1.4.2014 RO Jurnalul Oficial al Uniunii Europene C 96/1

II

(Comunicări)

COMUNICĂRI PROVENIND DE LA INSTITUȚIILE, ORGANELE ȘI ORGANISMELE UNIUNII EUROPENE

PARLAMENTUL EUROPEAN

DECIZIA BIROULUI PARLAMENTULUI EUROPEAN

din 15 aprilie 2013

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

(2014/C 96/01)

BIROUL PARLAMENTULUI EUROPEAN,

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

Întrucât:

(1) În lumina Acordului-cadru privind relațiile dintre Parlamentul European și Comisia Europeană ([1]), semnat la 20 octombrie 2010 (Acordul-cadru) și a acordului interinstituțional dintre Parlamentul European și Consiliu cu privire la transmiterea și manipularea de către Parlamentul European a informațiilor clasificate deținute de Consiliu cu privire la alte chestiuni decât cele din domeniul politicii externe și de securitate comune ([2]), semnat la 12 martie 2014 (Acordul interinstituțional), este necesar să se stabilească norme specifice cu privire la tratarea informațiilor confidențiale de către Parlamentul European.

(2) Tratatul de la Lisabona atribuie noi sarcini Parlamentului European și, pentru a dezvolta activitățile Parlamentului în acele domenii care necesită un anumit nivel 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, organe, 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) Dispozițiile prezentei decizii nu aduc prejudicii normelor prezente și viitoare privind accesul la documentele adoptate în conformitate cu articolul 15 din Tratatul privind funcționarea Uniunii Europene (TFUE).

([1]) JO L 304, 20.11.2010, p. 47.
([2]) JO C 95, 1.4.2014, p. 1.

(5) Dispozițiile prezentei decizii nu aduc prejudicii normelor prezente și viitoare privind protecția datelor personale adoptate în conformitate cu articolul 16 TFUE,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Obiectiv

Prezenta decizie reglementează gestionarea și manipularea informațiilor confidențiale de către Parlamentul European, inclusiv crearea, primirea, transmiterea și stocarea informațiilor confidențiale în vederea unei protecții adecvate a naturii confidențiale a acestora. Prezenta decizie pune în aplicare Acordul interinstituțional și Acordul-cadru, în special Anexa II la acesta.

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" și „alte informații confidențiale" neclasificate;

(c) „informații clasificate" înseamnă „informații clasificate UE" (ICUE) și „informații clasificate echivalente";

(d) „informații clasificate UE" (ICUE) înseamnă orice informație sau material, clasificat „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 Uniunii sau ale unuia sau mai multora dintre statele sale membre, indiferent dacă informația în cauză provine din cadrul instituțiilor, organelor, oficiilor sau agențiilor înființate în virtutea sau în baza tratatelor. În acest sens, informațiile și materialele clasificate la nivelul:

— „TRÈS SECRET UE/EU TOP SECRET" înseamnă 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" înseamnă 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" înseamnă 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" înseamnă informații și materiale a căror divulgare neautorizată ar putea dezavantaja interesele Uniunii sau ale unuia sau mai multora dintre statele membre;

(e) „informații clasificate echivalent" înseamnă informații clasificate emise de statele membre, țările terțe sau organizațiile internaționale, care poartă un marcaj de clasificare a securității echivalent cu unul dintre marcajele de clasificare a securității utilizate pentru ICUE și care au fost transmise Parlamentului European de către Consiliu sau Comisie;

(f) „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, organe, oficii și agenții înființate în virtutea sau în baza tratatelor sau de statele membre;

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

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

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

(j) „autorizație" înseamnă o decizie adoptată de Președinte, în cazul deputaților în Parlamentul European, sau de Secretarul General, în cazul funcționarilor Parlamentului European și al altor angajați ai Parlamentului European care lucrează pentru grupurile politice, de a permite accesul unei persoane la informații clasificate 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;

(k) „declasare" înseamnă o reducere a nivelului de clasificare;

(l) „declasificare" înseamnă eliminarea din orice sistem de clasificare;

(m) „marcaj" înseamnă un semn anexat „altor informații confidențiale", cu scopul de a identifica instrucțiuni specifice, predefinite, cu privire la manipularea acestora sau la domeniul vizat de un anumit document. Marcajul poate fi anexat, de asemenea, informațiilor clasificate, pentru a impune cerințe suplimentare cu privire la manipularea acestora.

(n) „demarcare" înseamnă eliminarea tuturor marcajelor;

(o) „emitent" înseamnă autorul informațiilor confidențiale, autorizat în mod corespunzător;

(p) „notificări de securitate" înseamnă măsurile de punere în aplicare prevăzute în Anexa II.

(q) „instrucțiuni de manipulare" înseamnă instrucțiuni tehnice pentru serviciile Parlamentului European cu privire la gestionarea informațiilor confidențiale.

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 prevăzute în Anexa I partea 1.

(2) Parlamentul European instituie un sistem de management al securității informațiilor (SMSI) în conformitate cu respectivele principii de bază și standarde minime. SMSI constă din notificările de securitate, instrucțiunile de manipulare și normele relevante din Regulamentul de procedură. SMSI urmărește facilitarea activităților parlamentare și administrative, garantând în același timp protecția oricărei informații confidențiale prelucrate de Parlamentul European, cu respectarea deplină a normelor stabilite de emitentul acestor informații, astfel cum se prevede în notificările de securitate.

Prelucrarea informațiilor confidențiale cu ajutorul unor sisteme informatice de comunicare(SIC) automate ale Parlamentului European, prevăzute în notificarea de securitate 3, se desfășoară în conformitate cu conceptul de asigurare a informațiilor (AI).

(3) Deputații în Parlamentul European pot consulta informații clasificate până la și incluzând nivelul „RESTREINT UE/EU RESTRICTED" în absența unei autorizații de securitate.

(4) Atunci când informațiile în cauză sunt clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL" sau la un nivel echivalent, accesul la astfel de informații se acordă acelor deputați în Parlamentul European care au fost autorizați de Președinte, în conformitate cu alineatul (5) sau care au semnat o declarație solemnă de nedezvăluire a acestor informații către persoanele terțe, de respectare a obligației de a proteja informațiile clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL" și de recunoaștere a consecințelor în caz de nerespectare a acesteia.

(5) Atunci când informațiile în cauză sunt clasificate la nivelul „SECRET UE/EU SECRET" sau „TRÈS SECRET/EU TOP SECRET" sau la un nivel echivalent, accesul la astfel de informații se acordă acelor deputați în Parlamentul European care sunt autorizați de Președinte după ce:

(a) au primit autorizația de securitate în conformitate cu Anexa I partea 2 din prezenta decizie sau

(b) a fost primită o notificare din partea unei autorități naționale competente conform căreia deputații în cauză sunt autorizați în mod corespunzător prin natura funcțiilor deținute în conformitate cu legislația națională.

(6) Înainte de a li se acorda acces la informațiile clasificate, deputații în Parlamentul European sunt informați cu privire la responsabilitatea lor de a proteja aceste informații și recunosc această responsabilitate, în conformitate cu Anexa I. Deputații în Parlamentul European sunt informați cu privire la mijloacele de asigurare a acestei protecții.

(7) 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. Accesul la informațiile clasificate este acordat doar dacă au fost informați și dacă au primit instrucțiuni scrise cu privire la responsabilitățile ce le revin în ceea ce privește protejarea acestor informații, precum și cu privire la mijloacele de asigurare a acestei protecții, precum și dacă au semnat o declarație de luare la cunoștință a acestor instrucțiuni și de asumare a obligației de a le respecta, în conformitate cu prezentele norme.

Articolul 4

Crearea de informații confidențiale și manipularea administrativă 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 notificările de securitate.

(2) Atunci când creează o informație clasificată, emitentul aplică nivelul adecvat de clasificare în conformitate cu standardele internaționale și definițiile menționate în Anexa I. De asemenea, emitentul decide, ca regulă generală, destinatarii care urmează a fi autorizați să consulte informațiile, în funcție de nivelul de clasificare. Informația respectivă se comunică Unității de Informații Confidențiale (UIC) atunci când documentul este depus la UIC.

(3) „Alte informații confidențiale" care fac obiectul secretului profesional sunt manipulate în conformitate cu anexele I și II și cu instrucțiunile de manipulare.

Articolul 5

Primirea de informații confidențiale de către Parlamentul European

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

(a) informațiile clasificate la nivelul „RESTREINT UE/EU RESTRICTED" sau la un nivel echivalent și „alte informații confidențiale", secretariatului organului/titularului de mandat parlamentar care a înaintat cererea sau direct UIC;

(b) informațiile clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL" „SECRET UE/EU SECRET" sau „TRÈS SECRET UE/EU TOP SECRET" sau la un nivel echivalent, UIC.

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

(3) Modalitățile convenite care urmează a fi stabilite de comun acord pentru a păstra confidențialitatea informațiilor, în cazul informațiilor confidențiale comunicate de Comisie în conformitate cu punctul 3.2 din Anexa II la Acordul-cadru sau, în cazul informațiilor clasificate transmise de Consiliu în conformitate cu articolul 5 alineatul (4) din Acordul interinstituțional, se depun împreună cu informația confidențială la secretariatul organului/titularului de mandat parlamentar sau la UIC, după caz.

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

(5) Pentru a asigura un nivel de protecție proporțional cu nivelul de clasificare „TRÈS SECRET UE/EU TOP SECRET" sau cu un nivel echivalent, Conferința președinților instituie un comitet de supraveghere. Informațiile clasificate la nivelul „TRÈS SECRET UE/EU TOP SECRET" sau la un nivel echivalent sunt comunicate Parlamentului European, făcând obiectul altor măsuri care urmează a fi convenite între Parlamentul European și instituția Uniunii de la care sunt primite informațiile.

Articolul 6

Comunicarea informațiilor clasificate de către Parlamentul European unor terți

Parlamentul European poate, sub rezerva consimțământului anterior scris al emitentului sau al instituției Uniunii care a comunicat informația clasificată Parlamentului European, după caz, să transmită aceste informații clasificate părților terțe, cu condiția ca acestea să asigure, la manipularea acestor informații, că se respectă norme similare celor menționate în prezenta decizie în cadrul serviciilor și sediilor.

Articolul 7

Incinte securizate

(1) În scopul gestionării informațiilor confidențiale, Parlamentul European instituie o zonă securizată și săli de lectură securizate.

(2) Zona securizată furnizează echipamente pentru înregistrarea, consultarea, arhivarea, transmiterea și manipularea informațiilor clasificate. Aceasta cuprinde, printre altele, o sală de lectură și o sală de reuniune pentru consultarea informațiilor clasificate și este gestionată de UIC.

(3) În afara zonei securizate, pot fi create săli de lectură securizate pentru a permite consultarea informațiilor clasificate la nivelul „RESTREINT UE/EU RESTRICTED" sau la un nivel echivalent, precum și alte „alte informații confidențiale". Aceste săli de lectură securizate sunt administrate de serviciile competente ale secretariatelor organului/titularului de mandat parlamentar sau de UIC, după caz. Acestea nu conțin copiatoare, telefoane, faxuri, scanere sau orice alt mijloc tehnic de reproducere sau transmitere de documente.

Articolul 8

Înregistrarea, manipularea și stocarea informațiilor confidențiale

(1) Informațiile clasificate la nivelul „RESTREINT UE/EU RESTRICTED" sau la un nivel echivalent și „alte informații confidențiale" sunt înregistrate și depozitate de serviciile competente ale secretariatelor organului/titularului de mandat parlamentar sau de UIC, în funcție de cine a primit informațiile.

(2) Următoarele condiții se aplică manipulării informațiilor clasificate la nivelul „RESTREINT UE/EU RESTRICTED” sau la un nivel echivalent și „altor informații confidențiale”:

(a) documentele se înmânează personal șefului secretariatului, care le înregistrează și furnizează o confirmare de primire;

(b) când nu sunt folosite în mod efectiv, astfel de documente se păstrează sub cheie, sub răspunderea secretariatului;

(c) în niciun caz informațiile nu pot fi salvate pe un alt suport sau transmise altei persoane; aceste documente pot fi reproduse numai cu ajutorul echipamentelor acreditate adecvat, astfel cum sunt definite în notificările de securitate;

(d) accesul la aceste informații este rezervat doar acelor persoane desemnate de emitent sau de instituția Uniunii care a comunicat informațiile Parlamentului European, în conformitate cu modalitățile menționate la articolul 4 alineatul (2) sau la articolul 5 alineatele (3), (4) și (5).

(e) secretariatul organului/titularului de mandat parlamentar ține un registru al persoanelor care au consultat informațiile, cuprinzând data și ora la care s-a efectuat consultarea, și transmite registrul către UIC la momentul depunerii informațiilor la UIC.

(3) Informațiile clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL”, „SECRET UE/EU SECRET” sau „TRÈS SECRET UE/EU TOP SECRET” sau la un nivel echivalent sunt înregistrate, tratate și depozitate de UIC în zona securizată, în conformitate cu nivelul specific al clasificării și astfel cum este definit în notificările de securitate.

(4) În situația unei încălcări a regulilor prevăzute la alineatele (1) — (3), funcționarul din cadrul secretariatului organului/titularului de mandat parlamentar sau al UIC, după caz, îl informează pe Secretarul General, care va prezenta situația Președintelui, în cazul în care persoana vinovată de a fi încălcat aceste reguli este un deputat în Parlamentul European.

Articolul 9

Accesul la incintele securizate

(1) Accesul în zona securizată este permis exclusiv:

(a) persoanelor care, în conformitate cu articolul 3 alineatele (4)-(7), sunt autorizate să consulte informațiile aflate acolo și care au prezentat o cerere în conformitate cu articolul 10 alineatul (1);

(b) persoanelor care, în conformitate cu articolul 4 alineatul (1) sunt autorizate să creeze informații clasificate și care au prezentat o cerere în conformitate cu articolul 10 alineatul (1);

(c) funcționarilor UIC din Parlamentul European;

(d) funcționarilor Parlamentului European responsabili cu gestionarea SIC;

(e) funcționarilor Parlamentului European responsabili cu securitatea și protecția împotriva incendiilor, atunci când este necesar;

(f) personalului de curățenie, dar numai în prezența și sub atenta supraveghere a unui funcționar din cadrul UIC.

(2) UIC poate refuza accesul în zona securizată oricărei persoane neautorizate. Toate contestațiile privind un astfel de refuz al accesului se transmit Președintelui, în cazul cererilor de acces ale deputaților în Parlamentul European, și Secretarului General, în alte cazuri.

(3) Secretarul General poate autoriza o reuniune pentru un număr limitat de persoane în sala de reuniune din cadrul zonei securizate.

(4) Accesul în sala de lectură securizată este permis exclusiv:

(a) deputaților în Parlamentul European, funcționarilor din cadrul Parlamentului European și altor angajați ai Parlamentului European care lucrează pentru grupurile politice, identificați în mod corespunzător, în scopul consultării informațiilor confidențiale sau al creării acestora;

(b) funcționarilor Parlamentului European responsabili cu gestionarea SIC, funcționarilor din cadrul secretariatului organului/titularului de mandat parlamentar care au primit informațiile și funcționarilor UIC;

(c) dacă este necesar, funcționarilor Parlamentului European responsabili cu securitatea și protecția împotriva incendiilor;

(d) personalului de curățenie, dar numai în prezența și sub atenta supraveghere a unui funcționar din cadrul secretariatului organului/titularului de mandat parlamentar sau al UIC, după caz;

(5) Secretariatul competent al organului/titularului de mandat parlamentar sau UIC, după caz, poate refuza accesul într-o sală de lectură securizată oricărei persoane neautorizate. Toate contestațiile privind un astfel de refuz al accesului se transmit Președintelui, în cazul cererilor de acces ale deputaților în Parlamentul European, și Secretarului General, în alte cazuri.

Articolul 10

Consultarea informațiilor confidențiale sau crearea acestora în incintele securizate

(1) Orice persoană care dorește să consulte sau să creeze informații confidențiale în zona securizată comunică în avans numele său UIC. UIC verifică identitatea persoanei respective și controlează dacă persoana respectivă este autorizată, în conformitate cu articolul 3 alineatele (3)-(7), articolul 4 alineatul (1) sau articolul (5) alineatele (3), (4) și (5), să consulte sau să creeze informații confidențiale.

(2) Orice persoană care dorește, în conformitate cu articolul 3 alineatele (3) și e (7), să consulte informațiile confidențiale clasificate la nivelul „RESTREINT UE/EU RESTRICTED" sau la un nivel echivalent sau „alte informații confidențiale" într-o sală de lectură securizată, își comunică numele în prealabil serviciilor competente ale secretariatului organului/titularului de mandat parlamentar sau UIC.

(3) 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 într-o incintă securizată, în prezența unui funcționar din cadrul secretariatului organului/titularului de mandat parlamentar sau al UIC.

(4) În timpul consultării, se interzice contactul cu exteriorul (inclusiv prin intermediul telefonului sau al altor echipamente tehnice), luarea de notițe și fotocopierea sau fotografierea informațiilor confidențiale consultate.

(5) Înainte să se permită unei persoane să părăsească sala de lectură securizată, funcționarul din cadrul secretariatului organului/titularului de mandat parlamentar sau al UIC se asigură de existența informațiilor confidențiale consultate și verifică dacă acestea sunt în continuare intacte și complete.

(6) În situația unei încălcări a regulilor de mai sus, funcționarul din cadrul secretariatului organului/titularului de mandat parlamentar sau al UIC îl informează pe Secretarul General, care va prezenta situația Președintelui, în cazul în care este implicat un deputat în Parlamentul European.

Articolul 11

Standarde minime privind consultarea informațiilor confidențiale în cadrul unei reuniuni in camera din afara incintelor securizate

(1) Informațiile clasificate la nivelul „RESTREINT UE/EU RESTRICTED" sau la un nivel echivalent și „alte informații confidențiale" pot fi consultate de membrii comisiilor parlamentare sau de alte organe politice și administrative ale Parlamentului European în cadrul unei reuniuni in camera din afara incintelor securizate.

(2) În cazul prevăzut la alineatul (1), secretariatul organului/titularului de mandat parlamentar responsabil pentru reuniune asigură respectarea următoarelor condiții:

(a) doar persoanele desemnate de președintele comisiei competente sau al organului politic să participe la reuniune pot intra în sala de reuniune;

(b) 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;

(c) procesul-verbal al reuniunii nu menționează conținutul discuției cu privire la informațiile avute în vedere. Numai decizia relevantă, în cazul în care aceasta există, poate fi consemnată în procesul-verbal;

(d) informațiile confidențiale furnizate oral destinatarilor din Parlamentul European se supun aceluiași nivel de protecție a informațiilor confidențiale ca acela aplicat informațiilor confidențiale furnizate în scris;

(e) în sălile de reuniune nu sunt ținute stocuri suplimentare de documente;

(f) la începutul reuniunii se distribuie participanților și interpreților doar numărul necesar de copii ale documentelor;

(g) statutul clasificării/marcajului documentelor este clarificat de președinte la începutul reuniunii;

(h) participanții nu scot documentele din sala de reuniune;

(i) toate copiile documentelor sunt adunate și verificate la sfârșitul reuniunii de secretariatul organului/titularului de mandat parlamentar; și

(j) niciun echipament electronic sau de comunicare nu este introdus în sala de reuniune în cazul când se consultă sau se discută informația confidențială în cauză.

(3) În cazul în care, în conformitate cu excepțiile prevăzute la punctul 3.2.2 din Anexa II la Acordul-cadru și în articolul 6 alineatul (5) din Acordul interinstituțional, informațiile clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL" sau la un nivel echivalent, se discută în cadrul unei reuniuni desfășurate in camera, secretariatul organului/titularului de mandat parlamentar responsabil cu reuniunea se asigură, pe lângă respectarea dispozițiilor prevăzute la alineatul (2), că persoanele desemnate să participe la reuniune respectă cerințele articolului 3 alineatele (4) și (7).

(4) În cazul prevăzut la alineatul (3), UIC furnizează secretariatului organului/titularului de mandat parlamentar responsabil cu reuniunea in camera numărul necesar de copii ale documentelor ce urmează a fi discutate, care sunt înapoiate UIC după reuniune.

Articolul 12

Arhivarea informațiilor confidențiale

(1) Se pun la dispoziție posibilități de arhivare sigure în zona securizată. UIC este responsabil de gestionarea arhivei securizate, în conformitate cu criteriile standard de arhivare.

(2) Informațiile clasificate depozitate definitiv la UIC și informațiile clasificate la nivelul „RESTREINT UE/EU RESTRICTED" sau la un nivel echivalent, depozitate la secretariatul organului/titularului de mandat parlamentar, sunt transferate în arhiva securizată din zona securizată după șase luni de la data ultimei consultări, dar nu mai târziu de un an de la data depozitării. „Alte informații confidențiale" sunt arhivate, dacă nu sunt depozitate la UIC, de secretariatul organului/titularului de mandat parlamentar respectiv, în conformitate cu normele generale privind gestionarea documentelor.

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

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

(b) cererea de consultare a informațiilor confidențiale trebuie prezentată UIC, care asigură transferul documentului în cauză în sala de lectură securizată;

(c) se aplică procedurile și condițiile privind consultarea informațiilor confidențiale stabilite la articolul 10.

Articolul 13

Declasare, declasificare și demarcarea informațiilor confidențiale

(1) Informațiile confidențiale pot fi declasate, declasificate sau demarcate doar cu consimțământul prealabil al emitentului și, dacă este necesar, după consultarea celorlalte părți în cauză.

(2) Declasarea sau declasificarea se confirmă în scris. Emitentul 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, emitenții specifică pe documentele clasificate o dată, o perioadă sau un eveniment de la care conținutul poate fi declasat sau declasificat. Altfel, aceștia revizuiesc documentele cel târziu o dată la cinci ani pentru a asigura necesitatea menținerii clasificării inițiale.

(3) Informațiile confidențiale păstrate în arhivele securizate sunt examinate la timp, cel mai târziu în al 25-lea an după data creării lor, pentru a decide dacă ar trebui sau nu declasificate, declasate sau demarcate. Examinarea și publicarea acestor informații are loc 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 emitentul informațiilor clasificate sau de către serviciul responsabil în momentul respectiv, în conformitate cu Anexa I, partea 1, secțiunea 10.

(4) În urma declasificării, informațiile anterior clasificate, păstrate în arhiva securizată, sunt transferate în arhivele istorice ale Parlamentului European în scopul păstrării permanente și al tratării lor ulterioare în conformitate cu normele aplicabile.

(5) În urma eliminării marcajului, fostele „alte informații confidențiale” fac obiectul normelor Parlamentului European privind gestionarea documentelor.

Articolul 14

Încălcările securității, pierderea sau compromiterea informațiilor confidențiale

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

(2) Încălcarea confidențialității de către un membru al personalului Parlamentului European atrage după sine aplicarea procedurilor și sancțiunilor prevăzute de Statutul funcționarilor și Regimul aplicabil altor agenți ai Uniunii Europene, prevăzut în Regulamentul (CEE, Euratom, ECSC) nr. 259/68 ([2]) („Statutul funcționarilor”).

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

(3) Președintele și/sau Secretarul General, după caz, organizează eventualele anchete care se impun în cazul încălcării confidențialității, astfel cum este definită la notificarea de securitate 6.

(4) Dacă informațiile confidențiale au fost comunicate Parlamentului European de către o instituție a Uniunii sau de către un stat membru, Președintele și/sau Secretarul General, după caz, informează instituția Uniunii sau statul membru în cauză cu privire la orice pierdere sau compromitere, dovedită sau suspectată, a informațiilor clasificate și cu privire la rezultatele anchetei și la măsurile adoptate pentru a preveni repetarea faptelor.

Articolul 15

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 este responsabil cu punerea în aplicare a prezentei decizii de către serviciile Parlamentului European și emite instrucțiunile de manipulare a chestiunilor care fac obiectul SMSI, în conformitate cu principiile stabilite de prezenta decizie.

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

Articolul 16

Dispoziții tranzitorii și finale

(1) Informațiile neclasificate care sunt deținute de UIC sau de oricare altă arhivă a Parlamentului European și care sunt considerate confidențiale și datate înainte de 1 aprilie 2014 sunt considerate „alte informații confidențiale" în sensul prezentei decizii. Emitentul informațiilor respective poate în orice moment să reexamineze nivelul de confidențialitate.

(2) Prin derogare de la articolul 5 alineatul (1) litera (a) și de la articolul 8 alineatul (1) din prezenta decizie, pentru o perioadă de 12 luni de la 1 aprilie 2014, informațiile furnizate de Consiliu în temeiul Acordului interinstituțional, și care sunt clasificate la nivelul „RESTREINT UE/EU RESTRICTED" sau la un nivel echivalent sunt depozitate, înregistrate și stocate la UIC. Aceste informații pot fi consultate în conformitate cu articolul 4 alineatul (2) literele (a) și (c) și cu articolul 5 alineatul (4) din Acordul interinstituțional.

(3) Decizia Biroului Parlamentului European din 6 iunie 2011 referitoare la normele de reglementare a tratamentului informațiilor confidențiale de către Parlamentul European este abrogată.

Articolul 17

Intrarea în vigoare

Prezenta decizie intră în vigoare în ziua publicării sale în *Jurnalul Oficial al Uniunii Europene*.

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 pentru protejarea informațiilor confidențiale care trebuie respectate de către Parlamentul European în toate punctele sale de lucru, inclusiv de către toți destinatarii informațiilor confidențiale și ai „altor informații confidențiale", astfel încât să se garanteze securitatea, toate părțile interesate fiind asigurate în legătură cu stabilirea unui standard comun de protecție. Aceste dispoziții sunt completate de notificările de securitate din Anexa II și de alte dispoziții care reglementează tratamentul informațiilor confidențiale de către comisiile parlamentare și de către alte organe parlamentare/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, subsidiaritatea și proporționalitatea.

Legalitatea presupune necesitatea de a menține strict în cadrul legal executarea funcțiilor de securitate și necesitatea de a respecta cerințele legale aplicabile. În plus, responsabilitățile din domeniul securității trebuie să se bazeze pe dispoziții juridice 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 sunt tratate în conformitate cu Regulamentul său de procedură și cu politica sa privind măsurile disciplinare.

Transparența 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. În plus, sunt necesare orientări scrise clare pentru punerea în aplicare a măsurilor de securitate.

Răspunderea presupune că responsabilitățile din domeniul securității trebuie să fie clar definite. În plus, presupune nevoia de a monitoriza cu regularitate corecta executare a acestor responsabilități.

Subsidiaritatea înseamnă că securitatea trebuie să fie organizată la cel mai jos nivel posibil și cât mai aproape posibil de Direcțiile Generale și de serviciile Parlamentului European. Proporționalitatea înseamnă că activitățile de securitate trebuie să se limiteze strict la ceea ce este absolut necesar și că măsurile de securitate trebuie să fie 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) sisteme informatice adecvate de comunicare (SIC). Acestea se află sub responsabilitatea autorității de securitate a Parlamentului European;

(b) în cadrul Parlamentului European, Autoritatea de asigurare a informațiilor (astfel cum este definită în notificarea de securitate 1) este însărcinată cu colaborarea cu autoritatea de securitate în cauză pentru a furniza informații și sfaturi privind amenințările tehnice la adresa SIC și mijloacele de protecție împotriva acestor amenințări;

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

4. **PRINCIPIILE SECURITĂȚII INFORMAȚIEI**

4.1. ***Obiective***

Principalele obiective ale securității informației sunt, după cum urmează:

(a) salvgardarea informațiilor confidențiale împotriva spionajului, compromiterii sau divulgării neautorizate;

(b) salvgardarea informațiilor clasificate 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 informațiile clasificate împotriva sabotajelor și a actelor intenționate de deteriorare;

(d) în caz de eșec al securității, evaluarea daunelor cauzate, limitarea consecințelor, 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, precum și pentru evaluarea nivelului de protecție necesar. Este esențial 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 nivel de protecție celor mai importante sedii care adăpostesc informații clasificate și celor mai sensibile puncte din interiorul acestora.

4.2.3. Responsabilitatea pentru clasificarea informațiilor îi revine exclusiv emitentului informațiilor în cauză.

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

4.2.5. Atunci când mai multe elemente de informație sunt grupate, clasificarea acestora este cel puțin egală cu nivelul de clasificare cel mai ridicat atribuit unuia dintre elementele individuale. Cu toate acestea, unui grup de informații i se poate atribui o clasificare mai înaltă decât cea a părților sale componente.

4.2.6 Clasificările sunt atribuite 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 informații clasificate, la mijloacele de transmitere a informațiilor clasificate și la „alte informații confidențiale”, precum și la toate sediile care conțin astfel de informații și la instalații importante;

(b) sunt concepute pentru a identifica persoanele a căror poziție (din punct de vedere al accesului, al relațiilor sau altele) ar putea pune în pericol securitatea unor asemenea informații și a instalațiilor importante care conservă 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 (prin prevenirea coruperii, a modificării neautorizate sau a ștergerii neautorizate) și disponibilitatea (accesul nu este refuzat celor care au nevoie de informații și au acces autorizat) informațiilor confidențiale, 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 informațiilor clasificate, 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 manipulate 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 terților la aceste informații doar cu condiția ca aceștia să garanteze că manipularea lor se realizează cu 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 informații clasificate 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 confirmă 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 incidente sau vulnerabilități evidente 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 asigure, 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, luarea de 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 informarea serviciul responsabil al Parlamentului European. Dacă se stabilește de către autoritatea națională de securitate competentă 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 informații clasificate.

7.1. ***Nevoia de protecție***

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

7.2. ***Verificări***

Înainte de a lăsa nesupravegheate zonele care conțin informații clasificate, persoanele care răspund de păstrarea informațiilor în cauză se asigură că acestea sunt stocate în siguranță și că au fost activate toate dispozitivele de securitate (încuietori, alarme etc.). După orele de program se efectuează verificări suplimentare independente.

7.3. ***Securitatea clădirilor***

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

Natura protecției asigurate informațiilor clasificate, de exemplu ferestre cu gratii, încuietori pentru uși, paznici la intrări, sisteme automate de control al accesului, verificări și patrule de securitate, sisteme de alarmă, sisteme de detectare a efracțiilor și câini de pază, depinde de:

(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 cazul 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 (d) 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).

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

Identificatorii de securitate sunt reglementați în detaliu în notificarea de securitate 2 și sunt definiți în instrucțiunile de manipulare.

8.2. ***Marcajele***

Un marcaj este utilizat pentru a specifica instrucțiunile specifice predefinite privind manipularea informațiilor confidențiale. Marcajele pot indica și domeniul vizat de document sau o difuzare specială conform principiului nevoii de a cunoaște sau (pentru informații neclasificate) pentru a indica sfârșitul unei interdicții.

Un marcaj nu este o clasificare și nu este utilizat în locul unei clasificări.

Marcajele sunt reglementate în detaliu în notificarea de securitate 2 și sunt definite în instrucțiunile de manipulare.

8.3. ***Aplicarea clasificării și a identificatorilor de securitate***

Aplicarea clasificării, a identificatorilor de securitate și a marcajelor se execută în conformitate cu notificarea de securitate 2, secțiunea E și cu instrucțiunile de manipulare.

8.4. ***Administrarea clasificărilor***

8.4.1 *În 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 emitentului.

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

Procedurile detaliate 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 informații clasificate la nivelul „TRÈS SECRET UE/EU TOP SECRET” este păstrat la minimum, iar numele persoanelor în cauză sunt înscrise pe o listă întocmită de UIC.

8.4.2 *Aplicarea clasificărilor*

Clasificarea unui document este determinată de nivelul de sensibilitate a conținutului său, în conformitate cu definiția de la articolul 2 litera (d). Este importantă utilizarea corectă și cu moderație a clasificării.

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

Emitentul unui document care urmează a fi clasificat ține cont de normele stabilite anterior și evită clasificarea 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 pentru securitate și evaluarea riscurilor a Parlamentului European, care poate solicita asistență din partea autorităților de securitate ale Consiliului sau ale Comisiei, efectuează inspecții interne periodice ale aranjamentelor de securitate stabilite pentru protecția informațiilor clasificate.

Autoritățile de securitate și serviciile competente ale instituțiilor Uniunii pot efectua, ca parte a unui proces convenit inițiat de oricare dintre părți, evaluări inter pares ale aranjamentelor de securitate pentru protecția informațiilor clasificate în circulație în temeiul acordurilor interinstituționale relevante.

10. **DECLASIFICAREA ȘI DEMARCAREA**

10.1. UIC examinează informațiile confidențiale conținute în registrul său și solicită acordul emitentului pentru declasificarea sau demarcarea unui document cu cel mult 25 de ani după data la care documentul a fost creat. Documentele care nu sunt declasificate sau demarcate după o primă examinare sunt reexaminate periodic, și cel puțin o dată la cinci ani. Pe lângă documentele care se află în arhivele sigure din incinta securizată și care sunt clasificate în mod adecvat, procesul de demarcare poate să acopere, de asemenea, alte informații confidențiale deținute de organul/titularul de mandat parlamentar sau de serviciul responsabil de arhivele istorice ale Parlamentului.

10.2 Decizia de declasificare sau de demarcare a unui document este luată, ca regulă generală, doar de emitent sau, în mod excepțional, în cooperare cu organul/titularul de mandat parlamentar care deține informațiile, anterior ca informațiile conținute să fie transmise serviciului responsabil de arhivele istorice ale Parlamentului. Informațiile clasificate pot fi declasificate sau demarcate numai cu acordul scris prealabil al emitentului. În cazul informațiilor din categoria „alte informații confidențiale", secretariatul organului/titularului de mandat parlamentar care deține respectivele informații decide, în cooperare cu emitentul, dacă documentul poate fi demarcat.

10.3. În numele emitentului, UIC îi revine responsabilitatea de a informa destinatarii documentului cu privire la modificarea clasificării sau a marcajului, 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 identificatorii de securitate sau marcajele care pot apărea pe document.

10.5. În cazul declasificării, 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 UIC. În cazul demarcării, marcajul original, din partea de sus și din cea de jos pe fiecare pagină este barat.

10.6. Textul documentului declasificat sau demarcat 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.

10.8. Pe lângă prevederile de la punctele 10.1-10.7, se aplică următoarele norme:

(a) în ceea ce privește documentele terților, UIC consultă terții în cauză înainte de a efectua declasificarea sau demarcarea.

(b) în ceea ce privește excepția privind viața privată și integritatea persoanei, procedura de declasificare sau de demarcare ține seama în special de acordul persoanei în cauză, sau, după caz, de imposibilitatea identificării persoanei în cauză;

(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 de la data publicării pentru a-și prezenta observațiile.

Partea 2

PROCEDURA DE ACORDARE A AUTORIZAȚIEI DE SECURITATE

11. **PROCEDURA DE ACORDARE A AUTORIZAȚIEI DE SECURITATE PENTRU DEPUTAȚII ÎN PARLAMENTUL EUROPEAN**

11.1. Pentru a avea acces la informații clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL" sau la un nivel echivalent, deputații în Parlamentul European trebuie să fi fost autorizați în conformitate cu procedura prevăzută la punctele 11.3 și 11.4 din prezenta anexă sau în baza unei declarații solemne de nedivulgare în temeiul articolului 3 alineatul (4) din prezenta decizie.

11.2 Pentru a avea acces la informații clasificate la nivelul „SECRET UE/EU SECRET" sau „TRÈS SECRET UE/EU TOP SECRET" sau la un nivel echivalent, deputații în Parlamentul European trebuie să fi fost autorizați în conformitate cu procedura menționată la punctele 11.3 și 11.14.

11.3. Autorizațiile se acordă doar deputaților 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 deputaților autorizația.

11.4 Președintele poate acorda autorizația scrisă 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 pentru securitate și evaluarea riscului a Parlamentului European păstrează o listă actualizată a tuturor deputaților în Parlamentul 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 pentru a dispune retragerea. Orice decizie de retragere a autorizației se notifică deputatului în Parlamentul European în cauză, care poate cere să fie audiat de către Președinte înainte ca retragerea autorizației să producă efecte, precum și autorității naționale competente.

11.8. Verificarea de securitate se efectuează cu sprijinul deputatului vizat și la cererea Președintelui. Autoritatea națională competentă pentru verificare este cea a statului membru al cărui cetățean este deputatul în cauză.

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

11.10. Președintele specifică în cererea sa către autoritatea națională competentă nivelul de clasificare a informațiilor care vor fi puse la dispoziția deputatului în Parlamentul European în cauză, astfel încât aceasta să poată desfășura verificarea de securitate.

11.11 Întregul proces de verificare de securitate desfășurat de autoritatea națională competentă și rezultatele obținute sunt supuse reglementărilor relevante în vigoare în statul membru în cauză, inclusiv celor privind căile de atac.

11.12. Dacă autoritatea națională competentă emite un aviz favorabil, Președintele poate elibera autorizația deputatului în Parlamentul European în cauză.

11.13. Un aviz negativ al autorității naționale competente se notifică deputatului în Parlamentul European în cauză, care poate cere să fie audiat de către Președinte. În cazul în care consideră necesar, Președintele se poate adresa autorității naționale competente pentru a-i solicita clarificări suplimentare. Dacă avizul negativ este confirmat, nu se acordă autorizația.

11.14. Toți deputații în Parlamentul European autorizați în sensul punctului 11.3 primesc, în momentul acordării autorizației și, ulterior, periodic, toate informațiile necesare privind protecția informațiilor clasificate și mijloacele care se asigură această protecție. Deputații în Parlamentul European semnează o declarație prin care confirmă primirea informațiilor.

11.15. În circumstanțe excepționale, după ce a notificat în prealabil autoritatea națională competentă și în cazul în care aceasta nu răspunde în termen de o lună, Președintele poate să acorde unui deputat în Parlamentul European o autorizație provizorie, pentru o perioadă care nu poate depăși șase luni, în așteptarea rezultatului verificării de securitate menționate la punctul 11.11. Autorizațiile provizorii astfel acordate nu permit accesul la informații clasificate „TRÈS SECRET UE/EU TOP SECRET" sau la un nivel echivalent.

12. PROCEDURA DE ACORDARE A AUTORIZAȚIEI 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 la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" sau „TRÈS SECRET UE/EU TOP SECRET" sau la un nivel echivalent, funcționarii Parlamentului European și alți angajați ai Parlamentului care lucrează pentru grupurile politice implicate trebuie să fi fost autorizați în conformitate cu procedura prevăzută 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 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 scrisă 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 pentru securitate și evaluarea riscului a Parlamentului European păstrează o listă actualizată a tuturor posturilor pentru care este necesară o procedură de acordare a autorizației 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 pentru a dispune retragerea. Orice decizie de retragere a autorizației se notifică funcționarului Parlamentului European și angajatului Parlamentului care lucrează pentru grupurile politice, care poate cere să fie audiat 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 funcționarului Parlamentului European și al angajatului Parlamentului care lucrează pentru grupurile politice 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 la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL”, „SECRET UE/EU SECRET” sau „TRÈS SECRET UE/EU TOP SECRET”.

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 autoritatea națională competentă tipul și nivelul de clasificare a informațiilor de care funcționarul Parlamentului European sau angajatul Parlamentului care lucrează pentru grupurile politice urmează să ia la cunoștință, astfel încât aceasta 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 autoritatea națională competentă și rezultatele obținute sunt supuse reglementărilor relevante în vigoare în statul membru în cauză, inclusiv celor privind căile de atac.

12.12. Dacă autoritatea națională competentă emite un aviz favorabil, Secretarul General poate acorda autorizația funcționarului în cauză al Parlamentului European sau angajatului Parlamentului care lucrează pentru grupurile politice.

12.13. Un aviz negativ al autorității naționale competente se notifică funcționarului Parlamentului European sau altui angajat al Parlamentului care lucrează pentru grupurile politice, care poate cere să fie audiat de către Secretarul General. În cazul în care consideră necesar, Secretarul General se poate adresa autorității naționale competente pentru a-i 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 autoritatea națională competentă și în cazul în care aceasta nu răspunde 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 la nivelul „TRÈS SECRET UE/EU TOP SECRET" sau la un nivel echivalent.

ANEXA II

INTRODUCERE

Prezentele dispoziții stabilesc notificările de securitate care reglementează și asigură tratarea și manipularea securizată a informațiilor confidențiale în cadrul Parlamentului European. Prezentele notificări de securitate, împreună cu instrucțiunile de manipulare se constituie în sistemul de management al securității informațiilor (SMSI) al Parlamentului European menționat la articolul 3 alineatul (2) din prezenta decizie:

NOTIFICAREA DE SECURITATE 1

Organizarea măsurilor de securitate în cadrul Parlamentului European în vederea protejării informațiilor

NOTIFICAREA DE SECURITATE 2

Gestionarea informațiilor confidențiale

NOTIFICAREA DE SECURITATE 3

Procesarea informațiilor confidențiale prin sistemele informatice automate de comunicare (CIS)

NOTIFICAREA DE SECURITATE 4

Securitatea fizică

NOTIFICAREA DE SECURITATE 5

Securitatea industrială

NOTIFICAREA DE SECURITATE 6

Încălcări ale securității, pierderea sau compromiterea unor informații confidențiale

NOTIFICAREA DE SECURITATE 1

ORGANIZAREA MĂSURILOR DE SECURITATE ÎN CADRUL PARLAMENTULUI EUROPEAN ÎN VEDEREA PROTEJĂRII INFORMAȚIILOR

1. Secretarul General este responsabil de punerea în aplicare completă și coerentă a prezentei decizii.

Secretarul General ia toate măsurile necesare pentru a se asigura că, în ceea ce privește manipularea și stocarea informațiilor confidențiale, prezenta decizie este corect aplicată în incintele Parlamentului European de către deputații în Parlamentul European, funcționarii Parlamentului European, orice alt angajat al Parlamentului care lucrează pentru grupurile politice sau orice contractant.

2. Secretarul General acționează în calitate de autoritate de securitate (AS). În această calitate, Secretarul General este responsabil pentru:

2.1. coordonarea tuturor aspectelor de securitate în activitățile Parlamentului privind protecția informațiilor confidențiale;

2.2. aprobarea amenajării unei incinte securizate, a unei săli de lectură securizate și a echipamentelor securizate;

2.3. aplicarea deciziilor de autorizare, în temeiul articolului 6 din prezenta decizie, a transmiterii de informații clasificate de către Parlamentul European către terți;

2.4. investigarea sau solicitarea unei investigații, în cooperare cu Președintele Parlamentului European, privind orice scurgere de informații confidențiale, în condițiile existenței unor indicii prima facie că aceasta ar fi putut avea loc în Parlament și în cazul în care un deputat în Parlamentul European ar fi implicat;

2.5. menținerea unor legături strânse cu autoritățile în materie de securitate ale altor instituții ale Uniunii și cu autoritățile naționale de securitate din statele membre, în vederea asigurării unei coordonări optime a politicii de securitate în materie de informații clasificate;

2.6. monitorizarea permanentă a politicii de securitate a Parlamentului și a procedurilor aferente și emiterea de recomandări adecvate în consecință;

2.7. raportarea către autoritatea națională de securitate care a efectuat procedura de verificare de securitate, în conformitate cu Anexa I partea 2 punctul 11.3, în cazurile în care informații nefavorabile ar putea afecta interesele respectivei autorități;

3. în cazul în care este vizat un deputat în Parlamentul European, Secretarul General își îndeplinește atribuțiile în colaborare strânsă cu Președintele Parlamentului European;

4. în îndeplinirea atribuțiilor sale prevăzute la punctele 2 și 3 Secretarul General este asistat de către Secretarul general adjunct, de către Direcția pentru securitate și evaluarea riscului, de Direcția pentru tehnologia informației (DTI) și de Unitatea pentru informații clasificate (UIC).

4.1. Direcția pentru securitate și pentru evaluarea riscului este responsabilă cu măsurile de protecție personală și, îndeosebi, pentru procedura de acordare a autorizației de securitate, astfel cum se prevede în Anexa I partea 2. Direcția pentru securitate și evaluarea riscului:

(a) este punctul de contact pentru autoritățile de securitate ale celorlalte instituții ale Uniunii și pentru autoritățile naționale de securitate, în ceea ce privește procedurile de acordare a autorizației de securitate deputaților în Parlamentul European, funcționarilor Parlamentului European și altor angajați ai Parlamentului care lucrează pentru grupurile politice;

(b) efectuează instructajele de securitate necesare privind obligația de protejare a informațiilor clasificate și consecințele nerespectării acesteia;

(c) supraveghează funcționarea incintei securizate și a sălilor de lectură securizate din cadrul incintei Parlamentului, în cooperare, după caz, cu serviciile de securitate ale altor instituții ale Uniunii și ale autorităților naționale de securitate;

(d) auditează, în cooperare cu serviciile de securitate ale altor instituții ale Uniunii și ale autorităților naționale de securitate, procedurile de stocare și manipulare a informațiilor clasificate, funcționarea incintei securizate și a sălilor de lectură securizate din cadrul incintei Parlamentului în condițiile manipulării de informații clasificate;

(e) prezintă Secretarului General un set de instrucțiuni corespunzătoare de manipulare.

4.2. DTI este responsabilă pentru manipularea de informații confidențiale de către sistemele securizate de TI din cadrul Parlamentului European.

4.3. UIC este responsabilă de:

(a) identificarea măsurilor de securitate necesare pentru protecția efectivă a informațiilor confidențiale, în strânsă cooperare cu Direcția pentru securitate și pentru evaluarea riscului și DTI și cu serviciile de securitate ale altor instituții ale Uniunii;

(b) identificarea tuturor aspectelor ale manipulării și stocării informațiilor confidențiale în cadrul Parlamentului, așa cum se prevede în instrucțiunile de manipulare;

(c) funcționarea incintei securizate;

(d) manipularea sau consultarea informațiilor confidențiale în incinta securizată sau în sala de lectură securizată a UIC, în conformitate cu articolul 7 alineatele (2) și (3) din prezenta decizie;

(e) gestionarea registrului UIC;

(f) raportarea către AS a oricăror încălcări de securitate, pierderi sau compromiteri, dovedite sau bănuite, ale informațiilor confidențiale stocate de UIC și conservate în incinta securizată sau în sala de lectură securizată a UIC.

5. În plus, Secretarul General, în calitate de AS, numește următoarele autorități:

(a) o autoritate de acreditare în materie de securitate (AAS);

(b) o autoritate operațională de asigurare a informațiilor (AOAI);

(c) o autoritate de distribuire a materialului criptografic (ADMC);

(d) o autoritate TEMPEST (AT);

(e) o autoritate de asigurare a informațiilor (AAI).

Exercitarea acestor funcții nu necesită entități organizaționale distincte. Ele au mandate separate. Cu toate acestea, aceste funcții și responsabilitățile aferente pot fi grupate sau integrate în aceeași entitate organizațională sau distribuite în entități organizaționale diferite, cu condiția să fie evitate conflictele interne de interese și paralelismele de sarcini.

6. AAS asigură consilierea în toate aspectele de securitate privind acreditarea oricărui sistem sau rețea de tehnologia informației în cadrul Parlamentului European, prin:

6.1. asigurarea conformității SIC cu toate politicile și orientările de securitate relevante, stabilirea unei declarații de conformitate pentru manipularea de către SIC a informațiilor clasificate la un anumit nivel de clasificare, în mediul său operațional, stabilirea termenilor și a condițiilor acreditării, precum și a criteriilor pentru determinarea obligativității reaprobării;

6.2. stabilirea unui proces de acreditare în materie de securitate, în conformitate cu politicile relevante, precizând în mod clar condițiile de aprobare pentru SIC aflate sub autoritatea sa;

6.3. definirea unei strategii de acreditare de securitate, stabilind un grad de detaliere a procesului de acreditare proporțional cu nivelul de asigurare cerut;

6.4. examinarea și aprobarea documentației de securitate, inclusiv a declarațiilor privind gestiunea riscului și riscul rezidual, a documentației de verificare a aplicării măsurilor de securitate și a procedurilor operaționale de securitate și asigurarea conformității acestora cu normele și politicile de securitate ale Parlamentului;

6.5. verificarea punerii în aplicare a măsurilor de securitate în ceea ce privește SIC prin efectuarea sau finanțarea unor evaluări, inspecții și reexaminări în materie de securitate;

6.6. identificarea cerințelor de securitate (precum nivelul autorizațiilor pentru personal) pentru pozițiile sensibile în relație cu SIC;

6.7. aprobarea sau, după caz, participarea la aprobarea comună a interconectării unui SIC cu alte SIC;

6.8. aprobarea normelor de securitate ale echipamentului tehnic vizat pentru manipularea securizată și pentru protecția informațiilor clasificate;

6.9. verificarea că produsele criptografice utilizate în cadrul Parlamentului sunt incluse în lista produselor aprobate din UE; și

6.10. consultarea furnizorului de sistem, a actorilor din domeniul securității și a reprezentanților utilizatorilor cu privire la managementul riscului de securitate, în special a riscului rezidual, și cu privire la termenii și condițiile declarației de aprobare.

7. AOAI este responsabilă de:

7.1. elaborarea unei documentații de securitate, în conformitate cu politicile și orientările de securitate, în special referitor la declarația privind riscul rezidual, procedurile operaționale de securitate și a planului criptografic în cadrul procesului de acreditare a SIC;

7.2. participarea la selectarea și testarea măsurilor tehnice de securitate, ale dispozitivelor și programelor informatice specifice sistemului, pentru a supraveghea punerea lor în aplicare și pentru a asigura instalarea, configurarea și întreținerea lor securizată, în conformitate cu documentația de securitate relevantă;

7.3. monitorizarea punerii în aplicare și a aplicării procedurilor operaționale de securitate și, după caz, delegarea responsabilităților în materie de securitate operațională proprietarului sistemului, respectiv UIC;

7.4. gestionarea și manipularea produselor criptografice, asigurând custodia elementelor criptografice și a elementelor controlate și, după caz, asigurarea generării de variabile criptografice;

7.5. efectuarea unor reexaminări și teste pentru analiza de securitate, în special pentru a produce rapoartele relevante privind riscurile, astfel cum solicită AAS;

7.6. furnizarea de formare în materie de asigurare a informațiilor, specifică SIC;

7.7. punerea în aplicare și utilizarea unor măsuri de securitate specifice SIC.

8. ADMC este responsabilă de:

8.1. gestionarea și evidența materialului criptografic al UE;

8.2. garantarea, în strânsă cooperare cu AAS, a impunerii unor proceduri și a stabilirii unor planuri pentru evidența, manipularea securizată, stocarea securizată și distribuirea securizată a întregului material criptografic al UE; și

8.3. asigurarea transferului materialului criptografic al UE de la sau către persoanele sau serviciile care îl utilizează.

9. AT este responsabilă de asigurarea conformității SIC cu politicile și orientările TEMPEST și cu instrucțiunile de manipulare. Aceasta aprobă contramăsurile TEMPEST pentru instalațiile și produsele de protecție a informațiilor clasificate la un anumit nivel de clasificare, în mediul său operațional.

10. AAI este responsabilă de toate aspectele privind manipularea și stocarea informațiilor confidențiale în cadrul Parlamentului și, mai ales:

10.1 elaborarea de politici de securitate și orientări de securitate privind asigurarea informațiilor și monitorizarea eficacității și pertinenței acestora;

10.2. protejarea și manipularea informațiilor tehnice privind produsele criptografice;

10.3. asigurarea compatibilității dintre măsurile de asigurare a informației selectate pentru protejarea informațiilor clasificate și politicile relevante care reglementează eligibilitatea și selecția acestora;

10.4. asigurarea selectării produselor criptografice în conformitate cu politicile care reglementează eligibilitatea și selecția acestora;

10.5. consultarea furnizorului de sistem, a actorilor din domeniul securității și a reprezentanților utilizatorilor cu privire la securitatea asigurării informației;

NOTIFICAREA DE SECURITATE 2

GESTIONAREA INFORMAȚIILOR CONFIDENȚIALE

A. **INTRODUCERE**

1. Prezenta notificare de securitate conține dispozițiile în materie de gestionare, în cadrul Parlamentului, a informațiilor confidențiale.

2. La emiterea informațiilor confidențiale, emitentul evaluează nivelul de confidențialitate necesar și decide în baza principiilor prezentate în prezenta notificare de securitate, referitor la clasificarea sau marcarea respectivei informații.

B. **CLASIFICAREA IUEC**

3. Decizia de a clasifica un document se ia înainte de crearea acestuia. În acest scop, clasificarea informațiilor ca IUEC implică o evaluare prealabilă a nivelului lor de confidențialitate, precum și decizia emitentului că divulgarea neautorizată a acestor informații ar putea cauza prejudicii de diferite amplori intereselor Uniunii Europene sau ale unuia sau mai multor state membre sau persoane.

4. După luarea deciziei de a clasifica informațiile, urmează o a doua evaluare prealabilă, pentru a determina nivelul de clasificare corespunzător. Clasificarea unui document este determinată de nivelul de sensibilitate a conținutului său.

5. Responsabilitatea pentru clasificarea informațiilor aparține exclusiv emitentului. Funcționarii Parlamentului clasifică informațiile la instrucțiunile Secretarului General sau în virtutea competențelor delegate de acesta.

6. Clasificarea se utilizează corect și cu moderație. Emitentul unui document care urmează a fi clasificat evită supra- sau subclasificarea.

7. Nivelul de clasificare atribuit informațiilor determină nivelul de protecție al acestora în domeniul securității personalului, securității fizice, securității procedurale și asigurării informațiilor.

8. Informațiile care justifică clasificarea sunt marcate și tratate ca atare, indiferent de forma lor fizică. Clasificarea acestor informații se comunică în mod clar destinatarilor, fie printr-un marcaj al clasificării de securitate (în cazul în care informațiile sunt comunicate în formă scrisă, pe hârtie sau printr-un SIC), fie printr-un anunț (în cazul în care informațiile sunt comunicate în formă orală, de exemplu în cursul unei conversații sau într-o reuniune cu ușile închise). Materialele clasificate se marchează fizic, pentru a permite identificarea fără dificultate a clasificării lor de securitate.

9. IUEC în format electronic pot fi create numai într-un SIC acreditat. Informațiile clasificate ca atare, precum și numele fișierului și dispozitivul de stocare (dacă este extern, cum ar fi un CD-ROM sau o cheie USB) poartă marcajul corespunzător al clasificării de securitate.

10. Informațiile se clasifică imediat ce au fost create. De exemplu, notele personale, proiectele sau mesajele e-mail care conțin informații justificând clasificarea trebuie marcate ca IUEC de la început și sunt produse și tratate în conformitate cu prezenta decizie și cu instrucțiunile de manipulare fizică și tehnică conținute în aceasta. Aceste informații pot lua ulterior forma unui document oficial, care, la rândul său, este marcat și tratat corespunzător. În cursul procesului de redactare, poate fi necesară reevaluarea și reclasarea unui document oficial la un nivel de clasificare superior sau inferior, în funcție de evoluția respectivă.

11. Emitentul poate decide să atribuie un nivel standard de clasificare categoriilor de informații pe care le creează în mod regulat. Cu toate acestea, în acest caz, emitentul evită să supra- sau subclasifice sistematic fiecare informație în parte.

12. IUEC poartă întotdeauna marcajul clasificării de securitate corespunzător nivelului său de clasificare de securitate.

B.1. ***Nivelurile de clasificare***

13. IUEC se clasifică pe unul dintre următoarele niveluri:

— „TRÈS SECRET UE/EU TOP SECRET”, nivel definit la articolul 2 litera (d) din prezenta decizie, în cazul în care compromiterea lor ar putea:

(a) amenința în mod direct stabilitatea internă a Uniunii ori a unuia sau mai multor state membre, state terțe sau organizații internaționale;

(b) provoca prejudicii extrem de grave în relațiile cu state terțe sau organizații internaționale;

(c) conduce în mod direct la pierderea la scară largă de vieți omenești;

(d) prejudicia în mod excepțional de grav eficacitatea operațională sau securitatea personalului desfășurat al statelor membre sau al altor contributori, ori eficacitatea continuă a unor operațiuni de securitate sau ale serviciilor de informații extrem de importante; sau

(e) provoca daune grave pe termen lung economiei Uniunii sau a statelor membre;

— „SECRET UE/EU SECRET", nivel definit la articolul 2 litera (d) din prezenta decizie, în cazul în care compromiterea lor ar putea:

(a) crește în mod semnificativ tensiunile internaționale;

(b) prejudicia în mod grav relațiile cu state terțe și cu organizații internaționale;

(c) amenința direct viața sau afecta în mod grav ordinea publică sau securitatea ori libertatea individuală;

(d) aduce prejudicii unor negocieri comerciale sau politice majore, provocând probleme operaționale semnificative Uniunii sau statelor membre;

(e) prejudicia în mod grav securitatea operațională a statelor membre sau eficacitatea unor operațiuni de securitate ori ale serviciilor de informații extrem de importante;

(f) provoca daune materiale substanțiale intereselor financiare, monetare, economice și comerciale ale Uniunii sau ale statelor membre;

(g) submina substanțial viabilitatea financiară a unor organizații sau operatori majori; sau

(h) prezenta un obstacol grav pentru dezvoltarea sau funcționarea politicilor Uniunii cu consecințe economice, comerciale sau financiare majore;

— „CONFIDENTIEL UE/EU CONFIDENTIAL", nivel definit la articolul 2 litera (d) din prezenta decizie, în cazul în care compromiterea lor ar putea:

(a) prejudicia în mod semnificativ relațiile diplomatice, de exemplu în cazul în care ar conduce la un protest formal sau alte sancțiuni;

(b) genera un risc pentru securitatea sau libertatea individuală;

(c) pune grav în pericol rezultatele unor negocieri comerciale sau de politică; provoca probleme operaționale Uniunii sau unuia sau mai multor state membre;

(d) prejudicia securitatea operațională a unuia sau mai multor state membre sau eficacitatea unor operațiuni de securitate ori ale serviciilor de informații;

(e) submina substanțial viabilitatea financiară a unor organizații sau operatori majori;

(f) împiedica anchetarea unor infracțiuni sau activități teroriste sau facilita comiterea acestora;

(g) contraveni semnificativ intereselor financiare, monetare, economice și comerciale ale Uniunii sau ale statelor membre; sau

(h) prezenta un obstacol grav pentru dezvoltarea sau funcționarea politicilor Uniunii cu consecințe economice, comerciale sau financiare majore;

— „RESTREINT UE/EU RESTRICTED”, nivel definit la articolul 2 litera (d) din prezenta decizie, în cazul în care compromiterea lor ar putea:

(a) prezenta dezavantaje pentru interesele generale ale Uniunii;

(b) afecta negativ relațiile diplomatice;

(c) provoca inconveniente substanțiale unor persoane sau companii;

(d) prezenta dezavantaje pentru Uniune sau pentru statele membre în negocierile comerciale sau politice;

(e) crea impedimente pentru menținerea unei securități efective în Uniune sau în unul sau mai multe state membre;

(f) împiedica dezvoltarea efectivă sau funcționarea politicilor Uniunii;

(g) submina buna gestionare a Uniunii și a operațiunilor sale;

(h) încălca angajamentele luate de Parlament de a menține statutul clasificat al unor informații furnizate de către terți;

(i) încălca restricțiile statutare privind comunicarea informațiilor;

(j) provoca pierderi financiare sau oferi câștiguri sau avantaje necuvenite unor persoane sau companii; sau

(k) prejudicia investigarea unor infracțiuni sau facilita comiterea lor.

B.2. ***Clasificarea compilațiilor, copertelor și a extraselor***

14. Nivelul de clasificare al unei scrisori sau al unei note care conține documente însoțitoare este egal cu cel mai înalt nivel de clasificare atribuit unuia dintre documentele însoțitoare. Emitentul indică clar la ce nivel ar trebui clasificată scrisoarea sau nota după separarea de documentele însoțitoare. În cazul în care nota/scrisoarea însoțitoare nu necesită clasificare, aceasta menționează la final următoarele: „Dacă este detașată de documentele însoțitoare, această notă/scrisoare este neclasificată”.

15. Documentele sau dosarele care conțin componente cu niveluri de clasificare diferite se structurează, atunci când este posibil, astfel încât componentele cu un nivel de clasificare diferit să poată fi identificate și detașate fără dificultate, dacă este necesar. Nivelul de clasificare general al unui document sau al unui dosar este cel puțin echivalent cu cel al componentei sale având cel mai ridicat nivel de clasificare.

16 Paginile individuale, paragrafele, secțiunile, anexele, apendicele și documentele însoțitoare ale unui anumit document pot necesita clasificări la niveluri diferite și se clasifică în consecință. În interiorul documentelor conținând IUEC pot fi utilizate abrevieri standard, pentru a indica nivelul de clasificare al unor secțiuni sau porțiuni de text care nu depășesc o pagină.

17. La compilarea unor informații din surse diferite, produsul final este reexaminat pentru a se stabili nivelul global al clasificării de securitate, întrucât poate fi necesară o clasificare superioară celei atribuite părților componente.

C. **ALTE INFORMAȚII CONFIDENȚIALE**

18. „Alte informații confidențiale” se marchează în conformitate cu punctul E din prezenta notificare de securitate și instrucțiunile de manipulare.

D. **CREAREA INFORMAȚIILOR CONFIDENȚIALE**

19. Numai persoanele abilitate corespunzător prin prezenta decizie sau autorizate de către AS pot crea informații confidențiale.

20. Informațiile confidențiale nu se includ în sistemele de management al documentelor pe internet sau intranet.

D.1. ***Crearea IUEC***

21. Pentru a crea IUEC clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" sau „TRÈS SECRET UE/EU TOP SECRET", este necesar ca persoana să fie abilitată prin prezenta decizie sau să fie în posesia unei autorizații prealabile acordate în conformitate cu articolul 4 alineatul (1) din prezenta decizie.

22. IUEC clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" sau „TRÈS SECRET UE/EU TOP SECRET" se creează doar în zona securizată.

23. Crearea IUEC respectă următoarele reguli:

(a) fiecare pagină este marcată clar cu nivelul de clasificare aplicabil;

(b) fiecare pagină este numerotată și menționează numărul total de pagini;

(c) documentul poartă un număr de referință pe prima pagină, precum și o indicație a obiectului său, care să nu fie ca atare o informație clasificată, cu excepția cazului în care se menționează acest lucru;

(d) documentul poartă o dată pe prima pagină;

(e) prima pagină a tuturor documentelor clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" sau „TRÈS SECRET UE/EU TOP SECRET" conține o listă cu toate anexele și documentele însoțitoare;

(f) documentele clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" sau „TRÈS SECRET UE/EU TOP SECRET" comportă pe fiecare pagină numărul de exemplare, în cazul în care sunt distribuite în mai multe exemplare. De asemenea, pe prima pagină a fiecărui exemplar se menționează numărul total de exemplare și de pagini; și

(g) în cazul în care documentul face trimitere la alte documente care conțin informații clasificate primite de la alte instituții ale Uniunii sau conține informații clasificate derivate din aceste documente, acesta comportă același nivel de clasificare ca și documentele respective și nu poate fi distribuit fără acordul prealabil scris al emitentului său altor persoane în afara celor specificate în lista de distribuție cu privire la documentul sau documentele originale care conțin informații clasificate.

24. Emitentul păstrează controlul asupra IUEC pe care le-a creat. Acordul său prealabil este necesar înainte ca IUEC să fie:

(a) declasate sau declasificate;

(b) utilizate în alte scopuri decât cele stabilite de emitent;

(c) dezvăluite oricărui stat terț sau organizație internațională;

(d) dezvăluite oricărei persoane, instituții, țări sau organizații internaționale în afară de destinatarii autorizați inițial de către emitent să consulte informațiile în cauză;

(e) dezvăluite unui contractant sau unui potențial contractant situat într-un stat terț;

(f) copiate sau traduse, în cazul în care informațiile sunt clasificate la nivelul „TRES SECRET UE/EU TOP SECRET";

(g) distruse.

D.2. ***Crearea altor informații confidențiale***

25. Secretarul General, acționând în calitate de AS, poate decide dacă autorizează sau nu crearea de „alte informații confidențiale" de către o anumită funcție, serviciu și/sau persoană.

26. „Alte informații confidențiale" poartă unul dintre marcajele definite în instrucțiunile de manipulare.

27. La crearea „altor informații confidențiale" se aplică următoarele reguli:

(a) marcajul se indică în partea de sus a primei pagini a documentului;

(b) fiecare pagină este numerotată și menționează numărul total de pagini;

(c) documentul poartă un număr de referință pe prima pagină,precum și o indicație a obiectului său;

(d) documentul poartă o dată pe prima pagină; și

(e) ultima pagină a documentului conține o listă cu toate anexele și documentele însoțitoare.

28. Crearea de „alte informații confidențiale" face obiectul unor reguli și proceduri specifice prevăzute în instrucțiunile de manipulare.

E. **IDENTIFICATORI ȘI MARCAJE DE SECURITATE**

29. Identificatorii și marcajele de securitate de pe documente sunt destinate controlării fluxul de informații și restricționării accesului la informații confidențiale pe baza principiului „necesității de a cunoaște".

30. Când sunt folosiți sau aplicați identificatorii și/sau marcajele de securitate, se face tot posibilul pentru a evita confuzia cu clasificările de securitate pentru IUEC: „RESTREINT UE/EU RESTRICTED", „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET", „TRES SECRET UE/EU SECRET".

31. Normele specifice privind utilizarea identificatorilor și marcajelor de securitate, împreună cu lista marcajelor de securitate aprobate de Parlamentul European, se stabilesc în instrucțiunile de manipulare.

E.1. ***Identificatorii de securitate***

32. Identificatorii de securitate pot fi utilizați numai în combinație cu o clasificare de securitate și nu se aplică separat documentelor. Un identificator de securitate poate fi aplicat IUEC, pentru a:

(a) stabili limita de valabilitate a unei clasificări (pentru informații clasificate aceasta înseamnă declasarea sau declasificarea automată);

(b) limita distribuirea IUEC respective;

(c) stabili modalități speciale de manipulare, în plus față de cele corespunzătoare nivelului clasificării de securitate.

33. Controalele suplimentare aplicabile manipulării și păstrării documentelor care conțin IUEC impun tuturor celor implicați eforturi suplimentare. Pentru a minimiza munca necesară în acest sens, o bună practică este cea de a stabili, atunci când se creează un astfel de document, o limită temporală sau un eveniment în urma căruia clasificarea expiră automat și informațiile conținute în document sunt declasate sau declasificate.

34. Atunci când un document este legat de un anumit domeniu de lucru, iar distribuția sa trebuie limitată și/sau face obiectul unor modalități speciale de manipulare, poate fi adăugată clasificării sale o declarație în acest sens, pentru a ajuta la identificarea publicului țintă.

E.2. ***Marcajele***

35. Marcajele nu constituie o clasificare de securitate. Scopul acestora este de a servi doar la a furniza instrucțiuni concrete de manipulare a documentului și nu se folosesc pentru a descrie conținutul documentului.

36. Marcajele pot fi aplicate separat documentelor sau pot fi utilizate în combinație cu o clasificare de securitate.

37. Ca regulă generală, marcajele se aplică informațiilor cu caracter de secret profesional în conformitate cu articolul 339 din Tratatul FUE și cu articolul 17 din Statutul funcționarilor, sau celor care trebuie protejate din motive juridice de către Parlament, dar pentru care clasificarea nu este necesară sau este imposibilă.

E.3. ***Utilizarea marcajelor în SIC***

38. Regulile de utilizare a marcajelor sunt aplicabile și SIC acreditate.

39. AAS stabilește norme specifice pentru utilizarea marcajelor în SIC acreditate.

F. **PRIMIREA INFORMAȚIILOR**

40. În cadrul Parlamentului, numai UIC este abilitată să primească de la terți informații clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" sau „TRÈS SECRET UE/EU TOP SECRET" sau la un nivel echivalent.

41. În ceea ce privește informațiile clasificate la nivelul „RESTREINT UE/EU RESTRICTED" sau la un nivel echivalent ori „alte informații confidențiale", atât UIC, cât și organ/titularul de mandat parlamentar competent pot fi abilitați să primească acest tip de informații de la terți și să aplice principiile enunțate în notificarea de securitate.

G. **ÎNREGISTRAREA**

42. Înregistrarea constă în aplicarea procedurilor de înregistrare a ciclului de viață al informațiilor confidențiale, inclusiv a diseminării, consultării și distrugerii acestora.

43. În sensul acestei notificări de securitate, „registru de evidență" înseamnă un registru în care se consemnează în special datele și orele la care informațiile confidențiale:

(a) intră sau ies din secretariatul organului/titularului de mandat parlamentar în cauză sau, dacă este cazul, din UIC;

(b) sunt accesate de o persoană care deține un certificat de securitate; și

(c) sunt distruse.

44. Emitentul informațiilor clasificate este responsabil de marcarea declarației inițiale la crearea unui document care conține astfel de informații. Această declarație se comunică UIC în momentul în care este creat documentul.

45. Informațiile clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" sau „TRÈS SECRET UE/EU TOP SECRET" sau la un nivel echivalent, pot fi înregistrate de către UIC doar pentru motive de securitate. Informațiile clasificate la nivelul „RESTREINT UE/EU RESTRICTED" sau la un nivel echivalent și „alte informații confidențiale" primite de la terți se înregistrează de către serviciul responsabil pentru primirea oficială a documentului, care este fie UIC, fie secretariatul organului/titularului de mandat parlamentar, în scopuri administrative. „Alte informații confidențiale" produse în cadrul Parlamentului se înregistrează de către emitent în scopuri administrative.

46. Informațiile clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" sau „TRÈS SECRET UE/EU TOP SECRET" sau la un nivel echivalent se înregistrează cu precădere în momentul în care:

(a) sunt create;

(b) ajung sau pleacă de la UIC; și

(c) ajung sau pleacă de la UIC.

47. Informațiile clasificate la nivelul „RESTREINT UE/EU RESTRICTED" sau la un nivel echivalent sau superior se înregistrează cu precădere în momentul în care:

(a) sunt create;

(b) ajung sau pleacă de la secretariatul organului/titularului de mandat parlamentar în cauză sau UIC; și

(c) ajung sau pleacă de la UIC.

48. Înregistrarea informațiilor confidențiale poate fi efectuată în registre de evidență/SIC sub formă tipărită sau electronică.

49. Pentru informații clasificate la nivelul „RESTREINT UE/EU RESTRICTED" sau la un nivel echivalent și pentru „alte informații confidențiale" se înregistrează cel puțin următoarele:

(a) data și ora intrării sau ieșirii din secretariatul organului/titularului de mandat parlamentar în cauză sau UIC, după caz;

(b) titlul documentului, nivelul de clasificare sau marcajul, data expirării clasificării/marcajului și toate numerele de referință atribuite documentului.

50. Pentru informații clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" sau „TRÈS SECRET UE/EU TOP SECRET" sau la un nivel echivalent, se înregistrează cel puțin următoarele:

(a) data și ora intrării sau ieșirii din UIC;

(b) titlul documentului, nivelul de clasificare sau marcajul, toate numerele de referință atribuite documentului și data expirării clasificării/marcajului.

(c) detaliile emitentului;

(d) o listă care menționează identitatea oricărei persoane căreia îi este acordat accesul la document și datai la care persoana respectivă a accesat documentul;

(e) o înregistrare a tuturor copiilor sau traducerilor documentului;

(f) data și ora pentru toate intrările și ieșirile din UIC ale copiilor sau traducerilor documentului, precum și detalii privind locul în care au fost trimise și persoana care le-a returnat;

(g) data și ora la care documentul a fost distrus și de către cine, în conformitate cu normele de securitate ale Parlamentului privind distrugerea; și

(h) declasificarea sau declasarea documentului.

51. Registrul de evidență se clasifică sau se marchează corespunzător. Registrul de evidență al informațiilor clasificate la nivelul „TRES SECRET UE/EU TOP SECRET" sau la un nivel echivalent se înregistrează pe același nivel.

52. Informațiile clasificate se pot înregistra:

(a) într-un singur registru de evidență; sau

(b) în registre de evidență separate, în funcție de nivelul lor de clasificare, de categoria căreia aparțin (intrări sau ieșiri) și de originea sau destinația lor.

53. În cazul gestionării electronice în SIC, procedurile de înregistrare se pot desfășura prin mijloacele din cadrul SIC care se conformează unor cerințe echivalente celor specificate anterior. Ori de câte ori IUEC părăsesc perimetrul SIC, se aplică procedura de înregistrare descrisă mai sus.

54. UIC păstrează o evidență a tuturor informațiilor clasificate comunicate de Parlament terților și a informațiilor clasificate primite de Parlament de la terți.

55. După finalizarea înregistrării informațiilor clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL",„SECRET UE/EU SECRET" sau „TRÈS SECRET UE/EU TOP SECRET" sau la un nivel echivalent, UIC verifică dacă destinatarul dispune de un certificat de securitate în vigoare. Dacă acesta este cazul, UIC notifică destinatarul. Consultarea informațiilor clasificate poate avea loc doar după înregistrarea documentului care le conține.

H. **DISTRIBUIREA**

56. Emitentul întocmește o listă inițială de distribuție pentru IUEC pe care le-a creat.

57. Informațiile clasificate la nivelul „RESTREINT UE/EU RESTRICTED" și alte informații confidențiale produse de Parlament se distribuie în cadrul Parlamentului de către emitent, în conformitate cu instrucțiunile de manipulare relevante și pe baza principiului „necesității de a cunoaște". Pentru informațiile clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" sau „TRÈS SECRET UE/EU TOP SECRET" create de Parlament în zona securizată, se furnizează UIC lista de distribuție (și toate instrucțiunile referitoare la distribuție), UIC fiind responsabilă de gestionarea acesteia.

58. IUEC produse de Parlament pot fi distribuite terților numai de către UIC, pe baza principiului „necesității de a cunoaște".

59. Informațiile confidențiale primite de UIC sau de oricare organ/titular de mandat parlamentar care a depus o solicitare în acest sens se distribuie în conformitate cu instrucțiunile primite de la emitent.

I. **MANIPULAREA, PĂSTRAREA ȘI CONSULTAREA**

60. Manipularea, păstrarea și consultarea informațiilor confidențiale se efectuează în conformitate cu notificarea de securitate 4 și cu instrucțiunile de manipulare.

J. **COPIEREA/TRADUCEREA/INTERPRETAREA INFORMAȚIILOR CLASIFICATE**

61. Documentele care conțin informații clasificate la nivelul „TRES SECRET UE/EU TOP SECRET" sau la un nivel echivalent nu se copiază și nu se traduc fără acordul prealabil scris al emitentului. Documentele care conțin informații clasificate la nivelul „SECRET UE/EU SECRET" sau la un nivel echivalent ori la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL" sau la un nivel echivalent pot fi copiate sau traduse la cererea deținătorului, cu condiția ca emitentul să nu fi interzis acest lucru.

62. Fiecare exemplar al unui document conținând informații clasificate la nivelul „TRES SECRET UE/EU TOP SECRET", „SECRET UE/EU SECRET" sau „CONFIDENTIEL UE/EU CONFIDENTIAL" sau la un nivel echivalent se înregistrează din motive de securitate.

63. Măsurile de securitate aplicabile documentului original conținând informații clasificate se aplică și copiilor și traducerilor acestuia.

64. Documentele provenind de la Consiliu ar trebui să fie primite în toate limbile oficiale.

65. Copiile și/sau traducerile documentelor care conțin informații clasificate pot fi solicitate de către emitent sau de către deținătorul copiei. Copiile documentelor care conțin informații clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" sau „TRES SECRET UE/EU TOP SECRET" sau la un nivel echivalent, pot fi produse numai în zona securizată și pe copiatoare care fac parte dintr-un SIC acreditat. Copiile documentelor care conțin informații clasificate la nivelul „RESTREINT UE/EU RESTRICTED" sau la un nivel echivalent și „alte informații confidențiale" se realizează cu ajutorul unui dispozitiv de reproducere acreditat, în interiorul clădirilor Parlamentului.

66. Toate copiile și traducerile oricărui document care conține informații confidențiale sau ale unei părți a acestuia se marchează, se numerotează și se înregistrează în mod corespunzător.

67. Nu se fac mai multe copii decât cele strict necesare. La sfârșitul perioadei de consultare, toate copiile se distrug în conformitate cu instrucțiunile de manipulare.

68. Numai interpreții și traducătorii care sunt funcționari ai Parlamentului pot avea acces la informații clasificate.

69. Interpreții și traducătorii care au acces la documentele care conțin informații clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" sau „TRES SECRET UE/EU TOP SECRET"sau la un nivel echivalent dispun de un certificat de securitate adecvat.

70. Atunci când se lucrează pe documente care conțin informații clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" sau „TRES SECRET UE/EU TOP SECRET" sau la un nivel echivalent interpreții și traducătorii lucrează în zona securizată.

K. **DECLASAREA, DECLASIFICREA ȘI DEMARCAREA INFORMAȚIILOR CONFIDENȚIALE**

K.1. ***Principii generale***

71. Informațiile confidențiale se declasifică, declasează sau sunt demarcate atunci când protecția nu mai este necesară sau nu mai este necesară la nivelul inițial.

72. Se poate întâmpla și ca deciziile de a declasa, declasifica sau demarca informațiile conținute în documentele produse în cadrul Parlamentului să trebuiască luate ad-hoc, de exemplu ca răspuns la o cerere de acces din partea publicului sau din partea altei instituții a Uniunii ori la inițiativa UIC sau a unui organ/titular de mandat parlamentar.

73. În momentul creării IUEC, emitentul IUEC indică, atunci când este posibil, dacă IUEC în cauză pot fi declasate sau declasificate la o anumită dată sau în urma unui anumit eveniment. Atunci când nu este posibilă precizarea acestor informații, emitentul, UIC sau organul/titularul de mandat parlamentar care deține informațiile revizuiește nivelul de clasificare a IUEC cel puțin o dată la cinci ani. În orice caz, IUEC pot fi declasate sau declasificate doar cu acordul prealabil scris al emitentului.

74. În cazul în care emitentul IUEC nu poate fi identificat sau găsit în ceea ce privește documentele produse în cadrul Parlamentului, AS revizuiește nivelul de clasificare a IUEC respective pe baza unei propuneri din partea organului/titularului de mandat parlamentar care deține informațiile, acesta putând consulta UIC în această privință.

75. UIC sau organul/titularul de mandat parlamentar care deține informațiile respective este responsabil de notificarea destinatarilor cu privire la declasificarea sau declasarea informațiilor, iar destinatarii, la rândul lor, au responsabilitatea de a notifica orice destinatar ulterior căruia i-au trimis sau pentru care au copiat documentul.

76. Declasificarea, declasarea sau demarcarea informațiilor conținute într-un document se înregistrează.

K.2. ***Declasificarea***

77. IUEC pot fi declasificate integral sau parțial. IUEC pot fi declasificate parțial atunci când protejarea unei anumite părți a documentului care le conține nu mai este necesară, însă se justifică pentru restul documentului.

78. Atunci când în urma revizuirii IUEC conținute într-un document creat în cadrul Parlamentului se decide declasificarea acestora, se verifică dacă documentul poate fi făcut public sau dacă trebuie să poarte un marcaj de distribuție (de exemplu a nu fi făcut public).

79. Atunci când IUEC sunt declasificate, declasificarea se înregistrează în registrul de evidență împreună cu următoarele date: data declasificării, numele persoanelor care au solicitat și care au autorizat declasificarea, numărul de referință al documentului declasificat și destinația finală a acestuia.

80. Vechile marcaje de clasificare din documentul declasificat și din toate copiile acestuia se barează. Documentele și toate copiile acestora se păstrează în mod corespunzător.

81. La declasificarea parțială a informațiilor clasificate, partea care a fost declasificată se materializează sub forma unui extras și se depozitează în condiții adecvate. Serviciul competent înregistrează:

(a) data declasificării parțiale;

(b) numele persoanelor care au solicitat și care au autorizat declasificarea; și

(c) numărul de referință al extrasului declasificat.

K.3. ***Declasarea***

82. În urma declasării unor informații clasificate, documentul care conține informațiile respective se înregistrează în registrele de evidență corespunzătoare atât nivelului de clasificare anterior, cât și noului nivel. Se înregistrează data la care a fost făcută declasarea, precum și numele persoanei care a autorizat-o.

83. Documentul care conține informațiile declasate și toate exemplarele aferente se clasifică la un nou nivel de clasificare și se păstrează în mod corespunzător.

L. **DISTRUGEREA INFORMAȚIILOR CONFIDENȚIALE**

84. Informațiile confidențiale (atât pe hârtie, cât și în format electronic) care nu mai sunt necesare se distrug sau se șterg, în conformitate cu instrucțiunile de manipulare și normele relevante de arhivare.

85. Informațiile clasificate la nivelul „TRES SECRET UE/EU TOP SECRET" sau la un nivel echivalent ori la nivelul „SECRET UE/EU SECRET" sau la un nivel echivalent se distrug de către UIC. La distrugere asistă o persoană care deține un certificat de securitate corespunzător cel puțin nivelului de clasificare a informațiilor ce urmează a fi distruse.

86. Informațiile clasificate la nivelul „TRES SECRET UE/EU TOP SECRET" sau la un nivel echivalent se distrug numai cu acordul prealabil scris al emitentului.

87. Informațiile clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" sau „TRES SECRET UE/EU TOP SECRET" sau la un nivel echivalent se distrug și se elimină de către UIC pe baza instrucțiunilor emitentului sau ale unei autorități competente. Registrele de evidență și alte registre se actualizează în consecință. Informațiile clasificate la nivelul „RESTREINT UE/EU RESTRICTED" sau la un nivel echivalent se distrug și se elimină de către UIC sau de către organul/titularul de mandat parlamentar relevant.

88. Funcționarul responsabil de distrugere și martorul la distrugere semnează un certificat de distrugere, care se îndosariază și se arhivează în UIC. UIC păstrează, împreună cu formularele de distribuție, certificatele de distrugere a informațiilor clasificate la nivelul „TRES SECRET UE/EU TOP SECRET" sau la un nivel echivalent pentru o perioadă de cel puțin zece ani, iar informații clasificate la nivelul „SECRET UE/EU SECRET" sau la un nivel echivalent și la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL" sau la un nivel echivalent, pentru o perioadă de cel puțin cinci ani.

89. Documentele care conțin informații clasificate se distrug prin metode care îndeplinesc standardele Uniunii din domeniu sau standarde echivalente, astfel încât să se împiedice reconstruirea în întregime sau în parte a acestora.

90. Distrugerea mijloacelor informatice de stocare utilizate pentru informațiile clasificate se efectuează în conformitate cu instrucțiunile de manipulare relevante.

91. Distrugerea informațiilor clasificate se înregistrează în registrul de evidență pertinent, împreună cu următoarele date:

(a) data și ora distrugerii;

(b) numele funcționarului responsabil de distrugere;

(c) identificarea documentului sau copiilor distruse;

(d) originalul în forma fizică al IUEC distruse;

(e) modalitatea de distrugere; și

(f) locul distrugerii.

M. **ARHIVAREA**

92. Informațiile clasificate, inclusiv nota/scrisoarea însoțitoare, anexele, avizul de trimitere și alte părți ale dosarului, se transferă în arhiva securizată din zona securizată la șase luni după ce au fost consultate ultima oară și cel târziu la un an după ce au fost transmise. Normele detaliate de arhivare a informațiilor clasificate se stabilesc în instrucțiunile de manipulare.

93. Pentru „alte informații confidențiale", normele generale de gestionare a documentelor se aplică fără a aduce atingere dispozițiilor specifice privind manipularea.

NOTIFICAREA DE SECURITATE 3

PROCESAREA INFORMAȚIILOR CONFIDENȚIALE PRIN SISTEMELE INFORMATICE AUTOMATE DE COMUNICARE (SIC)

A. **ASIGURAREA INFORMAȚIILOR CLASIFICATE TRATATE ÎN SISTEMELE INFORMATICE**

1. Asigurarea informațiilor (AI) în domeniul sistemelor informatice reprezintă încrederea în faptul că aceste sisteme vor proteja informațiile clasificate pe care le tratează și vor funcționa în modul și în momentul dorit, sub controlul utilizatorilor legitimi. O AI eficientă asigură grade adecvate de confidențialitate, integritate, disponibilitate, irefutabilitate și autenticitate. AI se bazează pe un proces de gestionare a riscurilor.

2. „Sistem informatic de comunicare" (SIC) pentru tratarea informațiilor clasificate înseamnă un sistem care permite tratarea informațiilor în format electronic. Acest sistem informatic cuprinde toate activele necesare pentru a funcționa, inclusiv infrastructură, organizare, personal și resurse informatice.

3. SIC tratează informațiile clasificate în conformitate cu conceptul de AI.

4. SIC sunt supuse unui proces de acreditare. Acreditarea urmărește să garanteze faptul că au fost puse în aplicare toate măsurile de securitate corespunzătoare și că s-a obținut un nivel suficient de protecție a informațiilor clasificate și a SIC, în conformitate cu prezenta notificare de securitate. Declarația de acreditare stabilește nivelul maxim de clasificare a informațiilor care pot fi gestionate de SIC, precum și termenii și condițiile aferente.

5. Următoarele proprietăți și concepte referitoare la AI sunt esențiale pentru securitatea și funcționarea corectă a operațiilor derulate în SIC:

(a) autenticitatea: garanția faptului că informațiile sunt originale și provin de la surse de bună credință;

(b) disponibilitatea: calitatea de a fi accesibile și utilizabile la cerere de către o entitate autorizată;

(c) confidențialitatea: proprietatea de a nu divulga informații persoanelor, entităților sau proceselor neautorizate;

(d) integritatea: proprietatea de a proteja acuratețea și caracterul complet al informațiilor și al activelor;

(e) irefutabilitatea: capacitatea de a dovedi că o acțiune sau eveniment a avut loc, astfel încât evenimentul sau acțiunea respectivă să nu poată fi negată ulterior.

B. **PRINCIPIILE DE ASIGURARE A INFORMAȚIILOR**

6. Dispozițiile enunțate în continuare formează baza pentru securitatea oricăror SIC care tratează informații clasificate. Cerințele detaliate pentru punerea în aplicare a acestor dispoziții sunt definite în politicile de securitate privind AI și în liniile directoare de securitate.

B.1. ***Gestionarea riscurilor de securitate***

7. Gestionarea riscurilor de securitate reprezintă o componentă esențială a definirii, dezvoltării, utilizării și întreținerii SIC. Gestionarea riscurilor (evaluarea, tratarea, acceptarea și comunicarea) se desfășoară sub forma unui demers iterativ, condus de reprezentanți ai proprietarilor de sisteme, autorităților de proiect, autorităților operaționale și autorităților de aprobare în materie de securitate, conform notificării de securitate 1, prin intermediul unui proces de evaluare a riscurilor confirmat, transparent și ușor de înțeles. Domeniul SIC și al activelor sale este definit clar în momentul inițierii procesului de gestionare a riscurilor.

8. Autoritățile competente, conform notificării de securitate 1, reexaminează potențialele amenințări la adresa SIC și efectuează evaluări precise și actualizate ale amenințărilor, care reflectă mediul operațional curent. Acestea își actualizează permanent cunoștințele privind problemele de vulnerabilitate și reexaminează periodic evaluarea vulnerabilității, pentru a ține pasul cu schimbările din domeniul tehnologiei informației (IT).

9. Rolul tratării riscurilor de securitate este de a aplica un set de măsuri de securitate care să ducă la un echilibru satisfăcător între cerințele utilizatorului, cost și riscul rezidual de securitate.

10. Acreditarea unui SIC include o declarație formală privind riscul rezidual și acceptarea riscului rezidual de către o autoritate responsabilă. Cerințele specifice, scara și gradul de detaliere stabilite de AAS competentă pentru acreditarea unui SIC este proporțională cu riscul evaluat, ținând seama de toți factorii relevanți, inclusiv nivelul de clasificare a informațiilor clasificate tratate în cadrul SIC.

B.2. ***Securitatea pe parcursul ciclului de viață al SIC***

11. Asigurarea securității constituie o obligație pe tot parcursul ciclului de viață al SIC, de la inițiere la retragerea din exploatare.

12. Se identifică rolul și interacțiunea fiecărui actor implicat într-un SIC, din punctul de vedere al securității, pentru fiecare fază a ciclului de viață.

13. SIC, inclusiv măsurile sale de securitate tehnice și netehnice, fac obiectul unor teste de securitate în cursul procesului de acreditare, în vederea obținerii unui nivel de asigurare corespunzător și a verificării corectitudinii aplicării, integrării și configurării SIC, inclusiv a măsurilor sale de securitate tehnice și netehnice,.

14. Evaluările, inspecțiile și reexaminările de securitate se efectuează periodic, în cursul operării și al întreținerii SIC, precum și în împrejurări excepționale.

15. Documentația privind securitatea SIC evoluează pe parcursul ciclului de viață al acestuia, ca parte integrantă a procesului de gestionare a modificărilor.

16. Procedurile de înregistrare efectuate de SIC sunt, după caz, verificate ca parte a procesului de acreditare.

B.3. ***Cele mai bune practici***

17. AAI dezvoltă cele mai bune practici pentru protecția informațiilor clasificate tratate prin SIC. Liniile directoare de bune practici descriu măsuri de securitate de ordin tehnic, fizic, organizatoric și procedural pentru SIC a căror eficacitate în contracararea anumitor amenințări și vulnerabilități a fost dovedită.

18. Protecția informațiilor clasificate tratate într-un SIC ia în considerare concluziile experiențelor entităților implicate în AI.

19. Diseminarea și punerea în aplicare ulterioară a celor mai bune practici contribuie la atingerea unui nivel de asigurare echivalent pentru diversele SIC operate de secretariatul Parlamentului care tratează informații clasificate.

B.4. ***Apărarea în profunzime***

20. În scopul atenuării riscului pentru SIC, sunt puse în aplicare o serie de măsuri de securitate tehnice și netehnice, organizate pe niveluri de apărare multiple. Aceste niveluri includ:

(a) Descurajarea: măsuri de securitate menite să descurajeze orice adversar care plănuiește să atace SIC;

(b) Prevenirea: măsuri de securitate menite să împiedice sau să blocheze un atac asupra SIC;

(c) Detectarea: măsuri de securitate menite să descopere comiterea unui atac asupra SIC;

(d) Rezistența: măsuri de securitate menite să limiteze impactul unui atac la un set minim de informații sau active SIC și să împiedice daunele ulterioare; și

(e) Recuperarea: măsuri de securitate menite să reinstaureze o situație securizată a SIC.

Gradul de strictețe a acestor măsuri de securitate se determină în urma unei evaluări a riscurilor.

21. Autoritățile competente, în conformitate cu Notificarea de securitate 1, se asigură că au capacitatea de a reacționa la incidente care pot depăși limitele organizațiilor, în scopul coordonării reacțiilor și al partajării informațiilor cu privire la astfel de incidente și la riscurile conexe (capacități informatizate de reacție în situații de urgență).

B.5. ***Principiul privilegiului minimalist și minim***

22. În vederea evitării riscurilor nenecesare, sunt puse în aplicare numai funcțiile, dispozitivele și serviciile esențiale pentru îndeplinirea cerințelor operaționale.

23. Utilizatorii și procesele automate ale SIC beneficiază numai de accesul, privilegiile sau autorizațiile necesare pentru îndeplinirea atribuțiilor lor, pentru a limita orice daune rezultate în urma accidentelor, erorilor sau utilizării neautorizate a resurselor SIC.

B.6. ***Conștientizarea elementelor de asigurare a informațiilor***

24. Conștientizarea riscurilor și a măsurilor de securitate disponibile constituie prima linie de apărare pentru securitatea SIC. În special, toți membrii personalului implicați în ciclul de viață al SIC, inclusiv utilizatorii, trebuie să înțeleagă că:

(a) breșele de securitate pot afecta semnificativ SIC care manipulează informații clasificate;

(b) daunele potențiale aduse altora, care pot fi determinate de interconectivitate și interdependență; și

(c) responsabilitatea și răspunderea individuală pentru securitatea SIC, în funcție de rolul deținut în cadrul sistemelor și proceselor.

25. Pentru a asigura înțelegerea responsabilităților de securitate, instruirea cu privire la AI și formarea cu rol de conștientizare sunt obligatorii pentru tot personalul implicat, inclusiv pentru cadrele superioare de conducere, deputații în Parlamentul European și utilizatorii SIC.

B.7. ***Evaluarea și aprobarea produselor de securitate IT***

26. SIC care manipulează informații clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" sau „TRÈS SECRET UE/EU TOP SECRET" sau la nivel echivalent sunt protejate astfel încât informațiile să nu poată fi compromise prin emisii electromagnetice accidentale („măsuri de securitate TEMPEST").

27. Atunci când protecția informațiilor clasificate este asigurată prin produse criptografice, produsele respective sunt certificate de AAS ca făcând parte din produsele criptografice aprobate de UE.

28. Pentru transmiterea de informații clasificate prin mijloace electronice se utilizează produse criptografice aprobate de UE. Fără a aduce atingere acestei cerințe, pot fi aplicate proceduri specifice sau configurații tehnice specifice în situații de urgență, în conformitate cu punctele 41-44.

29. Gradul necesar de încredere în măsurile de securitate, definit ca nivel de asigurare, este determinat în urma rezultatului procesului de gestionare a riscurilor și în conformitate cu politicile și orientările de securitate relevante.

30. Nivelul de asigurare se verifică prin utilizarea unor procese și metodologii recunoscute la nivel internațional sau aprobate la nivel național. Printre acestea se numără în special evaluarea, controalele și auditul.

31. AAS aprobă orientări de securitate privind calificarea și aprobarea produselor de securitate IT necriptografice.

B.8. ***Transmiterea în interiorul zonei securizate***

32. Atunci când informațiile clasificate sunt transmise în limitele zonei securizate, se poate recurge la distribuirea necriptată sau la o criptare la un nivel mai redus, în funcție de rezultatul procesului de gestionare a riscurilor și sub rezerva aprobării de către AAS.

B.9. ***Interconectarea securizată a SIC***

33. Interconectarea înseamnă conectarea directă a două sau mai multe sisteme IT cu scopul de a partaja date și alte resurse informaționale unidirecțional sau multidirecțional.

34. Un SIC tratează orice sistem IT interconectat drept sursă nefiabilă și aplică măsuri de protecție pentru a controla schimbul de informații clasificate cu orice alt SIC.

35. Pentru toate interconectările unui SIC cu un alt sistem IT sunt respectate următoarele cerințe de bază:

(a) cerințele economice sau operaționale pentru astfel de interconectări sunt stabilite și aprobate de autoritățile competente;

(b) interconectarea respectivă este supusă unui proces de gestionare a riscului și de acreditare și necesită aprobarea AAS competente;

(c) sunt puse în aplicare servicii de protecție (SP) la limitele SIC.

36. Nu se realizează interconectări între un SIC acreditat și o rețea neprotejată sau publică, cu excepția cazurilor în care SIC a aprobat SP instalate în acest scop între SIC și rețeaua neprotejată sau publică. Măsurile de securitate pentru astfel de interconectări sunt reexaminate de AAI competentă și sunt aprobate de AAS competentă.

37. Dacă rețeaua neprotejată sau publică este utilizată numai ca transportator, iar datele sunt criptate prin intermediul unui produs criptografic aprobat de UE în conformitate cu punctul 27, o astfel de conexiune nu este considerată ca fiind o interconectare.

38. Interconectarea directă sau în cascadă la o rețea neprotejată sau publică a unui SIC acreditat să gestioneze informații clasificate la nivelul „TRES SECRET UE/EU TOP SECRET" sau la un nivel echivalent la nivelul „SECRET UE/EU SECRET" sau la un nivel echivalent este interzisă.

B.10. ***Suporturile informatice de stocare***

39. Suporturile informatice de stocare sunt distruse în conformitate cu procedurile aprobate de autoritatea de securitate competentă.

40. Suporturile informatice de stocare se reutilizează, se înscriu într-un nivel de clasificare inferior sau se declasifică în conformitate cu instrucțiunile de manipulare.

B.11. ***Situații de urgență***

41. Procedurile specifice descrise mai jos pot fi utilizate în situații de urgență, cum ar fi, de exemplu, în caz de criză, conflict sau război, iminente sau în curs, ori în situații operaționale excepționale.

42. Informațiile clasificate pot fi transmise, cu acordul autorității competente, folosind produse criptografice aprobate pentru un nivel de clasificare inferior sau fără a fi criptate, în cazul în care o întârziere ar cauza un prejudiciu mult mai grav decât orice prejudiciu rezultat în urma divulgării materialului clasificat și dacă:

(a) expeditorul și destinatarul nu posedă capacitatea de criptare necesară sau nu dispun de nicio capacitate de criptare; și

(b) materialul clasificat nu poate fi transmis la timp prin alte mijloace.

43. Informațiile clasificate transmise în condițiile enunțate la punctul 41 nu poartă niciun marcaj sau indicație care să le distingă de orice informații neclasificate sau care pot fi protejate cu ajutorul unui produs de criptare disponibil. Destinatarilor le este notificat fără întârziere nivelul de clasificare, prin alte mijloace.

44. Dacă se recurge la punctele 41 și 42, această situație face obiectul unui raport adresat autorității competente.

NOTIFICAREA DE SECURITATE 4

SECURITATEA FIZICĂ

A. **INTRODUCERE**

Această notificare de securitate stabilește principiile de securitate pentru crearea unui mediu sigur în care să aibă loc procesarea corectă a informațiilor confidențiale în cadrul Parlamentului European. Aceste principii, inclusiv cele referitoare la securitatea tehnică, sunt completate de instrucțiuni de manipulare.

B. **GESTIONAREA RISCURILOR DE SECURITATE**

1. Riscurile la care sunt supuse informațiile clasificate sunt gestionate ca proces. Acest proces are drept scop determinarea riscurilor de securitate cunoscute, definirea măsurilor de reducere a acestor riscuri la un nivel acceptabil, conform principiilor fundamentale și a standardelor minime stabilite în prezenta notificare de securitate, și aplicarea acestor măsurilor în conformitate cu conceptul de apărare în profunzime definit în notificarea de securitate 3. Eficacitatea acestor măsuri este evaluată în permanență.

2. Măsurile de securitate pentru protejarea informațiilor clasificate pe toată durata ciclului de viață al acestora sunt proporționale în special cu clasificarea lor de securitate, forma și volumul informațiilor sau al materialelor, amplasarea și construcția obiectivelor care adăpostesc informațiile clasificate și evaluarea locală a amenințării reprezentate de activități rău-intenționate și/sau criminale, inclusiv spionaj, sabotaj și terorism.

3. Planurile de urgență iau în considerare necesitatea protejării informațiilor clasificate în situații de urgență, pentru a împiedica accesul neautorizat, divulgarea sau pierderea integrității sau a disponibilității.

4. Măsurile de prevenire și de recuperare destinate minimizării impactului erorilor sau incidentelor majore survenite în manipularea sau păstrarea informațiilor clasificate sunt incluse în planurile de continuare a activității.

C. **PRINCIPII GENERALE**

5. Nivelul de clasificare sau marcaj atribuit unor informații determină nivelul de protecție care li se asigură în domeniul securității fizice.

6. Informațiile care trebuie clasificate sunt marcate și tratate ca atare, indiferent de forma lor. Clasificarea lor este comunicată în mod clar destinatarilor, fie printr-un marcaj al clasificării (dacă informațiile sunt transmise în formă scrisă, indiferent dacă pe hârtie sau printr-un SIC), fie printr-un anunț (dacă informațiile sunt transmise oral, de exemplu, în cadrul unei conversații sau al unei prezentări). Materialele clasificate sunt marcate fizic, pentru a permite identificarea fără dificultate a clasificării lor de securitate.

7. Informațiile confidențiale nu trebuie, în niciun caz, să fie lecturate în locuri publice, unde ar putea fi de văzute către persoane pentru care cunoașterea lor nu este necesară, de exemplu în trenuri, avioane, cafenele, baruri etc. Acestea nu trebuie lăsate în camere sau seifuri de hotel, nici nu trebuie să rămână nesupravegheate în locuri publice.

D. **COMPETENȚE**

8. UIC este responsabilă pentru asigurarea securității fizice în cadrul gestionării informațiilor confidențiale depozitate în instalațiile sale securizate. UIC este, de asemenea, responsabilă pentru gestionarea instalațiilor sale securizate.

9. Responsabilitatea pentru securitatea fizică în cadrul gestionării informațiilor clasificate la nivelul „RESTREINT UE/EU RESTRICTED" sau la un nivel echivalent sau a „altor informații confidențiale" revine organului parlamentar/titularului de mandat în cauză.

10. Direcția pentru securitate și evaluarea riscurilor asigură securitatea personală și autorizarea de securitate necesară pentru a garanta manipularea în siguranță a informațiilor confidențiale în Parlamentul European.

11. DIT oferă consultanță și se asigură că orice UIC creată și funcțională respectă întru totul notificarea de securitate 3 și instrucțiunile de manipulare aplicabile.

E. **INSTALAȚII SECURIZATE**

12. Pot fi create instalații securizate specifice conform standardelor tehnice de securitate și în conformitate cu nivelul atribuit informațiilor confidențiale în conformitate cu articolul 7.

13. Instalațiile securizate sunt certificate de AAS și validate de AS.

F. **CONSULTAREA INFORMAȚIILOR CONFIDENȚIALE**

14. Atunci când informații clasificate la nivelul „RESTREINT UE/EU RESTRICTED" sau la un nivel echivalent ori „alte informații confidențiale" sunt depozitate în cadrul UIC și trebuie să fie consultate în afara zonei securizate, UIC transmite o copie serviciului autorizat în cauză, care se asigură că informațiile respective sunt manipulate și consultate cu respectarea articolului 8 alineatul (2) și a articolului 10 din prezenta decizie, precum și a instrucțiunilor de manipulare aplicabile.

15. Atunci când informații clasificate la nivelul „RESTREINT UE/EU RESTRICTED" sau la un nivel echivalent ori „alte informații confidențiale" sunt depozitate la un organ parlamentar/titularul unui mandat, altul decât UIC, secretariatul respectivului organ parlamentar/titular de mandat se asigură că informațiile respective sunt manipulate și consultate cu respectarea articolului 7 alineatul (3), a articolului 8 alineatele (1), (2) și (4), a articolului 9 alineatele (3), (4) și (5), a articolului 10 alineatele (2)-(6) și a articolului 11 din prezenta decizie, precum și a instrucțiunilor de manipulare aplicabile.

16. Atunci când este necesară consultarea în zona securizată a unor informații clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" sau „TRÈS SECRET UE/EU TOP SECRET" sau la un nivel echivalent, UIC se asigură că informațiile respective sunt manipulate și consultate cu respectarea articolelor 9 și 10 din prezenta decizie, precum și a instrucțiunilor de manipulare aplicabile.

G. **SECURITATEA TEHNICĂ**

17. Responsabilitatea pentru măsurile de securitate tehnică revine AAS, care stabilește în cadrul diverselor instrucțiuni de manipulare măsurile de securitate tehnice specifice care trebuie aplicate.

18. Sălile de lectură securizate pentru consultarea informațiilor clasificate la nivelul „RESTREINT UE/EU RESTRICTED" sau la un nivel echivalent sau a „altor informații confidențiale" respectă măsurile specifice de securitate tehnică, conform instrucțiunilor de manipulare.

19. Zona securizată cuprinde următoarele:

(a) o sală de verificare a accesului de securitate (VAS), instalată conform măsurilor de securitate tehnică prevăzute în instrucțiunile de manipulare. Accesul la această sală se înregistrează. VAS respectă standarde ridicate în ceea ce privește identificarea persoanelor care au acces și dispune de înregistrare video, un spațiu securizat pentru depozitarea bunurilor personale care nu pot fi introduse în sala securizată (telefoane, instrumente de scris etc.);

(b) o sală de comunicare pentru transmiterea și recepționarea informațiilor clasificate, inclusiv a informațiilor clasificate criptate, conform notificării de securitate 3 și instrucțiunilor de manipulare aplicabile;

(c) o arhivă securizată, în care containerele aprobate și certificate sunt utilizate separat pentru informațiile clasificate la nivelul „RESTREINT UE/EU RESTRICTED", „CONFIDENTIEL UE/EU CONFIDENTIAL" și „SECRET EU/EU SECRET" sau la un nivel echivalent. Informațiile clasificate la nivelul „TRES SECRETUE/EU TOP SECRET" sau la un nivel echivalent se păstrează într-o sală separată, într-un container certificat specific. Singurul element suplimentar disponibil în această sală este un birou de asistență pentru gestionarea arhivei de către UIC;

(d) o sală de înregistrare, în care sunt puse la dispoziție instrumentele necesare pentru a permite înregistrarea pe hârtie sau electronică și care este echipată cu echipamentele securizate necesare pentru instalarea SIC adecvat. Doar sala de înregistrare poate conține dispozitive acreditate și aprobate de reproducere (copii pe hârtie sau în format electronic). Instrucțiunile de manipulare precizează care sunt dispozitivele de reproducere aprobate și acreditate. În sala de înregistrare este suficient spațiu pentru păstrarea și manipularea materialelor acreditate astfel încât să se permită marcarea, copierea și transmiterea informațiilor clasificate sub formă fizică, în funcție de nivelul de clasificare. Toate materialele acreditate sunt definite de UIC și sunt acreditate de AAS, în conformitate cu opinia AOAI. Sala de înregistrare este echipată, de asemenea, cu un dispozitiv acreditat de distrugere aprobat pentru cel mai ridicat nivel de clasificare, conform instrucțiunilor de manipulare. Traducerea informațiilor clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL EU", „SECRET UE/EU SECRET" sau „TRÈS SECRET UE/EU TOP SECRET" sau la un nivel echivalent se face în sala de înregistrare, într-un sistem adecvat și acreditat. Sala de înregistrare este echipată cu posturi de lucru la care pot lucra maximum doi traducători simultan asupra aceluiași document. Trebuie să fie prezent un membru al personalului UIC.

(e) o sală de lectură, pentru consultarea individuală a informațiilor clasificate de către persoanele autorizate. Sala de lectură dispune de spațiu suficient pentru două persoane, inclusiv un membru al personalului UIC, care este prezent permanent în cursul oricărei consultări. Nivelul de securitate al acestei săli este prevăzut pentru consultarea informațiilor clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET UE/EU SECRET" sau „TRÈS SECRET UE/EU TOP SECRET" sau la un nivel echivalent. Sala de lectură poate fi echipată cu echipamente TEMPEST pentru a permite consultarea electronică, dacă este cazul, în funcție de nivelul de clasificare a informațiilor în cauză.

(f) o sală de ședințe dispunând de un spațiu suficient pentru până la 25 de persoane, pentru discutarea informațiilor clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL", „SECRET EU/EU SECRET" sau la un nivel echivalent. Sala de ședințe este echipată cu instalațiile securizate tehnic și certificate necesare pentru interpretarea în două limbi. Atunci când nu este utilizată pentru ședințe, sala poate fi utilizată, de asemenea, ca sală suplimentară de lectură pentru consultare individuală. În cazuri excepționale, UIC poate permite mai multor persoane autorizate să consulte informații clasificate, cu condiția ca nivelul de autorizare și necesitatea de a cunoaște sunt identice pentru toate persoanele din sală. Cel mult patru persoane pot fi autorizate să consulte informații clasificate în același timp. Sunt prezenți mai mulți membri ai personalului UIC;

(g) localuri tehnice securizate pentru păstrarea tuturor echipamentelor tehnice, legate de securitatea întregii zone securizate, și a serverelor IT securizate.

20. Zona securizată respectă standardele internaționale de securitate aplicabile și este certificată de Direcția pentru securitate și evaluarea riscurilor. Zona securizată îndeplinește următoarele cerințe tehnice minime de securitate:

(a) sisteme de alarmă și de monitorizare a securității;

(b) echipamente de siguranță și sisteme de urgență (sistem de avertizare dublu);

(c) sistem CCTV;

(d) sistem de detectare a intruziunilor;

(e) controlul accesului (inclusiv sistem biometric de securitate);

(f) containere;

(g) dulapuri închise;

(h) protecție antielectromagnetică.

21. Atunci când sunt necesare măsuri tehnice suplimentare de securitate, acestea pot fi adăugate de AAS, acționând în strânsă cooperare cu UIC și după aprobarea AS.

22. Echipamentele de infrastructură pot fi conectate la sistemele generale de gestionare a clădirii în care se află zona securizată. Cu toate acestea, echipamentele de securitate pentru controlul a accesului și SIC sunt independente de orice alte astfel de sisteme existente în Parlamentul European.

H. **INSPECȚIILE ÎN ZONA SECURIZATĂ**

23. Zona securizată este inspectată periodic de către AAS și la cererea UIC.

24. AAS întocmește și actualizează o listă de verificare pentru inspecțiile de securitate, cuprinzând elementele care trebuie verificate în cursul unei inspecții, în conformitate cu instrucțiunile de manipulare.

I. **TRANSPORTUL INFORMAȚIILOR CONFIDENȚIALE**

25. În cursul transportului, informațiile confidențiale sunt ascunse vederii, și nu se indică natura confidențială a conținutului, în conformitate cu instrucțiunile de manipulare.

26. Doar mesagerii și membrii personalului care au nivelul adecvat de autorizare de securitate pot transporta informații clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL”, „SECRET UE/EU SECRET” sau „TRÈS SECRET UE/EU TOP SECRET” sau la un nivel echivalent.

27. Informațiile confidențiale pot fi expediate numai prin intermediul serviciilor externe de poștă sau curierat în afara clădirii doar în condițiile prevăzute în instrucțiunile de manipulare.

28. Informațiile clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL”, „SECRET UE/EU SECRET” sau „TRÈS SECRET UE/EU TOP SECRET” sau la un nivel echivalent nu se transmit niciodată prin e-mail sau fax, chiar dacă este instalat un sistem de e-mail securizat sau un fax criptat. Informațiile clasificate la nivelul „RESTREINT UE/EU RESTRICTED” sau la un nivel echivalent și „alte informații confidențiale” pot fi trimise prin e-mail, utilizând un sistem de criptare acreditat.

J. **PĂSTRAREA INFORMAȚIILOR CONFIDENȚIALE**

29. Nivelul de clasificare sau de marcaj atribuit informațiilor confidențiale determină nivelul de protecție asigurat în vederea păstrării lor. Informațiile respective se păstrează în echipamente certificate în acest sens în conformitate cu instrucțiunile de manipulare.

30. Informațiile clasificate la nivelul „RESTREINT UE/EU RESTRICTED” sau la un nivel echivalent și „alte informații confidențiale”:

(a) sunt păstrate într-un dulap standard, din oțel, încuiat, într-un birou sau într-o zonă de lucru, atunci când nu se lucrează efectiv cu ele;

(b) nu sunt lăsate nesupravegheate, cu excepția cazului în care sunt încuiate și păstrate corespunzător;

(c) nu sunt lăsate pe birou, pe masă etc. astfel încât să poate fi citite sau luate de vreo persoană neautorizată, de exemplu vizitatori, personal de curățenie și întreținere etc.;

(d) nu sunt arătate unor persoane neautorizate sau discutate cu astfel de persoane.

31. Informațiile clasificate la nivelul „RESTREINT UE/EU RESTRICTED” sau la un nivel echivalent și „alte informații confidențiale” sunt păstrate doar în cadrul secretariatelor organelor parlamentare sau ale titularilor de mandate sau în UIC, în conformitate cu instrucțiunile de manipulare.

32. Informațiile clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL”, „SECRET UE/EU SECRET” sau „TRÈS SECRET UE/EU TOP SECRET” sau la un nivel echivalent:

(a) se stochează în zona securizată, într-un container de securitate sau o cameră tezaur. În mod excepțional, de exemplu dacă UIC este închisă, informațiile pot fi păstrate într-un seif aprobat și certificat din cadrul serviciilor de securitate;

(b) nu sunt niciodată lăsate nesupravegheate în zona securizată, fără a fi fost încuiate într-un seif aprobat (chiar și pentru o absență de foarte scurtă durată);

(c) nu sunt lăsate pe birou, pe masă etc. astfel încât să poate fi citite sau luate de vreo persoană neautorizată, chiar dacă membrul responsabil din cadrul personalului UIC rămâne în sală.

Atunci când în sala securizată se elaborează un document în format electronic care conține informații clasificate, computerul este blocat, iar accesul la ecran este împiedicat, dacă emitentul sau membrul responsabil din cadrul personalului UIC părăsește sala (chiar și pentru o absență de foarte scurtă durată). Un sistem automatizat de închidere care se declanșează după câteva minute nu este considerat o măsură suficientă.

NOTIFICAREA DE SECURITATE 5

SECURITATEA INDUSTRIALĂ

A. **INTRODUCERE**

1. Această notificare de securitate se referă doar la informațiile clasificate.

2. Aceasta conține dispoziții privind aplicarea standardelor minime comune din partea 1 din Anexa I la prezenta decizie.

3. „Securitatea industrială” reprezintă aplicarea de măsuri în vederea asigurării protecției informațiilor clasificate de către contractanți și subcontractanți în cursul negocierilor anterioare încheierii contractelor și pe toată durata contractelor clasificate. Astfel de contracte nu implică accesul la informații clasificate la nivelul „TRÈS SECRET UE/EU TOP SECRET”.

4. Atunci când atribuie contracte clasificate unor entități industriale sau de altă natură, Parlamentul European, în calitate de autoritate contractantă, asigură respectarea standardelor minime privind securitatea industrială stabilite în prezenta decizie și menționate în contract.

B. **ELEMENTE DE SECURITATE ÎNTR-UN CONTRACT CLASIFICAT**

B.1. ***Ghidul clasificărilor de securitate (GCS)***

5. Înainte de a iniția o procedură de ofertare sau de a atribui un contract clasificat, Parlamentul European, în calitate de autoritate contractantă, stabilește clasificarea de securitate a oricăror informații care urmează a fi furnizate ofertanților și contractanților, precum și clasificarea de securitate a oricăror informații care urmează să fie create de contractant. În acest sens, Parlamentul European elaborează un Ghid al clasificărilor de securitate (GCS) care să fie utilizat în executarea contractului.

6. Pentru a stabili clasificarea de securitate a diferitelor elemente ale unui contract clasificat, se aplică următoarele principii:

(a) la pregătirea unui GCS, Parlamentul European ia în considerare toate aspectele de securitate relevante, inclusiv clasificarea de securitate atribuită informațiilor, furnizate și aprobate de către emitentul informațiilor în vederea utilizării acestora în scopul contractului;

(b) nivelul general de clasificare a contractului nu poate fi mai scăzut decât clasificarea cea mai ridicată a oricăruia dintre elementele sale.

B.2. ***Scrisoarea privind aspectele de securitate (SAS)***

7. Cerințele de securitate specifice contractului sunt descrise în scrisoarea privind aspectele de securitate (SAS). SAS cuprinde, atunci când este cazul, GCS și constituie o parte integrantă a contractului sau a subcontractului clasificat.

8. SAS cuprinde dispozițiile prin care se solicită contractantului și/sau subcontractantului să respecte standardele minime prevăzute în prezenta decizie. Nerespectarea acestor standarde minime de securitate poate constitui motiv suficient pentru încetarea contractului.

B.3. ***Instrucțiuni de securitate pentru program/proiect (ISP)***

9. În funcție de domeniul de aplicare al programelor sau proiectelor care implică accesul, manipularea sau păstrarea IUEC, pot fi elaborate instrucțiuni de securitate pentru program/proiect (ISP) de către autoritatea contractantă desemnată să gestioneze respectivul program sau proiect.

C. **CERTIFICATUL DE SECURITATE PENTRU INCINTE (CSI)**

10. CSI se acordă de către ANS sau de către orice altă autoritate de securitate competentă a unui stat membru pentru a atesta că, în conformitate cu actele cu putere de lege și dispozițiile administrative naționale, o entitate industrială sau de altă natură poate proteja IUEC la nivelul de clasificare „CONFIDENTIEL UE/EU CONFIDENTIAL" sau „SECRET UE/EU SECRET" sau la un nivel echivalent în interiorul obiectivelor sale. Dovada acordării CSI se prezintă Parlamentului European, în calitate de autoritate contractantă, înainte ca unui contractant sau subcontractant ori unui potențial contractant sau subcontractant să îi poată fi furnizat sau acordat accesul la IUEC.

11. CSI:

(a) evaluează integritatea entității industriale sau de altă natură;

(b) evaluează regimul de proprietate, controlul sau potențialul de exersare a unei influențe necuvenite care ar putea fi considerată un risc de securitate;

(c) verifică faptul că entitatea industrială sau orice altă entitate a instituit un sistem de securitate în incintă, care include toate măsurile de securitate adecvate necesare pentru protecția informațiilor sau a materialelor clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL" sau „SECRET UE/EU SECRET", în conformitate cu cerințele prevăzute de prezenta decizie;

(d) verifică faptul că statutul în ceea ce privește securitatea a fost stabilit pentru personalul de conducere, proprietarii și angajații care necesită acces la informații clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL" sau „SECRET UE/EU SECRET", în conformitate cu cerințele prevăzute de prezenta decizie; și

(e) verifică faptul că entitatea industrială sau orice altă entitate a numit un agent de securitate al obiectivului, care este responsabil cu gestionarea acesteia în vederea aplicării obligațiilor de securitate în cadrul entității respective.

12. După caz, Parlamentul European, în calitate de autoritate contractantă, înștiințează ANS adecvată sau altă autoritate de securitate competentă că este necesar un CSI, fie în etapa precontractuală, fie pentru executarea contractului. Este necesar un CSI sau certificat de securitate personală (CSP) în etapa precontractuală în cazul în care trebuie furnizate informații clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL" sau „SECRET UE/EU SECRET" pe parcursul procesului de licitare.

13. Autoritatea contractantă nu atribuie un contract clasificat unui ofertant selectat înainte de a fi primit confirmarea eliberării unui CSI corespunzător, dacă acesta este necesar, din partea ANS sau a oricărei alte autorități de securitate competente a statului membru în care este înregistrat contractantul sau subcontractantul respectiv.

14. Orice autoritate de securitate competentă care a eliberat un CSI notifică Parlamentului European, în calitate de autoritate contractantă, orice modificări care afectează CSI. În cazul unui subcontract, autoritatea competentă de securitate este informată în mod corespunzător.

15. Retragerea unui CSI de către ANS sau de către orice altă autoritate de securitate competentă constituie temei suficient pentru Parlamentul European, în calitate de autoritate contractantă, să înceteze un contract clasificat sau să excludă un ofertant din competiție.

D. **CONTRACTE ȘI SUBCONTRACTE CLASIFICATE**

16. Atunci când informațiile clasificate sunt furnizate ofertanților potențiali în etapa precontractuală, invitațiile de participare conțin o dispoziție care obligă ofertanții care nu prezintă o ofertă sau care nu sunt selectați să restituie toate documentele clasificate într-un termen specificat.

17. Odată ce un contract sau un subcontract clasificat a fost atribuit, Parlamentul European, în calitate de autoritate contractantă, notifică dispozițiile în materie de securitate ale contractului clasificat ANS corespunzătoare contractantului și/sau subcontractantului sau oricărei alte autorități de securitate competente.

18. La încetarea unui astfel de contract, Parlamentul European, în calitate de autoritate contractantă (și/sau autoritatea de securitate competentă, după caz, în cazul subcontractelor) notifică de îndată ANS sau orice altă autoritate de securitate competentă a statului membru în care este înregistrat contractantul sau subcontractantul.

19. Ca regulă generală, contractantului sau subcontractantului i se solicită să înapoieze autorității contractante, la încheierea contractului sau subcontractului clasificat, orice informații clasificate pe care le deține.

20. Dispoziții specifice privind distrugerea informațiilor clasificate în timpul executării contractului sau la încheierea acestuia sunt prevăzute în SAS.

21. În cazul în care contractantul sau subcontractantul este autorizat să rețină informații clasificate după încheierea unui contract, sunt respectate în continuare standardele minime cuprinse în prezenta decizie, iar contractantul sau subcontractantul protejează în continuare confidențialitatea IUEC.

22. Condițiile pe care trebuie să le îndeplinească contractantul pentru a putea subcontracta sunt menționate în procedura de ofertare și în contract.

23. Un contractant trebuie să obțină permisiunea Parlamentului European, în calitate de autoritate contractantă, înainte de a subcontracta părți ale unui contract clasificat. Nu se atribuie subcontracte entităților industriale sau de altă natură înregistrate într-un stat terț care nu a încheiat un acord privind securitatea informațiilor cu Uniunea.

24. Contractantul este responsabil pentru asigurarea faptului că toate activitățile de subcontractare sunt întreprinse în conformitate cu standardele minime prevăzute în prezenta decizie și nu furnizează IUEC unui subcontractant fără consimțământul prealabil scris al autorității contractante.

25. În ceea ce privește informațiile clasificate create sau gestionate de contractant sau de subcontractant, drepturile care îi revin emitentului sunt exercitate de către autoritatea contractantă.

E. **VIZITE ÎN LEGĂTURĂ CU CONTRACTELE CLASIFICATE**

26. În cazul în care Parlamentul European, contractanții sau subcontractanții necesită acces la informații clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL" sau „SECRET UE/EU SECRET" în incintele celeilalte părți în scopul executării unui contract clasificat, vizitele sunt organizate în colaborare cu ANS sau cu orice altă autoritate de securitate competentă implicată. Cu toate acestea, în contextul unor proiecte specifice, ANS pot conveni, de asemenea, o procedură prin care astfel de vizite să poată fi organizate în mod direct.

27. Toți vizitatorii dețin un CSP adecvat sau „necesitatea de a cunoaște" pentru accesul la informațiile clasificate legate de contractul cu Parlamentul European.

28. Vizitatorilor li se asigură accesul la informațiile clasificate care au legătură cu scopul vizitei.

F. **TRANSMITEREA ȘI TRANSPORTUL INFORMAȚIILOR CLASIFICATE**

29. În ceea ce privește transmiterea informațiilor clasificate prin mijloace electronice, se aplică dispozițiile relevante din notificarea de securitate 3.

30. În ceea ce privește transportul informațiilor clasificate, se aplică dispozițiile relevante din notificarea de securitate 4 și instrucțiunile de manipulare relevante.

31. Pentru transportul ca marfă al materialelor clasificate, se aplică următoarele principii în stabilirea măsurilor de securitate:

(a) se garantează securitatea în toate etapele transportului, de la punctul de plecare până la destinația finală;

(b) nivelul de protecție acordat unui transport se stabilește în funcție de materialul cu cel mai înalt nivel de clasificare transportat;

(c) societățile de transport obțin un CSI de nivel corespunzător. În astfel de cazuri, personalul care se ocupă de transportul respectiv deține certificate de securitate, în conformitate cu Anexa I;

(d) înaintea oricărei deplasări transfrontaliere de materiale clasificate la nivelul „CONFIDENTIEL UE/EU CONFIDENTIAL" sau „SECRET UE/EU SECRET" sau la un nivel echivalent, expeditorul întocmește un plan de transport aprobat Secretarul General;

(e) călătoriile se realizează, ori de câte ori este posibil, de la un punct prestabilit de plecare și până la o destinație prestabilită și sunt finalizate cât mai repede, în funcție de împrejurări;

(f) itinerariile se stabilesc, ori de câte ori este posibil, prin statele membre.

G. **TRANSFERUL DE INFORMAȚII CLASIFICATE CĂTRE CONTRACTANȚI AFLAȚI ÎN STATE TERȚE**

32. Informațiile clasificate sunt transferate contractanților și subcontractanților aflați în state terțe în conformitate cu măsurile de securitate convenite între Parlamentul European, în calitate de autoritate contractantă, și statul terț în care este înregistrat contractantul.

H. **MANIPULAREA ȘI PĂSTRAREA INFORMAȚIILOR CLASIFICATE LA NIVELUL „RESTREINT UE/EU RESTRICTED"**

33. Parlamentul European, în calitate de autoritate contractantă, ținând legătura, după caz cu ANS a statului membru în cauză, are dreptul să efectueze vizite în incintele contractanților/subcontractanților în temeiul clauzelor contractuale, în scopul de a verifica dacă s-au aplicat măsurile de securitate pentru protecția IUEC la nivelul „RESTREINT UE/EU RESTRICTED" în conformitate cu cerințele contractului.

34. În măsura în care este necesar în temeiul actelor cu putere de lege și dispozițiilor administrative naționale, ANS sau orice altă autoritate de securitate competentă este înștiințată de Parlamentul European, în calitate de autoritate contractantă, cu privire la contractele sau subcontractele care conțin informații clasificate la nivelul „RESTREINT UE/EU RESTRICTED".

35. Pentru contractele atribuite de Parlamentul European care conțin informații clasificate la nivelul „RESTREINT UE/EU RESTRICTED" nu se solicită un CSI sau un CSP pentru contractanți sau subcontractanți și personalul acestora.

36. Parlamentul European, în calitate de autoritate contractantă, analizează răspunsurile la invitațiile de participare la procedurile de ofertare pentru contractele care necesită accesul la informații clasificate la nivelul „RESTREINT UE/EU RESTRICTED", fără a aduce atingere niciunei cerințe referitoare la CSI sau la CSP care poate exista în temeiul actelor cu putere de lege și dispozițiilor administrative naționale.

37. Condițiile pe care trebuie să le îndeplinească contractantul pentru a putea subcontracta sunt menționate în procedura de ofertare și în contract.

38. Dacă un contract implică manipularea de informații clasificate la nivelul „RESTREINT UE/EU RESTRICTED" în sisteme de comunicații și informații operate de contractant, Parlamentul European, în calitate de autoritate contractantă, se asigură că atât contractul, cât și eventualele subcontracte îndeplinesc cerințele tehnice și administrative necesare în ceea ce privește acreditarea sistemelor de comunicații și informații, proporțional cu riscurile evaluate, ținând seama de toți factorii relevanți. Nivelul de acreditare a acestor sisteme de comunicații și informații este convenit între autoritatea contractantă și ANS relevantă.

NOTIFICAREA DE SECURITATE 6

ÎNCĂLCĂRI ALE SECURITĂȚII, PIERDEREA SAU COMPROMITEREA UNOR INFORMAȚII CONFIDENȚIALE

1. Constituie o încălcare a securității un act sau o omisiune care contravine prezentei decizii și care poate pune în pericol sau compromite informații confidențiale.

2. Compromiterea informațiilor confidențiale survine în cazul în care informațiile în cauză ajung, integral sau parțial, în posesia unor persoane neautorizate, adică persoane care nu dețin certificatul de securitate corespunzător și pentru care cunoașterea informațiilor respective nu este necesară, sau în cazul în care există posibilitatea ca un astfel de lucru să se fi întâmplat.

3. Informațiile confidențiale pot fi compromise din neatenție, neglijență sau indiscreție, precum și ca urmare a activităților unor servicii care vizează Uniunea sau ale unor organizații subversive.

4. Atunci când descoperă o încălcare a securității ori pierderea sau compromiterea unor informații confidențiale, suspectată sau dovedită, sau este informat despre o astfel de situație, Secretarul General:

(a) stabilește situația de fapt;

(b) evaluează și reduce la minimum daunele produse;

(c) ia măsuri pentru a preveni repetarea acestei situații;

(d) notifică autoritatea competentă a părții terțe sau a statului membru care s-a aflat la originea informației sau care a transmis-o.

În cazul în care este vizat un deputat în Parlamentul European, Secretarul General acționează în colaborare cu Președintele Parlamentului European.

Atunci când informațiile se primesc de la alte instituții ale Uniunii, Secretarul General acționează în conformitate cu măsurile de securitate adecvate pentru informațiile clasificate și dispozițiile prevăzute în Acordul-cadru cu Comisia sau în Acordul interinstituțional cu Consiliul.

5. Toate persoanele care trebuie să gestioneze informații confidențiale sunt informate în detaliu cu privire la procedurile de securitate, pericolele prezentate de conversațiile indiscrete și relațiile lor cu media și, dacă este cazul, semnează o declarație prin care se angajează să nu dezvăluie conținutul informațiilor confidențiale unor terți, să respecte obligațiile de protejarea a informațiilor clasificate și prin care confirmă că au cunoștință de consecințele nerespectării acestor obligații. Accesul la informații clasificate sau utilizarea lor de către o persoană care nu a fost informată și nu a semnat declarația aferentă este considerată o încălcare a securității.

6. Deputații în Parlamentul European, funcționari Parlamentului European, și orice alți angajați ai Parlamentului care lucrează pentru grupurile politice sau orice contractanți anunță de îndată Secretarul General cu privire la orice încălcare de securitate, pierderea sau compromiterea unor informații confidențiale despre care ar putea avea cunoștință.

7. Orice persoană responsabilă de compromiterea unor informații clasificate este pasibilă de sancțiuni disciplinare conform regulamentelor și reglementărilor în vigoare. Aceasta nu aduce atingere acțiunilor în justiție, care pot fi inițiate în conformitate cu legislația aplicabilă.

8. Fără a aduce atingere altor acțiuni în justiție, încălcările comise de funcționari ai Parlamentului European și de alți angajați ai Parlamentului care lucrează pentru grupurile politice determină aplicarea procedurilor și a sancțiunilor prevăzute de Titlul VI din Statutul funcționarilor.

9. Fără a aduce atingere altor acțiuni în justiție, încălcările comise de deputați în Parlamentul European sunt tratate în conformitate cu articolul 9 alineatul (2) și articolele 152, 153 și 154 din Regulamentul de procedură al Parlamentului.