravni dogovor začne veljati in tajni podatki EU se izmenjajo le, če je rezultat tega ocenjevalnega obiska zadovoljiv in če so bila priporočila, ki so bila podana po obisku, upoštevana. Redno se izvajajo nadaljnji ocenjevalni obiski za preverjanje, ali se upravni dogovor spoštuje in ali so vzpostavljeni varnostni ukrepi še vedno v skladu z dogovorjenimi osnovnimi načeli in minimalnimi standardi.

5. Znotraj Komisije je register tajnih podatkov EU, ki ga upravlja generalni sekretariat, praviloma glavna točka vstopa in izstopa izmenjave tajnih podatkov z drugimi institucijami, agencijami, organi in uradi Unije. Če pa je iz varnostnih, organizacijskih ali operativnih razlogov z vidika varovanja tajnih podatkov EU to primerneje, lahko v skladu s tem sklepom in njegovimi izvedbenimi pravili lokalni registri tajnih podatkov EU, vzpostavljeni znotraj služb Komisije, delujejo kot točka vstopa in izstopa tajnih podatkov o zadevah v pristojnosti zadevnih služb Komisije.

6. Strokovna skupina Komisije za varnost mora biti obveščena o postopku sklenitve upravnih dogovorov v skladu z odstavkom 2.

Člen 53

Izmenjava tajnih podatkov EU z državami članicami

1. Tajni podatki EU se lahko izmenjujejo z državami članicami oziroma se jim posredujejo pod pogojem, da te navedene podatke varujejo v skladu z zahtevami, ki se uporabljajo za tajne podatke z oznako nacionalne stopnje tajnosti na enakovredni stopnji, kakor je določeno v preglednici enakovrednosti stopenj tajnosti v Prilogi I.

2. Če države članice v strukture ali omrežja Evropske unije vnesejo tajne podatke z oznako nacionalne stopnje tajnosti, Komisija 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 Prilogi I.

Člen 54

Izmenjava tajnih podatkov EU s tretjimi državami in mednarodnimi organizacijami

1. Kadar Komisija ugotovi, da obstaja dolgoročna potreba po izmenjavi tajnih podatkov s tretjimi državami ali mednarodnimi organizacijami, se sprejmejo potrebni ukrepi, da se v ta namen vzpostavi ustrezen pravni ali upravni okvir, kar pa lahko vključuje sporazume o varovanju tajnosti podatkov ali upravne dogovore, sklenjene v skladu z ustreznimi predpisi.

2. Takšni sporazumi o varovanju tajnosti podatkov in upravni dogovori iz odstavka 1 vsebujejo določbe, s katerimi se tajnim podatkom EU, ki jih prejmejo tretje države ali mednarodne organizacije, zagotovi varovanje, ustrezno njihovi stopnji tajnosti in v skladu z minimalnimi standardi, ki so enakovredni standardom iz tega sklepa.

3. Komisija lahko sklene upravne dogovore v skladu s členom 56, če stopnja tajnih podatkov EU praviloma ni višja od RESTREINT UE/EU RESTRICTED.

4. Upravni dogovori v zvezi z izmenjavo tajnih podatkov iz odstavka 3 vsebujejo določbe, s katerimi se tajnim podatkom EU, ki jih prejmejo tretje države ali mednarodne organizacije, zagotovi varovanje, ustrezno njihovi stopnji tajnosti in v skladu z minimalnimi standardi, ki so enakovredni standardom iz tega sklepa. V zvezi s sklenitvijo sporazumov o varnosti tajnih podatkov ali upravnih dogovorov se je treba posvetovati s strokovno skupino Komisije za varnost.

5. Odločitev o posredovanju tajnih podatkov EU z izvorom v Komisiji tretji državi ali mednarodni organizaciji sprejme služba Komisije kot tvorec zadevnih tajnih podatkov EU znotraj Komisije za vsak primer posebej glede na naravo in vsebino takih podatkov, potrebo prejemnika po vedenju ter obseg koristi, ki jih bo imela Unija. Če tvorec tajnih podatkov, ki bi se jih naj posredovalo, ali izvornega gradiva, ki naj bi jih ti vsebovali, ni Komisija, služba Komisije, ki ima te tajne podatke, najprej zaprosi za pisno soglasje tvorca, da sme zadevne tajne podatke posredovati. Če tvorca ni mogoče ugotoviti, služba Komisije, ki ima tajne podatke, prevzame odgovornost tvorca po posvetovanju s strokovno skupino Komisije za varnost.

Člen 55

Sporazumi o varovanju tajnosti podatkov

1. Sporazumi o varovanju tajnosti podatkov s tretjimi državami ali mednarodnimi organizacijami se sklenejo v skladu s členom 218 Pogodbe o delovanju Evropske unije.

2. Sporazumi o varovanju tajnosti podatkov:

(a) določajo temeljna načela in minimalne standarde, ki urejajo izmenjavo tajnih podatkov med Unijo in tretjo državo ali mednarodno organizacijo;

(b) vsebujejo tehnične izvedbene določbe, o katerih se dogovorijo pristojni varnostni organi zadevnih institucij in organov Unije ter pristojni varnostni organ zadevne tretje države ali mednarodne organizacije. Te določbe upoštevajo stopnjo varovanja, ki jo določajo veljavni varnostni predpisi, strukture in postopki v zadevni tretji državi ali mednarodni organizaciji;

(c) vsebujejo določbo, da se pred izmenjavo tajnih podatkov v skladu z zadevnim sporazumom zagotovi, da je stran prejemnica sposobna ustrezno zaščititi in varovati prejete tajne podatke.

3. Komisija se, kadar se v skladu s členom 51(1) ugotovi potreba po izmenjavi tajnih podatkov, posvetuje z Evropsko službo za zunanje delovanje, generalnim sekretariatom Sveta in drugimi institucijami in organi Unije, če je to ustrezno, da se ugotovi, ali je treba predložiti priporočilo v skladu s členom 218(3) PDEU.

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

5. Znotraj Komisije je register tajnih podatkov EU, ki ga upravlja generalni sekretariat, praviloma glavna točka vstopa in izstopa izmenjave tajnih podatkov s tretjimi državami in mednarodnimi organizacijami. Če pa je iz varnostnih, organizacijskih ali operativnih razlogov z vidika varovanja tajnih podatkov EU to primerneje, lahko v skladu s tem sklepom in njegovimi izvedbenimi pravili lokalni registri tajnih podatkov EU, vzpostavljeni znotraj služb Komisije, delujejo kot točka vstopa in izstopa tajnih podatkov o zadevah v pristojnosti zadevnih služb Komisije.

6. Za oceno učinkovitosti varnostnih predpisov, struktur in postopkov v zadevni tretji državi ali mednarodni organizaciji Komisija v sodelovanju z drugimi institucijami, agencijami ali organi Unije sodeluje pri ocenjevalnih obiskih v soglasju z zadevno tretjo državo ali mednarodno organizacijo. S takšnimi ocenjevalnimi obiski se ocenijo:

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

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

(c) dejanski varnostni ukrepi in postopki; ter

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

Člen 56

Upravni dogovori

1. Če obstaja dolgoročna potreba v kontekstu političnega ali pravnega okvira Unije po izmenjavanju tajnih podatkov, ki praviloma ne presegajo stopnje RESTREINT UE/EU RESTRICTED, s tretjo državo ali mednarodno organizacijo in je varnostni organ Komisije po posvetovanju s strokovno skupino Komisije za varnost zlasti ugotovil, da zadevna stran nima dovolj razvitega varnostnega sistema, da bi bila zmožna skleniti sporazum o varovanju tajnosti podatkov, se lahko Komisija odloči skleniti upravni dogovor z ustreznimi organi zadevne tretje države ali mednarodne organizacije.

2. Praviloma imajo takšni upravni dogovori obliko izmenjave pisem.

3. Pred sklenitvijo dogovora se opravi ocenjevalni obisk. O rezultatih ocenjevalnega obiska je treba obvestiti strokovno skupino Komisije za varnost. Če obstajajo izredni razlogi za nujno izmenjavo tajnih podatkov, se lahko tajni podatki EU posredujejo, pod pogojem, da se stori vse, da se ocenjevalni obisk opravi čim prej.

4. Tajni podatki EU se ne izmenjujejo z elektronskimi sredstvi, razen če ni to izrecno določeno v upravnem dogovoru.

Člen 57

***Ad hoc* posredovanje tajnih podatkov EU v izjemnih primerih**

1. Če ni sporazuma o varovanju tajnosti podatkov ali upravnega dogovora in če Komisija ali ena od njenih služb ugotovi, da obstajajo izjemne potrebe v kontekstu političnega ali pravnega okvira Unije za posredovanje tajnih podatkov EU tretji državi ali mednarodni organizaciji, varnostni organ Komisije v okviru možnosti pri varnostnih organih zadevne tretje države ali mednarodne organizacije preveri, ali njeni varnostni predpisi, strukture in postopki zagotavljajo, da bodo tajni podatki EU, ki ji bodo posredovani, zaščiteni v skladu s standardi, ki niso manj strogi od standardov iz tega sklepa.

2. Odločitev o posredovanju tajnih podatkov EU zadevni tretji državi ali mednarodni organizaciji po posvetovanju s strokovno skupino Komisije za varnost sprejme Komisija, in sicer na predlog člana Komisije, pristojnega za varnostne zadeve.

3. Po tem, ko je Komisija sprejela odločitev o posredovanju tajnih podatkov EU in ob predhodnem pisnem soglasju tvorca, vključno s tvorci izvornega gradiva, ki ga ti podatki lahko vsebujejo, pristojna služba Komisije posreduje zadevne informacije, ki nosijo oznako o dovoljenem prenosu v tretjo državo ali mednarodno organizacijo, kateri se dokument posreduje. Preden se tajni podatki dejansko posredujejo ali ob njihovi predaji se zadevna tretja stran pisno zaveže, da bo varovala prejete tajne podatke EU v skladu s temeljnimi načeli in minimalnimi standardi iz tega sklepa.

POGLAVJE 8

KONČNE DOLOČBE

Člen 58

Nadomestitev prejšnjega sklepa

Ta sklep razveljavlja in nadomešča Sklep Komisije 2001/844/ES, ESPJ, Euratom ([1]).

Člen 59

Tajni podatki, ustvarjeni pred začetkom veljavnosti tega sklepa

1. Varovanje vseh podatkov EU, ki so v skladu s Sklepom 2001/844/ES, ESPJ, Euratom imeli oznako tajnosti, se nadaljuje v skladu z ustreznimi določbami tega sklepa.

2. Vsi tajni podatki, ki jih ima Komisija na dan, ko je Sklep 2001/844/ES, ESPJ, Euratom začel veljati, razen tajnih podatkov Euratoma:

(a) če jih je ustvarila Komisija, še naprej štejejo, da so bili samodejno prerazvrščeni kot RESTREINT UE, razen če se je avtor odločil, da mu po 31. januarju 2002 dodeli drugo stopnjo tajnosti in je o tem obvestil vse naslovnike zadevnega dokumenta;

(b) če so jih ustvarili avtorji izven Komisije, obdržijo svojo prvotno stopnjo tajnosti in se tako obravnavajo kot tajni podatki EU na enakovredni ravni, razen če se avtor strinja s preklicem ali znižanjem stopnje tajnosti.

Člen 60

Izvedbena pravila in varnostna obvestila

1. Po potrebi bo sprejetje izvedbenih pravil za ta sklep predmet ločenega sklepa Komisije o pooblastitvi člana Komisije, pristojnega za varnostne zadeve, v skladu s poslovnikom.

2. Po tem, ko se ga pooblasti na podlagi zgoraj navedenega sklepa Komisije, lahko član Komisije, pristojen za varnostne zadeve, oblikuje varnostna obvestila, ki navajajo varnostne smernice in najboljše prakse v okviru področja uporabe tega sklepa in njegovih izvedbenih pravil.

3. Komisija lahko naloge, navedene v prvem in drugem odstavku tega člena, prenese na generalnega direktorja za človeške vire in varnost z ločenim delegiranim sklepom v skladu s poslovnikom.

Člen 61

Začetek veljavnosti

Ta sklep začne veljati dan po objavi v *Uradnem listu Evropske unije*.

V Bruslju, 13. marca 2015

Za Komisijo

Predsednik

Jean-Claude JUNCKER

([1]) Sklep Komisije 2001/844/ES, ESPJ, Euratom z dne 29. novembra 2001 o spremembah njenega poslovnika (UL L 317, 3.12.2001, str. 1).

PRILOGA I

ENAKOVREDNE STOPNJE TAJNOSTI

EU	TRÈS 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 okrajšava: ΑΑΠ	Απόρρητο okrajšava: (ΑΠ)	Εμπιστευτικό okrajšava: (ΕΜ)	Περιορισμένης Χρήσης okrajšava: (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 okrajšava: (ΑΑΠ)	Απόρρητο okrajšava: (ΑΠ)	Εμπιστευτικό okrajšava: (ΕΜ)	Περιορισμένης Χρήσης okrajšava: (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	TRÈS 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 ustrezne 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“.

PRILOGA II

SEZNAM KRATIC

Kratica	Pomen
CA	Organ za šifrirne metode in izdelke (Crypto Authority)
CAA	Organ za odobritev šifrirnih metod in izdelkov (Crypto Approval Authority)
CCTV	Sistem televizije zaprtega kroga (Closed Circuit Television)
CDA	Organ za razpošiljanje šifrirnega materiala (Crypto Distribution Authority)
KIS	Komunikacijski in informacijski sistemi (Communication and Information Systems)
DSA	Imenovani varnostni organ (Designated Security Authority)
EUCI	Tajni podatki EU (EU Classified Information)
FSC	Varnostno dovoljenje organizacije (Facility Security Clearance)
IA	Informacijska varnost (Information Assurance)
IAA	Organ za zagotavljanje informacijske varnosti (Information Assurance Authority)
IDS	Sistem odkrivanja vdorov (Intrusion Detection System)
IT	Informacijska tehnologija (Information Technology)
LSO	Lokalni uradnik za varnost
NSA	Nacionalni varnostni organ (National Security Authority)
PSC	Dovoljenje za dostop do tajnih podatkov (Personnel Security Clearance)
PSCC	Potrdilo za dostop do tajnih podatkov (Personnel Security Clearance Certificate)
PSI	Varnostna navodila za program/projekt (Programme/Project Security Instructions)
RCO	Nadzorni uradnik registra
SAA	Organ za varnostno akreditacijo (Security Accreditation Authority)
SAL	Listina o varnostnih vidikih (Security Aspects Letter)
SCG	Vodič po stopnjah tajnosti (Security Classification Guide)
SecOPs	Varnostno-operativni postopki (Security Operating Procedures)
TA	Organ TEMPEST
PDEU	Pogodba o delovanju EU

PRILOGA III

SEZNAM NACIONALNIH VARNOSTNIH ORGANOV

BELGIJA

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles
Tel. sekretariata +32 25014542
Faks +32 25014596
E-naslov: nvo-ans@diplobel.fed.be

BOLGARIJA

State Commission on Information Security
90 Cherkovna Str.
1505 Sofia
Tel. +359 29333600
Faks +359 29873750
E-naslov: dksi@government.bg
Spletno mesto: www.dksi.bg

ČEŠKA

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Tel. +420 257283335
Faks +420 257283110
E-naslov: czech.nsa@nbu.cz
Spletno mesto: www.nbu.cz

DANSKA

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Tel. +45 33148888
Faks +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Tel. +45 33325566
Faks +45 33931320

NEMČIJA

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin
Tel. +49 30186810
Faks +49 30186811441
E-naslov: oesIII3@bmi.bund.de

ESTONIJA

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn
Tel. +372 7170113 0019, +372 7170117
Faks +372 7170213
E-naslov: nsa@mod.gov.ee

GRČIJA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Τηλ.: +30 2106572045 (ώρες γραφείου)
+ 30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279; + 30 2106577612

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos – Athens
Tel. +30 2106572045
+ 30 2106572009
Faks +30 2106536279, +30 2106577612

ŠPANIJA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid
Tel. +34 913725000
Faks +34 913725808
E-naslov: nsa-sp@areatec.com

FRANCIJA

Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Paris 07 SP
Tel. +33 171758177
Faks + 33 171758200

HRVAŠKA

Office of the National Security Council
Croatian NSA
Jurjevska 34
HR-10000 Zagreb
Hrvaška
Tel. +385 14681222
Faks + 385 14686049
Spletno mesto: www.uvns.hr

IRSKA

National Security Authority
Department of Foreign Affairs
76 – 78 Harcourt Street
Dublin 2
Tel. +353 14780822
Faks +353 14082959

ITALIJA

Presidenza del Consiglio dei Ministri
D.I.S. – U.C.Se.
Via di Santa Susanna, 15
00187 Roma
Tel. +39 0661174266
Faks +39 064885273

CIPER

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia
Tel. +357 22807569, +357 22807643,
+357 22807764
Faks +357 22302351
E-naslov: cynsa@mod.gov.cy

LATVIJA

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV-1001 Riga
Tel. +371 67025418
Faks +371 67025454
E-naslov: ndi@sab.gov.lv

LITVA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority
Gedimino 40/1
LT-01110 Vilnius
Tel. +370 706 66701, +370 706 66702
Faks +370 706 66700
E-naslov: nsa@vsd.lt

LUKSEMBURG

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg
Tel. +352 24782210 centrala
+ 352 24782253 direktna številka
Faks +352 24782243

MADŽARSKA

Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tel. +36 (1) 7952303
Faks +36 (1) 7950344

Poštni naslov:
H-1357 Budapest, PO Box 2
E-naslov: nbf@nbf.hu
Spletno mesto: www.nbf.hu

MALTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Tel. +356 21249844
Faks +356 25695321

NIZOZEMSKA

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Tel. +31 703204400
Faks +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag
Tel. +31 703187060
Faks +31 703187522

AVSTRIJA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien
Tel. +43 1531152594
Faks +43 1531152615
E-naslov: ISK@bka.gv.at

POLJSKA

Agencja Bezpieczeństwa Wewnętrznego – ABW
(Internal Security Agency)
2A Rakowiecka St.
00-993 Warszawa
Tel. +48 22 58 57 944
Faks +48 22 58 57 443
E-naslov: nsa@abw.gov.pl
Spletno mesto: www.abw.gov.pl

PORTUGALSKA

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Tel. +351 213031710
Faks +351 213031711

ROMUNIJA

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA – ORNISS National Registry Office for Classified Information)
4 Mures Street
012275 Bucharest
Tel. +40 212245830
Faks +40 212240714
E-naslov: nsa.romania@nsa.ro
Spletno mesto: www.orniss.ro

SLOVENIJA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tel. +386 14781390
Faks +386 14781399
E-naslov: gp.uvtp@gov.si

SLOVAŠKA

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30 P.O.
P.O. Box 16
850 07 Bratislava
Tel. +421 268692314
Faks +421 263824005
Spletno mesto; www.nbusr.sk

FINSKA

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Tel. 16055890
Faks +358 916055140
E-naslov: NSA@formin.fi

ŠVEDSKA

Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
SE-103 39 Stockholm
Tel. +46 84051000
Faks +46 87231176
E-naslov: ud-nsa@foreign.ministry.se

ZDRUŽENO KRALJESTVO

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Tel. 1: +44 2072765649
Tel. 2: +44 2072765497
Faks +44 2072765651
E-naslov: UK-NSA@cabinet-office.x.gsi.gov.uk