IV

(Informacije)

INFORMACIJE INSTITUCIJ, ORGANOV, URADOV IN AGENCIJ EVROPSKE UNIJE

EVROPSKI PARLAMENT

SKLEP PREDSEDSTVA EVROPSKEGA PARLAMENTA

z dne 6. junija 2011

o pravilniku o obdelavi zaupnih podatkov s strani Evropskega parlamenta

(2011/C 190/02)

PREDSEDSTVO EVROPSKEGA PARLAMENTA JE –

ob upoštevanju člena 23(12) Poslovnika Evropskega parlamenta,

ob upoštevanju naslednjega:

(1) Z ozirom na Okvirni sporazum o odnosih med Evropskim parlamentom in Evropsko komisijo ([1]), podpisanega dne 20. oktobra 2010 (v nadaljnjem besedilu: Okvirni sporazum), je treba ponovno pregledati sklep predsedstva z dne 13. novembra 2006 o upravni obdelavi zaupnih dokumentov.

(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, vključno s tajnimi, 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 člen 15 Pogodbe o delovanju Evropske unije (v nadaljnjem besedilu: PDEU) in v Uredbo (ES) št. 1049/2001 Evropskega parlamenta in Sveta z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije ([2]).

(5) Določbe tega sklepa ne posegajo v člen 16 PDEU in v Uredbo (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov ([3]) –

SPREJELO NASLEDNJI SKLEP:

Člen 1

Cilj

Ta sklep ureja nastanek, sprejemanje, posredovanje in shranjevanje zaupnih podatkov s strani Evropskega parlamenta, zato da se ustrezno zaščiti njihova zaupna narava. Pomeni zlasti izvedbo Priloge 2 k Okvirnem sporazumu.

([1]) UL L 304, 20.11.2010, str. 47.

([2]) UL L 145, 31.5.2001, str. 43.

([3]) UL L 8, 12.1.2001, str. 1.

Člen 2

Opredelitev pojmov

Za namene tega sklepa:

(a) „podatki“ pomenijo vsak pisni ali ustni podatek, ne glede na nosilec in avtorja.

(b) „zaupni podatki“ pomenijo tajne podatke EU, tajne podatke ter druge netajne podatke zaupne narave.

(c) „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 EU ali ene ali več držav članic, ne glede na to, ali taki podatki izvirajo znotraj institucij, organov, uradov in agencij, ustanovljenih v okviru ali na podlagi Pogodb, ali pridejo iz držav članic, tretjih držav ali mednarodnih organizacij. Tako je:

— TRÈS SECRET UE/EU TOP SECRET stopnja tajnosti za podatke 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 stopnja tajnosti za podatke in gradivo, katerih nedovoljeno razkritje bi lahko resno škodovalo temeljnim interesom Unije ali ene ali več držav članic;

— CONFIDENTIEL UE/EU CONFIDENTIAL stopnja tajnosti za podatke in gradivo, katerih nedovoljeno razkritje bi lahko škodovalo temeljnim interesom Unije ali ene ali več držav članic;

— RESTREINT UE/EU RESTRICTED stopnja tajnosti za podatke in gradivo, katerih nedovoljeno razkritje bi bilo lahko neugodno za interese Unije ali ene ali več držav članic;

(d) „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.

(e) „dokument“ pomeni vse shranjene informacije, ne glede na njihovo fizično obliko ali značilnosti.

(f) „gradivo“ pomeni vse dokumente ali dele naprav ali opreme, bodisi izdelane bodisi v postopku izdelave.

(g) „potreba po seznanitvi“ pomeni potrebo osebe, da ima dostop do zaupnih podatkov, da lahko izvrši uradno dolžnost ali nalogo.

(h) „dovoljenje“ pomeni odločitev (odločitev o odobritvi) predsednika, če zadeva poslance Evropskega parlamenta, in generalnega sekretarja, če zadeva uradnike Evropskega parlamenta in druge uslužbence Parlamenta, ki delajo v političnih skupinah, o dovolitvi posamezniku, da dostopa do tajnih podatkov EU 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.

(i) „znižanje“ pomeni določitev nižje stopnje tajnosti.

(j) „odprava“ pomeni odstranitev vsakršne tajnosti.

(k) „avtor“ pomeni ustrezno pooblaščenega avtorja tajnega podatka EU ali katerega koli drugega zaupnega podatka.

(l) „varnostna obvestila“ pomenijo tehnične izvedbene ukrepe, kakor so določeni v Prilogi II [1].

Člen 3

Temeljna načela in minimalni standardi

1. Obdelava zaupnih podatkov s strani Evropskega parlamenta sledi temeljnim 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 informacij, katerega cilj je olajšati parlamentarno in upravno delo, hkrati pa zagotoviti varstvo vsakršnih zaupnih podatkov, ki jih obdela Parlament, ob popolnem upoštevanju pravil, ki jih opredeli avtor teh podatkov, kakor je določeno v varnostnih obvestilih.

Obdelava zaupnih podatkov s pomočjo avtomatskih informacijskih sistemov Evropskega parlamenta se izvaja v skladu z zasnovo zagotavljanja varnosti podatkov in se določi v varnostnih obvestilih.

[1] Priloga bo sprejeta naknadno.

3. Poslanci Evropskega parlamenta lahko brez varnostne odobritve dostopajo do tajnih podatkov vse do vključno stopnje CONFIDENTIEL UE/EU CONFIDENTIAL. Za dostop do podatkov, ki so določeni kot CONFIDENTIEL UE/EU CONFIDENTIAL, podpišejo častno izjavo, da vsebine teh podatkov ne bodo razkrili tretjim osebam. Podatki, ki jim je določena stopnja nad CONFIDENTIEL UE/EU CONFIDENTIAL, so na voljo le tistim poslancem, ki imajo ustrezno stopnjo varnostne odobritve.

4. 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.

Člen 4

Nastanek zaupnih podatkov in njihova upravna obdelava s strani Evropskega parlamenta

1. Predsednik Evropskega parlamenta, predsedniki zadevnih 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 Službi za zaupne podatke (v nadaljnjem besedilu: SZP), ko se dokument deponira pri SZP.

3. Zaupni podatki, za katere velja poklicna molčečnost, se obravnavajo v skladu z navodili za ravnanje, določenimi v varnostnih obvestilih.

Člen 5

Sprejemanje zaupnih podatkov s strani Evropskega parlamenta

1. Zaupni podatki, ki jih prejme Evropski parlament, se sporočijo, kakor je določeno v nadaljevanju:

— tajni podatki EU, določeni kot RESTREINT UE/EU RESTRICTED, in drugi zaupni podatki sekretariatu parlamentarnega telesa/nosilca funkcije, ki je vložil zahtevo zanje;

— tajni podatki EU, določeni kot CONFIDENTIEL UE/CONFIDENTIAL EU in višje, SZP.

2. Registracijo, shranjevanje in sledljivost zaupnih podatkov zagotovita bodisi sekretariat parlamentarnega telesa/nosilca funkcije, ki je prejel podatke, oziroma SZP.

3. Če gre za zaupne podatke, ki jih sporoči Komisija na podlagi Okvirnega sporazuma, se dogovori v smislu točke 3.2 Priloge 2 k Okvirnem sporazumu (določeni v medsebojnem soglasju in ki se nanašajo na naslovnike, postopek posvetovanja, tj. varno sobo za branje in zasedanje za zaprtimi vrati ali druge zadeve), katerih namen je ohranjati zaupnost podatkov, skupaj z zaupnimi podatki deponirajo pri sekretariatu parlamentarnega telesa/nosilca funkcije ali pri SZP, če je podatkom določena stopnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje.

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. Tajni podatki EU, določeni kot TRÈS SECRET UE/EU TOP SECRET, se posredujejo Evropskemu parlamentu v skladu z dodatnimi dogovori, o katerih se uskladita parlamentarno telo/nosilec funkcije, ki je vložil zahtevo za podatke, in institucije EU oziroma države članice, ki podatke sporočijo. Konferenca predsednikov ustanovi nadzorni odbor. Njegov cilj je zagotoviti stopnjo varstva, skladno s stopnjo tajnosti.

Člen 6

Sporočanje tajnih podatkov EU s strani Evropskega parlamenta tretjim osebam

Evropski parlament lahko, če avtor s tem soglaša, posreduje tajne podatke EU drugim institucijam, organom, uradom in agencijam, ustanovljenim v okviru ali na podlagi pogodb, ali državam članicam, pod pogojem, da pri obdelavi tajnih podatkov EU v njihovih službah in prostorih zagotavljajo spoštovanje pravil, enakovrednih tem iz tega sklepa.

Člen 7

Shranjevanje in vpogled v zaupne podatke v varnih območjih (varne sobe za branje)

1. Varna soba za branje omogoča varno shranjevanje in ne vsebuje fotokopirnih naprav, telefonov, telefaksa, optičnih čitalcev ali druge tehnične opreme za razmnoževanje ali prenos dokumentov.

2. Dostop do varne sobe za branje urejajo naslednji pogoji:

(a) dostop do varne sobe za branje imajo le naslednje osebe:

— poslanci Evropskega parlamenta, uradniki Evropskega parlamenta in drugi uslužbenci Parlamenta, ki delajo v političnih skupinah, katerih istovetnost je ustrezno ugotovljena, v skladu z določbami iz člena 4(2) ali člena 5(3) in (4);

— uradniki Evropskega parlamenta, ki so odgovorni za vodenje SZP;

— po potrebi uradniki Evropskega parlamenta, odgovorni za varnost in požarno varnost.

Čiščenje varnega območja poteka le v prisotnosti in pod strogim nadzorom uradnika, zaposlenega v SZP.

(b) vsakdo, ki želi dostopati do zaupnih podatkov, vnaprej sporoči svoje ime SZP. SZP preveri istovetnost vsakogar, ki predloži prošnjo za vpogled v te podatke, ter po potrebi preveri, ali ima ta oseba potrebno stopnjo varnostne odobritve in je za to pooblaščena v skladu z določbami iz člena 4(2) ali člena 5(3) in (4);

(c) SZP lahko zavrne dostop do sobe vsakomur, ki nima dovoljenja za vstop v skladu s točkama (a) in (b). Vsak ugovor zoper odločitev SZP se vloži pri predsedniku, če gre za poslance Evropskega parlamenta, ter pri generalnemu sekretarju v ostalih primerih.

3. Vpogled v zaupne podatke v varni sobi za branje urejajo naslednji pogoji:

(a) osebe, ki so pooblaščene za vpogled v podatke in ki so predložile vlogo iz točke (b) odstavka 2, se zglasijo pri SZP.

Razen v izjemnih primerih (denimo zaradi številnih zahtev za vpogled, vloženih v kratkem času), se samo eni osebi naenkrat dovoli vpogled v zaupne podatke v varni sobi za branje, v prisotnosti uradnika SZP.

Ta uradnik osebo, ki ima dovoljenje za vpogled v zaupne podatke, seznani z njenimi obveznostmi in jo zlasti prosi, da podpiše častno izjavo, da ne bo razkrila vsebine teh podatkov nobeni tretji osebi;

(b) med vpogledom so stik z zunanjim svetom (vključno z uporabo telefonov in druge tehnologije), izdelava zapiskov ter fotokopiranje ali fotografiranje zaupnih podatkov prepovedani;

(c) preden se osebi dovoli, da zapusti varno sobo za branje, odgovorni uradnik SZP iz točke (a) preveri, da so vsi zaupni podatki, v katere je bilo vpogledano, še vedno na mestu ter da so nedotaknjeni in popolni.

4. V primeru kršitve zgornjih pravil odgovorni uradnik SZP o tem obvesti generalnega sekretarja, ki zadevo preda predsedniku, če je kršitelj poslanec Evropskega parlamenta.

Člen 8

Minimalni standardi za druge vrste vpogleda v zaupne podatke

1. V zvezi z upravno obdelavo zaupnih podatkov na seji za zaprtimi vrati, sekretariat parlamentarnega telesa/nosilca funkcije, ki je odgovoren za sejo, zagotovi, da:

— se dovoli vstop v sejno sobo le osebam, ki naj bi sodelovale na seji in ki imajo potrebno stopnjo varnostne odobritve;

— so vsi dokumenti oštevilčeni, razdeljeni na začetku in pobrani na koncu seje, ter da se o teh dokumentih ne naredijo zapiski, fotokopije ali fotografije;

— se v zapisniku seje ne omenja vsebina razprave o podatkih, obravnavanih v skladu z zaupnim postopkom;

— za zaupne podatke, ki so prejemnikom v Evropskem parlamentu posredovani ustno, velja enakovredna stopnja varstva kakor za zaupne podatke, posredovane v pisni obliki. To lahko vključuje častno izjavo prejemnika podatkov, da jih ne bo razkril nobeni tretji osebi.

2. V zvezi z upravno obdelavo zaupnih podatkov s strani sekretariata parlamentarnega telesa/nosilca funkcije zunaj seje za zaprtimi vrati se uporabljajo naslednja pravila:

— fizični izvod dokumentov se izroči osebno vodji sekretariata, ki jih registrira in izda potrdilo o prejemu;

— taki dokumenti se hranijo pod ključem, zanje pa, ko niso v dejanski uporabi, odgovarja sekretariat;

— brez poseganja v upravno obdelavo zaupnih podatkov na seji za zaprtimi vrati, kakor je določeno v odstavku 1, jih v nobenem primeru ni dovoljeno razmnoževati, shraniti na drug nosilec ali jih komurkoli posredovati;

— dostop do takih dokumentov se omeji na njihove naslovnike, nadzoruje pa ga sekretariat v skladu z določbami iz člena 4(2) ali člena 5(3) ali (4);

— sekretariat vodi evidenco oseb, ki so vpogledali v dokumente, ter o datumu in uri vpogleda. Ta evidenca se posreduje SZP v okviru uvedbe letnega poročila iz člena 12.

Člen 9

Arhiviranje zaupnih podatkov

1. V prostorih Evropskega parlamenta so na voljo varni prostori za arhiviranje.

Zaupni podatki, ki so dokončno deponirani pri SZP ali sekretariatu parlamentarnega telesa/nosilca funkcije, se premestijo v varni arhiv v SZP šest mesecev zatem, ko je bilo vanje zadnjič vpogledano, in najpozneje eno leto zatem, ko so bili deponirani.

2. SZP je odgovorna za upravljanje varnih arhivov v skladu s standardnimi merili za arhiviranje.

3. V zaupne podatke, ki se hranijo v zaupnih arhivih, je mogoče vpogledati pod naslednjimi pogoji:

— le osebam, ki so z imenom ali funkcijo opredeljene v spremljevalnem dokumentu, sestavljenem, ko so bili zaupni podatki deponirani, se dovoli, da vpogledajo v te podatke;

— vlogo za vpogled v zaupne podatke je treba predložiti SZP, ki predmetne dokumente prenese v varno sobo za branje;

— uporabljajo se postopki in pogoji iz člena 7, ki urejajo vpogled v zaupne podatke.

Člen 10

Zniževanje stopenj tajnosti oziroma odprava tajnosti tajnih podatkov EU

1. Stopnja tajnosti tajnih podatkov EU se lahko zniža oziroma tajnost odpravi le z dovoljenjem avtorja in, če je to potrebno, po posvetovanju z drugimi zainteresiranimi stranmi. 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 stopnjo tajnosti oziroma tajnost odpravi. V nasprotnem primeru avtorji preverjajo dokumente najpozneje vsakih pet let, da se zagotovi, da je izvirna stopnja tajnosti potrebna.

2. Odprava tajnosti dokumentov v zaupnih arhivih se opravi najpozneje po 30 letih, 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.

Člen 11

Kršitev tajnosti zaupnih podatkov

1. Kršitve tajnosti na splošno, zlasti pa tega sklepa, v primeru poslancev Evropskega parlamenta pomenijo uporabo ustreznih kazenskih določb iz Poslovnika Evropskega parlamenta.

2. Te kršitve, ki jih opravijo zaposleni, vodijo 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).

3. Predsednik in generalni sekretar organizirata potrebne preiskave.

Člen 12

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

1. Generalni sekretar predlaga vse potrebne prilagoditve tega sklepa in prilog o njegovem izvajanju ter te predloge posreduje predsedstvu v odločanje.

2. Generalni sekretar predsedstvu predloži letno poročilo o uporabi tega sklepa.

([1]) UL L 43, 15.2.1983, str. 1.
([2]) UL L 56, 4.3.1968, str. 1.

Člen 13

Prehodne in končne določbe

1. Zaupnim podatkom, ki pred uporabo tega sklepa že obstajajo v SZP ali v arhivu, se samodejno določi stopnja tajnosti RESTREINT UE/EU RESTRICTED, razen če avtor v roku enega leta od dneva uveljavitve tega sklepa sklene, da se jih ne določi kot tajne ali da se jim določi višja stopnja tajnosti ali se jih ustrezno označi.

2. Če avtor sklene, da se takim zaupnim podatkom določi višja stopnja tajnosti, mu avtor ali njegovi pooblaščenci določijo najnižjo možno stopnjo, v sodelovanju s SZP in v skladu z merili iz Priloge I.

3. Razveljavi se sklep predsedstva z dne 13. novembra 2006 o pravilniku o upravni obdelavi zaupnih dokumentov.

4. Razveljavi se sklep predsedstva z dne 24. oktobra 2005, ki generalnega sekretarja pooblašča za ustanovitev odbora za odpravo tajnosti in za sprejemanje odločitev s področja odprave tajnosti.

Člen 14

Začetek veljavnosti

1. Ta sklep začne veljati z dnem objave v *Uradnem listu Evropske unije*.

2. Uporablja se od 1. julija 2011.

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, ki jih je treba upoštevati v vseh krajih dela Evropskega parlamenta, upoštevati pa jih morajo tudi vsi prejemniki tajnih podatkov EU in drugih zaupnih podatkov, tako da je varnost zagotovljena in da je vsakdo lahko prepričan, da je vzpostavljen skupni standard varstva. Dopolnjujejo ga pravila za obdelavo zaupnih podatkov s strani parlamentarnih odborov in drugih parlamentarnih teles/nosilcev funkcij.

2. **Splošna 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.

Načelo zakonitosti pri izvrševanju varnostnih funkcij predstavlja potrebo po doslednem delovanju v okviru pravnega sistema in po spoštovanju ustreznih pravnih zahtev. Pomeni tudi, da 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 pomeni, da je treba kršitve varnosti v okviru pristojnosti Evropskega parlamenta obravnavati na način, ki je v skladu s politiko Evropskega parlamenta o disciplinskih ukrepih.

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

Načelo odgovornosti pomeni, da so pristojnosti na področju varnosti jasno določene. Poleg tega predstavlja tudi potrebo po rednem preverjanju, ali se te pristojnosti pravilno izvajajo.

Načelo subsidiarnosti pomeni, da se varnost zagotovi na najnižji možni ravni in kolikor mogoče blizu generalnih direktoratov in služb Evropskega parlamenta. Načelo sorazmernosti pomeni, da se varnostne dejavnosti omejijo samo na najbolj nujno in da so varnostni ukrepi sorazmerni z interesi, ki jih je treba varovati, in z dejanskim ali morebitnim ogrožanjem teh interesov, z namenom omogočiti njihovo zaščito na način, ki povzroča čim manj motenj.

3. **Temelji varnosti podatkov**

Temelji zanesljive varnosti podatkov so:

(a) tehnični organ INFOSEC (varnost podatkov) v Evropskem parlamentu, ki je pristojen za to, da v sodelovanju z zadevnim varnostnim organom zagotavlja podatke in nasvete o nevarnostih tehničnega značaja ter sredstvih za zaščito pred njimi;

(b) tesno sodelovanje med pristojnimi službami Evropskega parlamenta in varnostnimi službami drugih institucij EU.

4. **Načela varovanja podatkov**

4.1 *Cilji*

Glavni cilji varovanja podatkov so naslednji:

(a) varovanje tajnih podatkov EU in drugih zaupnih podatkov pred vohunstvom, ogrožanjem ali nepooblaščenim razkritjem;

(b) varovanje tajnih podatkov EU, obdelovanih v komunikacijskih in informacijskih sistemih ter omrežjih, pred ogrožanjem njihove zaupnosti, celovitosti in razpoložljivosti;

(c) varovanje prostorov Evropskega parlamenta, v katerih se nahajajo tajni podatki EU, pred sabotažo in zlonamernimi naklepnimi poškodbami;

(d) v primeru varnostne napake ocena povzročene škode, omejitev njenih posledic, izvedba varnostnih preiskav ter sprejetje 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, ki omogoča uveljavitev načel iz tega oddelka; pri načrtovanju in organiziranju načinov za boj proti vohunstvu, sabotaži, terorizmu in drugim nevarnostim se uporabi podoben sistem določanja stopnje tajnosti, tako da je najpomembnejšim prostorom, v katerih so shranjeni tajni podatki EU, in najobčutljivejšim točkam znotraj njih namenjena največja možna mera varstva.

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

4.2.4 Stopnja tajnosti sme temeljiti izključno na vsebini podatkov.

4.2.5 Kadar se različni podatki povežejo v celoto, zanjo velja stopnja tajnosti, ki mora biti najmanj enaka najvišji stopnji, določeni posameznim podatkom. 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 EU, nosilcev tajnih podatkov EU 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 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 ti podatki razširjajo samo na podlagi načela potrebe po seznanitvi, ki je temeljno glede vseh vidikov varnosti;

(e) zagotavljajo celovitost (tj. preprečujejo ponarejanje, nedovoljeno spreminjanje ali nedovoljen izbris) in razpoložljivost (tj. da dostop ni prepovedan tistim, ki ga potrebujejo in so zanj pooblaščeni) vseh zaupnih podatkov, bodisi tajnih ali ne, zlasti pa podatkov, ki so shranjeni ali obdelani v elektromagnetni obliki oziroma se v taki obliki prenašajo.

5. **Skupni minimalni standardi**

Evropski parlament zagotovi, da vsi prejemniki tajnih podatkov EU 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 ravnalo 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 zunanjim organom le, če zagotovijo, da bodo pri rokovanju ravnali 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 za uradnike evropskega parlamenta in drugih uslužbencev parlamenta, ki delajo v političnih skupinah**

6.1 *Varnostni napotki za 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 EU, 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*

Vodstveno osebje je dolžno biti seznanjeno s tem, kateri podrejeni imajo pri svojem delu opravka s tajnimi podatki oziroma imajo dostop do zavarovanih komunikacijskih ali informacijskih sistemov, prav tako pa evidentirati in poročati 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 drugemu 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 se 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 EU.

7.1 *Potreba po varstvu*

Stopnja ukrepov fizičnega varovanja, ki se uporabljajo za zagotavljanje varstva tajnih podatkov EU, je sorazmerna z določitvijo stopnje tajnosti, obsegom in ogroženostjo predmetnih podatkov in gradiva. Vsi imetniki tajnih podatkov EU 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*

Preden se območja s tajnimi podatki EU pusti nenadzorovana, morajo osebe, ki so zadolžene za njihovo hrambo, zagotoviti, da so ti podatki 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 so tajni podatki EU ali zavarovani komunikacijski in informacijski sistemi, se zavarujejo pred nepooblaščenim dostopom.

Vrsta varstva tajnih podatkov EU, npr. rešetke na oknih, vratne ključavnice/zapahi, vhodna straža, samodejni sistemi nadzora dostopa, varnostna preverjanja in obhodne patrulje, alarmni sistemi, sistemi odkrivanja vsiljivcev 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.

Podobno je vrsta varstva komunikacijskih in informacijskih sistemov 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 *Načrt ukrepov ob nepredvidljivih dogodkih*

Vnaprej se pripravijo podrobni načrti za varstvo 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 členu 2(c) 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. Ta označevalnik je bodisi „UNTIL … (čas/datum)“ ali „UNTIL … (dogodek)“.

Dodatni varnostni označevalniki, kot so označevalniki CRYPTO ali kateri koli drugi varnostni označevalnik, ki ga priznava EU, se uporabljajo, kadar je poleg navedb stopnje tajnosti potrebno tudi omejeno pošiljanje in posebno ravnanje.

Varnostni označevalniki se uporabljajo le skupaj s stopnjo tajnosti.

8.2 *Oznake*

Z oznako je mogoče opredeliti področje, ki ga pokriva določeni dokument, ali pošiljanje na podlagi „potrebe po seznanitvi“ ali (pri podatkih, ki niso tajni) označiti konec embarga.

Oznaka ni stopnja tajnosti in se ne sme uporabljati namesto nje.

8.3 *Namestitev stopnje tajnosti in varnostnih označevalnikov*

Stopnja tajnosti se označi:

(a) na dokumentih stopnje RESTREINT UE/EU RESTRICTED z mehanskimi ali elektronskimi sredstvi;

(b) na dokumentih stopnje CONFIDENTIEL EU/EU CONFIDENTIAL z mehanskimi sredstvi, ročno ali s tiskanjem na predhodno žigosan in registriran papir;

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

Varnostni označevalniki se namestijo neposredno pod stopnjo tajnosti z uporabo enakih sredstev kot za namestitev stopnje tajnosti.

8.4 *Upravljanje s stopnjami tajnosti podatkov*

8.4.1 S p l o š n o

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 dokumentov stopnje TRÈS SECRET UE/EU TOP SECRET, mora ostati čim nižje, njihova imena pa se vodijo na seznamu SZP.

8.4.2 Uporaba stopnje tajnosti

Stopnja tajnosti dokumenta se določi glede na stopnjo občutljivosti njegove vsebine v skladu z opredelitvijo iz člena 2(c). Pomembno je, da se stopnja tajnosti uporablja pravilno in preudarno. To velja zlasti za stopnjo tajnosti TRÈS SECRET UE/EU TOP SECRET.

Stopnja tajnosti pisma ali zabeležke k priloženim delom je enaka najvišji stopnji tajnosti, določenih enemu njenih priloženih delov. 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 vsakršni težnji po previsoki ali prenizki stopnji 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. **Pregledi**

Direktorat Evropskega Parlamenta, pristojen za varnost, ki mu lahko pri izvajanju naloge pomaga SZP, redno preverja varnostno ureditev za varstvo tajnih podatkov EU.

Tudi direktorat Evropskega Parlamenta, pristojen za varnost, ter varnostne službe drugih institucij, organov, uradov in agencij, ustanovljenih v okviru ali na podlagi pogodb, ki ravnajo s tajnimi podatki EU, se lahko dogovorijo za izvajanje medsebojnih pregledov varnostne ureditve z namenom varstva zaupnih podatkov EU.

10. **Postopek odprave tajnosti**

10.1 SZP preuči tajne podatke EU in najpozneje 25. leto po datumu, ko je dokument nastal, poda predloge glede odprave tajnosti njegovemu avtorju. Dokumenti, pri katerih se tajnost ne odpravi ob prvem pregledu, se periodično pregledujejo najmanj vsakih pet let.

10.2 Poleg dokumentov, ki so že v varovanih arhivih in so razvrščeni v ustrezno stopnjo tajnosti, lahko postopek odprave tajnosti zajema tudi druge zaupne podatke, ki obstajajo v varovanih arhivih ali v Arhivu in dokumentacijskem centru Evropskega parlamenta (CARDOC).

10.3 SZP je zadolžena, da v imenu avtorja o spremembi stopnje 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 oznake, ki utegnejo biti nameščene na dokumentu.

10.5 Prvotna stopnja tajnosti na vrhu in dnu vsake strani se prečrta. Prva (naslovna) stran dokumenta se ožigosa in izpolni s podatki SZP.

10.6 Besedilo dokumenta z odpravljeno tajnostjo 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 velja naslednje:

(a) kadar gre za dokumente tretjih oseb, se SZP posvetuje z njimi, preden nadaljuje z odpravo tajnosti. Tretja oseba ima na voljo osem tednov časa, da poda pripombe;

(b) kadar gre za izjeme v zvezi z varovanjem zasebnosti in integritete posameznika, se pri postopku odprave tajnosti upošteva zlasti soglasje zadevne osebe, nemožnost ugotavljanja istovetnosti zadevne osebe in/ali dejstvo, da ta oseba ni več živa;

(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.

2. DEL

POSTOPEK PRIDOBITVE VARNOSTNE ODOBRITVE

11. **Postopek pridobitve varnostne odobritve za poslance Evropskega parlamenta**

11.1 Z ozirom na pravice in pristojnosti Evropskega parlamenta se lahko njegovim poslancem omogoči dostop do tajnih podatkov EU do vključno stopnje CONFIDENTIEL UE/EU CONFIDENTIAL brez varnostne odobritve. Za podatke stopnje CONFIDENTIEL UE/EU CONFIDENTIAL poslanci podpišejo častno izjavo, da ne bodo razkrili vsebine teh dokumentov nobeni tretji osebi.

11.2 Za dostop do podatkov stopnje TRÈS SECRET UE/EU TOP SECRET ali SECRET UE/EU SECRET morajo imeti poslanci Evropskega parlamenta dovoljenje v skladu s postopkom iz točk 11.3 in 11.4.

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 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, pristojen za varnost, 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 petih 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 organi države članice podajo 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 in potem, ko je o potrebnem uradno obvestil pristojne organe ter pod pogojem, da 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 podatkov stopnje TRÈS SECRET UE/EU TOP SECRET.

12. **Postopek pridobitve varnostne odobritve 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 podatkov stopnje TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET in CONFIDENTIEL UE/EU CONFIDENTIAL morajo imeti osebe iz točke 12.1 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 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, pristojen za varnost, 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 zadevne osebe 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 podatkov, ki jim je določena stopnja tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje.

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 zadevni osebi, da lahko pristojni nacionalni organi opravijo varnostno preverjanje in podajo mnenje o stopnji dovoljenja, ki bi ga bilo ustrezno 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 predpisi v zvezi s pritožbami.

12.12 Kadar pristojni nacionalni organi države članice podajo pozitivno mnenje, lahko generalni sekretar zadevni osebi izda ustrezno dovoljenje.

12.13 Kadar pristojni nacionalni organi podajo 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 pristojne nacionalne organe 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 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 tega oddelka in potem, ko je o potrebnem uradno obvestil pristojne nacionalne organe ter pod pogojem, da od njih 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 izdana začasna dovoljenja ne omogočajo dostopa do podatkov stopnje tajnosti TRÈS SECRET UE/EU TOP SECRET.