IV

(Informări)

INFORMĂRI PROVENIND DE LA INSTITUȚIILE, ORGANELE ȘI ORGANISMELE UNIUNII EUROPENE

PARLAMENTUL EUROPEAN

DECIZIA BIROULUI PARLAMENTULUI EUROPEAN

din 6 iunie 2011

referitor la normele de reglementare a tratamentului informațiilor confidențiale de către Parlamentul European

(2011/C 190/02)

BIROUL PARLAMENTULUI EUROPEAN,

având în vedere articolul 23 alineatul (12) din Regulamentul de procedură al Parlamentului European,

întrucât:

(1) În lumina noului Acord-cadru privind relațiile dintre Parlamentul European și Comisia Europeană [1], semnat la 20 octombrie 2010 (denumit în continuare „Acordul-cadru"), este necesară revizuirea deciziei Biroului din 13 noiembrie 2006 referitoare la normele care reglementează prelucrarea administrativă a documentelor confidențiale.

(2) Tratatul de la Lisabona atribuie noi sarcini Parlamentului European și, pentru a dezvolta activitățile Parlamentului în acele domenii care necesită un grad de confidențialitate, este necesar să se stabilească principii de bază, standarde minime de securitate și proceduri adecvate pentru tratamentul informațiilor confidențiale, inclusiv al celor clasificate, de către Parlamentul European.

(3) Normele stabilite în prezenta decizie vizează să asigure standarde echivalente de protecție și compatibilitatea cu normele adoptate de alte instituții, organisme, oficii și agenții înființate în virtutea sau pe baza tratatelor sau de statele membre pentru a facilita buna funcționare a procesului decizional în Uniunea Europeană.

(4) Prezentele dispoziții sunt adoptate fără a aduce atingere articolului 15 din Tratatul privind funcționarea Uniunii Europene (TFUE) și Regulamentului (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei [2].

(5) Dispozițiile prezentei decizii sunt adoptate fără a aduce atingere articolului 16 din TFUE și Regulamentului (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date [3],

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Obiectiv

Decizia reglementează crearea, primirea, transmiterea și stocarea informațiilor confidențiale de către Parlamentul European în vederea unei protecții adecvate a naturii confidențiale a acestora. Decizia implementează în special anexa 2 la Acordul-cadru.

[1] JO L 304, 20.11.2010, p. 47.

[2] JO L 145, 31.5.2001, p. 43.

[3] JO L 8, 12.1.2001, p. 1.

Articolul 2

Definiții

În sensul prezentei decizii:

(a) „informații” înseamnă orice informație scrisă sau orală, indiferent de suport sau de autor;

(b) „informații confidențiale” înseamnă „informații clasificate UE” (ICUE) și „alte informații confidențiale” neclasificate;

(c) „informații clasificate UE” (ICUE) înseamnă orice informație sau material, clasificat drept „TRÈS SECRET UE/EU TOP SECRET”, „SECRET UE/EU SECRET”, „CONFIDENTIEL UE/EU CONFIDENTIAL” sau „RESTREINT UE/EU RESTRICTED”, a cărui divulgare neautorizată ar putea cauza prejudicii de diverse niveluri la adresa intereselor UE sau ale unuia sau mai multora dintre statele sale membre, indiferent dacă informația în cauză provine din cadrul instituțiilor, organismelor, oficiilor și agențiilor înființate în virtutea și în baza tratatelor sau este primită de la state membre, țări terțe sau organizații internaționale. În acest sens:

— „TRÈS SECRET UE/EU TOP SECRET” este clasificarea pentru informații și materiale a căror divulgare neautorizată ar putea cauza prejudicii extrem de grave intereselor esențiale ale Uniunii sau ale unuia sau mai multora dintre statele membre;

— „SECRET UE/EU SECRET” este clasificarea pentru informații și materiale a căror divulgare neautorizată ar putea cauza prejudicii grave intereselor esențiale ale Uniunii sau ale unuia sau mai multora dintre statele membre;

— „CONFIDENTIEL UE/EU CONFIDENTIAL” este clasificarea pentru informații și materiale a căror divulgare neautorizată ar putea dăuna intereselor esențiale ale Uniunii sau ale unuia sau mai multora dintre statele membre;

— „RESTREINT UE/EU RESTRICTED” este clasificarea pentru informații și materiale a căror divulgare neautorizată ar putea dezavantaja interesele Uniunii sau ale unuia sau mai multora dintre statele membre;

(d) „alte informații confidențiale” înseamnă orice altă informație confidențială neclasificată, inclusiv informații vizate de normele privind protecția datelor sau de obligația de a respecta secretul profesional, creată în cadrul Parlamentului European sau transmisă Parlamentului European de alte instituții, organisme și agenții înființate în virtutea sau pe baza tratatelor sau de statele membre;

(e) „document” înseamnă orice informație înregistrată, indiferent de forma sa fizică sau de caracteristicile sale;

(f) „material” înseamnă orice document, aparat sau echipament, deja fabricat sau în curs de fabricație;

(g) „nevoie de a cunoaște” înseamnă necesitatea unei persoane de a avea acces la informații confidențiale pentru a putea îndeplini o funcție sau o sarcină oficială;

(h) „autorizație” înseamnă o decizie (decizie de autorizare) adoptată de președinte, în cazul membrilor Parlamentului European, sau de Secretarul General, în cazul funcționarilor Parlamentului European și al altor angajați ai Parlamentului care lucrează pentru grupurile politice, de a permite accesul unei persoane la ICUE până la un anumit nivel, pe baza rezultatului pozitiv al unei examinări de securitate (procedură de abilitare), efectuată de o autoritate națională în temeiul legislației naționale și în conformitate cu dispozițiile anexei I partea 2;

(i) „declasare” înseamnă o reducere a nivelului de clasificare;

(j) „declasificare” înseamnă eliminarea din orice sistem de clasificare;

(k) „autoritate de origine” înseamnă autorul, autorizat corespunzător, al ICUE sau al oricărei alte informații confidențiale;

(l) „reguli de securitate” înseamnă măsurile tehnice de implementare menționate în anexa II [1].

Articolul 3

Principii de bază și standarde minime

(1) Tratamentul informațiilor confidențiale de către Parlamentul European se efectuează în conformitate cu principiile de bază și standardele minime menționate în anexa I partea 1.

(2) Parlamentul European instituie un sistem de management al securității informațiilor (SMSI) în conformitate cu acele principii de bază și standarde minime care vizează facilitarea activităților parlamentare și administrative, garantând protecția oricărei informații confidențiale prelucrate de Parlamentul European, cu respectarea deplină a normelor stabilite de autoritatea de origine a unei astfel de informații astfel cum este stabilit în regulile de securitate.

Prelucrarea informațiilor confidențiale cu ajutorul unor sisteme de informare (SI) automate ale Parlamentului European se desfășoară în conformitate cu conceptul de asigurare a informațiilor (AI) și se menționează în regulile de securitate.

[1] Anexa urmează să fie adoptată.

(3) Membrii Parlamentului European pot consulta informații clasificate până la și incluzând nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL" în absența unei autorizări de securitate. În cazul informațiilor clasificate drept „CONFIDENTIEL UE/EU CONFIDENTIAL", ei trebuie să semneze o declarație pe proprie răspundere că nu vor dezvălui vreunui terț conținutul informațiilor respective. Informațiile clasificate peste nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL" sunt puse doar la dispoziția membrilor Parlamentului European care dispun de nivelul adecvat de autorizare de securitate.

(4) Funcționarii Parlamentului European și alți angajați ai Parlamentului care lucrează pentru grupurile politice pot consulta informații confidențiale dacă s-a stabilit în cazul lor „nevoia de a cunoaște" și pot consulta informații clasificate peste nivelul „RESTREINT UE/EU RESTRICTED" dacă dispun de nivelul adecvat de autorizare de securitate.

Articolul 4

Crearea de informații confidențiale și tratamentul administrativ de către Parlamentul European

(1) Președintele Parlamentului European, președinții comisiilor parlamentare vizate și Secretarul General și/sau orice persoană autorizată de acesta sau aceasta în scris poate crea informații confidențiale și/sau clasifica informațiile în conformitate cu regulile de securitate.

(2) Atunci când creează o informație clasificată, autoritatea de origine aplică nivelul adecvat de clasificare în conformitate cu standardele internaționale și definițiile menționate în anexa I. De asemenea, autoritatea de origine determină, ca regulă generală, destinatarii care urmează a fi autorizați să consulte informația în funcție de nivelul de clasificare. Informația respectivă se comunică Serviciului de Informații Confidențiale (SIC) atunci când documentul este depus la SIC.

(3) Informațiile confidențiale care fac obiectul secretului profesional sunt tratate în conformitate cu instrucțiunile de tratament definite în regulile de securitate.

Articolul 5

Primirea de informații confidențiale de către Parlamentul European

(1) Informațiile confidențiale primite de Parlamentul European se comunică după cum urmează:

— ICUE clasificate drept „RESTREINT UE/EU RESTRICTED" și alte informații confidențiale, secretariatului organului parlamentar/titularului de mandat care a înaintat cererea;

— ICUE clasificate drept „CONFIDENTIEL UE/EU CONFIDENTIAL" și superior, SIC.

(2) Înregistrarea, stocarea și trasabilitatea informațiilor confidențiale se asigură fie de secretariatul organului parlamentar/titularului de mandat care a primit informațiile, fie de SIC.

(3) În cazul informațiilor confidențiale comunicate de Comisie în conformitate cu Acordul-cadru din 20 octombrie 2010, măsurile convenite în sensul anexei 2 punctul 3.2 la Acordul Comun (stabilit de comun acord și privind destinatari, procedura de consultare, adică sală de lectură securizată și reuniuni cu ușile închise sau alte aspecte) destinate să protejeze confidențialitatea informațiilor se depun împreună cu informația confidențială la secretariatul organului parlamentar/titularului de mandat sau la SIC dacă informația este clasificată drept „CONFIDENTIEL UE/EU CONFIDENTIAL".

(4) Măsurile menționate la alineatul (3) pot fi aplicate *mutatis mutandis* și în cazul comunicării de informații confidențiale de către alte instituții, organisme, oficii și agenții înființate în virtutea sau în baza tratatelor sau de către statele membre.

(5) ICUE clasificate drept „TRÈS SECRET UE/EU TOP SECRET" sunt transmise Parlamentului European, făcând obiectul altor măsuri care urmează a fi convenite între organul parlamentar/titularul de mandat care a solicitat informațiile și instituțiile UE sau statele membre care le comunică. Se înființează un comitet de supraveghere de către Conferința președinților. Acesta vizează asigurarea unui nivel de protecție proporțional cu nivelul respectiv de clasificare.

Articolul 6

Comunicarea de ICUE de către Parlamentul European unor terți

Parlamentul European poate, sub rezerva consimțământului autorității de origine, să transmită ICUE altor instituții, organisme, oficii și agenții ale UE sau statelor membre cu condiția ca acestea să asigure, la tratarea ICUE, că se respectă norme similare celor menționate în prezenta decizie în cadrul serviciilor și sediilor lor.

Articolul 7

Stocarea și consultarea informațiilor confidențiale în spații securizate (săli de lectură securizate)

(1) Sălile de lectură securizate asigură stocarea sigură și nu conțin copiatoare, telefoane, faxuri, scanere sau orice alt mijloc tehnic de reproducere sau transmitere de documente.

(2) Următoarele condiții reglementează accesul în sala de lectură securizată:

(a) accesul în sala de lectură securizată este permis exclusiv:

— membrilor Parlamentului European, funcționarilor din cadrul Parlamentului European și altor angajați ai Parlamentului European care lucrează pentru grupurile politice, identificați în mod corespunzător, în conformitate cu prevederile articolului 4 alineatul (2) sau ale articolului 5 alineatele (3) și (4);

— funcționarilor Parlamentului European responsabili cu gestionarea SIC;

— după caz, funcționarilor Parlamentului European responsabili cu securitatea și protecția împotriva incendiilor.

Curățenia în spațiul securizat se realizează doar în prezența unui funcționar care lucrează în cadrul SIC, sub atenta supraveghere a acestuia;

(b) fiecare persoană care dorește să aibă acces la informații confidențiale comunică în avans numele său SIC. SIC verifică identitatea fiecărei persoane care depune o cerere de consultare a respectivelor informații și, controlează, după caz, dacă persoana respectivă dispune de nivelul necesar de autorizare de securitate și este autorizată în acest sens în conformitate cu măsurile menționate la articolul 4 alineatul (2) sau articolul 5 alineatele (3) și (4);

(c) SIC este abilitat să refuze accesul în sală oricărei persoane neautorizate în temeiul literelor (a) și (b). Toate contestațiile privind decizia SIC se transmit președintelui, în cazul membrilor Parlamentului European, și Secretarului General, în alte cazuri.

(3) Următoarele condiții reglementează consultarea informațiilor confidențiale în sala de lectură securizată:

(a) persoanele autorizate să consulte informații și care au depus cererea menționată la alineatul (2) litera (b) se prezintă personal la SIC.

În afara cazurilor excepționale (de exemplu în cazul în care sunt depuse solicitări numeroase de consultare într-un interval scurt), doar câte o singură persoană este autorizată să consulte informații confidențiale în sala de lectură securizată, în prezența unui funcționar din cadrul SIC.

Funcționarul respectiv comunică persoanei astfel autorizate obligațiile care îi revin și, în special, îi solicită să semneze o declarație pe proprie răspundere, prin care aceasta se angajează să nu divulge vreunui terț conținutul informațiilor;

(b) în timpul consultării, se interzice contactul cu exteriorul (inclusiv prin intermediul telefonului sau a altor tehnologii), luarea de notițe și fotocopierea sau fotografierea informațiilor confidențiale consultate;

(c) înainte să se permită unei persoane să părăsească sala de lectură securizată, funcționarul SIC menționat la litera (a) se asigură de existența informațiilor confidențiale consultate și verifică dacă acestea sunt în continuare intacte și complete.

(4) În situația unei încălcări a regulilor de mai sus, funcționarul responsabilul cu SIC îl informează pe Secretarul General, care va prezenta situația președintelui dacă persoana vinovată de a fi încălcat aceste reguli este un membru al Parlamentului European.

Articolul 8

Standarde minime pentru alte consultări ale informațiilor confidențiale

(1) În ceea ce privește prelucrarea administrativă a informațiilor confidențiale la o reuniune cu ușile închise, secretariatul organului parlamentar/titularului de mandat responsabil pentru reuniune asigură următoarele:

— doar persoanele desemnate să participe la reuniune și care dispun de nivelul necesar de autorizare de securitate pot intra în sala de reuniune;

— toate documentele sunt numerotate, distribuite la începutul reuniunii și colectate din nou la sfârșit, nu se iau notițe după respectivele documente și nu se fac fotocopii sau fotografii;

— procesul-verbal al reuniunii nu menționează conținutul discuției cu privire la informațiile avute în vedere în conformitate cu procedura de confidențialitate;

— informațiile confidențiale furnizate oral destinatarilor din Parlamentul European se supun aceluiași nivel de protecție a informațiilor confidențiale ca cel pentru informațiile furnizate în scris. Această modalitate include o declarație pe proprie răspundere dată de destinatarii informațiilor respective de a nu divulga conținutul acestora niciunui terț.

(2) Următoarele norme se aplică prelucrării administrative a informațiilor confidențiale de către secretariatul organului parlamentar/titularului de mandat în afara reuniunilor cu ușile închise:

— documentele pe suport de hârtie se înmânează personal șefului secretariatului, care le înregistrează și furnizează o confirmare de primire;

— astfel de documente se păstrează sub cheie, sub răspunderea secretariatului, atunci când nu sunt folosite în mod efectiv;

— fără a aduce atingere prelucrării administrative a informațiilor confidențiale la o reuniune cu ușile închise, prevăzută la alineatul (1), nu este permis în niciun caz să fie duplicate, salvate într-un alt mediu sau transmise oricărei persoane;

— accesul la astfel de documente se limitează la destinatari și are loc, în conformitate cu măsurile menționate la articolul 4 alineatul (2), articolul 5 alineatul (3) sau articolul 5 alineatul (4), sub supravegherea secretariatului;

— secretariatul ține un registru al persoanelor care au consultat documentele, cuprinzând data și ora la care s-a efectuat consultarea. Respectivul registru se transmite SIC în vederea întocmirii raportului anual menționat la articolul 12.

Articolul 9

Arhivarea informațiilor confidențiale

(1) În clădirile Parlamentului European se vor pune la dispoziție posibilități de arhivare sigure.

Informațiile confidențiale depozitate definitiv la SIC sau la secretariatul organului parlamentar/titularului de mandat sunt transferate în arhiva securizată de la SIC după șase luni de la data ultimei consultări, dar nu mai târziu de un an de la data depozitării.

(2) SIC este responsabil de gestionarea arhivelor sigure, în conformitate cu criteriile standard de arhivare.

(3) Informațiile confidențiale păstrate în arhivele securizate pot fi consultate sub rezerva îndeplinirii următoarelor condiții:

— singurele persoane autorizate să consulte aceste informații sunt cele menționate, nominal sau prin funcția deținută, în documentul însoțitor redactat în momentul depunerii informațiilor confidențiale;

— cererea de consultare a informațiilor confidențiale trebuie prezentată SIC, care asigură transferul documentului în cauză în sala de lectură securizată;

— se aplică procedurile și condițiile privind consultarea informațiilor confidențiale stabilite la articolul 7.

Articolul 10

Declasarea și declasificarea ICUE

(1) Nu poate fi redus nivelul de clasificare și nici nu pot fi declasificate ICUE decât cu permisiunea autorității de origine și, dacă este necesar, după consultarea celorlalte părți în cauză. Declasarea sau declasificarea se confirmă în scris. Autoritatea de origine trebuie să comunice modificarea destinatarilor documentelor, iar aceștia din urmă trebuie să informeze cu privire la modificare eventualii destinatari ulteriori, cărora le-au transmis documentele în cauză sau copii ale acestora. Dacă este posibil, autoritățile de origine specifică pe documentele clasificate o dată, o perioadă sau un eveniment de la care conținutul poate fi declasat sau declasificat. Altfel, acestea revizuiesc documentele cel târziu o dată la cinci ani pentru a asigura necesitatea menținerii clasificării inițiale.

(2) Declasificarea documentelor păstrate în arhivele securizate are loc cel târziu după 30 de ani, în conformitate cu dispozițiile Regulamentului (CEE, Euratom) nr. 354/83 al Consiliului din 1 februarie 1983 privind deschiderea către public a arhivelor istorice ale Comunității Economice Europene și ale Comunității Europene a Energiei Atomice ([1]). Declasificarea se efectuează de către autoritatea de origine a informațiilor clasificate sau de către serviciul responsabil în momentul respectiv, în conformitate cu anexa I partea 1 secțiunea 10.

Articolul 11

Nerespectarea confidențialității

(1) Nerespectarea confidențialității în general și, în special, a prezentei decizii atrage după sine, în cazul membrilor Parlamentului European, aplicarea dispozițiilor relevante privind sancțiunile stabilite în Regulamentul de procedură al Parlamentului European.

(2) Nerespectarea confidențialității de către personal atrage după sine aplicarea procedurilor și sancțiunilor prevăzute de Statutul funcționarilor și Regimul aplicabil altor agenți ai Uniunii Europene, prevăzut în Regulamentul (CEE, Euratom, CECO) nr. 259/68 ([2]) („Statutul funcționarilor”).

(3) Președintele și Secretarul General organizează eventualele anchete care se impun.

Articolul 12

Adaptarea prezentei decizii și normele sale de punere în aplicare și raportul anual privind aplicarea prezentei decizii

(1) Secretarul General propune orice adaptare necesară a prezentei decizii și a anexelor care o pun în aplicare și transmite aceste propuneri Biroului în vederea adoptării unei decizii.

(2) Secretarul General prezintă Biroului un raport anual privind aplicarea prezentei decizii.

([1]) JO L 43, 15.2.1983, p. 1.
([2]) JO L 56, 4.3.1968, p. 1.

Articolul 13

Dispoziții tranzitorii și finale

(1) Informațiile confidențiale care sunt în SIC sau în arhive înainte de aplicarea prezentei decizii sunt clasificate implicit drept „RESTREINT UE/EU RESTRICTED”, cu excepția cazului în care autoritatea de origine decide fie să nu clasifice informațiile, fie să le clasifice cu un nivel mai înalt sau cu un marcaj, în termen de un an de la data intrării în vigoare a prezentei decizii.

(2) În cazul în care autoritatea de origine decide să aplice informațiilor confidențiale un nivel de clasificare mai ridicat, acestea sunt clasificate la cel mai scăzut nivel posibil de către autoritatea de origine sau de către delegații acesteia, în colaborare cu SIC și în conformitate cu criteriile stabilite în anexa I.

(3) Se abrogă decizia Biroului din 13 noiembrie 2006 privind normele care reglementează prelucrarea administrativă a documentelor confidențiale.

(4) Se abrogă decizia Biroului din 24 octombrie 2005 prin care se conferă Secretarului General mandatul de a înființa un comitet de declasificare și de a adopta decizii legate de procesul de declasificare.

Articolul 14

Intrarea în vigoare

(1) Prezenta decizie intră în vigoare în ziua publicării în *Jurnalul Oficial al Uniunii Europene*.

(2) Aceasta se aplică de la 1 iulie 2011.

ANEXA I

PARTEA 1

PRINCIPII DE BAZĂ ȘI STANDARDE MINIME DE SECURITATE PENTRU PROTEJAREA INFORMAȚIILOR CONFIDENȚIALE

1. Introducere

Prezentele dispoziții stabilesc principiile de bază și standardele minime de securitate care trebuie respectate de către Parlamentul European în toate punctele sale de lucru, precum și de către toți destinatarii ICUE și ai altor informații confidențiale, astfel încât să se asigure securitatea și toate părțile interesate pot fi asigurate în legătură cu stabilirea unui standard comun de protecție. Acestea sunt suplimentate de normele care reglementează tratamentul informațiilor confidențiale de către comisiile parlamentare și de către alte organe parlamentare sau titulari de mandat.

2. Principii generale

Politica de securitate a Parlamentului European face parte integrantă din politica sa de gestionare internă generală și, prin urmare, se bazează pe principiile care reglementează respectiva politică generală. Aceste principii includ legalitatea, transparența, răspunderea și subsidiaritatea și proporționalitatea.

Principiul legalității presupune necesitatea de a menține strict în cadrul legal executarea funcțiilor de securitate și necesitatea de a respecta cerințele legale aplicabile. De asemenea, înseamnă că responsabilitățile din domeniul securității trebuie să se bazeze pe dispoziții legale adecvate. Se aplică integral dispozițiile din Statutul funcționarilor, în special articolul 17 privind obligația personalului de a se abține de la orice divulgare neautorizată a informațiilor care i-au fost aduse la cunoștință în exercitarea atribuțiilor sale și titlul său VI privind măsurile disciplinare. În fine, acest principiu înseamnă că încălcările normelor de securitate în domeniile de responsabilitate ale Parlamentului European trebuie tratate în conformitate cu politica Parlamentului European privind măsurile disciplinare.

Principiul transparenței presupune nevoia de claritate în ceea ce privește toate normele și dispozițiile de securitate, pentru găsirea unui echilibru între diversele servicii și diversele domenii (securitatea fizică în comparație cu protecția informațiilor etc.) și nevoia unei politici coerente și structurate de conștientizare a securității. De asemenea, înseamnă că sunt necesare orientări scrise clare pentru punerea în aplicare a măsurilor de securitate.

Principiul răspunderii presupune că responsabilitățile din domeniul securității vor fi clar definite. În plus, presupune nevoia de a monitoriza cu regularitate corecta executare a acestor responsabilități.

Principiul subsidiarității, sau proporționalitatea, înseamnă că securitatea este organizată la cel mai jos nivel posibil și cât mai aproape posibil de Direcțiile Generale și de serviciile Parlamentului European. Principiul subsidiarității înseamnă că activitățile de securitate se limitează strict la ceea ce este absolut necesar și că măsurile de securitate sunt proporționale cu interesele care trebuie protejate și cu amenințările reale sau potențiale care planează asupra acestor interese, astfel încât să permită o apărare care să determine cât mai puține perturbări posibile.

3. Fundamentele securității informației

Fundamentele unei bune securități a informației sunt:

(a) în cadrul Parlamentului European, o autoritate INFOSEC (securitatea informațiilor) – serviciu de asigurare însărcinat cu colaborarea cu autoritatea de securitate în cauză pentru a furniza informații și sfaturi privind amenințările tehnice la adresa securității și mijloacele de protecție împotriva acestora;

(b) cooperarea strânsă între serviciile responsabile ale Parlamentului European și serviciile de securitate ale altor instituții UE.

4. Principiile securității informațiilor

4.1. *Obiective*

Principalele obiective ale securității informațiilor sunt, după cum urmează:

(a) salvgardarea ICUE și a altor informații confidențiale împotriva spionajului, compromiterii sau divulgării neautorizate;

(b) salvgardarea ICUE prelucrate în sisteme și rețele informatice și de comunicații împotriva amenințărilor la adresa confidențialității, integrității și disponibilității acestora;

(c) salvgardarea sediilor Parlamentului European care adăpostesc ICUE împotriva sabotajelor și a actelor intenționate de deteriorare;

(d) în caz de eșec al securității, evaluarea daunelor cauzate, limitarea consecințelor acestora, efectuarea unor anchete de securitate și adoptarea măsurilor necesare de remediere.

4.2. *Clasificare*

4.2.1. În ceea ce privește confidențialitatea, este nevoie de atenție și experiență pentru selectarea informațiilor și a materialelor care trebuie protejate și pentru evaluarea gradului de protecție necesar. Este foarte important ca nivelul de protecție să corespundă sensibilității, în termeni de securitate, a elementului individual de informație sau a materialului care trebuie salvgardat. Pentru a asigura buna circulație a informațiilor, se evită atât clasificarea excesivă, cât și clasificarea insuficientă.

4.2.2. Sistemul de clasificare este instrumentul de aplicare a principiilor prevăzute în prezenta secțiune; un sistem similar de clasificare se aplică pentru planificarea și organizarea măsurilor de luptă împotriva spionajului, sabotajului, terorismului și a altor amenințări, astfel încât să se asigure cel mai înalt grad de protecție celor mai importante sedii care adăpostesc ICUE și celor mai sensibile puncte din interiorul acestora.

4.2.3. Responsabilitatea pentru clasificarea informațiilor îi revine exclusiv autorității de origine a informațiilor în cauză.

4.2.4. Nivelul de clasificare poate fi bazat exclusiv pe conținutul informațiilor în cauză.

4.2.5. În cazul în care mai multe elemente de informație sunt grupate împreună, nivelul de clasificare care trebuie aplicat grupului trebuie să fie cel puțin egal cu nivelul cel mai înalt de clasificare aplicat individual respectivelor elemente. Unui grup de informații i se poate totuși aloca o clasificare mai înaltă decât cea a părților sale componente.

4.2.6. Clasificările sunt alocate doar atunci când este necesar și pentru cât timp este necesar.

4.3. *Obiectivele măsurilor de securitate*

Măsurile de securitate:

(a) se aplică tuturor persoanelor care au acces la ICUE, la mijloacele de transmitere a ICUE și la alte informații confidențiale, precum și la toate sediile care conțin astfel de informații și la instalații importante;

(b) sunt concepute pentru a detecta persoanele a căror poziție ar putea pune în pericol securitatea unor asemenea informații și a instalațiilor importante care adăpostesc astfel de informații și pentru a asigura excluderea și îndepărtarea acestora;

(c) împiedică accesul oricărei persoane neautorizate la astfel de informații sau la instalațiile care le conțin;

(d) asigură difuzarea unor astfel de informații exclusiv pe baza principiului nevoii de a cunoaște, principiu fundamental tuturor aspectelor securității;

(e) asigură integritatea (adică prevenirea coruperii, a modificării neautorizate sau a ștergerii neautorizate) și disponibilitatea (adică accesul nu este refuzat celor care au nevoie de informații și au acces autorizat) tuturor informațiilor confidențiale, fie acestea clasificate sau neclasificate, și, în special, a informațiilor stocate, prelucrate sau transmise în formă electromagnetică.

5. **Standarde minime comune**

Parlamentul European asigură respectarea unor standarde minime comune de securitate de către toți destinatarii ICUE, din cadrul instituției și care țin de competența sa, și anume de către toate serviciile și toți contractanții săi, astfel încât informațiile să poată fi transmise cu asigurarea că sunt prelucrate cu aceleași precauții. Aceste standarde minime includ criteriile de autorizare de securitate a funcționarilor Parlamentului European și a altor angajați ai Parlamentului care lucrează pentru grupurile politice și procedurile de protecție a informațiilor confidențiale.

Parlamentul European permite accesul organismelor externe la aceste informații doar cu condiția ca acestea să asigure, la prelucrarea lor, respectarea unor dispoziții cel puțin strict echivalente cu aceste standarde minime comune.

Aceste standarde minime comune se aplică, de asemenea, atunci când, prin contract sau înțelegere privind subvențiile, Parlamentul conferă entităților industriale sau altor entități sarcini care implică informații confidențiale.

6. **Securitatea pentru funcționarii Parlamentului European și alți angajați ai Parlamentului care lucrează pentru grupurile politice**

6.1. *Instrucțiuni de securitate pentru funcționarii Parlamentului European și alți angajați ai Parlamentului care lucrează pentru grupurile politice*

Funcționarii Parlamentului European și alți angajați ai Parlamentului care lucrează pentru grupurile politice și care ocupă un post care le poate permite accesul la ICUE primesc, atât la intrarea în funcție, cât și ulterior, periodic, un instructaj amănunțit asupra măsurilor de securitate necesare și asupra procedurilor în vigoare în materie. Persoanele respective certifică în scris faptul că au citit și că înțeleg pe deplin dispozițiile curente de securitate aplicabile.

6.2. *Responsabilitățile conducerii*

Personalul de conducere are obligația de a ști care dintre membrii personalului propriu lucrează cu informații clasificate sau au acces la sisteme informatice sau de comunicații securizate și de a înregistra și raporta orice incident sau vulnerabilitate evidentă care ar putea afecta securitatea.

6.3. *Statutul de securitate al funcționarilor Parlamentului European și al altor angajați ai Parlamentului care lucrează pentru grupurile politice*

Se instituie proceduri care să permită, în momentul în care se obțin informații nefavorabile privind un funcționar al Parlamentului European sau un alt angajat al Parlamentului care lucrează pentru grupurile politice, se iau măsuri pentru a determina dacă persoana în cauză ocupă un post care implică accesul la informații clasificate sau dacă are acces la sisteme informatice sau de comunicații securizate și a informa serviciul responsabil al Parlamentului European. Dacă se stabilește că această persoană constituie un risc de securitate, ea este exclusă sau îndepărtată de la sarcinile în cadrul cărora ar putea pune în pericol securitatea.

7. **Securitatea fizică**

„Securitatea fizică" înseamnă aplicarea unor măsuri de protecție fizice sau tehnice pentru a preveni accesul neautorizat la ICUE.

7.1. *Nevoia de protecție*

Nivelul măsurilor de securitate fizică ce trebuie aplicate pentru a asigura protecția ICUE este proporțional cu clasificarea și volumul informațiilor și materialelor deținute și cu amenințarea la care acestea sunt expuse. Toți deținătorii de ICUE trebuie să se conformeze unor reguli standardizate de clasificare și să respecte criterii de protecție uniforme cu privire la deținerea, transmiterea și distrugerea informațiilor și materialelor care trebuie protejate.

7.2. *Verificări*

Înainte de a lăsa fără supraveghere un sector care cuprinde ICUE, persoanele care le dețin trebuie să se asigure că acestea sunt în siguranță și că toate dispozitivele de securitate (încuietori, alarme etc.) sunt activate. După orele de program se efectuează verificări suplimentare independente.

7.3. *Securitatea clădirilor*

Clădirile care adăpostesc ICUE sau sisteme informatice sau de comunicații securizate sunt protejate împotriva accesului neautorizat.

Natura protecției asigurate pentru ICUE (de exemplu, ferestre cu gratii, uși care pot fi încuiate, prezența paznicilor la intrări, sisteme automate de control la intrare, inspecții și ronduri de securitate, sisteme de alarmă, sisteme de detectare a intrușilor și câini de pază) depinde de următorii parametri:

(a) clasificarea, volumul și amplasarea în cadrul clădirii a informațiilor și a materialelor care trebuie protejate;

(b) calitatea containerelor de securitate care conțin informațiile și materialele în cauză; și

(c) natura fizică și amplasarea clădirii.

Natura protecției asigurate sistemelor informatice și de comunicații depinde, în mod similar, de evaluarea valorii activelor în cauză și a eventualelor daune cauzate prin compromiterea securității, de natura fizică și amplasarea clădirii în care este adăpostit sistemul și de localizarea sistemului respectiv în clădire.

7.4. *Planuri pentru situații de urgență*

Se pregătesc anticipat planuri detaliate pentru protecția informațiilor clasificate în timpul unor situații de urgență.

8. **Clasificări, identificatori de securitate, aplicare, mărci de securitate și gestionarea clasificării**

8.1. *Identificatori de securitate*

Nu sunt permise alte clasificări decât cele definite la articolul 2 litera (c) din prezenta decizie.

Se poate utiliza un identificator de securitate convenit, pentru a stabili limitele valabilității unei clasificări (însemnând, pentru informațiile clasificate, momentul declasării sau al declasificării automate). Identificatorul este fie „PÂNĂ LA … (oră/dată)", fie „PÂNĂ LA … (eveniment)".

Se aplică identificatori suplimentari de securitate, precum CRYPTO sau orice alt identificator recunoscut în UE, în cazul în care sunt necesare o distribuție limitată și o utilizare specială suplimentare față de cele desemnate de clasificarea de securitate.

Identificatorii de securitate se utilizează doar în combinație cu o clasificare.

8.2. *Mărci*

Se poate utiliza o marcă pentru a specifica domeniul vizat de document sau o difuzare specială conform principiului nevoii de a cunoaște sau (pentru informații neclasificate) pentru a indica sfârșitul unei interdicții.

O marcă nu este o clasificare și nu trebuie să fie utilizată în locul unei clasificări.

8.3. *Aplicarea clasificării și a identificatorilor de securitate*

Clasificarea se aplică după cum urmează:

(a) pe documentele clasificate drept „RESTREINT UE/EU RESTRICTED", prin mijloace mecanice sau electronice;

(b) pe documentele clasificate drept „CONFIDENTIEL UE/EU CONFIDENTIAL", prin mijloace mecanice, manual sau prin tipărire pe hârtie înregistrată și ștampilată în prealabil;

(c) pe documente clasificate drept „SECRET UE/EU SECRET" și „TRÈS SECRET UE/EU TOP SECRET", prin mijloace mecanice sau cu mâna.

Identificatorii de securitate se aplică imediat sub clasificare, prin aceleași mijloace utilizate pentru aplicarea clasificărilor.

8.4. *Administrarea clasificărilor*

8.4.1. General

Informațiile se clasifică doar dacă este necesar. Clasificarea se indică clar și corect și se menține doar atât timp cât informația trebuie protejată.

Responsabilitatea pentru clasificarea informațiilor și pentru orice declasare sau declasificare ulterioară aparține exclusiv autorității de origine.

Funcționarii Parlamentului European clasifică, declasează sau declasifică informații la instrucțiunile secretarului general sau în virtutea competențelor delegate de acesta.

Normele metodologice amănunțite privind tratamentul aplicat documentelor clasificate sunt astfel concepute pentru a asigura faptul că acestea beneficiază de un tip de protecție corespunzător cu informațiile conținute.

Numărul de persoane autorizate să emită documente „TRÈS SECRET UE/EU TOP SECRET" este păstrat la minimum, iar numele persoanelor în cauză sunt înscrise pe o listă întocmită de SIC.

8.4.2. Aplicarea clasificărilor

Clasificarea unui document este determinată de nivelul de sensibilitate al conținutului său, în conformitate cu definiția de la articolul 2 litera (c). Este important ca aplicarea unui anumit nivel de clasificare să fie făcută în mod corect și proporțional, în special pentru nivelul de clasificare „TRÈS SECRET UE/EU TOP SECRET".

Nivelul de clasificare al unei scrisori sau al unei note care conține documente însoțitoare este la fel de înalt ca cel mai înalt nivel de clasificare al documentelor însoțitoare. Autoritatea de origine indică clar la ce nivel ar trebui clasificată scrisoarea sau nota după separarea de documentele însoțitoare.

Autoritatea de origine a unui document care urmează a fi clasificat ține cont de normele stabilite anterior și limitează orice tendință de clasificare excesivă sau insuficientă.

Paginile individuale, paragrafele, secțiunile, anexele, apendicele și documentele însoțitoare ale unui anumit document pot necesita clasificări diferite și sunt clasificate în consecință. Clasificarea documentului per ansamblu este clasificarea de cel mai înalt nivel atribuită unei părți din document.

9. **Inspecții**

Direcția Parlamentului European responsabilă cu securitatea, care poate fi asistată de SIC în îndeplinirea acestei sarcini, efectuează inspecții periodice ale aranjamentelor de securitate stabilite pentru protecția informațiilor clasificate ale UE (ICUE).

Direcția Parlamentului European responsabilă cu securitatea și serviciile de securitate ale celorlalte instituții, organisme, oficii și agenții înființate în virtutea sau în baza tratatelor, care dețin ICUE pot, de asemenea, să convină asupra realizării unor evaluări reciproce ale aranjamentelor de securitate stabilite pentru protecția ICUE.

10. **Procedura de declasificare**

10.1. SIC va examina ICUE și va prezenta autorității de origine propuneri de declasificare a unui document cu cel mult 25 de ani după data la care documentul a fost creat. Documentele care nu sunt declasificate după o primă examinare sunt reexaminate periodic, dar cel puțin o dată la cinci ani.

10.2. Pe lângă documentele care se află în arhivele sigure și care sunt clasificate în mod adecvat, procesul de declasificare poate să acopere, de asemenea, alte informații confidențiale existente în arhivele sigure sau deținute de Centrul de Arhivistică și Documentare al Parlamentului European (CARDOC).

10.3. În numele autorității de origine, SIC îi revine responsabilitatea de a informa destinatarii documentului cu privire la modificarea clasificării, iar aceștia din urmă sunt responsabili, la rândul lor, să informeze eventualii destinatari ulteriori, cărora le-au transmis documentele în cauză sau copii ale acestora, cu privire la modificare.

10.4. Declasificarea nu afectează mărcile care pot apărea pe document.

10.5. Clasificarea originală, marcată în partea de sus și în cea de jos pe fiecare pagină este barată. Prima pagină a documentului (coperta) este ștampilată și completată cu referința SIC.

10.6. Textul documentului declasificat este atașat fișei electronice sau sistemului echivalent în care acesta a fost înregistrat.

10.7. În cazul documentelor care fac obiectul unei excepții privind viața privată și integritatea persoanei sau interesele comerciale ale unei persoane fizice sau juridice și în cazul documentelor sensibile se aplică dispozițiile prevăzute la articolul 2 din Regulamentul (CEE, Euratom) nr. 354/83 al Consiliului.

10.8. În afară de prevederile de la punctele 10.1-10.7, se aplică următoarele norme:

(a) în ceea ce privește documentele terților, SIC consultă terții în cauză înainte de a efectua declasificarea. Terții dispun de opt săptămâni pentru a-și prezenta observațiile;

(b) în ceea ce privește excepția privind viața privată și integritatea persoanei, procedura de declasificare ține seama în special de acordul persoanei în cauză, de imposibilitatea identificării persoanei în cauză și/sau de faptul că respectiva persoană nu mai este în viață;

(c) în ceea ce privește excepția privind interesele comerciale ale unei persoane fizice sau juridice, persoana în cauză poate fi notificată prin publicarea în *Jurnalul Oficial al Uniunii Europene*, acordându-se un termen de patru săptămâni din ziua publicării pentru a-și prezenta observațiile.

PARTEA 2

PROCEDURA DE ACORDARE A AUTORIZĂRII DE SECURITATE

11. **Procedura de acordare a autorizării de securitate pentru membrii Parlamentului European**

11.1. Ținând seama de prerogativele și competențele Parlamentului European, membrilor săi li se poate acorda accesul la ICUE cărora li s-a atribuit un nivel de clasificare până la și incluzând nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL" fără autorizare de securitate. Pentru informațiile clasificate drept „CONFIDENTIEL UE/EU CONFIDENTIAL", membrii Parlamentului European semnează o declarație pe proprie răspundere, prin care se angajează să nu divulge conținutul informațiilor respective niciunui terț.

11.2. Pentru a avea acces la informații clasificate drept „TRÈS SECRET UE/EU TOP SECRET" sau „SECRET UE/EU SECRET", membrii Parlamentului European trebuie să fi fost autorizați în conformitate cu procedura menționată la punctele 11.3 și 11.4.

11.3. Autorizațiile se acordă doar membrilor Parlamentului European care au fost supuși unei verificări de securitate de către autoritățile naționale competente ale statelor membre în conformitate cu procedura menționată la punctele 11.9-11.14. Președintelui îi revine responsabilitatea de a acorda autorizația membrilor Parlamentului European.

11.4. Președintele poate acorda autorizația după obținerea avizului emis de autoritățile naționale competente ale statelor membre pe baza verificării de securitate efectuate în conformitate cu punctele 11.8 și 11.13.

11.5. Direcția Parlamentului European responsabilă cu securitatea păstrează o listă actualizată a tuturor membrilor Parlamentului European cărora li s-a acordat o autorizație, inclusiv o autorizație provizorie în sensul punctului 11.15.

11.6. Autorizația este valabilă pe o perioadă de cinci ani sau pe durata sarcinilor pentru care a fost eliberată, oricare dintre aceste perioade este mai scurtă. Autorizația poate fi reînnoită în conformitate cu procedura stabilită la punctul 11.4.

11.7. Autorizația este retrasă de președinte în cazul în care acesta consideră că există motive justificate în acest sens. Orice decizie de retragere a autorizației se notifică membrului Parlamentului European în cauză, care poate cere să fie ascultat de către președinte înainte de intrarea în vigoare a retragerii, precum și autorității naționale competente.

11.8. Verificarea de securitate se efectuează cu sprijinul membrului Parlamentului European vizat și la cererea președintelui. Autoritatea națională competentă pentru verificare este cea a statului membru al cărui cetățean este membrul Parlamentului European în cauză.

11.9. În cadrul procedurii de verificare, membrul Parlamentului European în cauză trebuie să completeze un formular cu informații personale.

11.10. Președintele specifică în cererea sa către autoritățile naționale competente nivelul de clasificare al informațiilor care vor fi puse la dispoziția membrului Parlamentului European în cauză, astfel încât acestea să poată desfășura verificarea de securitate.

11.11. Întregul proces de verificare de securitate desfășurat de autoritățile naționale competente împreună cu rezultatele obținute sunt în conformitate cu reglementările relevante în vigoare în statul membru în cauză, inclusiv cele privind căile de apel.

11.12. Dacă autoritățile naționale competente din statele membre dau un aviz favorabil, președintele poate elibera autorizația membrului Parlamentului European în cauză.

11.13. Membrul Parlamentului European în cauză este informat în cazul unui aviz negativ al autorităților naționale competente și poate cere ascultarea sa de către președinte. În cazul în care consideră necesar, președintele se poate adresa autorităților naționale competente pentru a le solicita clarificări suplimentare. Dacă avizul negativ este confirmat, nu se acordă autorizația.

11.14. Toți membrii Parlamentului European autorizați în sensul punctului 11.3 primesc, la data autorizării și, ulterior, la intervale regulate, toate liniile directoare necesare privind protecția informațiilor clasificate și mijloacele de a asigura această protecție. Membrii Parlamentului European în cauză semnează o declarație prin care confirmă primirea informațiilor.

11.15. În circumstanțe excepționale, după ce a notificat în prealabil autoritățile naționale competente și în cazul în care acestea nu răspund în termen de o lună, președintele poate să acorde unui membru al Parlamentului European o autorizație provizorie, pentru o perioadă care nu poate depăși șase luni, în așteptarea rezultatului anchetei menționate la punctul 11.11. Autorizațiile provizorii astfel acordate nu permit accesul la informații clasificate drept „TRÈS SECRET UE/EU TOP SECRET".

12. **Procedura de acordare a autorizării de securitate pentru funcționarii Parlamentului European și alți angajați ai parlamentului care lucrează pentru grupurile politice**

12.1. Doar funcționarii Parlamentului European și alți angajați ai Parlamentului care lucrează pentru grupurile politice care, prin natura sarcinilor lor și pentru cerințe de serviciu, trebuie să cunoască sau să utilizeze informații clasificate deținute de Comisie au acces la astfel de informații.

12.2. Pentru a avea acces la informații clasificate drept „TRÈS SECRET UE/EU TOP SECRET", „SECRET UE/EU SECRET" și „CONFIDENTIEL UE/EU CONFIDENTIAL", persoanele menționate la punctul 12.1 anterior trebuie să fi fost autorizate în conformitate cu procedura stabilită la punctele 12.3 și 12.4.

12.3. Autorizațiile se acordă doar persoanelor menționate la punctul 12.1 care au fost supuse unei verificări de securitate de către autoritățile naționale competente ale statelor membre (ANS) în conformitate cu procedura menționată la punctele 12.9-12.14. Secretarul general este responsabil pentru procedura prin care autorizația este acordată funcționarilor Parlamentului European și altor angajați ai Parlamentului care lucrează pentru grupurile politice.

12.4. Secretarul general poate acorda autorizația după obținerea avizului emis de autoritățile naționale competente ale statelor membre pe baza verificării de securitate efectuate în conformitate cu punctele 12.8-12.13.

12.5. Direcția Parlamentului European responsabilă cu securitatea păstrează o listă actualizată a tuturor posturilor pentru care este necesară o procedură de acordare a autorizării de securitate, furnizată de serviciile competente ale Parlamentului European, și a tuturor persoanelor cărora li s-a acordat o autorizație, inclusiv o autorizație provizorie în sensul punctului 12.15.

12.6. Autorizația este valabilă pe o perioadă de cinci ani sau pe durata sarcinilor pentru care a fost eliberată, oricare dintre aceste perioade este mai scurtă. Autorizația poate fi reînnoită în conformitate cu procedura menționată la punctul 12.4.

12.7. Autorizația este retrasă de secretarul general în cazul în care acesta consideră că există motive justificate în acest sens. Orice decizie de retragere a autorizației se notifică funcționarului Parlamentului European și angajatului Parlamentului care lucrează pentru grupurile politice, care poate cere să fie ascultat de către secretarul general înainte ca retragerea autorizației să producă efecte, precum și autorității naționale competente.

12.8. Verificarea de securitate se efectuează cu sprijinul persoanei în cauză și la cererea secretarului general. Autoritatea națională competentă pentru verificare este cea a statului membru al cărui cetățean este persoana în cauză. În cazul în care acest lucru este permis de legislația și reglementările naționale, autoritățile naționale competente pot să supună persoane care nu sunt cetățeni ai statului membru respectiv unor investigații în cazul în care acestea solicită acces la informații clasificate drept „CONFIDENTIEL UE/EU CONFIDENTIAL" sau la informații cărora li s-a atribuit un nivel de clasificare mai înalt.

12.9. În cadrul procedurii de verificare, funcționarul Parlamentului European sau angajatul Parlamentului care lucrează pentru grupurile politice completează un formular cu informații personale.

12.10. Secretarul general specifică în cererea sa către autoritățile naționale competente tipul și nivelul de clasificare al informațiilor de care persoana în cauză urmează să ia la cunoștință, astfel încât acestea să poată desfășura verificarea de securitate și furniza un aviz cu privire la nivelul de autorizare care ar fi potrivit să îi fie acordat persoanei în cauză.

12.11. Întregul proces de verificare de securitate desfășurat de autoritățile naționale competente și rezultatele obținute sunt supuse reglementărilor relevante în vigoare în statul membru în cauză, inclusiv celor privind căile de apel.

12.12. Dacă autoritățile naționale competente din statul membru dau un aviz favorabil, secretarul general poate elibera autorizația persoanei în cauză.

12.13. Un aviz negativ al autorităților naționale competente se notifică funcționarului Parlamentului European sau altui angajat al Parlamentului care lucrează pentru grupurile politice, care poate cere să fie ascultat de către secretarul general. În cazul în care consideră necesar, secretarul general se poate adresa autorităților naționale competente pentru a le solicita clarificări suplimentare. Dacă avizul negativ este confirmat, nu se acordă autorizația.

12.14. Toți funcționarii Parlamentului European și angajații Parlamentului care lucrează pentru grupurile politice, autorizați în sensul punctelor 12.4 și 12.5 primesc, în momentul acordării autorizației și ulterior periodic, toate instrucțiunile necesare privind protecția informațiilor clasificate și mijloacele prin care se asigură această protecție. Acești funcționari și angajați semnează o declarație prin care confirmă că au primit aceste instrucțiuni și că se obligă să le respecte.

12.15. În circumstanțe excepționale, după ce a notificat în prealabil autoritățile naționale competente și în cazul în care acestea nu răspund în termen de o lună, secretarul general poate să acorde o autorizație provizorie unui funcționar al Parlamentului European sau unui alt angajat al Parlamentului care lucrează pentru grupurile politice, pentru o perioadă care nu poate depăși șase luni, în așteptarea rezultatului verificării de securitate menționate la punctul 12.11. Autorizațiile provizorii astfel acordate nu permit accesul la informații clasificate drept „TRÈS SECRET UE/EU TOP SECRET”.