IV

(Informácie)

INFORMÁCIE INŠTITÚCIÍ, ORGÁNOV, ÚRADOV A AGENTÚR EURÓPSKEJ ÚNIE

EURÓPSKY PARLAMENT

ROZHODNUTIE PREDSEDNÍCTVA EURÓPSKEHO PARLAMENTU

zo 6. júna 2011

o pravidlách zaobchádzania s dôvernými informáciami zo strany Európskeho parlamentu

(2011/C 190/02)

PREDSEDNÍCTVO EURÓPSKEHO PARLAMENTU,

so zreteľom na článok 23 ods. 12 Rokovacieho poriadku Európskeho parlamentu,

keďže:

(1) Vzhľadom na Rámcovú dohodu o vzťahoch medzi Európskym parlamentom a Európskou komisiou [1] podpísanú 20. októbra 2010 (ďalej len „rámcová dohoda“) je potrebná revízia rozhodnutia Predsedníctva z 13. novembra 2006 o predpisoch o zaobchádzaní s dôvernými dokumentmi.

(2) Lisabonská zmluva ukladá Európskemu parlamentu nové úlohy a aby mohol Európsky parlament vykonávať činnosti v tých oblastiach, ktoré si vyžadujú určitý stupeň utajenia, je potrebné stanoviť základné zásady, minimálne bezpečnostné normy a vhodné postupy pre zaobchádzanie s dôvernými informáciami zo strany Európskeho parlamentu, a to vrátane utajovaných skutočností.

(3) S cieľom uľahčiť hladké fungovanie rozhodovacieho procesu v Európskej únii majú pravidlá uvedené v tomto rozhodnutí zabezpečiť rovnakú úroveň ochrany ako zabezpečujú pravidlá prijaté ostatnými inštitúciami, orgánmi, úradmi a agentúrami zriadenými zmluvami alebo na základe zmlúv alebo členskými štátmi, ako aj ich zlučiteľnosť s týmito pravidlami.

(4) Ustanoveniami tohto rozhodnutia nie je dotknutý článok 15 Zmluvy o fungovaní Európskej únie (ZFEÚ) ani nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 z 30. mája 2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie [2].

(5) Ustanoveniami tohto rozhodnutia nie je dotknutý článok 16 ZFEÚ ani nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov [3],

PRIJALO TOTO ROZHODNUTIE:

Článok 1

Cieľ

Toto rozhodnutie upravuje vznik, prijímanie, zasielanie a ukladanie dôverných informácií v Európskom parlamente s cieľom zabezpečiť zodpovedajúcu ochranu dôvernej povahy týchto informácií. Najmä sa ním vykonáva príloha 2 rámcovej dohody.

[1] Ú. v. EÚ L 304, 20.11.2010, s. 47.

[2] Ú. v. ES L 145, 31.5.2001, s. 43.

[3] Ú. v. ES L 8, 12.1.2001, s. 1.

Článok 2

Vymedzenie pojmov

Na účely tohto rozhodnutia:

a) „informácie“ znamenajú akékoľvek písomné alebo ústne informácie, bez ohľadu na nosič informácií a autora;

b) „dôverné informácie“ znamenajú „utajované skutočnosti EÚ“ (USEÚ) a neutajované „ostatné dôverné informácie“;

c) „utajované skutočnosti EÚ“ (USEÚ) znamenajú akékoľvek informácie a materiály s označením „TRÈS SECRET UE/EU TOP SECRET“, „SECRET UE/EU SECRET“, „CONFIDENTIEL UE/EU CONFIDENTIAL“ alebo „RESTREINT UE/EU RESTRICTED“ alebo s ekvivalentným vnútroštátnym alebo medzinárodným označením utajenia, ktorých neoprávnené zverejnenie by mohlo spôsobiť rôzny stupeň poškodenia záujmov EÚ alebo jedného alebo viacerých členských štátov bez ohľadu na to, či takéto informácie pochádzajú z inštitúcií, orgánov, úradov a agentúr zriadených zmluvami alebo na základe zmlúv alebo sú získané z členských štátov, tretích krajín alebo medzinárodných organizácií. V tomto ohľade:

— „TRÈS SECRET UE/EU TOP SECRET“ je utajenie informácií a materiálov, ktorých neoprávnené zverejnenie by mohlo spôsobiť mimoriadne vážne poškodenie hlavných záujmov Únie alebo jedného či viacerých členských štátov;

— „SECRET UE/EU SECRET“ je utajenie informácií a materiálov, ktorých neoprávnené zverejnenie by mohlo spôsobiť vážne poškodenie hlavných záujmov Únie alebo jedného či viacerých členských štátov;

— „CONFIDENTIEL UE/EU CONFIDENTIAL“ je utajenie informácií a materiálov, ktorých neoprávnené zverejnenie by mohlo spôsobiť poškodenie hlavných záujmov Únie alebo jedného či viacerých členských štátov;

— „RESTREINT UE/EU RESTRICTED“ je utajenie informácií a materiálov, ktorých neoprávnené zverejnenie by mohlo byť nevýhodné pre záujmy Únie alebo jedného či viacerých členských štátov;

d) „Ostatné dôverné informácie“ znamenajú akékoľvek iné dôverné informácie nepodliehajúce utajeniu vrátane informácií, na ktoré sa vzťahuje ochrana údajov alebo povinnosť služobného tajomstva, ktoré vzniknú v Európskom parlamente alebo ich Európskemu parlamentu poskytnú iné inštitúcie, orgány, úrady a agentúry zriadené zmluvami alebo na základe zmlúv alebo členské štáty;

e) „dokument“ znamená akékoľvek zaznamenané informácie bez ohľadu na ich fyzickú podobu alebo vlastnosti;

f) „materiál“ znamená akýkoľvek dokument alebo časť zariadenia alebo vybavenia, či už vyrobeného alebo v procese výroby;

g) „potreba vedieť“ znamená potrebu určitej osoby mať prístup k dôverným informáciám, aby mohla vykonávať úradnú funkciu alebo splniť úlohu;

h) „povolenie“ znamená rozhodnutie (rozhodnutie o splnení podmienok), ktoré prijíma v prípade poslancov Európskeho parlamentu jeho predseda a v prípade úradníkov Európskeho parlamentu a ostatných zamestnancov pracujúcich pre politické skupiny generálny tajomník, a na základe ktorého sa jednotlivcom povoľuje prístup k utajovaným skutočnostiam EÚ do určitého stupňa utajenia, a to na základe kladného výsledku bezpečnostnej previerky vykonanej vnútroštátnym orgánom podľa vnútroštátneho práva a v súlade s ustanoveniami prílohy I časti 2;

i) „zaradenie do nižšieho stupňa“ znamená zníženie stupňa utajenia;

j) „odtajnenie“ znamená zrušenie akéhokoľvek utajenia;

k) „pôvodca“ znamená riadne splnomocneného autora utajovaných skutočností EÚ alebo iných dôverných informácií;

l) „bezpečnostné upozornenia“ znamenajú vykonávacie technické opatrenia stanovené v prílohe II ([1]).

Článok 3

Základné zásady a minimálne normy

1. Zaobchádzanie s dôvernými informáciami zo strany Európskeho parlamentu sa riadi základnými zásadami a minimálnymi normami stanovenými v prílohe I časti 1.

2. Európsky parlament vytvorí v súlade s týmito základnými zásadami a minimálnymi normami systém pre riadenie bezpečnosti informácií (ISMS), ktorého cieľom bude uľahčovať parlamentnú a administratívnu prácu a pritom zabezpečovať ochranu všetkých dôverných informácií, s ktorými Európsky parlament pracuje, pričom budú v plnom rozsahu dodržiavané pravidlá, ktoré pôvodca týchto informácií stanoví v bezpečnostnom upozornení.

Spracovanie dôverných informácií automatizovanými informačnými systémami (IS) Európskeho parlamentu sa uskutočňuje v súlade s koncepciou zabezpečenia informácií (IA) a je stanovené v bezpečnostnom upozornení.

([1]) Príloha bude prijatá neskôr.

3. Poslanci Európskeho parlamentu sa môžu oboznamovať s utajovanými informáciami až do a vrátane stupňa utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“ bez toho, aby prešli bezpečnostnou previerkou. Ak ide o informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, musia podpísať čestné vyhlásenie, že obsah týchto informácií neposkytnú žiadnej tretej osobe. Prístup k informáciám s vyšším stupňom utajenia ako je stupeň „CONFIDENTIEL UE/EU CONFIDENTIAL“, majú len poslanci, ktorí prešli bezpečnostnou previerkou na zodpovedajúcej úrovni.

4. Úradníci Európskeho parlamentu a ostatní zamestnanci Európskeho parlamentu pracujúci pre politické skupiny sa môžu oboznamovať s dôvernými informáciami, ak majú preukázateľnú „potrebu vedieť“, pričom s informáciami s vyšším stupňom utajenia než „RESTREINT UE/EU RESTRICTED“ sa môžu oboznamovať iba ak prešli bezpečnostnou previerkou na zodpovedajúcej úrovni.

Článok 4

Vznik dôverných informácií a ich administratívne spracovanie Európskym parlamentom

1. Predseda Európskeho parlamentu, predsedovia príslušných parlamentných výborov a generálny tajomník a/alebo akákoľvek iná osoba, ktorej bolo vydané riadne písomné povolenie, môže byť pôvodcom dôverných informácií a/alebo utajovaných informácií, ako sa stanovuje v bezpečnostných upozorneniach.

2. Pôvodca utajovaných informácií pri ich vzniku uplatní vhodný stupeň utajenia v súlade s medzinárodnými normami a vymedzeniami uvedenými v prílohe I. Pôvodca zároveň spravidla určí, kto je oprávnený oboznamovať sa s informáciami vzhľadom na daný stupeň utajenia. Tieto informácie sa oznámia oddeleniu pre dôverné informácie (CIS) vo chvíli, keď sa dokument na tomto oddelení uschová.

3. S dôvernými informáciami, na ktoré sa vzťahuje služobné tajomstvo, sa nakladá v súlade s pokynmi uvedenými v bezpečnostných upozorneniach.

Článok 5

Prijímanie dôverných informácií zo strany Európskeho parlamentu

1. Dôverné informácie, ktoré Európsky parlament dostane, sa oznamujú takto:

— utajované skutočnosti EÚ so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ a iné dôverné informácie sekretariátu parlamentného orgánu/funkcionára, ktorí podali žiadosť,

— utajované skutočnosti EÚ so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“ a vyšším oddeleniu CIS.

2. Registráciu, ukladanie a vysledovateľnosť dôverných informácií zabezpečuje buď sekretariát parlamentného orgánu/funkcionára, ktorí tieto informácie dostali, alebo oddelenie CIS.

3. V prípade dôverných informácií, ktoré poskytuje Komisia podľa rámcovej dohody, sú dohodnuté opatrenia v zmysle bodu 3.2 prílohy II rámcovej dohody určené na zachovanie dôvernosti informácií (opatrenia ustanovené spoločnou dohodou týkajúce sa adresátov, nahliadania do dokumentov, napríklad preskúmanie v zabezpečenej čitárni, schôdze za zatvorenými dverami a iné) uložené spoločne s dôvernými informáciami na sekretariáte parlamentného orgánu/funkcionára alebo na oddelení CIS, pokiaľ ide o informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“ alebo vyšším.

4. Opatrenia uvedené v odseku 3 sa môžu obdobne uplatniť aj na poskytovanie dôverných informácií zo strany iných inštitúcií, orgánov, úradov a agentúr zriadených zmluvami alebo na základe zmlúv alebo členskými štátmi.

5. Utajované skutočnosti EÚ so stupňom utajenia „TRÈS SECRET UE/EU TOP SECRET“ sa Európskemu parlamentu poskytujú v súlade s ďalšími opatreniami dohodnutými medzi parlamentným orgánom/funkcionárom, ktorí podali žiadosť o informáciu a inštitúciou EÚ alebo členským štátom, ktorý informáciu poskytol. Konferencia predsedov zriadi výbor dohľadu. Jeho cieľom bude zabezpečiť úroveň ochrany zodpovedajúcu danému stupňu utajenia.

Článok 6

Poskytovanie USEÚ Európskym parlamentom tretím stranám

Európsky parlament môže so súhlasom pôvodcu USEÚ poskytnúť USEÚ inej inštitúcii, orgánu, úradu alebo agentúre zriadeným zmluvami alebo na základe zmlúv alebo členského štátu pod podmienkou, že pri nakladaní s USEÚ v rámci ich oddelení a priestorov zabezpečia dodržiavanie pravidiel rovnocenných pravidlám stanoveným v tomto rozhodnutí.

Článok 7

Ukladanie a sprístupňovanie dôverných informácií v zabezpečených priestoroch (zabezpečené čitárne)

1. Zabezpečené čitárne umožňujú bezpečné ukladanie dokumentov a nie sú v nich kopírovacie stroje, telefóny, faxové zariadenia, skenery alebo iné technické zariadenie na reprodukciu alebo prenos dokumentov.

2. Na prístup do zabezpečenej čitárne sa uplatňujú tieto podmienky:

a) Prístup majú iba tieto osoby:

— poslanci Európskeho parlamentu, úradníci Európskeho parlamentu a iní zamestnanci Európskeho parlamentu pracujúci pre politické skupiny, ktorí sú riadne určení v súlade s opatreniami uvedenými v článku 4 ods. 2 alebo článku 5 ods. 3 a ods. 4;

— úradníci Európskeho parlamentu zodpovední za riadenie oddelenia CIS;

— v prípade potreby úradníci Európskeho parlamentu zodpovední za všeobecnú a požiarnu bezpečnosť.

Upratovanie v zabezpečených priestoroch sa vykonáva len za prítomnosti a pod dohľadom úradníka pracujúceho na oddelení CIS.

b) Každá osoba, ktorá má záujem o prístup k dôverným informáciám, poskytne svoje meno vopred oddeleniu CIS. Oddelenie CIS skontroluje totožnosť každej osoby, ktorá podá žiadosť o prístup k takýmto informáciám a v prípade potreby overí, či má daná osoba bezpečnostnú previerku na zodpovedajúcej úrovni a či je na základe opatrení uvedených v článku 4 ods. 2 alebo článku 5 ods. 3 a ods. 4 oprávnená na prístup k týmto informáciám.

c) Oddelenie CIS môže odmietnuť prístup do čitárne osobe, ktorá nie je oprávnená do nej vstúpiť podľa písmen a) a b). Akékoľvek námietky voči rozhodnutiu oddelenia CIS sa v prípade poslancov Európskeho parlamentu predložia predsedovi Európskeho parlamentu a v iných prípadoch generálnemu tajomníkovi.

3. Na sprístupňovanie dôverných informácií v zabezpečenej čitárni sa uplatňujú tieto podmienky:

a) Osoby, ktoré sú oprávnené oboznámiť sa s informáciami a ktoré predložili žiadosť podľa odseku 2 písm. b), sa dostavia na oddelenie CIS.

S výnimkou mimoriadnych okolností (napríklad v prípade početných žiadostí o sprístupnenie informácií podaných v krátkom čase) sa môžu dôverné informácie sprístupniť v zabezpečenej čitárni v jednom čase vždy len jednej osobe za prítomnosti úradníka oddelenia CIS.

Uvedený úradník informuje oprávnenú osobu o jej povinnostiach a najmä ju požiada, aby podpísala čestné vyhlásenie, ktorým sa zaviaže, že obsah informácie neoznámi žiadnej tretej osobe.

b) Počas oboznamovania sa s informáciami je zakázaná komunikácia s vonkajším prostredím (vrátane používania telefónov alebo iných technológií), robenie si poznámok a kopírovanie či fotografovanie sprístupnených dôverných informácií.

c) Predtým ako osoba dostane povolenie opustiť zabezpečenú čitáreň, zodpovedný úradník oddelenia CIS uvedený v písmene a) sa uistí o tom, či sú dôverné informácie, s ktorými sa osoba oboznamovala, na mieste, neporušené a úplné.

4. V prípade porušenia vyššie uvedených pravidiel zodpovedný pracovník oddelenia CIS informuje generálneho tajomníka, ktorý podá správu predsedovi, ak tieto pravidlá porušil poslanec Európskeho parlamentu.

Článok 8

Minimálne požiadavky pre iné formy sprístupnenia dôverných informácií

1. Pokiaľ ide o administratívne spracovanie dôverných informácií počas schôdzí za zatvorenými dverami, sekretariát parlamentného orgánu/funkcionára zodpovedného za schôdzu zabezpečí, aby:

— do miestnosti konania schôdze mohli vstúpiť len osoby, ktoré sa majú schôdze zúčastniť a ktoré majú bezpečnostnú previerku na potrebnej úrovni;

— boli všetky dokumenty očíslované, rozdané na začiatku schôdze a zozbierané na jej konci a aby sa z týchto dokumentov nerobili poznámky, aby sa nekopírovali ani nefotografovali;

— zápisnica zo schôdze neobsahovala zmienku o obsahu diskusie k informácii, ktorá sa prejednávala dôverným spôsobom;

— dôverné informácie poskytované ústne príjemcom v Európskom parlamente podliehali rovnakej úrovni ochrany ako písomné dôverné informácie. Súčasťou tejto ochrany môže byť čestné vyhlásenie zo strany príjemcov týchto informácií, že ich obsah nesprostredkujú žiadnej tretej osobe.

2. Na administratívne spracovanie dôverných informácií sekretariátom parlamentného orgánu/funkcionára mimo schôdzí za zatvorenými dverami sa uplatňujú tieto podmienky:

— vytlačené dokumenty sa osobne odovzdajú vedúcemu sekretariátu, ktorý ich zaregistruje a vydá potvrdenie o prijatí;

— tieto dokumenty v čase, keď sa práve nepoužívajú, uschová sekretariát na svoju zodpovednosť na uzamknutom mieste;

— bez toho, aby bolo dotknuté administratívne spracovanie dôverných informácií počas schôdzí za zatvorenými dverami ustanovené v odseku 1, sa tieto dokumenty v žiadnom prípade nemôžu kopírovať, uchovávať na inom nosiči alebo komukoľvek postupovať;

— prístup k takým dokumentom sa obmedzí na ich adresátov a v súlade s opatreniami uvedenými v článku 4 ods. 2, článku 5 ods. 3 alebo ods. 4 prebieha pod dohľadom sekretariátu;

— sekretariát vedie záznamy o osobách, ktoré nahliadali do dokumentov, ako aj o dátumoch a časoch nahliadnutia. Tieto záznamy sa postúpia oddeleniu CIS so zreteľom na zostavenie výročnej správy uvedenej v článku 12.

Článok 9

Archivovanie dôverných informácií

1. V priestoroch Európskeho parlamentu je zaistený bezpečný systém archivovania.

Dôverné informácie definitívne uložené na oddelení CIS alebo na sekretariáte parlamentného orgánu/funkcionára sa presúvajú do bezpečného archívu na oddelení CIS po šiestich mesiacoch odo dňa, keď boli naposledy sprístupnené, a najneskôr rok odo dňa, keď boli uložené.

2. Oddelenie CIS je zodpovedné za spravovanie bezpečného archívu v súlade so štandardnými archivačnými kritériami.

3. Sprístupnenie dôverných informácií archivovaných v bezpečných archívoch sa uskutočňuje za týchto podmienok:

— prístup k dôverným informáciám majú len osoby, ktorých meno alebo funkcia boli overené na základe sprievodného dokladu vyplneného pri uložení týchto informácií;

— žiadosť o sprístupnenie dôverných informácií treba predložiť oddeleniu CIS, ktoré zabezpečí presun príslušného dokumentu do zabezpečenej čitárne;

— uplatňujú sa postupy a podmienky pre sprístupňovanie dôverných informácií uvedené v článku 7.

Článok 10

Zaradenie do nižšieho stupňa a odtajnenie USEÚ

1. Zníženie stupňa utajenia a odtajnenie USEÚ je možné len s povolením ich pôvodcu a, ak je to potrebné, po prediskutovaní s ostatnými zainteresovanými stranami. Zníženie stupňa utajenia alebo odtajnenie sa potvrdzuje písomne. Pôvodca je zodpovedný za informovanie adresátov o tejto zmene a títo adresáti sú zase povinní informovať o tejto zmene akýchkoľvek iných následných adresátov, ktorým dokument alebo jeho kópiu zaslali. Ak je to možné, pôvodcovia vyznačujú na utajovaných dokumentoch dátum, obdobie alebo udalosť, keď sa stupeň utajenia obsahu môže znížiť alebo sa obsah môže odtajniť. Inak dokumenty revidujú aspoň každých päť rokov, aby sa presvedčili, či je pôvodné utajenie potrebné.

2. Odtajnenie dokumentov uložených v bezpečných archívoch sa uskutoční najneskôr po uplynutí 30 rokov v súlade s ustanoveniami nariadenia Rady (EHS, Euratom) č. 354/83 z 1. februára 1983 o otvorení historických archívov Európskeho hospodárskeho spoločenstva a Európskeho spoločenstva pre atómovú energiu pre verejnosť [1]. Odtajnenie uskutoční pôvodca dôverných informácií alebo útvar, ktorý je práve za ne zodpovedný, v súlade s prílohou I časťou 1 oddielom 10.

Článok 11

Porušenie dôvernosti

1. Porušenie dôvernosti vo všeobecnosti a najmä porušenie tohto rozhodnutia v prípade poslancov Európskeho parlamentu znamená uplatnenie príslušných ustanovení týkajúcich sa trestov vymedzených v Rokovacom poriadku Európskeho parlamentu.

2. Porušenia zo strany zamestnancov vedú k uplatneniu postupov a trestov stanovených v Služobnom poriadku úradníkov Európskej únie alebo v Podmienkach zamestnávania ostatných zamestnancov Európskej únie ustanovených nariadením (EHS, Euratom, ESUO) č. 259/68 [2] (ďalej len „služobný poriadok“).

3. Predseda a generálny tajomník v prípade potreby nariadia vyšetrovanie.

Článok 12

Úpravy tohto rozhodnutia a jeho vykonávacích predpisov a výročné správy o uplatňovaní tohto rozhodnutia

1. Generálny tajomník navrhuje každú potrebnú úpravu tohto rozhodnutia a jeho vykonávacích príloh a príslušné návrhy postúpi Predsedníctvu, ktoré o nich rozhodne.

2. Generálny tajomník každoročne predkladá Predsedníctvu správu o vykonávaní tohto rozhodnutia.

[1] Ú. v. ES L 43, 15.2.1983, s. 1.
[2] Ú. v. ES L 56, 4.3.1968, s. 1.

Článok 13

Prechodné a záverečné ustanovenia

1. Dôverné informácie, ktoré existovali na oddelení CIS alebo v archívoch pred prijatím tohto rozhodnutia, sa automaticky utajujú na úrovni „RESTREINT UE/EU RESTRICTED“, pokiaľ sa ich pôvodca nerozhodne neutajiť ich alebo utajiť ich s vyšším stupňom utajenia alebo s označením do jedného roka od dátumu nadobudnutia účinnosti tohto rozhodnutia.

2. Ak sa pôvodca týchto dôverných informácií rozhodne použiť pre takéto dôverné informácie vyšší stupeň utajenia, pôvodca alebo ním poverení zástupcovia označia dokumenty najnižším možným stupňom utajenia a postupujú v súčinnosti s oddelením CIS a v súlade s kritériami stanovenými v prílohe I.

3. Rozhodnutie predsedníctva z 13. novembra 2006 o predpisoch o zaobchádzaní s dôvernými dokumentmi sa zrušuje.

4. Rozhodnutie predsedníctva z 24. októbra 2005 poverujúce generálneho tajomníka vytvorením výboru pre odtajňovanie a prijatím rozhodnutí o otázke odtajňovania sa zrušuje.

Článok 14

Nadobudnutie účinnosti

1. Toto rozhodnutie nadobúda účinnosť dňom jeho uverejnenia v *Úradnom vestníku Európskej únie*.

2. Uplatňuje sa od 1. júla 2011.

PRÍLOHA I

ČASŤ 1

ZÁKLADNÉ ZÁSADY A MINIMÁLNE NORMY BEZPEČNOSTI PRE OCHRANU DÔVERNÝCH INFORMÁCIÍ

1. **Úvod**

Tieto ustanovenia určujú základné zásady a minimálne bezpečnostné normy, ktoré musí dodržiavať Európsky parlament na všetkých miestach zamestnávania, rovnako ako všetci príjemcovia USEÚ a iných dôverných informácií, aby sa zaručila bezpečnosť a všetci zainteresovaní si mohli byť istí, že je zabezpečená spoločná úroveň ochrany. Dopĺňajú ich pravidlá týkajúce sa zaobchádzania s dôvernými informáciami zo strany parlamentných výborov a iných parlamentných orgánov/funkcionárov.

2. **Všeobecné zasady**

Bezpečnostná politika Európskeho parlamentu tvorí neoddeliteľnú súčasť jeho všeobecnej politiky vnútorného riadenia a vychádza teda zo zásad upravujúcich jeho všeobecnú politiku. Medzi tieto zásady patrí zákonnosť, transparentnosť, zodpovednosť a subsidiarita a proporcionalita.

Princíp zákonnosti predstavuje potrebu ostať pri vykonávaní bezpečnostných funkcií prísne v právnom rámci a dodržať uplatniteľné právne náležitosti. Znamená to tiež, že povinnosti v oblasti bezpečnosti musia vychádzať z príslušných ustanovení právnych predpisov. V plnej miere sa uplatňujú ustanovenia služobného poriadku, najmä jeho článok 17 o povinnosti zamestnancov zdržať sa nepovoleného zverejnenia informácií získaných pri vykonávaní služby a jeho hlava IV o disciplinárnych opatreniach. Napokon to znamená, že porušenie bezpečnosti v rámci zodpovednosti Európskeho parlamentu sa musí riešiť spôsobom, ktorý je v súlade s politikou Európskeho parlamentu o disciplinárnych opatreniach.

Princíp transparentnosti znamená, že v súvislosti so všetkými pravidlami a ustanoveniami týkajúcimi sa bezpečnosti je potrebná jednoznačnosť, rovnováha medzi rôznymi útvarmi a rôznymi oblasťami (fyzická bezpečnosť v porovnaní s ochranou informácií atď.) a je nevyhnutná konzistentná a štruktúrovaná politika informovanosti o bezpečnosti. Tiež to znamená potrebu jasných písomných usmernení o vykonávaní bezpečnostných opatrení.

Princíp zodpovednosti znamená, že povinnosti v oblasti bezpečnosti musia byť jednoznačne vymedzené. Okrem toho poukazuje na potrebu pravidelne monitorovať, či sa tieto povinnosti riadne plnia.

Princíp subsidiarity znamená, že bezpečnosť sa organizuje na čo najnižšej úrovni a čo najbližšie ku generálnym riaditeľstvám a útvarom Európskeho parlamentu. Princíp proporcionality znamená, že bezpečnostné činnosti sa musia prísne obmedziť iba na to, čo je absolútne nevyhnutné, a že bezpečnostné opatrenia musia byť úmerné k záujmom, ktoré sa majú chrániť, a k skutočnej alebo potenciálnej hrozbe voči týmto záujmom, aby tieto záujmy boli chránené spôsobom, ktorý spôsobuje čo najmenšie narušenie.

3. **Základy bezpečnosti informácií**

Základmi dobrej bezpečnosti informácií sú:

a) v rámci Európskeho parlamentu útvar zaisťovania informačnej bezpečnosti INFOSEC zodpovedný za spoluprácu s príslušným bezpečnostným orgánom s cieľom poskytovať informácie a poradenstvo v oblasti technických bezpečnostných hrozieb a prostriedkov ochrany proti nim;

b) úzka spolupráca medzi zodpovednými útvarmi Európskeho parlamentu a bezpečnostnými službami ostatných inštitúcií EÚ.

4. **Zásady informačnej bezpečnosti**

4.1. *Ciele*

Hlavné ciele informačnej bezpečnosti sú:

a) chrániť utajované skutočnosti EÚ (USEÚ) a iné dôverné skutočnosti pred špionážou, ohrozením alebo neoprávneným prezradením;

b) chrániť USEÚ, s ktorými sa narába v komunikačných a informačných systémoch a sieťach, pred ohrozením ich dôvernosti, celistvosti a dostupnosti;

c) chrániť priestory Európskeho parlamentu, v ktorých sa uchovávajú USEÚ, pred sabotážou a úmyselným poškodením;

d) v prípade zlyhania bezpečnosti posúdiť spôsobenú škodu, obmedziť jej dôsledky, uskutočniť bezpečnostné vyšetrovanie a prijať potrebné nápravné opatrenia.

4.2. *Utajovanie*

4.2.1. Ak ide o dôvernosť, potrebná je starostlivosť a skúsenosti s výberom informácií a materiálu, ktoré sa majú chrániť, a posúdenie stupňa ochrany, ktorú si vyžadujú. Podstatné je, aby stupeň ochrany zodpovedal bezpečnostnej citlivosti jednotlivej informácie alebo materiálu, ktoré treba zabezpečiť. Aby sa zabezpečil hladký tok informácií, treba predchádzať nadmernému alebo nedostatočnému utajovaniu.

4.2.2. Systém utajenia je nástroj na realizovanie zásad ustanovených v tomto oddiele; podobný systém utajovania sa dodržiava pri plánovaní a organizovaní spôsobov čelenia špionáži, sabotáži, terorizmu a iným hrozbám tak, aby sa zabezpečila maximálna ochrana najdôležitejších priestorov, v ktorých sa uchovávajú USEÚ, a najdôležitejších bodov v rámci takýchto priestorov.

4.2.3. Zodpovednosť za utajovanie informácií spočíva výlučne na pôvodcovi danej informácie.

4.2.4. Stupeň utajenia môže závisieť výlučne na obsahu danej informácie.

4.2.5. Ak je viacero informácií zoskupených spolu, stupeň utajenia, ktorý sa vzťahuje na celok, musí byť aspoň taký, ako je najvyšší stupeň utajenia uplatňovaný na jednotlivé takto zoskupené položky. Súbor informácií však môže mať pridelený vyšší stupeň utajenia ako jeho jednotlivé časti.

4.2.6. Utajenie sa stanoví iba vtedy, ak je potrebné, a na dobu, na akú je potrebné.

4.3. *Ciele bezpečnostných opatrení*

Bezpečnostné opatrenia:

a) sa vzťahujú na všetky osoby, ktoré majú prístup k USEÚ, nosiče informácií uchovávajúce USEÚ a iné dôverné informácie, ako aj na všetky priestory, v ktorých sa nachádzajú takéto informácie, a na dôležité zariadenia;

b) sú navrhnuté tak, aby sa zistili osoby, ktorých postavenie môže ohroziť bezpečnosť takýchto informácií a dôležitých zariadení, ktoré uchovávajú takéto informácie, a aby umožnili vylúčenie alebo odvolanie takýchto osôb;

c) zabraňujú akejkoľvek nepovolanej osobe v prístupe k takýmto informáciám alebo k zariadeniam, ktoré ich obsahujú;

d) zabezpečujú, aby sa takéto informácie rozširovali výlučne na základe zásady „potreba vedieť“, ktorá je zásadná pre všetky aspekty bezpečnosti;

e) zabezpečujú celistvosť (t. j. prevenciu pred poškodením, neoprávnenou zmenou alebo neoprávneným vymazaním) a dostupnosť (tým, ktorí potrebujú a majú povolený prístup) všetkých dôverných informácií, utajovaných alebo neutajovaných, a najmä takých informácií, ktoré sa uchovávajú, spracúvajú alebo prenášajú v elektromagnetickej podobe.

5. **Spoločné minimálne normy**

Európsky parlament zabezpečuje, aby spoločné minimálne bezpečnostné normy dodržiavali všetci príjemcovia USEÚ v rámci inštitúcie a pod jej právomocou, najmä všetky servisy a všetci dodávatelia tak, aby tieto informácie bolo možné odovzdať s dôverou, že sa s nimi bude zaobchádzať s rovnakou starostlivosťou. Takéto minimálne normy obsahujú kritériá pre bezpečnostnú previerku úradníkov Európskeho parlamentu a iných zamestnancov Európskeho parlamentu pracujúcich pre politické skupiny a postupy na ochranu dôverných informácií.

Európsky parlament umožní prístup k týmto informáciám vonkajším orgánom iba za podmienky, že zabezpečia, aby sa s nimi nakladalo v súlade s ustanoveniami, ktoré sú aspoň na striktne rovnocennej úrovni, ako sú tieto spoločné minimálne normy.

Takéto spoločné minimálne normy sa tiež uplatnia, keď Európsky parlament zmluvou alebo dohodou o grante zverí úlohy zahŕňajúce dôverné informácie priemyselným alebo iným subjektom.

6. **Bezpečnosť úradníkov Európskeho parlamentu a iných zamestnancov Európskeho parlamentu pracujúcich pre politické skupiny**

6.1. *Bezpečnostné poučenie úradníkov Európskeho parlamentu a iných zamestnancov Európskeho parlamentu pracujúcich pre politické skupiny*

Všetci úradníci Európskeho parlamentu a iní zamestnanci Európskeho parlamentu pracujúci pre politické skupiny vo funkciách, kde by mohli mať prístup k USEÚ, sú pri prevzatí úlohy a potom v pravidelných intervaloch dôkladne poučení o potrebe bezpečnosti a o postupoch na jej dosiahnutie. Takéto osoby musia písomne potvrdiť, že si uplatniteľné bezpečnostné opatrenia prečítali a plne im porozumeli.

6.2. *Zodpovednosť vedúcich pracovníkov*

Vedúci pracovníci majú povinnosť poznať tých členov svojho personálu, ktorí pri práci prichádzajú do styku s utajovanými skutočnosťami, alebo ktorí majú prístup k zabezpečeným komunikačným alebo informačným systémom, a zaznamenávať a hlásiť akékoľvek udalosti alebo zjavné citlivé miesta, u ktorých je pravdepodobné, že by mohli mať vplyv na bezpečnosť.

6.3. *Bezpečnostné postavenie úradníkov Európskeho parlamentu a iných zamestnancov Európskeho parlamentu pracujúcich pre politické skupiny*

Vypracujú sa postupy, ktoré zabezpečia, že v prípade zistenia nepriaznivej informácie o úradníkovi Európskeho parlamentu alebo inom zamestnancovi Európskeho parlamentu pracujúcom pre politickú skupinu sa podniknú kroky na určenie, či daný jednotlivec pracuje s utajovanými skutočnosťami alebo má prístup k zabezpečeným komunikačným alebo informačným systémom, a informuje sa o tom zodpovedný útvar Európskeho parlamentu. Ak sa preukáže, že takýto jednotlivec predstavuje bezpečnostné riziko, je vylúčený alebo odvolaný z plnenia úloh, pri ktorých by mohol ohrozovať bezpečnosť.

7. **Fyzická bezpečnosť**

Fyzická bezpečnosť znamená uplatňovanie fyzických a technických ochranných opatrení na zamedzenie neoprávneného prístupu k USEÚ.

7.1. *Potreba ochrany*

Stupeň opatrení fyzickej bezpečnosti, ktoré sa majú uplatňovať na zaistenie ochrany USEÚ, je úmerný utajeniu, rozsahu a ohrozeniu uchovávaných informácií a materiálu. Všetky osoby, ktoré majú k dispozícii USEÚ, dodržiavajú jednotné postupy týkajúce sa utajovania týchto informácií a musia spĺňať spoločné normy ochrany týkajúce sa uchovávania, prenosu a likvidácie informácií a materiálu vyžadujúceho ochranu.

7.2. *Kontrola*

Pred zanechaním priestorov obsahujúcich USEÚ bez dozoru osoby, ktoré ich spravujú, zabezpečia, aby takéto utajované skutočnosti boli bezpečne uschované a aby sa aktivovali všetky bezpečnostné zariadenia (zámky, poplašné zariadenia atď.). Po pracovnom čase sa vykonávajú ďalšie nezávislé kontroly.

7.3. *Bezpečnosť budov*

Budovy, v ktorých sa uchovávajú USEÚ alebo zabezpečené komunikačné a informačné systémy, sa chránia proti neoprávnenému prístupu.

Povaha ochrany, ktorá sa poskytuje USEÚ, napríklad zamrežovanie okien, zámky na dverách, stráž pri vstupoch, automatizované systémy kontroly vstupu, bezpečnostné kontroly a hliadky, poplašné systémy, systémy na zisťovanie narušenia a strážne psy, závisí od:

a) utajenia, množstva a umiestnenia informácií a materiálov, ktoré sa majú chrániť, v rámci budovy;

b) kvality bezpečnostných schránok pre dotknuté informácie a materiály a

c) fyzickej povahy a umiestnenia budovy.

Povaha ochrany poskytovaná komunikačným a informačným systémom podobne závisí od stanovenia hodnoty príslušného majetku a možnej škody, ak by bola ohrozená bezpečnosť, od fyzickej povahy a umiestnenia budovy, v ktorej sa nachádza systém, a od umiestnenia tohto systému v budove.

7.4. *Pohotovostné plány*

Vopred sa vypracujú podrobné plány na ochranu utajovaných skutočností počas núdzovej situácie.

8. **Vymedzenie zabezpečenia, označenia, uvedenie a riadenie utajovania**

8.1. *Vymedzenie zabezpečenia*

Nie sú povolené žiadne iné stupne utajenia ako stupne vymedzené v článku 2 tohto rozhodnutia.

Na určenie limitov platnosti utajenia (znamenajúce pre utajované skutočnosti automatické zníženie stupňa utajenia alebo odtajnenie) sa môže použiť dohodnuté vymedzenie zabezpečenia. Toto vymedzenie je buď „AŽ DO … (čas/dátum)“ alebo „AŽ DO … (udalosť)“.

Dodatočné vymedzenie zabezpečenia ako CRYPTO alebo ľubovoľné iné vymedzenie zabezpečenia uznané v EÚ sa uplatňuje, ak existuje potreba obmedzenej distribúcie a osobitného nakladania s utajovanou skutočnosťou v porovnaní s tým, čo určuje stupeň utajenia.

Vymedzenia zabezpečenia sa používajú iba v kombinácii s utajením.

8.2. *Označenia*

Označenie sa môže používať na špecifikovanie oblasti, na ktorú sa vzťahuje daný dokument, alebo konkrétnej distribúcie na základe potreby vedieť, alebo (pre neutajované skutočnosti) na označenie konca zákazu.

Označenie nie je utajenie a nesmie sa použiť namiesto utajenia.

8.3. *Uvedenie utajení a vymedzení zabezpečenia*

Utajenia sa uvádzajú takto:

a) na dokumenty stupňa utajenia „RESTREINT UE/EU RESTRICTED“ mechanickými alebo elektronickými prostriedkami;

b) na dokumenty stupňa utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“ mechanickými prostriedkami alebo ručne alebo tlačou na vopred opečiatkovaný zaevidovaný papier;

c) na dokumenty „SECRET UE/EU SECRET“ a „TRÈS SECRET UE/EU TOP SECRET“ mechanickými prostriedkami alebo ručne.

Vymedzenia zabezpečenia sa uvádzajú priamo pod stupňom utajenia rovnakými prostriedkami ako uvedenie utajenia.

8.4. *Riadenie utajovania*

8.4.1. V š e o b e c n e

Informácie sa utajujú iba vtedy, ak je to potrebné. Utajenie sa uvedie jasne a správne a zachováva sa iba dovtedy, pokiaľ si informácie vyžadujú ochranu.

Zodpovednosť za utajovanie informácií a za prípadné následné zníženie stupňa utajenia alebo odtajnenie spočíva výlučne na pôvodcovi.

Úradníci Európskeho parlamentu utajujú informácie, znižujú ich stupeň utajenia alebo ich odtajňujú na základe pokynov generálneho tajomníka alebo na základe jeho poverenia.

Podrobné postupy na zaobchádzanie s utajovanými dokumentmi sa koncipujú tak, aby sa zaistila ochrana primeraná informáciám, ktoré obsahujú.

Počet osôb oprávnených byť pôvodcom dokumentov „TRÈS SECRET UE/EU TOP SECRET“ je čo najmenší a ich mená sú uvedené na zozname vypracovanom oddelením CIS.

8.4.2. Uplatňovanie utajenia

Utajovanie dokumentov je určené úrovňou citlivosti ich obsahu v súlade s vymedzeniami uvedenými v článku 2 písm. c). Dôležité je, aby sa utajenie používalo správne a striedmo, najmä pokiaľ ide o utajenie stupňa „TRÈS SECRET UE/EU TOP SECRET“.

Stupeň utajenia listu alebo dokumentu obsahujúceho prílohy je rovnaký, ako najvyšší stupeň utajenia jeho príloh. Pôvodca dokumentu jasne uvedie úroveň utajenia listu alebo nóty v prípade oddelenia od príloh.

Pôvodca dokumentu, ktorý sa má utajovať, musí mať na pamäti pravidlá uvedené vyššie a obmedziť tendenciu nadmerného alebo nedostatočného utajovania.

Jednotlivé strany, odseky, oddiely, prílohy, dodatky, doplnky a vložky daného dokumentu môžu vyžadovať rozličné stupne utajenia a musia sa podľa toho utajiť. Stupeň utajenia dokumentu ako celku je rovnaký, ako má jeho časť s najvyšším stupňom utajenia.

9. **Kontroly**

Riaditeľstvo Európskeho parlamentu zodpovedné za bezpečnosť vykonáva pravidelné kontroly bezpečnostných mechanizmov na ochranu USEÚ, pri čom mu môže pomáhať oddelenie CIS.

Riaditeľstvo Európskeho parlamentu zodpovedné za bezpečnosť a útvary pre bezpečnosť iných inštitúcií, orgánov, úradov a agentúr zriadených zmluvami alebo na základe zmlúv, ktoré disponujú USEÚ, sa tiež môžu dohodnúť, že budú vykonávať partnerské hodnotenie bezpečnostných mechanizmov na ochranu USEÚ.

10. **Postup pri odtajňovaní**

10.1. Oddelenie CIS preskúma USEÚ a predloží pôvodcovi dokumentu návrhy na odtajnenie v každom prípade najneskôr v 25. roku od dátumu vytvorenia dokumentu. Dokumenty, ktoré sa neodtajnia pri prvom preskúmaní, sa opätovne pravidelne preskúmajú najmenej každých päť rokov.

10.2. Okrem dokumentov, ktoré sa v skutočnosti nachádzajú v zabezpečených archívoch a sú riadne utajené, sa postup odtajnenia môže týkať aj iných dôverných informácií, ktoré sa nachádzajú buď v zabezpečených archívoch alebo v Archívnom a dokumentačnom stredisku Európskeho parlamentu (CARDOC).

10.3. Oddelenie CIS bude v mene pôvodcu zodpovedné za informovanie adresátov dokumentu o tejto zmene utajenia a adresáti sú zase zodpovední za informovanie akýchkoľvek následných adresátov, ktorým dokument alebo jeho kópiu zaslali, o tejto zmene.

10.4. Odtajnenie nemá vplyv na žiadne označenia, ktoré sa na dokumente môžu vyskytovať.

10.5. Pôvodný stupeň utajenia v hornej a dolnej časti každej strany sa škrtne. Prvá (titulná) strana dokumentu sa opečiatkuje a doplní referenčným číslom CIS.

10.6. Text odtajneného dokumentu sa pripojí k elektronickej zložke alebo rovnocennému systému, v ktorom bol zaregistrovaný.

10.7. V prípade dokumentov spadajúcich pod výnimku súvisiacu so súkromím a integritou jednotlivca alebo obchodnými záujmami a v prípade citlivých dokumentov sa uplatní článok 2 nariadenia (EHS, Euratom) č. 354/83.

10.8. Okrem ustanovení v bodoch 10.1 až 10.7 sa uplatňujú tieto pravidlá:

a) pokiaľ ide o dokumenty tretích strán, oddelenie CIS pred odtajnením konzultuje s dotknutou treťou stranou. Tretia strana má osem týždňov na predloženie pripomienok;

b) pokiaľ ide o výnimku súvisiacu so súkromím a integritou jednotlivca, pri odtajnení sa zohľadní najmä súhlas danej osoby, nemožnosť identifikácie danej osoby a/alebo skutočnosť, že táto osoba už nie je nažive;

c) pokiaľ ide o výnimku súvisiacu s obchodnými záujmami fyzickej alebo právnickej osoby, dotknutá osoba môže byť informovaná prostredníctvom uverejnenia v *Úradnom vestníku Európskej únie* a môže sa jej dať lehota štyroch týždňov od dňa zverejnenia na prípadné pripomienky.

ČASŤ 2

POSTUP BEZPEČNOSTNEJ PREVIERKY

11. **Postup bezpečnostnej previerky poslancov Európskeho parlamentu**

11.1. Vzhľadom na výsady a právomoci Európskeho parlamentu sa jeho poslanci bez bezpečnostnej previerky môžu oboznamovať s USEÚ až do stupňa utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“ vrátane. Ak ide o informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, musia podpísať čestné vyhlásenie, že obsah týchto informácií neposkytnú žiadnej tretej osobe.

11.2. Na prístup k informáciám so stupňom utajenia „TRÈS SECRET UE/EU TOP SECRET“ alebo „SECRET UE/EU SECRET“ musia poslanci Európskeho parlamentu získať povolenie v súlade s postupom uvedeným v bodoch 11.3 a 11.4.

11.3. Povolenie sa udelí iba poslancom Európskeho parlamentu, ktorí prešli bezpečnostnou previerkou príslušných vnútroštátnych orgánov členských štátov v súlade s postupom uvedeným v bodoch 11.9 až 11.14. Za udelenie povolenia poslancom zodpovedá predseda.

11.4. Predseda môže udeliť povolenie po získaní stanoviska príslušných vnútroštátnych orgánov členských štátov na základe bezpečnostnej previerky, ktorá sa vykonala v súlade s bodmi 11.8 až 11.13.

11.5. Riaditeľstvo Európskeho parlamentu zodpovedné za bezpečnosť vedie aktualizovaný zoznam všetkých poslancov Európskeho parlamentu, ktorým sa udelilo povolenie, vrátane dočasného povolenia v zmysle bodu 11.15.

11.6. Povolenie je platné počas obdobia piatich rokov alebo počas doby trvania úloh, v súvislosti s ktorými bolo udelené, podľa toho, ktoré z týchto období je kratšie. Môže sa obnoviť v súlade s postupom uvedeným v bode 11.4.

11.7. Predseda odoberie povolenie, ak sa domnieva, že na to existujú opodstatnené dôvody. Rozhodnutie odobrať povolenie sa oznámi danému poslancovi Európskeho parlamentu, ktorý môže požiadať, aby ho vypočul predseda pred tým, ako odobratie nadobudne účinnosť, a príslušnému vnútroštátnemu orgánu.

11.8. Bezpečnostná previerka sa vykonáva za pomoci dotknutého poslanca Európskeho parlamentu a na žiadosť predsedu. Príslušným vnútroštátnym orgánom na vykonanie previerky je orgán členského štátu, ktorého je dotknutý poslanec štátnym príslušníkom.

11.9. Ako súčasť postupu previerky musí daný poslanec Európskeho parlamentu vyplniť formulár s osobnými informáciami.

11.10. Predseda vo svojej žiadosti príslušným vnútroštátnym orgánom spresní stupeň utajovaných skutočností, s ktorými príde daný poslanec Európskeho parlamentu do styku, aby tieto orgány mohli vykonať previerku.

11.11. Celý proces bezpečnostného preverovania vykonávaný príslušnými vnútroštátnymi orgánmi spolu so získanými výsledkami musí byť v súlade s príslušnými pravidlami a predpismi platnými v danom členskom štáte, a to vrátane pravidiel, ktoré sa týkajú odvolaní.

11.12. Ak príslušné vnútroštátne orgány členského štátu vydajú kladné stanovisko, predseda môže príslušnému poslancovi Európskeho parlamentu udeliť povolenie.

11.13. Negatívne stanovisko oznámia príslušné vnútroštátne orgány danému poslancovi Európskeho parlamentu, ktorý môže požiadať, aby ho vypočul predseda. Ak to predseda považuje za potrebné, môže požiadať príslušné vnútroštátne orgány o doplňujúce vysvetlenia. Ak sa potvrdí negatívne stanovisko, povolenie sa neudelí.

11.14. Všetci poslanci Európskeho parlamentu, ktorým je udelené povolenie v zmysle bodu 11.3, dostávajú pri udelení povolenia a v pravidelných intervaloch potrebné usmernenia týkajúce sa ochrany utajovaných skutočností a prostriedkov na zabezpečenie tejto ochrany. Takíto poslanci podpíšu vyhlásenie potvrdzujúce prijatie týchto usmernení.

11.15. Za výnimočných okolností môže predseda po zaslaní oznámenia príslušným vnútroštátnym orgánom a za predpokladu, že do jedného mesiaca nereagujú, udeliť poslancovi Európskeho parlamentu dočasné povolenie na obdobie nepresahujúce šesť mesiacov pred obdržaním výsledku previerky uvedenej v bode 11.11. Takto udelené dočasné povolenia neoprávňujú na prístup k informáciám stupňa utajenia „TRÈS SECRET UE/EU TOP SECRET".

12. **Postup bezpečnostnej previerky pre úradníkov Európskeho parlamentu a iných zamestnancov Európskeho parlamentu pracujúcich pre politické skupiny**

12.1. Iba úradníci Európskeho parlamentu a ostatní zamestnanci Európskeho parlamentu pracujúci pre politické skupiny, ktorí z dôvodu svojich povinností a požiadaviek služby musia mať vedomosť o utajovaných skutočnostiach alebo s nimi musia pracovať, môžu mať prístup k takýmto informáciám.

12.2. Na prístup k informáciám so stupňom utajenia „TRÈS SECRET UE/EU TOP SECRET", „SECRET UE/EU SECRET" a „CONFIDENTIEL UE/EU CONFIDENTIAL" musia osoby uvedené v bode 12.1 získať povolenie v súlade s postupom uvedeným v bodoch 12.3 a 12.4.

12.3. Povolenie sa udelí iba osobám uvedeným v bode 12.1, ktoré prešli bezpečnostnou previerkou príslušných vnútroštátnych orgánov členských štátov v súlade s postupom uvedeným v bodoch 12.9 až 12.14. Za udelenie povolenia úradníkom Európskeho parlamentu a ostatným zamestnancom Európskeho parlamentu pracujúcim pre politické skupiny zodpovedá generálny tajomník.

12.4. Generálny tajomník môže udeliť povolenie po získaní stanoviska príslušných vnútroštátnych orgánov členských štátov na základe bezpečnostnej previerky, ktorá sa vykonala v súlade s bodmi 12.8 až 12.13.

12.5. Riaditeľstvo Európskeho parlamentu zodpovedné za bezpečnosť vedie aktualizovaný zoznam všetkých pracovných miest, ktoré si vyžadujú bezpečnostnú previerku a ktoré poskytujú príslušné servisy Európskeho parlamentu, a všetkých osôb, ktorým sa udelilo povolenie vrátane dočasného povolenia podľa bodu 12.15.

12.6. Povolenie je platné počas obdobia piatich rokov alebo počas doby trvania úloh, v súvislosti s ktorými bolo udelené, podľa toho, ktoré z týchto období je kratšie. Môže sa obnoviť v súlade s postupom uvedeným v bode 12.4.

12.7. Generálny tajomník odoberie povolenie, ak sa domnieva, že na to existujú opodstatnené dôvody. Rozhodnutie odobrať povolenie sa oznámi danému úradníkovi Európskeho parlamentu alebo inému zamestnancovi Európskeho parlamentu pracujúcemu pre politickú skupinu, ktorý môže požiadať, aby ho vypočul generálny tajomník pred tým, ako odobratie nadobudne účinnosť, a príslušnému vnútroštátnemu orgánu.

12.8. Bezpečnostná previerka sa vykonáva za pomoci dotknutej osoby a na žiadosť generálneho tajomníka. Príslušným vnútroštátnym orgánom na vykonanie previerky je orgán členského štátu, ktorého je dotknutá osoba štátnym príslušníkom. Ak to umožňujú vnútroštátne predpisy a pravidlá, príslušné vnútroštátne orgány môžu vykonať prešetrenie týkajúce sa iných štátnych príslušníkov, ktorí žiadajú o prístup k informáciám so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL" alebo vyšším.

12.9. Ako súčasť postupu previerky musí daný úradník Európskeho parlamentu alebo iný zamestnanec Európskeho parlamentu pracujúci pre politickú skupinu vyplniť formulár s osobnými informáciami.

12.10. Generálny tajomník vo svojej žiadosti príslušným vnútroštátnym orgánom spresní stupeň utajovaných skutočností, ktoré majú byť sprístupnené danej osobe, aby tieto orgány mohli vykonať previerku a poskytnúť svoje stanovisko, pokiaľ ide o úroveň povolenia, ktorú by bolo vhodné udeliť tejto osobe.

12.11. Celý proces bezpečnostného preverovania vykonávaný príslušnými vnútroštátnymi orgánmi spolu so získanými výsledkami podlieha príslušným pravidlám a predpisom platným v danom členskom štáte, vrátane pravidiel, ktoré sa týkajú odvolaní.

12.12. Ak príslušné vnútroštátne orgány členského štátu vydajú kladné stanovisko, generálny tajomník môže danej osobe udeliť povolenie.

12.13. Negatívne stanovisko príslušných vnútroštátnych orgánov sa oznámi dotknutému úradníkovi Európskeho parlamentu alebo inému zamestnancovi Európskeho parlamentu pracujúcemu pre politickú skupinu, ktorý môže požiadať, aby ho vypočul generálny tajomník. Ak to generálny tajomník považuje za potrebné, môže požiadať príslušné vnútroštátne orgány o doplňujúce vysvetlenia. Ak sa potvrdí negatívne stanovisko, povolenie sa neudelí.

12.14. Všetci úradníci Európskeho parlamentu a ostatní zamestnanci Európskeho parlamentu pracujúci pre politické skupiny, ktorým sa udelilo povolenie v zmysle bodov 12.4 a 12.5, dostávajú pri udelení povolenia a v pravidelných intervaloch potom potrebné pokyny týkajúce sa ochrany utajovaných skutočností a prostriedkov na zabezpečenie tejto ochrany. Takíto úradníci a zamestnanci podpíšu vyhlásenie, ktorým potvrdia prijatie pokynov a ktorým sa zaviažu ich dodržiavať.

12.15. Za výnimočných okolností môže generálny tajomník po zaslaní oznámenia príslušným vnútroštátnym orgánom a za predpokladu, že do jedného mesiaca nereagujú, udeliť úradníkovi Európskeho parlamentu alebo inému zamestnancovi Európskeho parlamentu pracujúcemu pre politickú skupinu dočasné povolenie na obdobie nepresahujúce šesť mesiacov pred obdržaním výsledku previerky uvedenej v bode 12.11. Takto udelené dočasné povolenia neoprávňujú na prístup k informáciám stupňa utajenia „TRÈS SECRET UE/EU TOP SECRET“.