

Uradni list

Evropske unije

C 96



Slovenska izdaja

Informacije in objave

Zvezek 57

1. april 2014

Vsebina

II *Sporočila*

SPOROČILA INSTITUCIJ, ORGANOV, URADOV IN AGENCIJ EVROPSKE UNIJE

Evropski parlament

2014/C 96/01

Sklep predsedstva Evropskega parlamenta z dne 15. aprila 2013 o pravilniku o obdelavi zaupnih podatkov v Evropskem parlamentu

1

SL

II

(Sporočila)

SPOROČILA INSTITUCIJ, ORGANOV, URADOV IN AGENCIJ EVROPSKE UNIJE

EVROPSKI PARLAMENT

SKLEP PREDSEDSTVA EVROPSKEGA PARLAMENTA

z dne 15. aprila 2013

o pravilniku o obdelavi zaupnih podatkov v Evropskem parlamentu

(2014/C 96/01)

PREDSEDSTVO EVROPSKEGA PARLAMENTA JE –

ob upoštevanju člena 23(12) Poslovnika Evropskega parlamenta,

ob upoštevanje naslednjega:

- (1) Glede na Okvirni sporazum o odnosih med Evropskim parlamentom in Evropsko komisijo ⁽¹⁾, podpisan dne 20. oktobra 2010 (v nadaljnjem besedilu: Okvirni sporazum), ter Medinstitucionalni sporazum med Evropskim parlamentom in Svetom o pošiljanju tajnih podatkov Sveta o zadevah, ki niso s področja skupne zunanje in varnostne politike, Evropskemu parlamentu in njihovi obdelavi s strani Evropskega parlamenta ⁽²⁾, podpisan dne 12. marca 2014 (v nadaljnjem besedilu: Medinstitucionalni sporazum), je treba določiti posebna pravila o obdelavi zaupnih podatkov v Evropskem parlamentu.
- (2) Lizbonska pogodba Evropskemu parlamentu dodeljuje nove naloge, zato je treba za razvoj dejavnosti Parlamenta na teh področjih, ki zahtevajo določeno stopnjo zaupnosti, določiti temeljna načela, minimalne varnostne standarde in ustrezne postopke za obdelavo zaupnih podatkov, tudi tajnih, s strani Evropskega parlamenta.
- (3) Cilj pravilnika, določenega s tem sklepom, je zagotoviti enakovredne standarde varstva in združljivost s pravilniki drugih institucij, organov, uradov in agencij, ustanovljenih v okviru ali na podlagi Pogodb ali s strani držav članic, da se omogoči nemoteno delovanje postopka sprejemanja odločitev Evropske unije.
- (4) Določbe tega sklepa ne posegajo v sedanja in prihodnja pravila o dostopu do dokumentov, sprejetih v skladu s členom 15 Pogodbe o delovanju Evropske unije (v nadaljnjem besedilu: PDEU).

⁽¹⁾ UL L 304, 20.11.2010, str. 47.⁽²⁾ UL C 95, 1.4.2014, str. 1.

- (5) Določbe tega sklepa ne posegajo v sedanja in prihodnja pravila o varstvu osebnih podatkov, sprejeta v skladu s členom 16 PDEU –

SPREJELO NASLEDNJI SKLEP:

Člen 1

Cilj

Ta sklep ureja upravljanje in ravnanje z zaupnimi podatki v Evropskem parlamentu, kar vključuje nastanek, sprejemanje, posredovanje in shranjevanje zaupnih podatkov, zato da se ustrezno zaščiti njihova zaupna narava. Pomeni zlasti izvedbo Medinstitucionalnega sporazuma in Okvirni sporazum, zlasti Priloge II k Okvirnemu sporazumu.

Člen 2

Opredelitev pojmov

V tem sklepu:

- (a) „podatki“ pomenijo vsak pisni ali ustni podatek, ne glede na nosilec in avtorja;
- (b) „zaupni podatki“ pomenijo tajne podatke in druge netajne podatke zaupne narave;
- (c) „tajni podatki“ pomenijo tajne podatke EU in „enakovredne tajne podatke“;
- (d) „tajni podatki EU“ pomenijo vse podatke in gradivo, določene kot TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL ali RESTREINT UE/EU RESTRICTED, katerih nedovoljeno razkritje bi lahko v različni meri posegalo v interese Unije ali ene ali več držav članic, ne glede na to, ali taki podatki izvirajo znotraj institucij, organov, uradov ali agencij, ustanovljenih v okviru ali na podlagi Pogodb. Tako so podatki in gradivo stopnje tajnosti:
 - TRÈS SECRET UE/EU TOP SECRET podatki in gradivo, katerih nedovoljeno razkritje bi lahko povzročilo izjemno hude posledice za temeljne interese Unije ali ene ali več držav članic;
 - SECRET UE/EU SECRET podatki in gradivo, katerih nedovoljeno razkritje bi lahko resno škodovalo temeljnim interesom Unije ali ene ali več držav članic;
 - CONFIDENTIEL UE/EU CONFIDENTIAL podatki in gradivo, katerih nedovoljeno razkritje bi lahko škodovalo temeljnim interesom Unije ali ene ali več držav članic;
 - RESTREINT UE/EU RESTRICTED podatki in gradivo, katerih nedovoljeno razkritje bi bilo lahko neugodno za interese Unije ali ene ali več držav članic;
- (e) „enakovredni tajni podatki“ pomenijo tajne podatke, ki jih izdajo države članice, tretje države ali mednarodne organizacije, z oznako stopnje tajnosti, enakovredno eni od oznak stopenj tajnosti, ki se uporabljajo za tajne podatke EU, Evropskemu parlamentu pa jih je posredoval Svet ali Komisija;

- (f) „drugi zaupni podatki“ pomenijo vse druge netajne zaupne podatke, vključno s podatki, ki jih zajemajo predpisi o varstvu osebnih podatkov ali obveznost poklicne molčečnosti, ki nastanejo v Evropskem parlamentu ali jih Evropskemu parlamentu posredujejo druge institucije, organi, uradi in agencije, ustanovljene v okviru ali na podlagi Pogodb ali s strani držav članic;
- (g) „dokument“ pomeni vse shranjene podatke, ne glede na njihovo fizično obliko ali značilnosti;
- (h) „gradivo“ pomeni vse dokumente ali dele naprav ali opreme, bodisi izdelane bodisi v postopku izdelave;
- (i) „potreba po seznanitvi“ pomeni potrebo osebe, da ima dostop do zaupnih podatkov, da lahko izvrši uradno dolžnost ali nalogo;
- (j) „dovoljenje“ pomeni odločitev predsednika, če zadeva poslance Evropskega parlamenta, ali generalnega sekretarja, če zadeva uradnike Evropskega parlamenta in druge uslužbence Evropskega parlamenta, ki delajo v političnih skupinah, o dovolitvi posamezniku, da dostopa do tajnih podatkov do določene stopnje, na podlagi pozitivnega rezultata varnostnega pregleda (preverjanja), ki ga izvede nacionalni organ v skladu z notranjo zakonodajo in z določbami iz dela 2 Priloge I;
- (k) „znižanje“ pomeni določitev nižje stopnje tajnosti;
- (l) „odprava“ pomeni odstranitev vsakršne tajnosti;
- (m) „oznaka“ pomeni znak, ki ga nosijo drugi zaupni podatki, namenjen pa je prepoznavanju vnaprej opredeljenih posebnih navodil v zvezi z ravnanjem z njimi ali področjem, ki ga pokriva nek dokument. Lahko jo nosijo tudi tajni podatki, da se določijo dodatne zahteve za ravnanje z njimi;
- (n) „odprava oznake“ pomeni odstranitev vsakršne oznake;
- (o) „avtor“ pomeni ustrezno pooblaščenega avtorja zaupnega podatka;
- (p) „varnostna obvestila“ pomenijo izvedbene ukrepe, določene v Prilogi II;
- (q) „navodila za ravnanje“ pomenijo tehnična navodila službam Evropskega parlamenta o upravljanju zaupnih podatkov.

Člen 3

Temeljna načela in minimalni standardi

1. Obdelava zaupnih podatkov s strani Evropskega parlamenta sledi temeljnemu načelom in minimalnim standardom iz dela 1 Priloge I.

2. Evropski parlament v skladu s temeljnimi načeli in minimalnimi standardi vzpostavi sistem za upravljanje varnosti podatkov. Sistem za upravljanje varnosti podatkov sestavljajo varnostna obvestila, navodila za ravnanje in ustrezni členi Poslovnika. Cilj sistema je olajšati parlamentarno in upravno delo, hkrati pa zagotoviti varstvo vsakršnih zaupnih podatkov, ki jih obdelata Parlament, ob popolnem upoštevanju pravil, ki jih opredeli avtor teh podatkov, kakor je določeno v varnostnih obvestilih.

Obdelava zaupnih podatkov s pomočjo avtomatskih komunikacijskih in informacijskih sistemov Evropskega parlamenta se izvaja v skladu z zasnovo zagotavljanja varnosti podatkov, kot je določeno v varnostnem obvestilu 3.

3. Poslanci Evropskega parlamenta lahko brez varnostne odobritve dostopajo do tajnih podatkov vse do vključno stopnje RESTREINT UE/EU RESTRICTED.

4. Kadar so zadevni podatki tajni podatki stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali enakovredne stopnje, se lahko dajo na voljo poslancem Evropskega parlamenta, ki jih je za to pooblastil predsednik v skladu s členom 5 ali po tem, ko so podpisali častno izjavo, da vsebine teh podatkov ne bodo razkrili tretjim osebam in da bodo spoštovali obveznost varovanja podatkov, ki so tajni podatki stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, ter da se zavedajo posledic, če tega ne bodo upoštevali.

5. Kadar so zadevni podatki tajni podatki stopnje SECRET UE/EU SECRET ali TRÈS SECRET/EU TOP SECRET ali temu enakovredne stopnje se lahko dajo na voljo poslancem Evropskega parlamenta, ki jih je za to pooblastil predsednik, potem ko:

- (a) so opravili varnostno preverjanje v skladu z delom 2 Priloge I k temu sklepu ali
- (b) je od pristojnih nacionalnih organov prejel uradno obvestilo, da so zadevni poslanci ustrezno pooblaščen zaradi svoje funkcije v skladu z nacionalnim pravom.

6. Preden se poslancem Evropskega parlamenta odobri dostop do tajnih podatkov, jih je treba obvestiti, poslanci pa morajo zavedati, da morajo varovati te podatke v skladu s Prilogo I. Obvestiti jih je treba tudi o sredstvih za zagotavljanje takega varstva.

7. Uradniki Evropskega parlamenta in drugi uslužbenci Parlamenta, ki delajo v političnih skupinah, lahko dostopajo do zaupnih podatkov, če je zanje ugotovljena „potreba po seznanitvi“, do tajnih podatkov nad stopnjo RESTREINT UE/EU RESTRICTED pa, če imajo ustrezno stopnjo varnostne odobritve. Dostop do tajnih podatkov se odobri samo, če so bili obveščeni in so prejeli pisna navodila glede dolžnosti v zvezi z varstvom teh podatkov, pa tudi sredstev za zagotavljanje tega varstva, ter če so podpisali izjavo, v kateri so potrdili prejem teh navodil in se zavezali k njihovem izpolnjevanju v skladu s tem pravilnikom.

Člen 4

Nastanek zaupnih podatkov in njihova upravna obdelava v Evropskem parlamentu

1. Predsednik Evropskega parlamenta, predsedniki ustreznih parlamentarnih odborov ter generalni sekretar in/ali vse osebe, ki jih on ustrezno pisno pooblasti, lahko osnujejo zaupne podatke in/ali določajo stopnjo njihove tajnosti, kakor je določeno v varnostnih obvestilih.
2. Avtor tajnih podatkov te ob njihovem nastanku označi z ustrezno stopnjo tajnosti v skladu z mednarodnimi standardi in opredelitvami iz Priloge I. Avtor praviloma določi tudi naslovnike, ki naj se jim v skladu s stopnjo tajnosti dovoli seznanitev s podatki. Ti podatki se sporočijo oddelku za tajne podatke, ko se dokument deponira pri njem.
3. Drugi zaupni podatki, za katere velja poklicna molčečnost, se obravnavajo v skladu s prilogama I in II ter navodili za ravnanje.

Člen 5

Sprejem zaupnih podatkov v Evropskem parlamentu

1. Zaupni podatki, ki jih prejme Evropski parlament, se sporočijo, kakor je določeno v nadaljevanju:
 - (a) tajni podatki stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje in „drugi zaupni podatki“: sekretariatu parlamentarnega telesa/nosilca funkcije, ki je vložil zahtevo zanje, ali neposredno oddelku za tajne podatke;
 - (b) tajni podatki stopnje CONFIDENTIEL UE/CONFIDENTIAL EU, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje: oddelku za tajne podatke.

2. Registracijo, shranjevanje in sledljivost zaupnih podatkov zagotovita, odvisno od primera, bodisi sekretariat parlamentarnega telesa/nosilca funkcije, ki je prejel podatke, oziroma oddelek za tajne podatke.
3. Če gre za zaupne podatke, ki jih sporoči Komisija v skladu s točko 3.2 Priloge II k Okvirnem sporazumu, ali za tajne podatke, ki jih v skladu s členom 5(4) Medinstitucionalnega sporazuma posreduje Svet, se dogovori, vzpostavljeni z medsebojnim soglasjem za ohranitev zaupnosti podatkov, skupaj z zaupnimi podatki deponirajo pri sekretariatu parlamentarnega telesa/nosilca funkcije ali pri oddelku za tajne podatke, odvisno od primera.
4. Dogovori iz odstavka 3 se lahko smiselno uporabijo tudi za sporočanje zaupnih podatkov s strani drugih institucij, organov, uradov in agencij, ustanovljenih v okviru ali na podlagi Pogodb ali s strani držav članic.
5. Da se zagotovi raven varstva, sorazmerna s stopnjo tajnosti TRÈS SECRET UE/EU TOP SECRET ali enakovredno stopnjo, konferenca predsednikov ustanovi nadzorni odbor. Tajni podatki stopnje TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje se sporočijo Evropskemu parlamentu v skladu z dodatnimi dogovori, o katerih se uskladita Evropski parlament in institucija Unije, ki je podatke sporočila.

Člen 6

Tajni podatki, ki jih Evropski parlament sporoči tretjim osebam

Če je avtor ali institucija Unije, ki je Evropskemu parlamentu sporočila tajne podatke, odvisno od primera, pred tem podala pisno soglasje, lahko Evropski parlament take tajne podatke posreduje tretjim osebam, pod pogojem, da pri obdelavi takih podatkov v njihovih službah in prostorih zagotavljajo spoštovanje pravil, enakovrednih pravilom iz tega sklepa.

Člen 7

Zavarovani prostori

1. Evropski parlament za upravljanje zaupnih podatkov vzpostavi zavarovano območje in zavarovane čitalnice.
2. Zavarovano območje ima zmogljivosti za registracijo, vpogled, arhiviranje, prenos in ravnanje s tajnimi podatki. Sestavljeno je med drugim iz čitalnice in sejne sobe za vpogled v tajne podatke, upravlja pa ga oddelek za tajne podatke.
3. Zavarovane čitalnice je mogoče odpreti tudi zunaj zavarovanega območja, da se omogoči vpogled v tajne podatke stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje, ter v „druge zaupne podatke“. Te zavarovane čitalnice upravljajo pristojne službe sekretariata parlamentarnega telesa/nosilca funkcije ali oddelek za tajne podatke, odvisno od primera. V njih ni fotokopirnih strojev, telefonov, telefaksa, optičnih bralnikov in druge tehnične opreme za razmnoževanje ali posredovanje dokumentov.

Člen 8

Registracija, ravnanje z zaupnimi podatki in njihovo hranjenje

1. Tajni podatki stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje in „drugi zaupni podatki“ se registrirajo in shranijo pri pristojnih službah sekretariata parlamentarnega telesa/nosilca funkcije ali oddelku za tajne podatke, odvisno od tega, kdo je podatke prejel.

2. Za ravnanje s tajnimi podatki stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje in „drugimi zaupnimi podatki“, se uporabljajo naslednji pogoji:

- (a) dokumenti se izročijo osebno vodji sekretariata, ki jih registrira in izda potrdilo o prejemu;
- (b) ko taki dokumenti niso v dejanski uporabi, se hranijo pod ključem, zanje pa odgovarja sekretariat;
- (c) v nobenem primeru teh podatkov ni dovoljeno shraniti na drug nosilec ali jih komur koli posredovati. Take podatke je dovoljeno razmnoževati le z ustrezno akreditirano opremo, kot je določeno v varnostnih obvestilih;
- (d) dostop do teh podatkov je omejen na osebe, ki jih imenuje avtor ali institucija Unije, ki je podatke sporočila Evropskemu parlamentu, v skladu z določbami iz člena 4(2) ali člena 5(3), (4) in (5);
- (e) sekretariat parlamentarnega telesa/nosilca funkcije vodi evidenco oseb, ki so imele vpogled v podatke, ter o datumu in uri takega vpogleda ter evidenco posreduje oddelku za tajne podatke v trenutku, ko so podatki deponirani pri oddelku za tajne podatke.

3. Tajne podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, ali enakovredne stopnje registrira, obdeluje in hrani oddelk za tajne podatke v zavarovanem območju, v skladu s posebno stopnjo tajnosti in kot je to opredeljeno v varnostnih obvestilih.

4. V primeru kršitve pravil, določenih v odstavkih 1 do 3, odgovorni uradnik sekretariata parlamentarnega telesa/nosilca funkcije ali oddelka za tajne podatke, odvisno od primera, o tem obvesti generalnega sekretarja, ki zadevo preda predsedniku, če gre za poslanca Evropskega parlamenta.

Člen 9

Dostop do zavarovanih prostorov

1. Dostop do zavarovanega območja imajo le naslednje osebe:

- (a) osebe, ki jim je v skladu s členom 3(4) do (7) dovoljen vpogled v podatke, ki se tam hranijo, in so vložile prošnjo v skladu s členom 10(1);
- (b) osebe, ki jim je v skladu s členom 4(1) dovoljeno, dé ustvarjajo tajne podatke in so vložile prošnjo v skladu s členom 10(1);
- (c) uradniki Evropskega parlamenta iz oddelka za tajne podatke;
- (d) uradniki Evropskega parlamenta, ki so odgovorni za upravljanje komunikacijskih in informacijskih sistemov;
- (e) uradniki Evropskega parlamenta, odgovorni za varnost in požarno varnost, kadar je potrebno;
- (f) osebje za čiščenje, vendar le v prisotnosti in pod strogim nadzorom uradnika, zaposlenega v oddelku za tajne podatke.

2. Oddelk za tajne podatke lahko nepooblaščenim osebam zavrne dostop do zavarovanega območja. Vsak ugovor zoper tako zavrnitev dostopa se vloži pri predsedniku, če gre za prošnjo za dostop poslanca Evropskega parlamenta, ter pri generalnemu sekretarju v ostalih primerih.

3. Generalni sekretar lahko odobri sestanek za omejeno število oseb v sejni sobi znotraj zavarovanega območja.

4. Dostop do zavarovane čitalnice imajo le naslednje osebe:
- (a) poslanci Evropskega parlamenta, uradniki Evropskega parlamenta in drugi uslužbenci Evropskega parlamenta, ki delajo v političnih skupinah, katerih istovetnost je ustrezno ugotovljena za namene vpogleda v zaupne podatke ali njihovega ustvarjanja;
 - (b) uradniki Evropskega parlamenta, odgovorni za upravljanje komunikacijskih in informacijskih sistemov, uradniki sekretariata parlamentarnega telesa/nosilca funkcije, ki je prejel podatke, in uradniki oddelka za tajne podatke;
 - (c) kadar je potrebno, uradniki Evropskega parlamenta, odgovorni za varnost in požarno varnost;
 - (d) osebje za čiščenje, vendar le v prisotnosti in pod strogim nadzorom uradnika, zaposlenega v sekretariatu parlamentarnega telesa/nosilca funkcije ali oddelka za tajne podatke, odvisno od primera.
5. Pristojni sekretariat parlamentarnega telesa/nosilca funkcije ali oddelka za tajne podatke, odvisno od primera, lahko zavrne dostop do zavarovane čitalnice vsakomur, ki nima dovoljenja za vstop. Vsak ugovor zoper tako zavrnitev dostopa se vloži pri predsedniku, če gre za prošnjo za dostop poslanca Evropskega parlamenta, ter pri generalnemu sekretarju v ostalih primerih.

Člen 10

Vpogled v zaupne podatke ali njihovo ustvarjanje v zavarovanih prostorih

1. Vsaka oseba, ki želi imeti v zavarovanem območju vpogled v zaupne podatke ali jih tam ustvariti, vnaprej sporoči svoje ime oddelku za tajne podatke. Oddelek za tajne podatke preveri istovetnost te osebe ter se prepriča, ali ji je v skladu členom 3(3) do (7), členom 4(1) ali členom 5(3), (4) in (5) dovoljeno vpogledati v zaupne podatke ali njihovo ustvarjanje.
2. Vsaka oseba, ki želi imeti v skladu s členom 3(3) in (7) v zavarovani čitalnici vpogled v zaupne podatke stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje in „druge zaupne podatke“, vnaprej sporoči svoje ime pristojnim službam sekretariata parlamentarnega telesa/nosilca funkcije ali oddelku za tajne podatke.
3. Razen v izjemnih primerih (denimo zaradi številnih zahtev za vpogled, vloženih v kratkem času), se vpogled v zaupne podatke v zavarovanem prostoru naenkrat dovoli samo eni osebi, ob navzočnosti uradnika sekretariata parlamentarnega telesa/nosilca funkcije ali oddelka za tajne podatke.
4. Med vpogledom so stik z zunanjim svetom (vključno z uporabo telefonov in drugih tehnoloških naprav), izdelava zapiskov ter fotokopiranje ali fotografitiranje zaupnih podatkov prepovedani.
5. Preden se osebi dovoli, da zapusti zavarovani prostor, odgovorni uradnik sekretariata parlamentarnega telesa/nosilca funkcije ali oddelka za tajne podatke preveri, da so vsi zaupni podatki, v katere je bilo vpogledano, še vedno na mestu ter da so nedotaknjeni in popolni.
6. V primeru kršitve zgornjih pravil uradnik sekretariata parlamentarnega telesa/nosilca funkcije ali oddelka za tajne podatke o tem obvesti generalnega sekretarja, ki zadevo preda predsedniku, kadar gre za poslanca Evropskega parlamenta.

Člen 11

Minimalni standardi za vpogled v zaupne podatke na sejah za zaprtimi vrati zunaj zavarovanih prostorov

1. Vpogled v tajne podatke stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje in „druge zaupne podatke“ se lahko dovoli parlamentarnim odborom ali drugim političnim in upravnim organom Evropskega parlamenta, kadar se sestanejo za zaprtimi vrati zunaj zavarovanih prostorov.

2. V okoliščinah iz odstavka 1 sekretariat parlamentarnega telesa/nosilca funkcije, ki je odgovoren za sejo, zagotovi, da se spoštujejo naslednji pogoji:

- (a) vstop v sejno sobo se dovoli le osebam, ki jih je predsedujoči pristojnega odbora ali telesa določil, da bodo sodelovale na seji;
- (b) vsi dokumenti so oštevilčeni, razdeljeni na začetku in pobrani na koncu seje, ter o teh dokumentih se ne naredijo zapiski, fotokopije ali fotografije;
- (c) v zapisniku seje se ne omenja vsebina razprave o obravnavanih podatkih. Zapiše se lahko le morebitna odločitev v zvezi s tem;
- (d) za zaupne podatke, ki so prejemnikom v Evropskem parlamentu posredovani ustno, velja enakovredna stopnja varstva kakor za zaupne podatke, posredovane v pisni obliki;
- (e) v sejni sobi ne sme biti dodatnih izvodov dokumentov;
- (f) izvodi dokumentov se razdelijo le v določenem številu udeležencem in tolmačem na začetku seje;
- (g) klasifikacijo/oznako dokumentov na začetku seje pojasni predsedujoči seji;
- (h) udeleženci dokumentov ne odnesejo iz sejne sobe;
- (i) sekretariat parlamentarnega telesa/nosilca funkcije ob koncu seje zbere in prešteje vse izvode dokumentov; ter
- (j) v sejni sobi, v kateri je omogočen vpogled v zaupne podatke ali kjer se o njih razpravlja, niso dovoljene nobene naprave za elektronsko komunikacijo ali druge elektronske naprave;

3. Kadar se na seji za zaprtimi vrati v skladu z izjemami iz točke 3.2.2 Priloge II k Okvirnemu sporazumu in iz člena 6(5) Medinstitucionalnega sporazuma razpravlja o tajnih podatkih stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali enakovredne stopnje, sekretariat parlamentarnega telesa/nosilca funkcije, ki je odgovoren za sejo, poleg zagotavljanja spoštovanja določb iz odstavka 2 zagotovi tudi, da osebe, določene, da sodelujejo na seji, izpolnjujejo zahteve iz člena 3(4) in (7).

4. V primeru iz odstavka 3 oddelek za tajne podatke sekretariatu parlamentarnega telesa/nosilca funkcije, odgovornemu za sejo za zaprtimi vrati, zagotovi določeno število izvodov dokumentov, o katerih se bo razpravljalo, ki jih je treba po seji vrniti oddelku za tajne podatke.

Člen 12

Arhiviranje zaupnih podatkov

1. V zavarovanem območju so na voljo varni prostori za arhiviranje. Oddelek za tajne podatke je odgovoren za upravljanje varnih arhivov v skladu s standardnimi merili za arhiviranje.

2. Tajni podatki, ki so dokončno deponirani pri oddelku za tajne podatke, in tajni podatki stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje, ki so deponirani pri sekretariatu parlamentarnega telesa/nosilca funkcije, se premeštujejo v varni arhiv v zavarovanem območju šest mesecev zatem, ko je bilo vanje zadnjič vpogledano, in najpozneje eno leto zatem, ko so bili deponirani. „Drugi zaupni podatki“ se arhivirajo, razen če so bili deponirani pri oddelku za tajne podatke, pri sekretariatu zadevnega parlamentarnega telesa/nosilca funkcije v skladu s splošnimi pravili o upravljanju dokumentov.

3. V zaupne podatke, ki se hranijo v varnih arhivih, je mogoče vpogledati pod naslednjimi pogoji:
 - (a) le osebam, ki so z imenom, funkcijo ali položajem opredeljene v spremljevalnem dokumentu, sestavljenem, ko so bili zaupni podatki deponirani, se dovoli, da vpogledajo v te podatke;
 - (b) vlogo za vpogled v zaupne podatke se predloži oddelku za tajne podatke, ki zadevne dokumente prenese v zavarovano čitalnico; ter
 - (c) uporabljajo se postopki in pogoji iz člena 10, ki urejajo vpogled v zaupne podatke.

Člen 13

Zniževanje stopenj tajnosti, odprava tajnosti in odstranitev oznak zaupnih podatkov

1. Stopnja tajnosti zaupnih podatkov se lahko zniža oziroma tajnost odpravi ali oznaka odstrani le z dovoljenjem avtorja in, če je to potrebno, po posvetovanju z drugimi zainteresiranimi stranmi.
2. Zniževanje stopenj tajnosti oziroma odprava tajnosti se potrdi pisno. Avtor je dolžen o spremembi obvestiti svoje naslovnike, ti pa so dolžni o tej spremembi obvestiti vse nadaljnje naslovnike, ki so jim poslali dokument ali njegovo kopijo. Če je mogoče, avtorji na tajnem dokumentu določijo datum, obdobje ali dogodek, ko se vsebini lahko zniža stopnja tajnosti oziroma tajnost odpravi. V nasprotnem primeru avtorji preverjajo dokumente najpozneje vsakih pet let, da se zagotovi, da je izvirna stopnja tajnosti potrebna.
3. Zaupni podatki v varnih arhivih se preučijo v razumnem času in najpozneje v 25. letu od njihovega nastanka, da se sprejme odločitev o znižanju stopnje njihove tajnosti, odpravi tajnosti in odstranitvi oznak. Pregled in objava teh podatkov potekata v skladu z določbami Uredbe 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 ⁽¹⁾. Odpravo tajnosti opravi avtor tajnih podatkov ali služba, takrat odgovorna za to, v skladu z oddelkom 10 dela 1 Priloge I.
4. Po odpravi tajnosti se podatki, ki so bili prej določeni za tajne in se hranijo v varnem arhivu, prenesejo v zgodovinski arhiv Evropskega parlamenta za trajno hrambo in nadaljnjo obdelavo v skladu z veljavnimi pravili.
5. Po odstranitvi oznake za nekdanje „druge zaupne podatke“ veljajo pravila Evropskega parlamenta o upravljanju dokumentov.

Člen 14

Kršitve varnosti, izguba ali ogrožanje zaupnih podatkov

1. Kršitev tajnosti na splošno, zlasti pa tega sklepa, v primeru poslancev Evropskega parlamenta pomeni uporabo ustreznih kazenskih določb iz Poslovnika Evropskega parlamenta.
2. Kršitev, ki jo storijo zaposleni v Evropskem parlamentu, vodi k uporabi postopkov in kazni iz Kadrovskih predpisov za uradnike Evropskih skupnosti oziroma Pogojev za zaposlitev drugih uslužbencev Evropske unije, določenih v Uredbi (EGS, Euratom, ESPJ) št. 259/68 ⁽²⁾ (Kadrovski predpisi).

⁽¹⁾ UL L 43, 15.2.1983, str. 1.

⁽²⁾ UL L 56, 4.3.1968, str. 1.

3. Predsednik in/ali generalni sekretar, odvisno od primera, organizirata potrebne preiskave v primeru kršitve, kot je opredeljeno v varnostnem obvestilu 6.
4. Če je zaupne podatke Evropskemu parlamentu sporočila druga institucija unije ali država članica, predsednik in/ali generalni sekretar, odvisno od primera, zadevno institucijo unije ali državo članico obvesti o vseh dokazanih ali domnevnih izgubah ali ogrožanju tajnih podatkov ter o izidu preiskave in ukrepih, sprejetih za preprečitev njihove ponovitve.

Člen 15

Prilagoditev tega sklepa in njegovih izvedbenih določb ter letno poročanje o uporabi tega sklepa

1. Generalni sekretar predlaga vse potrebne prilagoditve tega sklepa in prilog o njegovem izvajanju ter te predloge posreduje predsedstvu v odločanje.
2. Generalni sekretar je odgovoren za izvajanje tega sklepa v službah Evropskega parlamenta in izda navodila o ravnanju o zadevah, ki jih zajema sistem za upravljanje varnosti podatkov, v skladu z načeli iz tega sklepa.
3. Generalni sekretar predsedstvu predloži letno poročilo o uporabi tega sklepa.

Člen 16

Prehodne in končne določbe

1. Netajni podatki, ki se hranijo v oddelku za tajne podatke ali v katerem drugem arhivu Evropskega parlamenta in veljajo za zaupne, z datumom pred 1. aprila 2014, se za namene tega sklepa štejejo za „druge zaupne podatke“. Avtor lahko kadar koli ponovno preuči stopnjo njihove zaupnosti.
2. Z odstopanjem od točke (a) člena 5(1) in člena 8(1) tega sklepa za obdobje dvanajstih mesecev od 1. aprila 2014 velja, da se podatki, ki jih posreduje Svet v skladu z Medinstitucionalnim sporazumom in so tajni stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje deponirajo, registrirajo in shranijo v oddelku za tajne podatke. Vpogled v take podatke je dovoljen v skladu s točkama (a) in (c) člena 4(2) in s členom 5(4) Medinstitucionalnega sporazuma.
3. Sklep predsedstva z dne 6. junija 2011 o pravilniku o obdelavi zaupnih podatkov s strani Evropskega parlamenta se razveljavi.

Člen 17

Začetek veljavnosti

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

PRILOGA I

Del 1

TEMELJNA NAČELA IN MINIMALNI VARNOSTNI STANDARDI ZA VARSTVO ZAUPNIH PODATKOV

1. UVOD

Te določbe določajo temeljna načela in minimalne varnostne standarde za varstvo zaupnih podatkov, ki jih je treba spoštovati in/ali upoštevati v vseh krajih dela Evropskega parlamenta, upoštevati pa jih morajo tudi vsi prejemniki tajnih podatkov in „drugih zaupnih podatkov“, tako da je varnost zagotovljena in da je vsakdo lahko prepričan, da je vzpostavljen skupni standard varstva. Te določbe dopolnjujejo varnostna obvestila iz Priloge II in drugi predpisi o obdelavi zaupnih podatkov s strani parlamentarnih odborov in drugih parlamentarnih teles/nosilcev funkcij.

2. TEMELJNA NAČELA

Varnostna politika Evropskega parlamenta tvori sestavni del splošne notranje politike upravljanja, zato temelji na načelih, ki urejajo njegovo splošno politiko. To so med drugim načela zakonitosti, preglednosti, odgovornosti ter subsidiarnosti in sorazmernosti.

Zakonitost pri izvrševanju varnostnih funkcij predstavlja potrebo po doslednem delovanju v okviru pravnega sistema in po spoštovanju ustreznih pravnih zahtev. Poleg tega morajo pristojnosti na področju varnosti temeljiti na ustreznih pravnih predpisih. Določbe Kadrovskih predpisov se uporabljajo v celoti, zlasti člen 17 o dolžnosti osebja, da se vzdrži vsakega nedovoljenega razkritja podatkov, ki jih prejme v okviru službenih dolžnosti, ter Naslov VI o disciplinskih ukrepih. Prav tako se kršitve varnosti v okviru pristojnosti Evropskega parlamenta obravnavajo na način, ki je v skladu z njegovim poslovníkom in politikó o disciplinskih ukrepih.

Preglednost predstavlja potrebo po jasnosti vseh varnostnih predpisov in določb, po vzpostavitvi ravnotežja med različnimi službami in različnimi področji (fizična varnost v primerjavi z varstvom podatkov itd.) in po dosledni in strukturirani politiki ozaveščanja na področju varnosti. Obstaja tudi potreba po jasnih pisnih smernicah za izvajanje varnostnih ukrepov.

Odgovornost pomeni, da morajo biti pristojnosti na področju varnosti jasno določene. Poleg tega predstavlja potrebo po rednem preverjanju, ali se te pristojnosti pravilno izvajajo.

Subsidiarnost pomeni, da mora biti varnost zagotovljena na najnižji možni ravni in kolikor mogoče blizu generalnih direktorátov in služb Evropskega parlamenta.

Sorazmernost pomeni, da morajo biti varnostne dejavnosti strogo omejene na najnujnejše in da morajo biti varnostni ukrepi sorazmerni z interesi, ki jih je treba varovati, pa tudi z dejanskim ali morebitnim ogrožanjem teh interesov, z namenom omogočiti zaščito teh interesov na način, ki povzroča najmanj motenj.

3. TEMELJI VARNOSTI PODATKOV

Temelji zanesljive varnosti podatkov so:

- (a) primerni komunikacijski in informacijski sistemi. Ti sistemi spadajo v odgovornost varnostnega organa Evropskega parlamenta (kot je opredeljen v varnostnem obvestilu 1);
- (b) v Evropskem parlamentu, organ za zagotavljanje varnosti podatkov (kot je opredeljen v varnostnem obvestilu 1), ki je pristojen za to, da v sodelovanju z zadevnim varnostnim organom zagotavlja podatke in nasvete o nevarnostih tehničnega značaja za komunikacijske in informacijske sisteme ter sredstvih za zaščito pred temi nevarnostmi;
- (c) tesno sodelovanje med pristojnimi službami Evropskega parlamenta in varnostnimi službami drugih institucij unije.

4. NAČELA VAROVANJA PODATKOV

4.1. Cilji

Glavni cilji varovanja podatkov so naslednji:

- (a) varovanje zaupnih podatkov pred vohunstvom, ogrožanjem ali nepooblaščenim razkritjem;
- (b) varovanje tajnih podatkov, s katerimi se upravlja v komunikacijskih in informacijskih sistemih ter omrežjih, pred ogrožanjem njihove tajnosti, celovitosti in razpoložljivosti;
- (c) varovanje prostorov Evropskega parlamenta, v katerih se nahajajo tajni podatki, pred sabotžo in zlonamernimi naklepnimi poškodbami;
- (d) v primeru varnostne napake ocena povzročene škode, omejitev njenih posledic, izvedba varnostnih preiskav ter sprejetje morebitnih potrebnih korektivnih ukrepov.

4.2. Določitev stopnje tajnosti

4.2.1. Na področju zaupnosti so pri izboru podatkov in gradiva, ki ga je treba zavarovati, in pri oceni zahtevane stopnje varstva potrebni skrben pristop in izkušnje. Bistvenega pomena je, da bi morala stopnja varstva ustrezati občutljivosti v zvezi z varnostjo posameznega podatka in gradiva, ki ga je treba zavarovati. Da bi zagotovili nemoten pretok podatkov, se izogne določitvi previsoke ali prenizke stopnje tajnosti.

4.2.2. Sistem določanja stopnje tajnosti je instrument za uveljavitev načel iz tega oddelka. Pri načrtovanju in organiziranju metod za boj proti vohunstvu, sabotžam, terorizmu in drugim nevarnostim se upošteva podoben sistem določanja stopenj tajnosti, tako da se za najpomembnejše prostore, v katerih so shranjeni tajni podatki, in najboljčutljivejše točke znotraj teh prostorov zagotovi najvišja raven varovanja.

4.2.3. Za določanje stopnje tajnosti podatkov je odgovoren izključno avtor zadevnih podatkov.

4.2.4. Stopnja tajnosti sme temeljiti izključno na vsebini zadevnih podatkov.

4.2.5. Kadar so različni podatki povezani v celoto, je njihova stopnja tajnosti najmanj enaka najvišji stopnji, določeni za posamezni del. Lahko pa se zbirki podatkov dodeli višja stopnja tajnosti kot njenim sestavnim delom.

4.2.6. Stopnja tajnosti se določi le po potrebi in le za tako dolgo, kot je potrebno.

4.3. Cilji varnostnih ukrepov

Varnostni ukrepi:

- (a) veljajo za vse osebe, ki imajo dostop do tajnih podatkov, nosilcev tajnih podatkov in drugih zaupnih podatkov, kakor tudi vseh prostorov, v katerih so taki podatki, ter pomembnih objektov;
- (b) so načrtovani tako, da omogočajo odkrivanje oseb, ki bi s svojim položajem (v smislu dostopa, povezav ali drugače) lahko ogrozile varnost takih podatkov in pomembnih objektov, v katerih se taki podatki nahajajo, in zagotavljajo njihovo izključitev ali odstranitev;

- (c) preprečujejo nepooblaščenim osebam dostop do teh podatkov ali objektov, ki jih vsebujejo,
- (d) zagotavljajo, da se taki podatki razširjajo samo na podlagi načela potrebe po seznanitvi, ki je temeljno glede vseh vidikov varnosti,
- (e) zagotavljajo celovitost (s preprečevanjem ponarejanja, nedovoljenega spreminjanja ali nedovoljenega izbrisa) in razpoložljivost (za tiste, ki potrebujejo dovoljenje za dostop do podatkov) zaupnih podatkov, zlasti kadar so podatki shranjeni ali obdelani v elektromagnetni obliki oziroma se v taki obliki prenašajo.

5. SKUPNI MINIMALNI STANDARDI

Evropski parlament zagotovi, da vsi prejemniki tajnih podatkov upoštevajo skupne minimalne standarde varnosti, tako znotraj institucije kot v okviru njenih pristojnosti, namreč vse njegove službe in pogodbeni sodelavci, tako da se ti podatki lahko posredujejo v prepričanju, da se bo z njimi povsod ravnilo enako skrbno. Minimalni standardi vključujejo merila za pridobitev varnostnih odobritev za uradnike Evropskega parlamenta in druge uslužbence Parlamenta, ki delajo v političnih skupinah, in postopke za varstvo zaupnih podatkov.

Evropski parlament dovoli dostop do teh podatkov tretjim osebam le, če te tretje osebe zagotovijo, da bodo pri roko-
vanju ravnale v skladu z določbami, ki so vsaj tako stroge kot navedeni minimalni standardi.

Taki skupni minimalni standardi se uporabljajo tudi, kadar Evropski parlament na podlagi pogodbe ali donacije industrijskim ali drugim organom dodeli naloge, ki vključujejo zaupne podatke.

6. VARNOST KAR ZADEVA URADNIKE EVROPSKEGA PARLAMENTA IN DRUGE USLUŽBENCE PARLAMENTA, KI DELAJO V POLITIČNIH SKUPINAH

6.1. *Varnostni napotki kar zadeva uradnike Evropskega parlamenta in druge uslužbence Parlamenta, ki delajo v političnih skupinah*

Uradnikom Evropskega parlamenta in drugim uslužbencem Parlamenta, ki delajo v političnih skupinah, na delovnih mestih, kjer bi utegnili imeti dostop do tajnih podatkov, je treba ob začetku izvajanja nalog in v rednih časovnih presledkih dati podrobna navodila v zvezi s potrebo po varnosti in s postopki za njeno doseganje. Od teh oseb se zahteva, da pisno potrdijo, da so prebrali ustrezne predpise o varnosti in jih v celoti razumejo.

6.2. *Odgovornosti vodstvenega osebja*

Del nalog vodstvenega osebja mora biti, da so seznanjeni s tem, kateri podrejeni imajo pri svojem delu opravka s tajnimi podatki oziroma imajo dostop do zavarovanih komunikacijskih ali informacijskih sistemov, ter da evidentirajo in poročajo o vseh izrednih dogodkih ali očitnih ranljivostih, ki bi lahko imeli posledice za varnost.

6.3. *Varnostni status uradnikov Evropskega parlamenta in drugih uslužbencev Parlamenta, ki delajo v političnih skupinah*

Uvedejo se postopki, s katerimi se zagotovi, da se v primeru, ko se o uradniku Evropskega parlamenta ali drugem uslužbencu Parlamenta, ki dela v politični skupini, odkrijejo dejstva negativne narave, ugotovi, ali ima ta pri svojem delu opravka s tajnimi podatki in ali ima dostop do zavarovanih komunikacijskih ali informacijskih sistemov, in da se o tem obvesti pristojna služba Evropskega parlamenta. Če pristojni nacionalni varnostni organ ugotovi, da tak posameznik predstavlja varnostno tveganje, se mu prepreči opravljanje nalog, kjer bi lahko škodoval interesom varnosti, oziroma se ga od njihovega opravljanja odstrani.

7. FIZIČNO VAROVANJE

„Fizično varovanje“ pomeni uporabo fizičnih in tehničnih zaščitnih ukrepov za preprečevanje nepooblaščenega dostopa do tajnih podatkov.

7.1. *Potreba po varovanju*

Stopnja ukrepov fizičnega varovanja, ki se uporabljajo za zagotavljanje varstva tajnih podatkov, je sorazmerna z določitvijo stopnje tajnosti, obsegom in ogroženostjo predmetnih podatkov in gradiva. Vsi imetniki **tajnih podatkov** v zvezi s stopnjo tajnosti teh podatkov upoštevajo enotno prakso in morajo ravnati v skladu s skupnimi standardi varstva glede hrambe, prenosa ter uničenja podatkov in gradiva, ki zahtevajo varstvo.

7.2. *Preverjanje*

Osebe, ki so zadolžene za nadzor tajnih podatkov, pred odhodom s področij, kjer se tajni podatki nahajajo brez nadzora, zagotovijo, da so ti varno shranjeni in da so aktivirane vse varnostne naprave (ključavnice, alarmi itd.). Zunaj delovnega časa se izvajajo dodatna neodvisna preverjanja.

7.3. *Varnost zgradb*

Zgradbe, v katerih se nahajajo tajni podatki ali varni komunikacijski in informacijski sistemi, se zavarujejo pred dostopom nepooblaščenih oseb.

Vrsta varovanja tajnih podatkov, npr. rešetke na oknih, vratne ključavnice/zapahi, vhodna straža, samodejni sistemi nadzora dostopa, varnostna preverjanja in obhodne patrulje, alarmni sistemi, sistemi odkrivanja dejavnosti nepooblaščenih oseb in psi čuvaji, je odvisna od:

- (a) stopnje tajnosti, obsega varovanih podatkov in gradiva ter njihove lokacije v zgradbi;
- (b) kakovosti varnostnih vsebnikov za hranjenje predmetnih podatkov in gradiva ter
- (c) fizičnih značilnosti in lokacije zgradbe.

Vrsta varstva komunikacijskih in informacijskih sistemov je odvisna od ocene vrednosti predmetnega premoženja in morebitne škode, ki bi lahko nastala v primeru ogrožene varnosti, od fizičnih značilnosti in lokacije zgradbe, v kateri se sistem nahaja, ter od lokacije sistema znotraj zgradbe.

7.4. *Načrti ukrepanja ob izrednih razmerah*

Vnaprej se pripravijo podrobni načrti za zagotovitev varstva zaupnih podatkov v primeru izrednih razmer.

8. VARNOSTNI OZNAČEVALNIKI, OZNAKE, NAMESTITEV IN UPRAVLJANJE S STOPNJAMI TAJNOSTI

8.1. *Varnostni označevalniki*

Dovoljene so le stopnje tajnosti, opredeljene v točki (d) člena 2 tega sklepa.

Da bi se določile omejitve veljavnosti stopenj tajnosti (to za tajne podatke pomeni samodejno znižanje stopnje tajnosti oziroma odpravo tajnosti), se lahko uporabi dogovorjen varnostni označevalnik.

Varnostni označevalniki se uporabljajo le skupaj s stopnjo tajnosti.

Podrobnejše določbe glede varnostnih označevalnikov so v varnostnem obvestilu 2, njihova opredelitev pa v navodilih za ravnanje.

8.2. *Oznake*

Oznaka se uporabi za določitev vnaprej opredeljenih posebnih navodil v zvezi z ravnanjem z zaupnimi podatki. Z oznako se lahko tudi opredeli področje, ki ga pokriva določeni dokument, ali pošiljanje na podlagi „potrebe po seznanitvi“ ali (pri podatkih, ki niso tajni) označi konec embarga.

Oznaka ni stopnja tajnosti in se ne **uporablja** namesto nje.

Podrobnejše določbe glede oznak so v varnostnem obvestilu 2, njihova opredelitev pa v navodilih za ravnanje.

8.3. *Namestitev stopnje tajnosti in varnostnih označevalnikov*

Stopnja tajnosti in varnostni označevalniki se namestijo v skladu z razdelkom E varnostnega obvestila 2 in navodili za ravnanje.

8.4. *Upravljanje s stopnjami tajnosti podatkov*

8.4.1 *Splošno*

Podatki se določijo kot tajni le, če je to potrebno. Stopnja tajnosti se jasno in pravilno označi ter se ohrani le, dokler je za podatke potrebno varstvo.

Za določitev stopnje tajnosti podatkov ter vsako nadaljnje znižanje stopnje tajnosti oziroma odpravo tajnosti je odgovoren izključno avtor.

Uradniki Evropskega parlamenta določajo stopnjo tajnosti podatkov, jo znižujejo ali odpravljajo tajnost na podlagi napotkov ali pooblastila generalnega sekretarja.

Podrobni postopki za obdelavo tajnih dokumentov so določeni tako, da tem dokumentom zagotavljajo varstvo, ustrezno podatkom, ki jih vsebujejo.

Število oseb, pooblaščenih za izdajanje tajnih podatkov stopnje TRÈS SECRET UE/EU TOP SECRET, mora ostati čim nižje, njihova imena pa se navedejo na seznamu, ki ga pripravi oddelek za tajne podatke.

8.4.2 *Uporaba stopnje tajnosti*

Stopnja tajnosti dokumenta se določi glede na stopnjo občutljivosti njegove vsebine v skladu z opredelitvijo iz točke (d) člena 2. Pomembno je, da se stopnja tajnosti dodeljuje pravilno in uporablja preudarno.

Stopnja tajnosti pisma ali zabeležke, ki vsebuje priloge, je najmanj enaka najvišji stopnji tajnosti, določeni posameznim priloženim delom. Avtor jasno določi stopnjo tajnosti za primer, ko sta pismo ali zabeležka ločena od priloženih delov.

Pri stopnji tajnosti dokumenta njegov avtor upošteva zgoraj navedena pravila in se izogiba določitvi previsoke ali prenizke stopnje tajnosti.

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

9. INŠPEKCIJSKI PREGLEDI

Direktorat Evropskega parlamenta za varnost in oceno tveganja opravlja redne notranje inšpekcijske preglede varnostne ureditve za varstvo tajnih podatkov, pri tem pa lahko za pomoč zaprosi varnostne organe Sveta ali Komisije.

Varnostni organi in pristojne službe institucij Unije lahko v okviru dogovorjenega postopka na pobudo katere koli strani opravijo medsebojne preglede varnostne ureditve za varstvo zaupnih podatkov, ki jih izmenjujejo v okviru ustreznih medinstitucionalnih sporazumov.

10. POSTOPKA ODPRAVE TAJNOSTI IN ODSTRANITVE OZNAKE

10.1. Oddelek za tajne podatke preuči tajne podatke v svojem registru in najpozneje 25. leto od nastanka dokumenta, njegovega avtorja zaprosi za privolitev k odpravi tajnosti ali odstranitvi oznake. Dokumenti, pri katerih se tajnost ne odpravi ali se oznaka ne odstrani ob prvem pregledu, se periodično pregledujejo najmanj vsakih pet let. Poleg dokumentov, ki so že v varnih arhivih v zavarovanem območju in so razvrščeni v ustrezno stopnjo tajnosti, lahko postopek odstranitve oznake zajema tudi druge zaupne podatke, ki obstajajo bodisi v službi ali organu Parlamenta bodisi v službi, ki skrbi za zgodovinske arhive Parlamenta.

10.2. Odločitev glede odprave tajnosti ali odstranitve oznake dokumenta praviloma sprejme avtor sam ali izjemoma v sodelovanju s parlamentarnim telesom/nosilcem funkcije, ki poseduje take podatke, in sicer preden se podatki iz tega dokumenta posredujejo službi, ki skrbi za zgodovinske arhive Parlamenta. Za tajne podatke se tajnost lahko odpravi ali odstrani oznaka zgolj po predhodni pisni privolitvi avtorja. V primeru „drugih zaupnih podatkov“ sekretariat parlamentarnega telesa/nosilca funkcije, ki poseduje take podatke, v sodelovanju z avtorjem odloči, ali se lahko dokumentu odstrani oznaka.

10.3. Oddelek za tajne podatke je zadolžen, da v imenu avtorja o spremembi stopnje ali oznake tajnosti obvesti naslovnike dokumenta, naslovniki pa so zadolženi, da obvestijo vse nadaljnje naslovnike, ki so jim poslali dokument ali njegovo kopijo.

10.4. Odprava tajnosti ne vpliva na varnostne označevalnike ali oznake, ki utegnejo biti nameščeni na dokumentu.

10.5. V primeru odprave tajnosti se prvotna stopnja tajnosti na vrhu in dnu vsake strani prečrta. Prva (naslovna) stran dokumenta se ožigosa in izpolni s podatki Oddelka za tajne podatke. V primeru odstranitve oznake se prvotna oznaka na vrhu vsake strani prečrta.

10.6. Besedilo dokumenta z odpravljenjo tajnostjo ali odstranjenjo oznako se priloži elektronski podatkovni kartici ali enakovrednemu sistemu, v katerem je bil dokument registriran.

10.7. Za dokumente, za katere veljajo izjeme v zvezi z zasebnostjo ali integriteto posameznika oziroma s poslovnimi interesi, ter za dokumente občutljive narave se uporabljajo določbe iz člena 2 Uredbe (EGS, Euratom) št. 354/83.

10.8. Poleg navedenih določb iz točk 10.1 do 10.7 se uporablja naslednje:

- (a) kadar gre za dokumente tretjih oseb, se Oddelek za tajne podatke posvetuje z njimi, preden nadaljuje z odpravo tajnosti ali odstranitvijo oznake;
- (b) kadar gre za izjeme v zvezi z varovanjem zasebnosti in integritete posameznika, se pri postopku odprave tajnosti ali odstranitve oznake upošteva zlasti soglasje zadevne osebe ali, če gre za tak primer, dejstvo, da ni mogoče ugotoviti istovetnosti zadevne osebe;
- (c) kadar gre za izjeme v zvezi s poslovnimi interesi fizične ali pravne osebe, se informacije o zadevni osebi lahko objavijo v *Uradnem listu Evropske unije* in določi rok štirih tednov od te objave za predložitev morebitnih pripomb.

Del 2

POSTOPEK PRIDOBITVE VARNOSTNE ODOBREDITVE

11. POSTOPEK PRIDOBITVE VARNOSTNE ODOBREDITVE ZA POSLANCE EVROPSKEGA PARLAMENTA

11.1. Za dostop do tajnih podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali enakovredne stopnje imajo poslanci Evropskega parlamenta dovoljenje bodisi v skladu s postopkom iz točk 11.3 in 11.4 te priloge bodisi na podlagi častne izjave o nerazkritju v skladu s členom 3(4) tega Sklepa.

11.2 Za dostop do tajnih podatkov stopnje SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje imajo poslanci Evropskega parlamenta dovoljenje v skladu s postopkom iz točk 11.3 in 11.14.

11.3. Dovoljenje se izda samo poslancem Evropskega parlamenta, za katere so pristojni varnostni organi držav članic opravili varnostno preverjanje v skladu s postopkom iz točk 11.9 do 11.14. Predsednik je pristojen za izdajo dovoljenj poslancem.

11.4 Predsednik lahko izda pisno dovoljenje, potem ko pridobi mnenje pristojnih organov države članice na podlagi varnostnega preverjanja, opravljenega v skladu s točkami 11.8 do 11.13.

11.5. Direktorat Evropskega parlamenta za varnost in oceno tveganja vodi posodobljen seznam vseh poslancev Evropskega parlamenta, ki jim je bilo izdano dovoljenje, vključno z začasnim dovoljenjem v smislu točke 11.15.

11.6. Dovoljenje velja za obdobje pet let ali za čas trajanja nalog, na podlagi katerih je bilo izdano, če je ta krajši. Dovoljenje je mogoče obnoviti v skladu s postopkom iz točke 11.4.

11.7. Če predsednik meni, da ima upravičene razloge za odvzem dovoljenja, lahko to stori. Vsaka odločitev o odvzemu dovoljenja se sporoči zadevnemu poslancu Evropskega parlamenta, ki lahko zahteva zaslišanje pred predsednikom, preden odvzem začne veljati, in pristojnemu nacionalnemu organu.

11.8. Varnostno preverjanje se opravi s sodelovanjem zadevnega poslanca Evropskega parlamenta in na zahtevo predsednika. Za preverjanje je pristojen nacionalni organ države članice, katere državljan je zadevni poslanec.

11.9. Kot del postopka preverjanja mora zadevni poslanec Evropskega parlamenta izpolniti obrazec z osebnimi podatki.

11.10. Predsednik v svoji zahtevi pristojnim nacionalnim organom navede stopnjo tajnosti podatkov, ki naj bi bili na voljo zadevnemu poslancu Evropskega parlamenta, da ti lahko opravijo varnostno preverjanje.

11.11. Celotni postopek varnostnega preverjanja, ki ga opravijo pristojni nacionalni organi, in dobljeni rezultati so v skladu z relevantnimi predpisi, ki veljajo v zadevni državi članici, vključno s tistimi v zvezi s pritožbami.

11.12. Kadar pristojni nacionalni organ poda pozitivno mnenje, lahko predsednik zadevnemu poslancu Evropskega parlamenta izda ustrezno dovoljenje.

11.13. Kadar pristojni nacionalni organi podajo negativno mnenje, se o tem obvesti zadevnega poslanca Evropskega parlamenta, ki lahko zaprosi predsednika za zaslišanje. Če predsednik meni, da je to potrebno, lahko zaprosi pristojne nacionalne organe za dodatna pojasnila. V primeru potrditve negativnega mnenja se dovoljenje ne izda.

11.14. Vsi poslanci Evropskega parlamenta, ki jim je bilo izdano dovoljenje v smislu točke 11.3, ob njegovi izdaji in zatem v rednih presledkih prejemajo vse potrebne smernice o varstvu tajnih podatkov in sredstvih za zagotavljanje varstva. Ti poslanci podpišejo izjavo, v kateri potrdijo, da so navedene smernice prejeli.

11.15. V izjemnih okoliščinah lahko predsednik, medtem ko čaka na izid varnostnega preverjanja iz točke 11.11 ter potem, ko je uradno obvestil pristojne organe in od njih v roku enega meseca ni dobil odgovora, poslancu izda začasno dovoljenje za obdobje, ki ne presega šest mesecev. Tako podeljena začasna pooblastila ne omogočajo dostopa do tajnih podatkov stopnje TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje.

12. POSTOPEK PRIDOBITVE VARNOSTNE ODOBRITEVE ZA URADNIKE EVROPSKEGA PARLAMENTA IN DRUGE USLUŽBENCE PARLAMENTA, KI DELAJO V POLITIČNIH SKUPINAH

12.1. Pravico dostopa do tajnih podatkov imajo lahko samo uradniki Evropskega parlamenta in drugi uslužbenci Parlamenta, ki delajo v političnih skupinah, ki morajo zaradi opravljanja svojih nalog in izpolnjevanja zahtev službe poznati ali uporabljati take podatke.

12.2. Za dostop do tajnih podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje morajo imeti zadevni uradniki Evropskega parlamenta in drugi uslužbenci Parlamenta, ki delajo v političnih skupinah, dovoljenje v skladu s postopkom iz točk 12.3 in 12.4.

12.3. Dovoljenje se izda samo osebam iz točke 12.1, za katere so pristojni varnostni organi držav članic opravili varnostno preverjanje v skladu s postopkom iz točk 12.9 do 12.14. Generalni sekretar je pristojen za izdajo dovoljenja uradnikom Evropskega parlamenta in drugim uslužbencem Parlamenta, ki delajo v političnih skupinah.

12.4. Generalni sekretar lahko izda pisno dovoljenje, potem ko pridobi mnenje pristojnih organov držav članic na podlagi varnostnega preverjanja, opravljenega v skladu s točkami 12.8 do 12.13.

12.5. Direktorat Evropskega Parlamenta za varnost in oceno tveganja vodi posodobljen seznam vseh delovnih mest, za katera se zahteva varnostna odobritev, ki jo zagotovijo ustrezne službe Evropskega parlamenta, in vseh oseb, ki jim je bilo izdano dovoljenje, vključno z začasnim v smislu točke 12.15.

12.6. Dovoljenje velja za obdobje pet let ali za čas trajanja nalog, na podlagi katerih je bilo izdano, če je ta krajši. Dovoljenje je mogoče obnoviti v skladu s postopkom iz točke 12.4.

12.7. Če generalni sekretar meni, da ima upravičene razloge za odvzem dovoljenja, lahko to stori. Vsaka odločitev o njegovem odvzemu se sporoči zadevnemu uradniku Evropskega parlamenta ali drugemu uslužbencu Parlamenta, ki dela v politični skupini, ki lahko zahteva zaslišanje pred generalnim sekretarjem, preden odvzem začne veljati, in pristojnemu nacionalnemu organu.

12.8. Varnostno preverjanje se opravi s sodelovanjem zadevnega uradnika Evropskega parlamenta ali drugega uslužbenca Parlamenta, ki dela v politični skupini, in na zahtevo generalnega sekretarja. Za preverjanje je pristojen nacionalni organ države članice, katere državljanstvo ima zadevna oseba. Če nacionalna zakonodaja in predpisi to omogočajo, pristojni nacionalni organi opravijo preiskavo v zvezi z osebami, ki niso državljani, ki potrebujejo dostop do tajnih podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET.

12.9. Kot del postopka preverjanja mora zadevni uradnik Evropskega parlamenta ali drugi uslužbenec Parlamenta, ki dela v politični skupini, izpolniti obrazec z osebnimi podatki.

12.10. Generalni sekretar v svoji zahtevi pristojnim nacionalnim organom navede vrsto in stopnjo tajnosti podatkov, ki naj bi bili na voljo zadevnemu uradniku Evropskega parlamenta ali drugemu uslužbencu Parlamenta, ki dela v politični skupini, da lahko pristojni nacionalni organi opravijo varnostno preverjanje in podajo mnenje o stopnji dovoljenja, ki bi ga bilo primerno izdati tej osebi.

12.11. Celotni postopek varnostnega preverjanja, ki ga opravijo pristojni nacionalni organi, in dobljeni rezultati so v skladu z relevantnimi predpisi, ki veljajo v zadevni državi članici, vključno s tistimi v zvezi s pritožbami.

12.12. Kadar pristojni nacionalni organ poda pozitivno mnenje, lahko generalni sekretar zadevnemu uradniku Evropskega parlamenta ali drugemu uslužbencu Parlamenta, ki dela v politični skupini, izda ustrezno dovoljenje.

12.13. Kadar pristojni nacionalni organ poda negativno mnenje, se o tem obvesti zadevnega uradnika Evropskega parlamenta oziroma drugega uslužbenca Parlamenta, ki dela v politični skupini, ki lahko zaprosi generalnega sekretarja za zaslišanje. Če generalni sekretar meni, da je to potrebno, lahko zaprosi pristojni nacionalni organ za dodatna pojasnila. V primeru potrditve negativnega mnenja se dovoljenje ne izda.

12.14. Vsi uradniki Evropskega parlamenta in drugi uslužbenci Parlamenta, ki delajo v političnih skupinah, ki jim je bilo izdano dovoljenje v smislu točk 12.4 in 12.5, ob izdaji pooblastila in zatem v rednih presledkih prejemajo vse potrebne napotke glede varstva tajnih podatkov in o sredstvih za zagotavljanje varstva. Ti uradniki in uslužbenci podpišejo izjavo, v kateri potrdijo prejem teh napotkov ter se zavežejo, da jih bodo spoštovali.

12.15. V izjemnih okoliščinah lahko generalni sekretar, medtem ko čaka na izid varnostnega preverjanja iz točke 12,11 ter potem, ko je uradno obvestil pristojni nacionalni organ in od njega v roku enega meseca ni dobil odgovora, uradniku Evropskega parlamenta ali drugemu uslužbencu Parlamenta, ki dela v politični skupini, izda začasno dovoljenje za obdobje, ki ne presega šest mesecev. Tako podeljena začasna pooblastila ne omogočajo dostopa do tajnih podatkov stopnje TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje.

PRILOGA II

UVOD

V teh določbah so opredeljena varnostna obvestila, ki urejajo in zagotavljajo varno obdelavo in upravljanje zaupnih podatkov v Evropskem parlamentu. Varnostna obvestila skupaj z navodili za ravnanje določajo sistem Evropskega parlamenta za upravljanje varnosti podatkov iz člena 3(2) tega sklepa:

VARNOSTNO OBVESTILO 1

Organizacija varnosti v Evropskem parlamentu za varstvo zaupnih podatkov

VARNOSTNO OBVESTILO 2

Upravljanje zaupnih podatkov

VARNOSTNO OBVESTILO 3

Obdelava zaupnih podatkov s samodejnimi komunikacijskimi in informacijskimi sistemi

VARNOSTNO OBVESTILO 4

Fizično varovanje

VARNOSTNO OBVESTILO 5

Industrijska varnost

VARNOSTNO OBVESTILO 6

Kršitev varnosti, izguba ali ogrožanje zaupnih podatkov

VARNOSTNO OBVESTILO 1

ORGANIZACIJA VARNOSTI V EVROPSKEM PARLAMENTU ZA VARSTVO ZAUPNIH PODATKOV

1. Generalni sekretar je odgovoren za splošno in dosledno izvajanje tega sklepa.

Generalni sekretar sprejme vse potrebne ukrepe, s katerimi zagotovi, da v prostorih Parlamenta poslanci in uradniki Evropskega parlamenta, drugi uslužbenci Parlamenta, ki delajo v političnih skupinah, ter pogodbeni izvajalci spoštujejo ta sklep pri ravnanju z zaupnimi podatki ali njihovi hrambi.

2. Generalni sekretar je varnostni organ in je v tej vlogi odgovoren za:

- 2.1. usklajevanje vseh varnostnih zadev v zvezi z dejavnostmi Parlamenta glede varstva zaupnih podatkov;

- 2.2. odobritev vzpostavitve zavarovanega območja, zavarovanih čitalnic in namestitve varnostne opreme;
 - 2.3. izvedbene sklepe, s katerimi se v skladu s členom 6 tega sklepa odobri posredovanje tajnih podatkov tretjim osebam s strani Parlamenta;
 - 2.4. opravljanje ali naročanje preiskav v primeru razkritja zaupnih podatkov, do katerega je *prima facie* prišlo v Parlamentu, v sodelovanju s predsednikom Evropskega parlamenta, če je udeležen poslanec Evropskega parlamenta;
 - 2.5. vzdrževanje tesnih stikov z varnostnimi organi drugih institucij Unije ter nacionalnimi varnostnimi organi v državah članicah, ki zagotavljajo optimalno usklajevanje varnostne politike v zvezi z zaupnimi podatki;
 - 2.6. nenehno preverjanje varnostne politike in postopkov Parlamenta in izdajanje ustreznih priporočil, ki temeljijo na tako pridobljenih ugotovitvah;
 - 2.7. poročanje nacionalnemu varnostnemu organu, ki je izvedel postopek varnostnega preverjanja, v skladu s točko 11.2 dela 2 Priloge I, v primeru negativnih informacij, ki utegnejo zadevati ta organ.
3. Kadar so udeleženi poslanci Evropskega parlamenta, jih generalni sekretar v tesnem sodelovanju s predsednikom Evropskega parlamenta razreši dolžnosti.
4. Pri izpolnjevanju dolžnosti iz odstavkov 2 in 3 generalnemu sekretarju pomagajo njegov namestnik, direktorat za varnost in oceno tveganja, direktorat za informacijsko tehnologijo in oddelek za tajne podatke.
- 4.1. Direktorat za varnost in oceno tveganja je odgovoren za osebne varnostne ukrepe in zlasti za postopek pridobitve varnostne odobritve iz dela 2 Priloge I. Direktorat za varnost in oceno tveganja predvsem:
- (a) deluje kot kontaktna točka za varnostne organe drugih institucij Unije ter nacionalne varnostne organe v zadevah, povezanih s postopki pridobitve varnostne odobritve za poslance in uradnike Evropskega parlamenta ter druge uslužbence Parlamenta, ki delajo v političnih skupinah;
 - (b) skrbi za potrebna splošna varnostna navodila o obveznosti varovanja tajnih podatkov in posledicah, če ta obveznost ni izpolnjena;
 - (c) spremlja delovanje zavarovanega območja in zavarovanih čitalnic v prostorih Parlamenta, če je treba v sodelovanju z varnostnimi službami drugih institucij Unije in držav članic;
 - (d) v sodelovanju z varnostnimi službami drugih institucij Unije in držav članic pregleduje postopke za upravljanje in hrambo tajnih podatkov, zavarovano območje in zavarovane čitalnice v prostorih Parlamenta, v katerih se dela s tajnimi podatki;
 - (e) predlaga generalnemu sekretarju ustrezna navodila za ravnanje.

4.2. Direktorat za informacijsko tehnologijo je odgovoren za ravnanje z zaupnimi podatki prek varnih sistemov informacijske tehnologije v Evropskem parlamentu.

4.3. Oddelek za tajne podatke je odgovoren za:

- (a) opredelitev varnostnih potreb za učinkovito varstvo zaupnih podatkov v tesnem sodelovanju z direktoratom za varnost in oceno tveganja in direktoratom za informacijsko tehnologijo in z varnostnimi službami drugih institucij Unije;
- (b) opredelitev vseh vidikov upravljanja in hrambe zaupnih podatkov v Parlamentu, kot je določeno v navodilih za ravnanje;
- (c) delovanje zavarovanega območja;
- (d) upravljanje zaupnih podatkov ali vpogled vanje na zavarovanem območju ali v zavarovani čitalnici na oddelku za tajne podatke v skladu z odstavkoma 2 in 3 člena 7 tega sklepa;
- (e) vodenje registra oddelka za tajne podatke;
- (f) poročanje varnostnemu organu o vsaki dokazani ali domnevni kršitvi varnosti, izgubi ali ogrožanju zaupnih podatkov, deponiranih na oddelku za tajne podatke in hranjenih na zavarovanem območju ali v zavarovani čitalnici oddelka za tajne informacije.

5. Generalni sekretar kot varnostni organ imenuje tudi naslednje organe:

- (a) organ za varnostno akreditacijo;
- (b) operativni organ za zagotavljanje varnosti podatkov;
- (c) organ za razpošiljanje šifrirnega materiala;
- (d) organ TEMPEST;
- (e) organ za zagotavljanje varnosti podatkov.

Za izvajanje teh nalog niso potrebni enotni organizacijski subjekti. Imajo ločena pooblastila. Naloge in dolžnosti, ki izhajajo iz njih, se lahko združijo ali vključijo v isti organizacijski subjekt ali se porazdelijo po različnih organizacijskih subjektih, če to ne povzroči navzkrižja interesov ali podvajanja nalog.

6. Organ za varnostno akreditacijo svetuje o vseh varnostnih zadevah, povezanih z akreditacijo vsakega informacijskega sistema in omrežja v Parlamentu, tako da:

6.1. zagotovi, da so komunikacijski in informacijski sistemi usklajeni z ustreznimi varnostnimi politikami in varnostnimi smernicami, in v ta namen pripravi izjavo o odobritvi ravnanja z zaupnimi podatki za tak sistem do določene stopnje tajnosti v njegovem operativnem okolju, v kateri so navedeni pogoji za akreditacijo in merila, v skladu s katerimi je potrebna ponovna odobritev;

6.2. vzpostavi postopek varnostne akreditacije v skladu z ustreznimi politikami, pri čemer jasno določi pogoje za odobritev komunikacijskega in informacijskega sistema v njegovi pristojnosti;

6.3. pripravi strategijo za varnostno akreditacijo, ki določa stopnjo natančnosti za akreditacijski postopek, ki ustreza zahtevani stopnji jamstva;

6.4. pregleda in odobri dokumentacijo, povezano z varovanjem tajnosti, tudi izjave o obvladovanju tveganja in preostalem tveganju, dokumentacijo o preverjanju izvajanja varovanja tajnosti in varnostno-operativne postopke, ter zagotavlja, da je skladna z varnostnimi pravili in politikami Parlamenta;

6.5. preverja izvajanje varnostnih ukrepov v zvezi s komunikacijskim in informacijskim sistemom in v ta namen izvaja ali naroča varnostne ocene, inšpekcije ali preglede;

6.6. določi varnostne zahteve (npr. stopnje varnostnih odobritev osebja) za občutljiva delovna mesta, povezana s komunikacijskimi in informacijskimi sistemi;

6.7. odobri medsebojno povezavo komunikacijskega in informacijskega sistema z drugimi komunikacijskimi in informacijskimi sistemi ali, kjer je to ustrezno, sodelovanje pri skupni odobritvi;

6.8. odobri varnostne standarde za tehnično opremo, predvideno za ravnanje s tajnimi podatki in njihovo varstvo;

6.9. zagotovi, da se šifrirni izdelki, uporabljeni v Parlamentu, uvrstijo na seznam produktov, odobrenih s strani EU; ter

6.10. se posvetuje s ponudnikom sistema, akterji na področju varovanja tajnosti in predstavniki uporabnikov o obvladovanju varnostnega tveganja, zlasti preostalega tveganja, in pogojih za izjavo o odobritvi.

7. Operativni organ za zagotavljanje varnosti podatkov je odgovoren za:

7.1. pripravo varnostne dokumentacije v skladu z varnostnimi politikami in varnostnimi smernicami, zlasti izjav o preostalem tveganju, varnostno-operativnih postopkov in načrtov za šifriranje v okviru postopka akreditacije komunikacijskega in informacijskega sistema;

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

7.3. spremljanje izvajanja in uporabe varnostno-operativnih postopkov, pri čemer lahko po potrebi odgovornost v zvezi z varnostjo delovanja prenese na lastnika sistema, oddelek za tajne podatke;

7.4. upravljanje šifrirnih izdelkov in ravnanje z njimi, zagotavljanje hrambe šifrirnih in nadzorovanih predmetov ter po potrebi zagotavljanje oblikovanja šifrirnih spremenljivk;

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

7.6. pripravo usposabljanja o zagotavljanju varnosti podatkov v komunikacijskem in informacijskem sistemu;

7.7. izvajanje in vodenje varnostnih ukrepov za komunikacijske in informacijske sisteme.

8. Organ za razpošiljanje šifrirnega materiala je odgovoren za:

8.1. upravljanje šifrirnega materiala EU ter vodenje evidenc o tem materialu;

8.2. zagotavljanje v tesnem sodelovanju z organom za varnostno akreditacijo, da se uporabljajo ustrezni postopki in da so vzpostavljeni načrti za vodenje evidenc, varno ravnanje z vsem šifrirnim materialom EU, hrambo in razpošiljanje tega materiala; ter

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

9. Organ TEMPEST je odgovoren za zagotavljanje skladnosti komunikacijskih in informacijskih sistemov s politikami TEMPEST in navodili za ravnanje. Organ odobri protiukrepe TEMPEST za naprave in izdelke za varovanje tajnih podatkov do določene stopnje tajnosti v njegovem operativnem okolju.

10. Organ za zagotavljanje varnosti podatkov je odgovoren za vse vidike upravljanja zaupnih podatkov v Parlamentu in ravnanja z njimi, zlasti za:

10.1. razvijanje zagotavljanja varnosti podatkov in varnostnih smernic zanj ter spremljanje njihove učinkovitosti in ustreznosti;

10.2. varovanje tehničnih informacij, povezanih s šifrirnimi izdelki, ter ravnanje z njimi;

10.3. zagotavljanje, da so ukrepi za zagotavljanje varnosti podatkov, izbrani za zaščito tajnih podatkov, v skladu z ustreznimi politikami, ki določajo njihovo upravičenost in urejajo njihov izbor;

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

10.5. posvetovanje s ponudnikom sistema, akterji na področju varovanja tajnosti in predstavniki uporabnikov glede zagotavljanja varnosti podatkov.

VARNOSTNO OBVESTILO 2

UPRAVLJANJE ZAUPNIH PODATKOV

A. UVOD

1. V tem varnostnem obvestilu so opredeljene določbe o upravljanju zaupnih podatkov v Parlamentu.

2. Avtor zaupnih podatkov zanje ob njihovem nastanku oceni stopnjo tajnosti in sprejme odločitev o stopnji tajnosti in oznaki te informacije na podlagi načel, določenih v tem varnostnem obvestilu.

B. STOPNJA TAJNOSTI TAJNIH PODATKOV EU

3. Odločitev o obravnavi dokumenta kot tajnega se sprejme pred njegovim nastankom. V ta namen je pri določanju podatkov za tajne podatke EU treba predhodno oceniti njihovo stopnjo tajnosti, avtor pa mora sprejeti odločitev, da bi nedovoljeno razkritje teh podatkov v različnih stopnjah škodovalo interesom Evropske unije, ene ali več držav članic ali posameznikov.

4. Ko je odločitev o obravnavi podatkov kot tajnih sprejeta, sledi druga predhodna ocena, s katero se določi ustrezna stopnja tajnosti. Stopnja tajnosti dokumenta se določi glede na stopnjo občutljivosti njegove vsebine.
5. Za določanje stopnje tajnosti podatkov je odgovoren izključno avtor zadevnih podatkov. Uradniki Parlamenta določajo stopnjo tajnosti podatkov na podlagi napotkov ali pooblastila generalnega sekretarja.
6. Stopnja tajnosti se uporablja pravilno in preudarno. Pri stopnji tajnosti dokumenta se avtor izogiba vsakršni težnji po previsoki ali prenizki stopnji tajnosti.
7. Stopnja tajnosti, določena za podatke, določa stopnjo njihovega varovanja na področju osebne varnosti, fizične varnosti, postopkovne varnosti in zagotavljanja varnosti podatkov.
8. Podatke, ki jih je treba določiti za tajne, je treba kot takšne označiti in obravnavati ne glede na njihovo fizično obliko. Prejemnikom podatkov je treba jasno sporočiti, da gre za tajne podatke, in sicer z oznako stopnje tajnosti (v pisni obliki na papirju ali prek komunikacijskega in informacijskega sistema) ali z obvestilom (v ustni obliki, kot sta na primer pogovor ali seja za zaprtimi vrati). Tajno gradivo mora biti fizično označeno, da je jasno razvidna njegova varnostna razvrstitev.
9. Tajni podatki EU v elektronski obliki se lahko ustvarijo zgolj z akreditiranim komunikacijskim in informacijskim sistemom. Sami tajni podatki ter ime datoteke in naprava za shranjevanje podatkov (če je zunanja, kot na primer zgoščenke ali ključi USB) morajo biti označeni z ustrezno stopnjo tajnosti.
10. Takoj ko podatek dobi določeno obliko, se ga določiti za tajnega. Osebne zapiske, osnutke ali elektronska sporočila, na primer, ki vsebujejo podatke, ki jih je treba določiti za tajne, je treba že na začetku označiti kot tajne podatke EU ter jih ustvariti in z njimi ravnati v skladu z materialnimi in tehničnimi zahtevami iz tega sklepa in pripadajočimi navodili za ravnanje. Na podlagi takšnih podatkov lahko nastane uraden dokument, ki se ustrezno označi, nato pa se z njim ustrezno ravna. V procesu priprave uradnega dokumenta se lahko pojavi potreba po njegovi ponovni oceni in dodelitvi višje ali nižje stopnje tajnosti.
11. Avtor se lahko odloči, da bo tistim kategorijam podatkov, ki jih redno ustvarja, dodelil standardno stopnjo tajnosti. Vendar pa zagotovi, da pri tem posameznim podatkom ne določi sistematično previsoke ali prenizke stopnje tajnosti.
12. Tajni podatki EU imajo vedno oznako stopnje tajnosti, ki ustreza njihovi stopnji tajnosti.

B.1. Stopnje tajnosti

13. Tajni podatki EU imajo naslednje stopnje tajnosti:

— TRÈS SECRET UE/EU TOP SECRET, ki je opredeljena v točki (d) člena 2 tega sklepa, ogrožanje teh podatkov pa bi lahko:

- (a) neposredno ogrozilo notranjo stabilnost Unije ali ene ali več njenih držav članic ali tretjih držav ali mednarodnih organizacij;
- (b) izjemno hudo škodovalo odnosom s tretjimi državami ali mednarodnimi organizacijami;
- (c) neposredno povzročilo veliko smrtnih žrtev;

(d) povzročilo izjemno hudo škodo operativni učinkovitosti ali varnosti osebja, razporejenega iz držav članic ali drugih držav, ki dajejo svoj prispevek, ali nadaljnji učinkovitosti izredno koristnih varnostnih ali obveščevalnih operacij, ali

(e) povzročilo hudo dolgotrajno škodo gospodarstvu Unije ali držav članic;

— SECRET UE/EU SECRET, ki je opredeljena v točki (d) člena 2 tega sklepa, ogrožanje teh podatkov pa bi lahko:

(a) sprožilo znatne mednarodne napetosti;

(b) resno škodovalo odnosom s tretjimi državami in mednarodnimi organizacijami;

(c) neposredno ogrozilo življenje ali resno škodovalo javnemu redu ali varnosti ali svobodi posameznika;

(d) škodovalo pomembnim trgovskim ali političnim pogajanjem in Unije ali državam članicam povzročilo znatne operativne težave;

(e) povzročilo resno škodo operativni varnosti držav članic ali učinkovitosti zelo koristnih varnostnih ali obveščevalnih operacij,

(f) povzročilo znatno materialno škodo finančnim, denarnim, gospodarskim in trgovskim interesom Unije ali države članice,

(g) občutno oslabilo finančno sposobnost za preživetje večjih organizacij ali subjektov,

(h) resno oviralo razvoj ali izvajanje politik Unije in imelo občutne gospodarske, trgovske ali finančne posledice;

— CONFIDENTIEL UE/EU CONFIDENTIAL, ki je opredeljena v točki (d) člena 2 tega sklepa, ogrožanje teh podatkov pa bi lahko:

(a) bistveno škodilo diplomatskim odnosom, tj. lahko bi povzročilo formalne proteste ali druge sankcije;

(b) ogrozilo varnost ali svobodo posameznika;

(c) ogrozilo izide trgovskih ali političnih pogajanj in Uniji ali državam članicam povzročilo operativne težave;

(d) povzročilo škodo operativni varnosti držav članic ali učinkovitosti varnostnih ali obveščevalnih operacij;

(e) občutno oslabilo finančno sposobnost za preživetje večjih organizacij ali subjektov;

(f) oviralo preiskave ali olajšalo storitev kaznivih dejanj ali terorističnih dejavnosti;

(g) znatno škodovalo finančnim, denarnim, gospodarskim in trgovskim interesom Unije ali držav članic, ali

(h) resno oviralo razvoj ali izvajanje politik Unije in imelo občutne gospodarske, trgovske ali finančne posledice;

- RESTREINT UE/EU RESTRICTED, ki je opredeljena v točki (d) člena 2 tega sklepa, ogrožanje teh podatkov pa bi lahko:
- (a) bilo neugodno za splošne interese Unije;
 - (b) škodljivo vplivalo na diplomatske odnose;
 - (c) povzročilo hudo stisko posameznikov;
 - (d) bilo neugodno za Unijo ali države članice v trgovinskih ali političnih pogajanjih;
 - (e) otežilo vzdrževanje učinkovite varnosti v Uniji ali državah članicah;
 - (f) oviralo učinkovit razvoj ali izvajanje politik Unije;
 - (g) ogrozilo pravilno upravljanje Unije in njenih dejavnosti;
 - (h) prekršilo dane zaveze Parlamenta o ohranitvi statusa tajnosti za podatke, ki jih predložijo tretje strani;
 - (i) prekršilo zakonske omejitve razkritja podatkov;
 - (j) povzročilo finančno izgubo ali omogočilo neupravičene koristi ali ugodnost posameznikom ali gospodarskim družbam, ali
 - (k) vplivalo na preiskave ali olajšalo storitev kaznivih dejanj.

B.2. Določanje stopnje tajnosti zbirk, naslovnice in izvlečkov

14. Stopnja tajnosti pisma ali zabeležke, ki vsebuje priložene dele, je enaka najvišji stopnji tajnosti, določeni enemu njenih priloženih delov. Avtor jasno določi stopnjo tajnosti za primer, ko sta pismo ali zabeležka ločena od priloženih delov. Če spremne zabeležke ali pisma ni potrebno obravnavati kot tajnega, se mora besedilo zaključiti z naslednjim: „Če je zabeležka ali pismo ločeno od priloženih delov, se ne obravnava kot tajno.“

15. Dokumente ali datoteke, ki so označene z različnimi stopnjami tajnosti, je treba, kolikor je to mogoče, oblikovati tako, da je mogoče posamezne dele z različnimi stopnjami tajnosti brez težav najti in jih po potrebi izločiti. Splošna stopnja tajnosti dokumenta ali datoteke je vsaj tako visoka, kot del istega dokumenta z najvišjo stopnjo tajnosti.

16. Za posamezne strani, odstavke, oddelke, priloge, dodatke, dodane in priložene dele posameznega dokumenta so lahko potrebne, in se v skladu s tem določijo, različne stopnje tajnosti. V dokumentih, ki vsebujejo tajne podatke EU, se lahko uporabljajo standardizirane okrajšave za označevanje stopnje tajnosti delov ali segmentov besedila, krajših od ene strani.

17. 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.

C. DRUGI ZAUPNI PODATKI

18. Drugi zaupni podatki se označijo v skladu s točko E tega varnostnega obvestila in navodili za ravnanje.

D. USTVARJANJE ZAUPNIH PODATKOV

19. Zaupne podatke lahko ustvari zgolj oseba, ki ima to pooblastilo v skladu s tem sklepom ali ki jo za to pooblasti varnostni organ.

20. Zaupnih podatkov ni dovoljeno vnašati v internetne ali intranetne sisteme upravljanja dokumentov.

D.1. Ustvarjanje tajnih podatkov EU

21. Zadevna oseba mora imeti za ustvarjanje tajnih podatkov EU stopnje CONFIDENTIEL UE/EU CONFIDENTIAL in višje dovoljenje v skladu s členom 4(1) tega sklepa.

22. Tajni podatki EU stopnje CONFIDENTIEL UE/EU CONFIDENTIAL in višje se lahko ustvarijo zgolj v zavarovanem območju.

23. Za ustvarjanje tajnih podatkov EU veljajo naslednja pravila:

- (a) vsaka stran se jasno označi z določeno stopnjo tajnosti;
- (b) vsaka stran se oštevilči, na njej pa je zabeleženo tudi skupno število strani;
- (c) na prvi strani dokumenta sta navedena njegova opravilna številka in predmet, ki pa sama po sebi nista tajni podatek, razen če ni tako označeno;
- (d) na prvi strani dokumenta je naveden datum;
- (e) na prvi strani vsakega tajnega dokumenta stopnje CONFIDENTIEL UE/EU, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET CONFIDENTIAL je seznam vseh prilog in priloženih delov;
- (f) pri tajnih dokumentih stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET se na vsaki strani navede številko kopije, če se razpošiljajo v več izvodih. Na vsaki kopiji je na prvi strani navedeno tudi skupno število kopij in strani; ter
- (g) če se dokument sklicuje na druge dokumente, ki vsebujejo tajne podatke, prejete iz drugih institucij Unije, ali če vsebuje tajne podatke, ki izhajajo iz teh dokumentov, mora biti označen z enako stopnjo tajnosti kot ti dokumenti in se ga brez predhodnega pisnega soglasja avtorja ne sme poslati osebam, ki niso na seznamu za razpošiljanje izvirnega dokumenta ali dokumentov, ki vsebujejo tajne podatke.

24. Avtor ohrani nadzor nad tajnimi podatki EU, ki jih je ustvaril. Njegovo predhodno pisno soglasje je potrebno, preden se:

- (a) zniža stopnja tajnosti tajnih podatkov EU ali se odpravi njihova tajnost;
- (b) tajni podatki EU uporabijo za namene, ki jih avtor ni določil;
- (c) tajni podatki EU razkrijejo kateri koli tretji državi ali mednarodni organizaciji;
- (d) tajni podatki EU razkrijejo osebam, institucijam, državam ali mednarodnim organizacijam, ki niso med naslovniki, ki jim je avtor izvirno dovolil vpogled v zadevne podatke;

- (e) tajni podatki EU razkrijejo izvajalcu ali morebitnemu izvajalcu iz tretje države;
- (f) tajni podatki EU kopirajo ali prevedejo, če gre za tajne podatke stopnje TRES SECRET UE/EU TOP SECRET;
- (g) tajni podatki EU uničijo.

D.2. Ustvarjanje drugih zaupnih podatkov

25. Generalni sekretar lahko v vlogi varnostnega organa odloči, ali se določeni funkciji, službi ali posamezniku dovoli, da ustvari druge zaupne podatke.
26. Drugi zaupni podatki morajo imeti eno od oznak, opredeljenih v navodilih za ravnanje.
27. Za ustvarjanje drugih zaupnih podatkov veljajo naslednja pravila:
- (a) njihova oznaka se navede na vrhu prve strani dokumenta;
 - (b) vsaka stran se oštevilči, na njej pa je zabeleženo tudi skupno število strani;
 - (c) na prvi strani dokumenta sta navedena njegova opravilna številka in predmet;
 - (d) na prvi strani dokumenta je naveden datum; ter
 - (e) na zadnji strani dokumenta je seznam vseh prilog in priloženih delov.
28. Za ustvarjanje drugih zaupnih podatkov veljajo posebna pravila in postopki, določeni v navodilih za ravnanje.

E. VARNOSTNI OZNAČEVALNIKI IN OZNAKE

29. Varnostni označevalniki in oznake na dokumentih so namenjeni nadzoru pretoka podatkov in omejitvi dostopa do zaupnih podatkov na podlagi načela potrebe po seznanitvi.
30. Če se uporabijo ali namestijo varnostni označevalniki ali oznake, se je treba pazljivo izogniti zamenjavi z oznakami stopnje tajnosti za tajne podatke EU: RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRES SECRET UE/EU TOP SECRET.
31. Posebna pravila za uporabo varnostnih označevalnikov in oznak skupaj s seznamom varnostnih oznak, odobrenih s strani Evropskega parlamenta, se določijo v navodilih za ravnanje.

E.1. Varnostni označevalniki

32. Varnostni označevalniki se uporabijo le skupaj s stopnjo tajnosti in se na dokumentih ne uporabljajo posebej. Varnostni označevalnik se lahko uporabi za tajne podatke EU, da se:
- (a) določijo omejitve veljavnosti stopenj tajnosti (za tajne podatke to pomeni samodejno znižanje stopnje tajnosti oziroma odpravo tajnosti);
 - (b) omeji razpošiljanje zadevnih tajnih podatkov EU;
 - (c) določijo posebni dogovori o ravnanju, poleg tistih, ki ustrezajo stopnji tajnosti.

33. Dodatni nadzor, ki velja za ravnanje z dokumenti, ki vsebujejo tajne podatke EU, vsem udeleženiim nalaga dodatne obremenitve. Da se kar najbolj zmanjša potrebno delo, ki je s tem povezano, je ob nastanku takega dokumenta dobra praksa določitev časovnega roka ali dogodka, po katerem stopnja tajnosti samodejno preneha veljati in se podatkom v dokumentu zniža stopnja tajnosti ali se tajnost odpravi.

34. Če dokument obravnava posebna delovna področja in je treba omejiti njegovo razpošiljanje ali če zanj veljajo posebni dogovori o ravnanju, se lahko v ta namen k stopnji tajnosti doda izjava, ki bo pomagala opredeliti njegovo ciljno skupino.

E.2. Oznake

35. Oznake ne označujejo stopnje tajnosti. Služile naj bi zgolj kot konkretna navodila za ravnanje z dokumentom in se ne uporabljajo za opis vsebine takega dokumenta.

36. Oznake se lahko na dokumentih uporabijo posebej ali pa skupaj s stopnjo tajnosti.

37. Na splošno se oznake uporabijo za podatke, za katere velja poklicna molčečnost iz člena 339 PDEU in člena 17 Kadrovskih predpisov ali ki jih mora Parlament varovati iz pravnih razlogov, vendar niso ali ne morejo biti tajni.

E.3. Uporaba oznak v komunikacijskih in informacijskih sistemih

38. Pravila za uporabo oznak veljajo tudi za akreditirane komunikacijske in informacijske sisteme.

39. Organ za varnostno akreditacijo določi posebna pravila za uporabo oznak v akreditiranih komunikacijskih in informacijskih sistemih.

F. SPREJEMANJE PODATKOV

40. Zgolj oddelek za tajne podatke sme v Parlamentu od tretjih oseb prejeti tajne podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje.

41. V primerih tajnih podatkov stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje in drugih zaupnih podatkov sta za njihov sprejem od tretjih oseb in za uporabo načel, določenih v tem varnostnem obvestilu, odgovorna oddelek za tajne podatke ali ustrezno parlamentarno telo/nosilec funkcije.

G. REGISTRACIJA

42. Registracija pomeni uporabo postopkov, ki evidentirajo življenjski cikel zaupnih podatkov, vključno z njihovim razširjanjem, vpogledom vanje ter njihovim uničenjem.

43. Za namene tega varnostnega obvestila pomeni vpisnik register, v katerega se evidentirajo zlasti datum in čas, ko:

- (a) zaupni podatki prispejo na ustrezni sekretariat parlamentarnega telesa/nosilca funkcije oziroma oddelek za tajne podatke ali ga zapustijo;
- (b) oseba z varnostno odobritvijo dostopa do zaupnih podatkov ali se ji ti posredujejo; ter
- (c) se zaupni podatki uničijo.

44. Avtor zaupnih podatkov je odgovoren za oznako začetne izjave ob nastanku dokumenta, ki vsebuje take podatke. Ta izjava se sporoči oddelku za tajne podatke, ko se dokument ustvari.

45. Podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje lahko iz varnostnih razlogov registrira zgolj oddlek za tajne podatke. Tajne podatke stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje in „druge zaupne podatke, prejete od tretjih oseb, za upravne namene registrira služba, pristojna za uradno sprejetje dokumenta, ki je bodisi oddlek za tajne podatke bodisi sekretariat parlamentarnega telesa/nosilca funkcije. Druge zaupne podatke, ustvarjene v Parlamentu za upravne namene registrira avtor.

46. Podatki stopnje CONFIDENTIEL UE/CONFIDENTIAL EU, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje se registrirajo zlasti, ko:

- (a) se ustvarijo;
- (b) prispejo na oddlek za tajne podatke ali ga zapustijo; ter
- (c) prispejo v komunikacijski in informacijski sistem ali ga zapustijo.

47. Tajni podatki stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje se registrirajo zlasti, ko:

- (a) se ustvarijo;
- (b) prispejo na ustrezni sekretariat parlamentarnega telesa/nosilca funkcije oziroma oddlek za tajne podatke ali ga zapustijo; ter
- (c) prispejo v komunikacijski in informacijski sistem ali ga zapustijo.

48. Registracija zaupnih podatkov se lahko opravi v vpisnik/komunikacijski in informacijski sistem v papirni ali elektronski obliki.

49. Za tajne podatke stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje in druge zaupne podatke je treba registrirati vsaj naslednje:

- (a) datum in čas, ko podatki prispejo na ustrezni sekretariat parlamentarnega telesa/nosilca funkcije oziroma oddlek za tajne podatke ali ga zapustijo;
- (b) naslov dokumenta, stopnjo tajnosti ali oznako, datum izteka veljavnosti stopnje tajnosti/oznake in morebitno opravilno številko dokumenta.

50. Za podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje je treba registrirati vsaj naslednje:

- (a) datum in čas, ko podatki prispejo na oddlek za tajne podatke ali ga zapustijo;
- (b) naslov dokumenta, stopnjo tajnosti ali oznako, morebitno opravilno številko dokumenta in datum izteka veljavnosti stopnje tajnosti/oznake;
- (c) podatke o avtorju;

- (d) evidenco identitete vseh oseb, ki jim je bil odobren dostop do dokumenta, in datum dostopa teh oseb;
- (e) evidenco morebitnih kopij ali prevodov dokumenta;
- (f) datum in čas, ko kopija ali prevod dokumenta zapusti oddelek za tajne podatke ali se vrne nanj, in podatke o tem, kam je bil poslan in kdo jih je vrnil;
- (g) datum in čas, ko se dokument uniči, in kdo ga je uničil, v skladu z varnostnimi predpisi Parlamenta o uničenju; ter
- (h) odpravo tajnosti in znižanje stopnje tajnosti dokumenta.

51. Vpisniki imajo po potrebi stopnjo tajnosti ali oznako. Vpisniki za tajne podatke stopnje TRES SECRET UE/EU TOP SECRET ali enakovredne stopnje se registrirajo na enaki stopnji.

52. Tajni podatki se lahko registrirajo:

- (a) v en sam vpisnik; ali
- (b) v ločene vpisnike glede na njihovo stopnjo tajnosti, status – ali gre za vstopne ali izstopne podatke – in na njihov izvor ali destinacijo.

53. V primeru elektronske obdelave v komunikacijskem in informacijskem sistemu se registracijski postopki lahko opravijo prek postopkov v samih komunikacijskih in informacijskih sistemih, ki izpolnjujejo zahteve, enakovredne zgoraj navedenim. Ko tajni podatki EU zapustijo območje komunikacijskega in informacijskega sistema, se uporablja zgoraj navedeni postopek registracije.

54. Oddelek za tajne podatke vodi evidenco vseh tajnih podatkov, ki jih Parlament da tretjim osebam, in tajnih podatkov, ki jih Parlament prejme od tretjih oseb.

55. Ko je registracija tajnih podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje zaključena, oddelek za tajne podatke preveri, ali ima naslovnik veljavno varnostno pooblastilo. V takem primeru oddelek za tajne podatke obvesti naslovnika. Vpogled v tajne podatke je mogoč šele po registraciji dokumenta, ki te podatke vsebuje.

H. RAZPOŠILJANJE

56. Avtor pripravi začetni seznam za razpošiljanje tajnih podatkov EU, ki jih je ustvaril.

57. Tajne podatke stopnje RESTREINT UE/EU RESTRICTED in druge zaupne podatke, ki se ustvarijo v Parlamentu, znotraj Parlamenta razpošlje avtor v skladu z ustreznimi navodili za ravnanje in na podlagi načela potrebe po seznanitvi. Za tajne podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET, ki se ustvarijo v Parlamentu znotraj zavarovanega območja, se seznam za razpošiljanje (ter vsa dodatna navodila za razpošiljanje) predloži oddelku za tajne podatke, ki je odgovoren za upravljanje z njim.

58. Tajne podatke EU, ustvarjene v Parlamentu, lahko tretjim osebam razpošlje zgolj oddelek za tajne podatke na podlagi načela potrebe po seznanitvi.

59. Zaupni podatki, ki jih prejme bodisi oddelek za tajne podatke bodisi parlamentarno telo/nosilec funkcije, ki je vložil zahtevo zanje, se razpošljejo v skladu z navodili avtorja.

I. RAVNANJE, HRAMBA IN VPOGLEDE

60. Ravnanje z zaupnimi podatki, njihova hramba in vpogled vanje se opravljajo v skladu z varnostnim obvestilom 4 in navodili za ravnanje.

J. KOPIRANJE/PREVAJANJE/TOLMAČENJE TAJNIH PODATKOV

61. Dokumenti, ki vsebujejo tajne podatke stopnje TRES SECRET UE/EU TOP SECRET ali enakovredne stopnje, se ne smejo kopirati ali prevajati brez predhodnega pisnega soglasja avtorja. Dokumenti, ki vsebujejo tajne podatke stopnje SECRET UE/EU SECRET ali enakovredne stopnje ali tajne podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali enakovredne stopnje, se lahko kopirajo ali prevajajo po navodilu imetnika, če avtor tega ni prepovedal.

62. Iz varnostnih razlogov je treba registrirati vsako kopijo dokumenta, ki vsebuje tajne podatke stopnje TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET EU ali CONFIDENTIEL UE/EU CONFIDENTIAL ali enakovredne stopnje.

63. Varnostni ukrepi, ki veljajo za izvorni dokument, ki vsebuje tajne podatke, veljajo tudi za kopije in prevode.

64. Dokumenti, ki jih pošlje Svet, naj bi prispeli v vseh uradnih jezikih.

65. Kopije ali prevode dokumentov, ki vsebujejo tajne podatke, lahko zahteva avtor ali imetnik kopije. Kopije dokumentov, ki vsebujejo tajne podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje, se lahko ustvarijo zgolj na zavarovanem območju in na kopirnih strojih, ki so del akreditiranega komunikacijskega in informacijskega sistema. Kopije dokumentov, ki vsebujejo tajne podatke stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje in „druge zaupne podatke, se ustvarijo z akreditirano napravo za reprodukcijo v prostorih Parlamenta.

66. Vse kopije in prevode dokumentov ali dele kopij dokumentov, ki vsebujejo zaupne podatke, je treba ustrezno označiti, oštevilčiti in registrirati.

67. Ustvari se zgolj toliko kopij, kot je nujno potrebno. Vse kopije je treba po izteku časa za vpogled uničiti v skladu z navodili za ravnanje.

68. Le tolmači in prevajalci ki so uradniki Parlamenta, lahko imajo dostop do tajnih podatkov.

69. Tolmači in prevajalci, ki imajo dostop do dokumentov, ki vsebujejo tajne podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje, morajo imeti ustrezno varnostno odobritev.

70. Tolmači in prevajalci morajo z dokumenti, ki vsebujejo tajne podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje, delati na zavarovanem območju.

K. ZNIŽEVANJE STOPENJ TAJNOSTI, ODPRAVA TAJNOSTI IN ODSTRANITEV OZNAK ZAUPNIH PODATKOV**K.1. Splošna načela**

71. Zaupnim podatkom se odpravi tajnost, zniža stopnja tajnosti ali se jim odstrani oznaka, če zaščita na prvotni ravni ni več potrebna.

72. Odločitev o znižanju stopnje tajnosti, odpravi tajnosti ali odstranitvi oznake za podatke v dokumentih, ustvarjenih znotraj Parlamenta, se utegne sprejeti tudi *ad hoc*, na primer kot odgovor na zahtevo javnosti ali druge institucije Unije za dostop ali na pobudo oddelka za tajne podatke ali parlamentarnega telesa/nosilca funkcije.

73. Avtor ob ustvarjanju tajnih podatkov EU po možnosti navede, ali se stopnja tajnosti zadevnih tajnih podatkov EU lahko zniža ali se tajnost odpravi na določen datum ali po določenem dogodku. Če takih informacij ni mogoče zagotoviti, avtor, oddelek za tajne podatke ali parlamentarno telo/nosilec funkcije, ki poseduje podatke, pregleda stopnjo tajnosti tajnih podatkov EU najmanj vsakih pet let. V vseh primerih se tajnim podatkom EU lahko zniža stopnja tajnosti ali odpravi tajnost zgolj s predhodnim pisnim soglasjem avtorja.

74. Če za dokumente, ustvarjene v Parlamentu, ni mogoče ugotoviti ali najti avtorja, varnostni organ pregleda stopnjo tajnosti tajnih podatkov EU na podlagi predloga parlamentarnega telesa/nosilca funkcije, ki poseduje podatke, ta pa se v zvezi s tem lahko posvetuje z oddelkom za tajne podatke.

75. Oddelek za tajne podatke ali parlamentarno telo/nosilec funkcije, ki poseduje podatke, je zadolžen, da o odpravi tajnosti ali znižanju stopnje tajnosti obvesti noslovnike dokumenta, noslovniki pa so zadolženi, da obvestijo vse nadaljnje noslovnike, ki so jim poslali dokument ali njegovo kopijo.

76. Zniževanje stopenj tajnosti, odprava tajnosti in odstranitev oznak za podatke v dokumentih se evidentira.

K.2. Odprava tajnosti

77. Tajnim podatkom EU se lahko odpravi tajnost v celoti ali delno. Delna odprava tajnosti tajnih podatkov EU je mogoča, če zaščita za določen del dokumenta, v katerem so ti podatki, ni več potrebna, vendar je še naprej upravičena v preostalem delu dokumenta.

78. Ko je na podlagi pregleda tajnih podatkov EU v dokumentu, ustvarjenem v Parlamentu, sprejet sklep, da se odpravi njegova tajnost, je treba ugotoviti, ali bi bilo treba dokument objaviti in ali naj nosi oznako za razpošiljanje (tj. naj se ne objavi).

79. Pri odpravi tajnosti tajnih podatkov EU je odpravo treba vpisati v vpisnik skupaj z naslednjimi podatki: datumom odprave tajnosti, imeni oseb, ki so odpravo zahtevale in odobrile, opravilno številko dokumenta, katerega tajnost se odpravi, in njegovo končno destinacijo.

80. Na dokumentu, katerega tajnost se odpravi, in na vseh njegovih kopijah je treba prečrtati označbe stare stopnje tajnosti. Dokumenti in njihove kopije morajo biti ustrezno hranjeni.

81. Pri delni odpravi tajnosti tajnih podatkov se pripravi del, katerega tajnost je odpravljena, v obliki izvlečka, ki se ustrezno hrani. Pristojna služba registrira:

- (a) datum delne odprave tajnosti;
- (b) imena oseb, ki so ki so odpravo zahtevale in odobrile; ter
- (c) opravilno številko izvlečka, katerega tajnost se odpravi.

K.3. Znižanje stopnje tajnosti

82. Ko se dokumentu zniža stopnja tajnosti, se registrira v vpisnike, ki ustrezajo tako stari kot novi stopnji tajnosti. Vpisati je treba datum znižanja stopnje tajnosti in ime osebe, ki jo je odobrila.

83. Dokument, v katerem so podatki z znižano stopnjo tajnosti, in vse kopije se označijo z novo stopnjo tajnosti in ustrezno hranijo.

L. UNIČENJE ZAUPNIH PODATKOV

84. Zaupni podatki (v papirnati ali elektronski obliki), ki niso več potrebni, se uničijo ali izbrišejo v skladu z navodili za ravnanje in ustreznimi pravili o arhiviranju.

85. Tajne podatke stopnje TRES SECRET UE/EU TOP SECRET ali enakovredne stopnje oziroma stopnje SECRET UE/EU SECRET ali enakovredne stopnje uniči oddelek za tajne podatke, kot priča pa je prisotna oseba, ki ima stopnjo varnostne odobritve, ki ustreza vsaj stopnji tajnosti podatkov, ki se uničujejo.

86. Tajni podatki stopnje TRES SECRET UE/EU TOP SECRET ali enakovredne stopnje se lahko uničijo zgolj s predhodnim pisnim soglasjem avtorja.

87. Tajne podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje uniči in odstrani oddelek za tajne podatke po navodilu avtorja ali pristojnega organa. Vpisniki in drugi registri se ustrezno posodobijo. Tajne podatke stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje uniči in odstrani bodisi oddelek za tajne podatke bodisi ustrezno parlamentarno telo/nosilec funkcije.

88. Uradnik, pristojen za uničenje, in oseba, ki priča uničenju, podpišeta potrdilo o uničenju, ki se shrani in arhivira na oddelku za tajne podatke. Oddelek za tajne podatke hrani, skupaj z obrazci za razpošiljanje, potrdila o uničenju tajnih podatkov stopnje TRES SECRET UE/EU TOP SECRET ali enakovredne stopnje vsaj deset let, za tajne podatke stopnje SECRET UE/EU SECRET ali enakovredne stopnje in CONFIDENTIEL UE/EU CONFIDENTIAL ali enakovredne stopnje pa vsaj pet let.

89. Dokument, ki vsebuje tajne podatke, se uniči po metodah, ki ustrezajo standardom Unije ali enakovrednim standardom, tako da jih ni mogoče v celoti ali delno rekonstruirati.

90. Uničenje računalniških nosilcev podatkov, ki se uporabljajo za tajne podatke, poteka v skladu z ustreznimi navodili za ravnanje.

91. Uničenje tajnih podatkov je treba evidentirati v ustreznem vpisniku z naslednjimi podatki:

- (a) datumom in časom uničenja;
- (b) imenom uradnika, odgovornega za uničenje;
- (c) opravlno številko uničenega dokumenta ali kopij;
- (d) izvorno fizično obliko uničenih tajnih podatkov EU;

- (e) načinom uničenja; ter
- (f) krajem uničenja.

M. ARHIVIRANJE

92. Tajni podatki, vključno s spremno zabeležko ali pismom, prilogami, potrdilu o oddaji in drugimi deli dokumentacije se premestijo v varni arhiv na zavarovanem območju šest mesecev zatem, ko je bilo vanje zadnjič vpogledano, in najpozneje eno leto zatem, ko so bili deponirani. Podrobna pravila za arhiviranje tajnih podatkov se določijo v navodilih za ravnanje.

93. Za „druge zaupne podatke“ veljajo splošna pravila o upravljanju dokumentov brez poseganja v druge posebne določbe o ravnanju z njimi.

VARNOSTNO OBVESTILO 3

OBDELAVA ZAUPNIH PODATKOV Z AVTOMATIZIRANIMI KOMUNIKACIJSKIMI IN INFORMACIJSKIMI SISTEMI

A. ZAGOTAVLJANJE VARNOSTI TAJNIH PODATKOV, S KATERIMI POTEKA DELO V INFORMACIJSKIH SISTEMIH

1. „Zagotavljanje varnosti podatkov“ v informacijskih sistemih je jamstvo, da bodo tajni podatki v teh sistemih zaščiteni in da bodo ti sistemi delovali tako, kot morajo, kadar morajo, pod nadzorom zakonitih uporabnikov. Pri učinkovitem zagotavljanju varnosti podatkov se poskrbi za ustrezno stopnjo tajnosti, celovitosti, razpoložljivosti, nezatajljivosti in avtentičnosti. Zagotavljanje informacijske varnosti temelji na postopku obvladovanja tveganja.
2. „Komunikacijski in informacijski sistem“ za ravnanje s tajnimi podatki pomeni sistem, ki omogoča delo s podatki v elektronski obliki. Tak komunikacijski in informacijski sistem zajema vse elemente, potrebne za njegovo delovanje, vključno z infrastrukturo, organizacijo, osebjem in informacijskimi viri.
3. V komunikacijskih in informacijskih sistemih delo s tajnimi podatki poteka v skladu z načelom zagotavljanja varnosti podatkov.
4. Za vse komunikacijske in informacijske sisteme se opravi postopek akreditacije. Cilj akreditacije je pridobiti zagotovilo, da so bili izvedeni vsi ustrezni varnostni ukrepi in da je bila dosežena zadostna stopnja zaščite tajnih podatkov ter komunikacijskih in informacijskih sistemov v skladu s tem varnostnim obvestilom. V izjavi o akreditaciji so določeni najvišja stopnja tajnosti podatkov, s katerimi se lahko dela v komunikacijskih in informacijskih sistemih, in ustrezni pogoji.
5. Za varovanje tajnosti in pravilno delovanje operacij v komunikacijskih in informacijskih sistemih so ključne naslednje značilnosti in pojmi v zvezi z zagotavljanjem varnosti podatkov:
 - (a) avtentičnost: zagotovilo, da so podatki pravi in izhajajo iz zaupanja vrednih virov;
 - (b) razpoložljivost: podatki so dostopni ter na voljo za uporabo na zahtevo pooblaščenega subjekta;
 - (c) zaupnost: podatki se ne razkrijejo nepooblaščenim posameznikom ali subjektom oziroma ne uporabijo v postopkih, kjer to ni dovoljeno;

- (d) celovitost: zagotavljanje točnosti in popolnosti podatkov in premoženja;
- (e) nezatajljivost: zmožnost dokazati, da se je dejanje zgodilo, tako da se vnaprej izključi možnost vsakršnega poznejšega zanikanja.

B. NAČELA ZA ZAGOTAVLJANJE VARNOSTI PODATKOV

6. Določbe v nadaljevanju so podlaga za varovanje vseh komunikacijskih in informacijskih sistemov, v okviru katerih poteka delo s tajnimi podatki. Natančne zahteve za izvajanje teh določb so opredeljene v politikah o zagotavljanju varnosti podatkov in varnostnih smernicah.

B.1. Obvladovanje varnostnega tveganja

7. Obvladovanje varnostnega tveganja je sestavni del določanja, razvijanja, delovanja in vzdrževanja komunikacijskih in informacijskih sistemov. Postopek obvladovanja tveganja (ocena, obravnava, sprejemanje in obveščanje) vsakič znova skupaj izvajajo predstavniki lastnikov sistema, projektnih organov, operativnih organov in varnostnih organov za odobritev iz varnostnega obvestila 1, ki uporabljajo preverjen, pregleden ter razumljiv postopek ocene tveganja. Področje uporabe komunikacijskega in informacijskega sistema ter njegovih sestavnih delov je jasno določeno na začetku izvajanja postopka za obvladovanje tveganja.

8. Pristojni organi iz varnostnega obvestila 1 preučijo morebitne nevarnosti za komunikacijske in informacijske sisteme in poskrbijo za posodobljene in natančne ocene nevarnosti, ki odražajo trenutno operativno okolje. Stalno posodablajo znanje o vprašanih glede izpostavljenosti in redno pregledujejo ocene ranljivih točk ter tako sledijo spremembam na področju informacijske tehnologije (IT).

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

10. Akreditacija komunikacijskega in informacijskega sistema vključuje uradno izjavo pristojnega organa o preostalem tveganju in sprejemanju tega tveganja. Konkretna zahteva, obseg in stopnja natančnosti, ki jih za akreditacijo komunikacijskih in informacijskih sistemov določi pristojni organ za varnostno akreditacijo, morajo biti sorazmerni z ocenjenim tveganjem ob upoštevanju vseh pomembnih dejavnikov, med drugim stopnjo tajnosti podatkov, s katerimi se dela v teh komunikacijskih in informacijskih sistemih.

B.2. Varnost skozi celotni življenjski cikel komunikacijskega in informacijskega sistema

11. Zagotovitev varnosti je ena od zahtev, ki velja skozi celoten življenjski cikel komunikacijskega in informacijskega sistema od njegove uvedbe do prenehanja delovanja.

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

13. Komunikacijski in informacijski sistemi, vključno s tehničnimi in netehničnimi varnostnimi ukrepi, se v okviru akreditacijskega postopka varnostno preskusijo, da se zagotovi ustreznost stopnja jamstva in preveri, ali se komunikacijski in informacijski sistemi, vključno s tehničnimi in netehničnimi varnostnimi ukrepi, pravilno izvajajo ter ali so pravilno integrirani in konfigurirani.

14. Varnostne ocene, inšpekcijski pregledi in pregledi se med obratovanjem komunikacijskega in informacijskega sistema in v času njegovega vzdrževanja izvajajo v rednih časovnih presledkih, pa tudi v izjemnih okoliščinah.
15. Varnostna dokumentacija za komunikacijski in informacijski sistem se razvija skozi celoten življenjski cikel v sklopu procesa sledenja spremembam.
16. Vpisni postopki, ki se po potrebi opravijo v komunikacijskem in informacijskem sistemu, se preverijo v okviru postopka akreditacije.

B.3. Najboljša praksa

17. Organ za zagotavljanje varnosti podatkov oblikuje najboljšo prakso za varovanje tajnih podatkov, s katerimi poteka delo v okviru komunikacijskih in informacijskih sistemov. Smernice glede najboljših praks določajo tehnične, fizične, organizacijske in postopkovne varnostne ukrepe za komunikacijske in informacijske sisteme, katerih učinkovitost pri preprečevanju določenih nevarnosti in ranljivih točk je dokazana.
18. K zaščiti tajnih podatkov, s katerimi poteka delo v okviru komunikacijskega in informacijskega sistema, prispevajo tudi izkušnje subjektov, ki delujejo na področju zagotavljanja varnosti podatkov.
19. Razširjanje najboljših praks in nato njeno izvajanje prispeva k doseganju enakovredne ravni jamstva pri različnih komunikacijskih in informacijskih sistemih, ki jih upravlja sekretariat Parlamenta in v okviru katerih poteka delo s tajnimi podatki.

B.4. Globinska obramba

20. Za ublažitev tveganja za komunikacijski in informacijski sistem se izvaja vrsta tehničnih in netehničnih varnostnih ukrepov, ki so organizirani kot večplastna obramba. Te plasti zajemajo:
- (a) odvrčanje: varnostni ukrepi za odvrnitev od načrtovanja sovražnih napadov na komunikacijski in informacijski sistem;
 - (b) preprečevanje: varnostni ukrepi za oviranje ali zaustavitev napadov na komunikacijski in informacijski sistem;
 - (c) odkrivanje: varnostni ukrepi za odkrivanje napadov na komunikacijski in informacijski sistem;
 - (d) odpornost: varnostni ukrepi za omejitev učinka napadov na najmanjši možen sklop podatkov ali sestavnih delov komunikacijskega in informacijskega sistema ter preprečevanje nadaljnje škode ter
 - (e) ponovna vzpostavitev: varnostni ukrepi za ponovno vzpostavitev varnosti v okviru komunikacijskega in informacijskega sistema.

Stopnja strogosti takšnih varnostnih ukrepov se določi po oceni tveganja.

21. Pristojni organi iz varnostnega obvestila 1 zagotovijo, da se lahko odzovejo na incidente, ki lahko presegajo organizacijske meje, da bi uskladili odzive in izmenjavo informacij o teh dogodkih in z njimi povezanih tveganjih (zmogljivosti odzivanja na izredne razmere na področju informatike).

B.5. Načelo minimalnosti in najmanjšega privilegija

22. V izogib nepotrebnemu tveganju se izvajajo le ključne funkcionalnosti, naprave in storitve, potrebne za obratovanje.
23. Uporabniki komunikacijskega in informacijskega sistema ter avtomatizirani postopki dobijo le takšen dostop, privilegije in pooblastila, ki jih potrebujejo za opravljanje svojih nalog, da se omeji škoda, ki bi nastala zaradi nesreč, napak ali nepooblaščen uporabe virov komunikacijskega in informacijskega sistema.

B.6. Osveščenost o zagotavljanju varnosti podatkov

24. Za varnost komunikacijskih in informacijskih sistemov je v prvi vrsti pomembno poznavanje tveganj in razpoložljivih varnostnih ukrepov. Zlasti vsi člani osebja, vključeni v življenjski cikel komunikacijskega in informacijskega sistema, vključno z uporabniki, se morajo zavedati:

- (a) da lahko kršitve varnosti povzročijo znatno škodo v komunikacijskih in informacijskih sistemih, v okviru katerih poteka delo s tajnimi podatki;
- (b) da lahko zaradi medsebojne povezanosti in soodvisnosti nastane škoda za druge subjekte ter
- (c) svojih individualnih obveznosti in odgovornosti v zvezi z varnostjo komunikacijskih in informacijskih sistemov glede na vlogo, ki jo imajo v teh sistemih in postopkih.

25. Da bi zagotovili ustrezno razumevanje odgovornosti glede varovanja tajnosti, mora biti izobraževanje o zagotavljanju varnosti podatkov in usposabljanje za krepitev osveščenosti obvezno za vse zadevno osebje, vključno z višjim vodstvom, poslanci Evropskega parlamenta in uporabniki komunikacijskih in informacijskih sistemov.

B.7. Ocena in odobritev varnostnih izdelkov IT

26. Komunikacijski in informacijski sistemi, v okviru katerih poteka delo s tajnimi podatki stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje, so zaščiteni tako, da podatki ne morejo biti ogroženi zaradi nenamernega elektromagnetnega oddajanja (ukrepi za varovanje tajnosti TEMPEST).

27. Kjer se zaščita tajnih podatkov zagotavlja s šifrirnimi izdelki, mora organ za varnostno akreditacijo potrditi, da taki izdelki spadajo med šifrirne izdelke, potrjene v EU.

28. Med prenašanjem tajnih podatkov z elektronskimi sredstvi se uporabljajo šifrirni izdelki, odobreni v EU. Ne glede na navedeno zahtevo se lahko v izrednih razmerah ali specifičnih tehničnih konfiguracijah uporabijo posebni postopki, določeni v točkah 41 do 44.

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

30. Stopnja jamstva se preveri z mednarodno priznanimi postopki in metodologijami ali postopki in metodologijami, ki so odobreni na nacionalni ravni. To so predvsem ocena, pregled in revizija.

31. Organ za varnostno akreditacijo odobri varnostne smernice glede ustreznosti in odobritve nešifrirnih varnostnih izdelkov IT.

B.8. Prenos v varovanem območju

32. V primerih, ko je prenos tajnih podatkov omejen na varovano območje, se lahko uporabi nešifrirano pošiljanje ali šifriranje na nižji stopnji, in sicer na podlagi izida postopka obvladovanja tveganja in odobritve organa za varnostno akreditacijo.

B.9. Varne medsebojne povezave komunikacijskih in informacijskih sistemov

33. Medsebojna povezanost pomeni neposredno povezavo dveh ali več sistemov IT za namen izmenjave podatkov in drugih informacijskih virov v eni ali več smereh.

34. Komunikacijski in informacijski sistem vsak sistem IT, povezan z njim, samodejno obravnava kot nezanesljiv in izvede zaščitne ukrepe, s katerimi nadzoruje izmenjavo tajnih podatkov z drugim komunikacijskim in informacijskim sistemom.

35. Povezave komunikacijskih in informacijskih sistemov z drugimi sistemi IT ustrezajo naslednjim osnovnim zahtevam:

- (a) pristojni organi določijo in odobrijo poslovne ali operativne zahteve za takšne povezane sisteme;
- (b) za zadevne povezane sisteme se izvedeta postopek obvladovanja tveganja in akreditacijski postopek, odobriti pa jih mora pristojni organ za varnostno akreditacijo;
- (c) storitve v zvezi z zaščito se izvajajo v varnostnem perimetru komunikacijskih in informacijskih sistemov.

36. Akreditiran komunikacijski in informacijski sistem ter nezaščiten ali javno omrežje ne smeta biti med seboj povezana, razen če ima komunikacijski in informacijski sistem v ta namen med komunikacijskim in informacijskim sistemom ter nezaščitenim ali javnim omrežjem nameščene odobrene storitve v zvezi z zaščito. Varnostne ukrepe za takšne medsebojne povezave pregleda pristojni organ za zagotavljanje varnosti podatkov, odobri pa jih pristojni organ za varnostno akreditacijo.

37. Če se nezaščiten ali javno omrežje uporablja izključno za prenos in so podatki šifrirani s šifrirnim izdelkom EU, potrjenim v skladu z odstavkom 27, se takšna povezava ne šteje za medsebojno povezavo.

38. Neposredna ali kaskadna medsebojna povezava komunikacijskega in informacijskega sistema, akreditiranega za delo s tajnimi podatki stopnje TRES SECRET UE/EU TOP SECRET ali enakovredne stopnje ter tajnimi podatki stopnje SECRET UE/EU SECRET ali enakovredne stopnje, z nezaščitenim ali javnim omrežjem je prepovedana.

B.10. Računalniški nosilci podatkov

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

40. Računalniški nosilci podatkov se lahko ponovno uporabijo in stopnja njihove tajnosti se lahko zniža ali odpravi v skladu z navodili za ravnanje.

B.11. Izredne razmere

41. Posebni postopki, opisani v nadaljevanju, se lahko uporabijo v izrednih razmerah, na primer v času preteče ali dejanske krize, spopada, vojnih razmer ali v izjemnih operativnih okoliščinah.

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

- (a) pošiljatelj in prejemnik nimata potrebnih naprav za šifriranje ali nimata nobenih takih naprav; ter
- (b) tajnega materiala ni mogoče pravočasno poslati na drug način.

43. Tajni podatki, preneseni pod pogoji iz odstavka 41, 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.

44. Če se uporabi odstavek 41 ali 42, se pristojnemu organu naknadno pošlje poročilo.

VARNOSTNO OBVESTILO 4

FIZIČNO VAROVANJE

A. UVOD

To varnostno obvestilo določa varnostna načela za vzpostavitev varnega okolja za pravilno obdelavo zaupnih podatkov v Evropskem parlamentu. Načela, vključno s tehničnim varovanjem, bodo dopolnjevala navodila za ravnanje.

B. OBVLADOVANJE VARNOSTNEGA TVEGANJA

1. Za obvladovanje tveganja, povezanega s tajnimi podatki, je predviden poseben postopek. Njegov cilj je opredeliti znana varnostna tveganja, določiti varnostne ukrepe za njihovo zmanjšanje na sprejemljivo raven v skladu s temeljnimi načeli in minimalnimi standardi iz tega varnostnega obvestila ter uporabljati te ukrepe ob upoštevanju koncepta globinske obrambe, kakor je opredeljena v varnostnem obvestilu 3. Učinkovitost teh ukrepov se nenehno ocenjuje.

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

3. V načrtih ukrepanja ob izrednih razmerah je upoštevana potreba po varovanju tajnih podatkov v izrednih razmerah, da se prepreči nepooblaščen dostop, razkritje ali izguba celovitosti podatkov ali njihove razpoložljivosti.

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

C. SPLOŠNA NAČELA

5. Stopnja tajnosti podatkov ali oznaka določa stopnjo zaščite, ki je bodo ti podatki deležni na področjih fizičnega varovanja.

6. Podatki, ki jih je treba določiti za tajne, se kot takšni označijo in obravnavajo ne glede na njihovo fizično obliko. Prejemnikom podatkov se jasno sporoči, da gre za tajne podatke, in sicer z oznako stopnje tajnosti (v pisni obliki na papirju ali prek komunikacijskega in informacijskega sistema) ali z obvestilom (v ustni obliki, kot sta na primer pogovor ali predstavitev). Tajno gradivo mora biti fizično označeno, da je jasno razvidna njegova varnostna razvrstitev.

7. Zaupnih podatkov se v nobenih okoliščinah ne sme brati na javnih mestih, kjer bi jih utegnili videti oseba, ki nima potrebe po seznanitvi s podatki, na primer na vlakih, letalih, v kavarnah, barih itd. Ne sme se jih puščati v hotelskih sefih ali sobah brez nadzora na javnih mestih.

D. PRISTOJNOSTI

8. Oddelek za tajne podatke je pristojen za fizično varovanje pri upravljanju zaupnih podatkov, shranjenih v njegovih varovanih prostorih. Oddelek za tajne podatke je pristojen tudi za upravljanje svojih varovanih prostorov.
9. Fizično varovanje pri upravljanju tajnih podatkov stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje in „drugih zaupnih podatkov“ je v pristojnosti posameznega parlamentarnega telesa/nosilca funkcije.
10. Direktor za varnost in oceno tveganja zagotovi varnostno preverjanje oseb in varnostne odobritve, potrebne za zagotovitev varnega ravnanja z zaupnimi podatki v Evropskem parlamentu.
11. Direktor za informacijsko tehnologijo svetuje pri vzpostavljanju in uporabi komunikacijskih in informacijskih sistemov ter zagotovi, da je vsak tak sistem skladen z varnostnim obvestilom 3 in z ustreznimi navodili za ravnanje.

E. ZAVAROVANI PROSTORI

12. V okviru tehničnih varnostnih standardov in v skladu s stopnjo, dodeljeno zaupnim podatkom, se lahko namestijo zavarovani prostori, kakor so opredeljeni v členu 7.
13. Te zavarovane prostore potrdi organ za varnostno akreditacijo in varnostni organ.

F. VPOGLED V ZAUPNE PODATKE

14. Ko so tajni podatki stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje ter „drugi zaupni podatki“ deponirani pri oddelku za tajne podatke in je treba omogočiti vpogled vanje zunaj zavarovanega območja, oddelek za tajne podatke pošlje kopijo podatkov ustrezni pooblašeni službi, ki zagotovi, da sta vpogled v zadevne podatke in ravnanje z njimi skladna s členom 8(2) in členom 10 tega sklepa ter ustreznimi navodili za ravnanje.
15. Ko so tajni podatki stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje ter drugi zaupni podatki deponirani pri parlamentarnem telesu/nosilcu funkcije, ki ni oddelek za tajne podatke, sekretariat parlamentarnega telesa/nosilca funkcije zagotovi, da sta vpogled v zadevne podatke in ravnanje z njimi skladna s členom 7(3), členom 8(1), (2) in (4), členom 9(3), (4) in (5), členom 10(2) do (6) ter členom 11 tega sklepa ter ustreznimi navodili za ravnanje.
16. Ko je treba omogočiti vpogled v tajne podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje v zavarovanem območju, oddelek za tajne podatke zagotovi, da sta vpogled v zadevne podatke in ravnanje z njimi skladna s členoma 9 in 10 tega sklepa ter ustreznimi navodili za ravnanje.

G. TEHNIČNO VAROVANJE

17. Za ukrepe tehničnega varovanja je pristojen organ za varnostno akreditacijo, ki v ustreznih navodilih za ravnanje določi specifične ukrepe tehničnega varovanja, ki jih je treba uporabiti.
18. Zavarovane čitalnice za vpogled v tajne podatke stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje ter v „druge zaupne informacije“ so skladne s specifičnimi ukrepi tehničnega varovanja, kot so določeni v navodilih za ravnanje.

19. Zavarovano območje zajema naslednje prostore:

- (a) prostor za varnostno preverjanje, ki se namesti v skladu z ukrepi tehničnega varovanja, kot je določeno v navodilih za ravnanje. Dostop do tega prostora se zabeleži. Prostor za varnostno preverjanje ustreza visokim standardom v smislu identifikacije oseb z dostopom, videonadzora, zavarovanega prostora za odlaganje osebnih predmetov, ki jih ni dovoljeno nesti s seboj v zavarovane prostore (telefoni, pisala itd.);
- (b) komunikacijski prostor za pošiljanje in prejemanje tajnih podatkov, vključno s šifriranimi tajnimi podatki, v skladu z varnostnim obvestilom 3 in ustreznimi navodili za ravnanje;
- (c) zavarovani arhiv, v katerem se uporabljajo odobreni in potrjeni zabojniki ločeno za tajne podatke stopnje RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET EU/EU SECRET ali enakovredne stopnje. Tajni podatki stopnje TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje se hranijo v ločenem prostoru v posebej za to potrjenem zabojniku. V tem ločenem prostoru je poleg tega dovoljeno namestiti le pult, ki oddelku za tajne podatke omogoča delo z arhivom.
- (d) prostor za vpis, v katerem so orodja, potrebna za to, da se vpis izvede na papirju in v elektronski obliki ter se tako opremi v varnimi zmogljivostmi, potrebnimi za namestitve komunikacijskih in informacijskih sistemov. Prostor za vpis je edini prostor, v katerem so lahko odobrene in akreditirane naprave za reprodukcijo (kopije na papirju ali v elektronski obliki). V navodilih za ravnanje se določi, katere naprave so potrjene in akreditirane. Prostor za vpis ima tudi prostor, potreben za shranjevanje in uporabe akreditiranega materiala na način, ki omogoča označevanje, kopiranje in pošiljanje tajnih podatkov v fizični obliki glede na stopnjo tajnosti. Ves akreditiran material opredeli oddelk za tajne podatke in akreditira organ za varnostno akreditacijo v skladu z nasvetom, ki ga prejme od operativnega organa za zagotavljanje varnosti podatkov. Prostor za vpis je opremljen tudi z akreditirano napravo za uničevanje, odobreno za najvišjo raven tajnosti, kot je opisano v navodilih za ravnanje. Prevajanje tajnih podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje se opravi v prostoru za registracijo v primernem in akreditiranem sistemu. Prostor za registracijo vsebuje delovni prostor za največ dva prevajalca naenkrat za isti dokument. Pri tem je prisoten en uslužbenec oddelka za tajne podatke.
- (e) čitalnico, v kateri imajo osebe z ustreznim dovoljenjem individualni vpogled v tajne podatke. Čitalnica je dovolj velika za dve osebi, vključno z uslužbencem oddelka za tajne podatke, ki je prisoten ob vsakem vpogledu. Varovanje v tem prostoru ustreza vpogledu v tajne podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET. Čitalnica je lahko opremljena z opremo TEMPEST, ki po potrebi omogoča elektronski vpogled v skladu s stopnjo tajnosti zadevnih podatkov;
- (f) sejno sobo, ki mora biti dovolj velika, da lahko 25 oseb v njej razpravlja o tajnih podatkih stopnje CONFIDENTIEL UE/EU CONFIDENTIAL in SECRET EU/EU SECRET ali enakovredne stopnje. Sejna soba je opremljena z varovanimi in potrjenimi tehničnimi zmogljivostmi za tolmačenje v največ dva jezika. Kadar se sejna soba ne uporablja za sestanke, se lahko uporablja kot dodatna čitalnica za individualen vpogled. V izjemnih primerih lahko oddelk za tajne podatke dovoli vpogled v tajne podatke več kot eni pooblaščen osebi, če imajo vse osebe v prostoru enako stopnjo varnostne odobritve in enako potrebo po seznanitvi s podatki. Vpogled v tajne podatke se dovoli največ štirim osebam sočasno. Prisotnost uslužbencev oddelka za tajne podatke se okrepi;
- (g) zavarovane tehnične prostore za namestitve vse tehnične opreme, povezane z varovanjem celotnega zavarovanega območja, ter zavarovanih strežnikov IT.

20. Zavarovano območje je skladno z veljavnimi mednarodnimi varnostnimi standardi in ga potrdi direktorat za varnost in oceno tveganja. Zavarovano območje vsebuje naslednjo minimalno varnostno tehnično opremo:

- (a) alarme in varnostne sisteme za nadzor;
- (b) varnostno opremo in zasilne sisteme (dvosmerni sistem za opozarjanje);

- (c) sistem televizije zaprtega kroga (CCTV);
- (d) sistem odkrivanja vdorov;
- (e) nadzor dostopa (vključno z biometričnim varnostnim sistemom);
- (f) zabojnike;
- (g) omarice s ključavnico;
- (h) zaščito proti elektromagnetnemu sevanju.

21. Organ za varnostno akreditacijo lahko v tesnem sodelovanju z oddelkom za tajne podatke in po odobritvi varnostnega organa uvede druge dodatne ukrepe tehničnega varovanja.

22. Infrastrukturalna oprema je lahko povezana s sistemi splošnega upravljanja v stavbi, v kateri se nahaja zavarovano območje. Kljub temu je varnostna oprema, namenjena nadzoru dostopa ter komunikacijskim in informacijskim sistemom, ločena od vseh drugih obstoječih sistemov v Evropskem parlamentu.

H. INŠPEKCIJSKI PREGLEDI ZAVAROVANEGA OBMOČJA

23. Organ za varnostno akreditacijo na zahtevo oddelka za tajne podatke redno opravlja inšpekcijske preglede zavarovanega območja.

24. Organ za varnostno akreditacijo pripravi in posodablja kontrolni seznam varnostnih vidikov, ki jih je treba preveriti med inšpekcijskim pregledom v skladu z navodili za ravnanje.

I. PRENAŠANJE ZAUPNIH PODATKOV

25. Pri prenašanju se zaupne podatke zakrije in se ne navede nobena oznaka, ki bi izdajala zaupno naravo vsebine, v skladu z navodili za ravnanje.

26. Tajne podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje smejo prenašati zgolj kurirji ali uslužbenci z ustrežno stopnjo varnostne odobritve.

27. Zaupni podatki se lahko pošiljajo z zunanjo pošto ali ročno izven stavbe zgolj v skladu s pogoji iz navodil za ravnanje.

28. Tajni podatki stopnje CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje se nikoli ne pošiljajo po elektronski pošti ali telefaksu, tudi če je nameščen „varen“ e-poštni sistem ali telefaks s sistemom šifriranja. Tajne podatke stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje in druge zaupne podatke je dovoljeno pošiljati po elektronski pošti z uporabo akreditiranega šifrirnega sistema.

J. HRAMBA ZAUPNIH PODATKOV

29. Stopnja tajnosti ali oznaka, dodeljena zaupnim podatkom, določa raven zaščite teh podatkov pri njihovi hrambi. Hranijo se na opremi, potrjeni za ta namen v skladu z navodili za ravnanje.

30. Tajni podatki stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje in drugi zaupni podatki se:
- (a) hranijo, kadar se ne uporabljajo, v standardnih jeklenih zaklenjenih omarah, bodisi v pisarni bodisi v območju, kjer poteka delo;
 - (b) ne puščajo brez nadzora, razen če so ustrezno zaklenjeni in shranjeni;
 - (c) ne puščajo na pultu, mizi itd. na način, da bi jih lahko prebrala ali odstranila katerakoli nepooblaščen oseba, npr. obiskovalec, čistilec, vzdrževalec itd.;
 - (d) ne pokaže nobeni nepooblaščen osebi, niti se z nepooblaščen osebno o njih ne razpravlja.
31. Tajni podatki stopnje RESTREINT UE/EU RESTRICTED ali enakovredne stopnje in drugi zaupni podatki se hranijo izključno v sekretariatih parlamentarnih teles/nosilcev funkcij ali v oddelku za tajne podatke v skladu z navodili za ravnanje.
32. Tajni podatki stopnje CONFIDENTIEL UE/CONFIDENTIAL EU, SECRET UE/EU SECRET ali TRÈS SECRET UE/EU TOP SECRET ali enakovredne stopnje se:
- (a) hranijo v zavarovanem območju v zabojniku ali v trezorju. Izjemoma, na primer če je oddelek za tajne podatke zaprt, se lahko shranijo v odobrenem in potrjenem sefu pri varnostni službi;
 - (b) v zavarovanem območju nikoli ne puščajo brez nadzora, ne da bi jih prej zaklenili v odobren sef (tudi v primeru najkrajše odsotnosti);
 - (c) ne puščajo na pultu, mizi itd. na način, da bi jih lahko prebrala ali odstranila nepooblaščen oseba, tudi če je v prostoru prisoten odgovorni uslužbenec oddelka za tajne podatke.

Kadar se dokument, ki vsebuje tajne podatke, ustvari v elektronski obliki v zavarovanem območju, se računalnik zaklene in prepreči dostop do zaslona, če avtor dokumenta ali odgovorni uslužbenec oddelka za tajne podatke zapusti prostor (tudi v primeru najkrajše odsotnosti). Avtomatski sistem zaklepanja po nekaj trenutkih se ne šteje za zadosten ukrep.

VARNOSTNO OBVESTILO 5

INDUSTRIJSKA VARNOST

A. UVOD

1. To varnostno obvestilo zadeva samo tajne podatke.
2. Določa predpise za izvajanje skupnih minimalnih standardov iz 1. dela Priloge I k temu sklepu.
3. „Industrijska varnost“ je uporaba ukrepov, s katerimi se zagotovi, da izvajalci ali podizvajalci varujejo tajne podatke med pogajanjem za sklenitev pogodbe in v življenjskem ciklu pogodb s tajnimi podatki. Te pogodbe ne vključujejo dostopa do tajnih podatkov stopnje TRÈS SECRET UE/EU TOP SECRET.
4. Pri dodeljevanju pogodb s tajnimi podatki industrijskim ali drugim subjektom Evropski parlament kot naročnik zagotovi, da so izpolnjeni minimalni standardi industrijske varnosti iz tega sklepa in pogodbe.

B. VARNOSTNI ELEMENTI V POGODBAH S TAJNIMI PODATKI**B.1. Vodič po stopnjah tajnosti**

5. Pred objavo razpisa ali sklenitvijo pogodbe s tajnimi podatki Evropski parlament kot naročnik določi stopnjo tajnosti podatkov, ki se posredujejo ponudnikom in izvajalcem, pa tudi stopnjo tajnosti podatkov, ki jih bo ustvaril izvajalec. Za ta namen pripravi vodič po stopnjah tajnosti, ki se uporablja pri izvedbi naročila.

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

- (a) Evropski parlament pri pripravi vodiča po stopnjah tajnosti upošteva vse pomembne varnostne vidike, tudi stopnjo tajnosti, določeno posredovanim in odobrenim podatkom, ki jo avtor podatkov zagotovi in odobri za uporabo glede pogodbe;
- (b) splošna stopnja tajnosti naročila ne sme biti nižja od najvišje stopnje tajnosti njegovih posameznih elementov.

B.2. Listina o varnostnih vidikih

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

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

B.3. Varnostna navodila za program/projekt

9. Odvisno od obsega programov ali projektov, ki vključujejo dostop do tajnih podatkov EU ali delo z njimi ali njihovo hrambo, lahko naročnik, imenovan za vodenje programa ali projekta, pripravi posebna varnostna navodila za program/projekt.

C. VARNOSTNO DOVOLJENJE ORGANIZACIJE

10. Varnostno dovoljenje organizacije izda nacionalni varnostni organ ali kateri koli drug pristojni varnostni organ države članice, kar skladno z nacionalnimi zakoni in predpisi pomeni, da je industrijski ali drugi subjekt v svojih prostorih zmožen varovati tajne podatke EU stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET ali enakovredne stopnje. Dokaz o izdaji varnostnega dovoljenja organizacije se predloži Evropskemu parlamentu kot naročniku, še preden se izvajalcu ali podizvajalcu ali morebitnemu izvajalcu ali podizvajalcu posredujejo tajni podatki EU ali se mu odobri dostop do njih.

11. V varnostnem dovoljenju organizacije se:

- (a) oceni integriteta industrijskega ali drugega subjekta;
- (b) oceni lastništvo, nadzor ali vsako morebitno nedovoljeno vplivanje, ki lahko predstavlja varnostno tveganje;

- (c) preveri, ali ima industrijski ali drug subjekt v svojih prostorih vzpostavljen varnostni sistem z vsemi ustreznimi varnostnimi ukrepi, potrebnimi za varovanje tajnih podatkov ali materiala stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET v skladu z zahtevami iz tega sklepa;
- (d) preveri, ali so člani uprave, lastniki in zaposleni, ki naj bi imeli dostop do tajnih podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET, varnostno preverjeni v skladu z zahtevami iz tega sklepa, in
- (e) preveri, ali je industrijski ali drug subjekt imenoval svojega varnostnega uradnika, ki vodstvu odgovarja za izvajanje varnostnih obveznosti v subjektu.

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

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

14. Vsak pristojni varnostni organ, ki je izdal varnostno dovoljenje organizacije, uradno obvesti Evropski parlament kot naročnika o vseh spremembah, ki zadevajo varnostno dovoljenje organizacije. V primeru podizvajalske pogodbe se ustrezno obvesti ta pristojni varnostni organ.

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

D. POGODBE IN PODIZVAJALSKE POGODBE S TAJNIMI PODATKI

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

17. Ko je pogodba ali podizvajalska pogodba s tajnimi podatki dodeljena, Evropski parlament kot naročnik obvesti nacionalni varnostni organ ali kateri koli drug pristojni varnostni organ izvajalca ali podizvajalca o varnostnih določbah pogodbe s tajnimi podatki.

18. Ob prenehanju take pogodbe, Evropski parlament kot naročnik (in/ali pristojni varnostni organ v primeru podizvajalske pogodbe) nemudoma obvesti nacionalni varnostni organ ali kateri koli drug pristojni varnostni organ države članice, v kateri je izvajalec ali podizvajalec registriran.

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

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

21. Če sme izvajalec ali podizvajalec tajne podatke obdržati tudi po prenehanju veljavnosti pogodbe, se še naprej uporabljajo minimalni standardi iz tega sklepa in tajnost podatkov še vedno varuje izvajalec ali podizvajalec.
22. Pogoji, v skladu s katerimi lahko izvajalec sklene podizvajalsko pogodbo, so določeni v razpisu in v pogodbi.
23. Izvajalec pred oddajo delov pogodbe s tajnimi podatki podizvajalcu pridobi dovoljenje Evropskega parlamenta kot naročnika. Podizvajalska pogodba se ne sme dodeliti industrijskim ali drugim subjektom, registriranim v tretji državi, ki z Unijo ni sklenila sporazuma o varovanju tajnosti podatkov.
24. Izvajalec zagotovi, da se vse podizvajalske dejavnosti opravljajo v skladu z minimalnimi standardi iz tega sklepa, in podizvajalcu ne zagotovi tajnih podatkov brez predhodnega pisanega soglasja naročnika.
25. Kar zadeva tajne podatke, ki jih izvajalec ali podizvajalec ustvari ali z njimi dela, pravice avtorja uveljavlja naročnik.

E. OBISKI V ZVEZI S POGODBAMI S TAJNIMI PODATKI

26. Če morajo imeti Evropski parlament, izvajalci ali podizvajalci za izvajanje pogodbe s tajnimi podatki dostop do tajnih podatkov stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET v prostorih enih ali drugih, se v sodelovanju z zadevnimi nacionalnimi varnostnimi organi ali katerim koli drugim pristojnim varnostnim organom organizirajo obiski. Nacionalni varnostni organi pa se lahko za posebne projekte tudi sporazumejo o postopku, na podlagi katerega se je mogoče o takšnih obiskih dogovoriti neposredno.
27. Vsi obiskovalci imajo ustrezno dovoljenje za dostop do tajnih podatkov in zanje velja potreba po seznanitvi s podatki, kar jim omogoča dostop do tajnih podatkov, povezanih s pogodbo z Evropskim parlamentom.
28. Obiskovalci imajo dostop le do tajnih podatkov, povezanih z namenom obiska.

F. POŠILJANJE IN PRENOS TAJNIH PODATKOV

29. Za pošiljanje tajnih podatkov z elektronskimi sredstvi se uporabljajo ustrezne določbe iz varnostnega obvestila 3.
30. Za prenos tajnih podatkov se uporabljajo ustrezne določbe iz varnostnega obvestila 4 in ustreznih navodil za ravnanje.
31. Za prevoz tajnega gradiva kot tovora se pri določanju varnostnega režima upoštevajo naslednja načela:
- (a) varnost je zagotovljena v vseh fazah prevoza, od odhodnega kraja do namembnega kraja;
 - (b) stopnja zaščite se za pošiljko določi na podlagi gradiva z najvišjo stopnjo tajnosti, ki ga pošiljka vsebuje;
 - (c) za prevoznika se pridobi varnostno dovoljenje organizacije na ustrezni stopnji. V teh primerih mora biti osebje, ki dela s pošiljko, varnostno preverjeno v skladu s Prilogo I;

- (d) pošiljatelj pred vsakim čezmejnem premikom tajnega materiala stopnje CONFIDENTIEL UE/EU CONFIDENTIAL ali SECRET UE/EU SECRET ali enakovredne stopnje pripravi načrt prevoza, ki ga odobri generalni sekretar;
- (e) prevoze se, če je le mogoče, opravi od določenega odhodnega kraja do določenega namembnega kraja in v najkrajšem možnem času, ki ga dovoljujejo okoliščine;
- (f) če je le mogoče, se uporabljajo poti skozi države članice Unije.

G. POŠILJANJE TAJNIH PODATKOV IZVAJALCEM V TRETJIH DRŽAVAH

32. Pošiljanje tajnih podatkov izvajalcem in podizvajalcem v tretjih državah poteka v skladu z varnostnimi ukrepi, dogovorjenimi med Evropskim parlamentom kot naročnikom in zadevno tretjo državo, v kateri je registriran izvajalec.

H. DELO S TAJNIMI PODATKI STOPNJE RESTREINT UE/EU RESTRICTED IN NJIHOVA HRAMBA

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

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

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

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

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

38. Če pogodba vključuje delo s tajnimi podatki stopnje RESTREINT UE/EU RESTRICTED v komunikacijskih in informacijskih sistemih, ki jih upravlja izvajalec, Evropski parlament kot naročnik zagotovi, da se v pogodbi ali morebitni podizvajalski pogodbi določijo potrebne tehnične in upravne zahteve glede akreditacije teh komunikacijskih in informacijskih sistemov, ki so v sorazmerju z ocenjenim tveganjem ob upoštevanju vseh ustreznih dejavnikov. Naročnik in ustrezni nacionalni varnostni organ se dogovorita o obsegu akreditacije takšnih komunikacijskih in informacijskih sistemov.

VARNOSTNO OBVESTILO 6

KRŠITVE VAROVANJA TAJNOSTI, IZGUBA ALI OGROŽANJE ZAUPNIH PODATKOV

1. Kršitev varovanja tajnosti je posledica posameznikovega dejanja ali opustitve dejanja v nasprotju s tem sklepom, ki bi lahko ogrozilo ali razkrilo zaupne podatke.

2. Do ogrožanja zaupnih podatkov pride, kadar so ti podatki v celoti ali delno prišli v roke nepooblaščenim osebam, tj. osebam, ki nimajo niti ustreznega varnostne odobritve niti zanje ne velja potreba po seznanitvi s podatki, ali kadar obstaja možnost, da se je kaj takega zgodilo.

3. Do ogrožanja zaupnih podatkov lahko pride zaradi nepazljivosti, malomarnosti ali indiskretnosti, pa tudi zaradi dejavnosti služb, ki delujejo proti Uniji, ali subverzivnih organizacij.

4. Kadar generalni sekretar ugotovi oziroma je obveščen, da je dokazano prišlo do kršitve varovanja tajnosti, izgube ali ogrožanja v zvezi z zaupnimi podatki, ali v primeru suma take kršitve, izgube ali razkritja:

- (a) ugotovi dejstva;
- (b) oceni in zmanjša povzročeno škodo na minimum;
- (c) ukrepa, da se kršitev ne bi ponovila;
- (d) obvesti pristojni organ tretje strani ali države članice, ki je avtor zaupnih podatkov ali jih je posredovala.

Kadar gre za poslanca Evropskega parlamenta, generalni sekretar ukrepa skupaj s predsednikom Evropskega parlamenta.

Če so bili podatki pridobljeni od drugih institucij Unije, generalni sekretar ukrepa v skladu z ustreznimi varnostnimi ukrepi za tajne podatke in vzpostavljeno ureditvijo, določeno na podlagi Okvirnega sporazuma s Komisijo ali Medinstitucionalnega sporazuma s Svetom.

5. Vse osebe, ki morajo ravnati z zaupnimi podatki, se temeljito podučijo o varnostnih postopkih, nevarnostih indiskretnega razpravljanja in odnosih z mediji, te osebe pa po potrebi podpišejo izjavo, da ne bodo razkrile vsebine zaupnih podatkov tretjim osebam, da bodo spoštovale obveznosti glede zaščite tajnih podatkov ter da so seznanjene s posledicami ravnanja v nasprotju s to izjavo. Dostop do tajnih podatkov ali njihova uporaba s strani osebe, ki ni tako seznanjena in ki ni podpisala ustrezne izjave, se šteje kot kršitev varovanja tajnosti.

6. Poslanci Evropskega parlamenta, uradniki Parlamenta in drugi uslužbenci Parlamenta, ki dela v politični skupini ali za pogodbenega sodelavca, generalnemu sekretarju nemudoma poroča o vsakršni kršitvi varovanja tajnosti, izgubi ali ogrožanju zaupnih podatkov, za katero bi utegnili izvedeti.

7. Vsaka oseba, ki je odgovorna za ogrožanje zaupnih podatkov, je disciplinsko odgovorna v skladu z ustreznimi pravili in predpisi. Tako disciplinsko ukrepanje ne posega v noben sodni postopek, ki se lahko sproži v skladu z veljavno zakonodajo.

8. Brez poseganja v druge sodne postopke, se za kršitve, ki jih storijo uradniki Parlamenta in drugi uslužbenci Parlamenta, ki delajo v političnih skupinah, uporabljajo postopki in kazni iz naslova VI Kadrovskih predpisov.

9. Brez poseganja v druge sodne postopke, se kršitve, ki jih storijo poslanci Evropskega parlamenta, obravnavajo v skladu s členom 9(2) ter členi 152, 153 in 154 Poslovnika Evropskega parlamenta.

