DECIZIA (UE, Euratom) 2015/444 A COMISIEI

din 13 martie 2015

privind normele de securitate pentru protecția informațiilor UE clasificate

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 249,

având în vedere Tratatul de instituire a Comunității Europene a Energiei Atomice, în special articolul 106,

având în vedere Protocolul nr. 7 privind privilegiile și imunitățile Uniunii Europene anexat la tratate, în special articolul 18,

întrucât:

(1) Dispozițiile în materie de securitate ale Comisiei referitoare la protecția informațiilor clasificate ale Uniunii Europene (IUEC) necesită o revizuire și o actualizare care să țină seama de evoluțiile instituționale, organizatorice, operaționale și tehnologice.

(2) Comisia Europeană a lansat, împreună cu guvernele Belgiei, Luxemburgului și Italiei ([1]), instrumente privind aspectele legate de securitate pentru principalele sale locații.

(3) Comisia, Consiliul și Serviciul European de Acțiune Externă își asumă angajamentul de a aplica standarde echivalente de securitate pentru protecția IUEC.

(4) Este important ca Parlamentul European și alte instituții, agenții, organe sau oficii ale Uniunii să fie asociate, atunci când este cazul, la principiile, standardele și normele de protecție a informațiilor clasificate necesare pentru protejarea intereselor Uniunii și ale statelor sale membre.

(5) Riscul la adresa IUEC este gestionat ca proces. Acest proces urmărește determinarea riscurilor de securitate cunoscute, definirea măsurilor de securitate care vizează reducerea acestor riscuri la un nivel acceptabil în conformitate cu principiile de bază și standardele minime de securitate stabilite în prezenta decizie și aplicarea acestor măsuri în conformitate cu conceptul apărării în profunzime. Eficacitatea acestor măsuri este evaluată în permanență.

(6) În cadrul Comisiei, securitatea fizică ce vizează protejarea informațiilor clasificate reprezintă aplicarea măsurilor de protecție fizică și tehnică menite să împiedice accesul neautorizat la IUEC.

(7) Gestionarea IUEC constă în aplicarea unor măsuri administrative în scopul de a controla IUEC pe durata ciclului lor de viață, pentru a completa măsurile prevăzute la capitolele 2, 3 și 5 din prezenta decizie, contribuind astfel la descurajarea, detectarea și remedierea compromiterii sau a pierderii deliberate ori accidentale a informațiilor de acest tip. Măsurile respective se referă, în special, la crearea, păstrarea, înregistrarea, copierea, traducerea, scăderea nivelului de clasificare, declasificarea, gestionarea și distrugerea IUEC și completează normele generale privind gestionarea documentelor Comisiei [Deciziile 2002/47/CE, CECO, Euratom ([2]) și 2004/563/CE, Euratom ([3])].

([1]) A se vedea următoarele acorduri: „Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité", încheiat la 31 decembrie 2004, „Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois", încheiat la 20 ianuarie 2007 și „Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale", încheiat la 22 iulie 1959.

([2]) Decizia Comisiei 2002/47/CE, CESO, Euratom din 23 ianuarie 2002 de modificare a regulamentului de procedură (JO L 21, 24.1.2002, p. 23).

([3]) Decizia Comisiei din 7 iulie 2004 de modificare a regulamentului său de procedură (JO L 251, 27.7.2004, p. 9).

(8) Dispoziția din prezenta decizie nu aduce atingere:

(a) Regulamentului (Euratom) nr. 3 ([1]);

(b) Regulamentului (CE) nr. 1049/2001 al Parlamentului European și al Consiliului ([2]);

(c) Regulamentului (CE) 45/2001 al Parlamentului European și al Consiliului ([3]);

(d) Regulamentului (CEE, Euratom) nr. 354/83 al Consiliului ([4]),

ADOPTĂ PREZENTA DECIZIE:

CAPITOLUL 1

PRINCIPII DE BAZĂ ȘI STANDARDE MINIME

Articolul 1

Definiții

În sensul prezentei decizii, se aplică următoarele definiții:

1. „departament al Comisiei" înseamnă orice direcție generală ori serviciu al Comisiei sau orice cabinet al unui membru al Comisiei;

2. „material criptografic (criptat)" înseamnă algoritmi criptografici, module criptografice hardware și software și produse însoțite de modalități de instalare și documentația aferentă, precum și materialul de criptare;

3. „declasificare" înseamnă eliminarea oricărei clasificări de securitate;

4. „apărare în profunzime" înseamnă aplicarea unei serii de măsuri de securitate organizate pe niveluri de apărare multiple;

5. „document" reprezintă orice informație înregistrată, indiferent de forma sau caracteristicile sale fizice;

6. „reducerea nivelului de securitate" înseamnă atribuirea unui nivel de clasificare inferior;

7. „gestionarea" IUEC înseamnă toate acțiunile posibile al căror obiect îl pot face IUEC de-a lungul ciclului lor de viață. Aceasta cuprinde crearea, înregistrarea, prelucrarea, transportul, reducerea nivelului de clasificare, declasificarea și distrugerea. În ceea ce privește sistemele informatice și de comunicații (SIC), gestionarea cuprinde, de asemenea, colectarea, afișarea, transmiterea și păstrarea.

8. „deținător" înseamnă o persoană autorizată în mod corespunzător, în privința căreia s-a stabilit necesitatea de a cunoaște, care se află în posesia unei informații UE clasificate și, în consecință, răspunde de protecția acesteia;

9. „norme de punere în aplicare" înseamnă orice set de norme sau notificări de securitate adoptate în conformitate cu capitolul 5 din Decizia (UE, Euratom) 2015/443 a Comisiei ([5]);

10. „material" înseamnă orice suport, suport de date sau orice aparat ori echipament deja fabricat sau în curs de fabricație;

11. „emitent" înseamnă instituția, agenția sau organul Uniunii, statul membru, statul terț sau organizația internațională sub a cărei (cărui) autoritate s-au creat și/sau introdus în structurile Uniunii informațiile clasificate;

12. „incinte" înseamnă orice bunuri imobile sau asimilate acestora și orice proprietăți deținute de Comisie;

([1]) Regulamentul (Euratom) nr. 3 al Consiliului din 31 iulie 1958 de punere în aplicare a articolului 24 din Tratatul de instituire a Comunității Europene a Energiei Atomice (JO 17, 6.10.1958, p. 406/58).

([2]) Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei (JO L 145, 31.5.2001, p. 43).

([3]) Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).

([4]) Regulamentul (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 (JO L 43, 15.2.1983, p. 1)

([5]) Decizia Comisiei (UE, Euratom) 2015/443 din 13 martie 2015 privind securitatea în cadrul Comisiei (a se vedea pagina 41 din prezentul Jurnal Oficial).

13. „proces de management al riscului de securitate" înseamnă întregul proces de identificare, control și reducere la minimum a influenței evenimentelor incerte care pot afecta securitatea unei organizații sau a oricăruia dintre sistemele pe care aceasta le folosește. Procesul acoperă întregul spectru al activităților legate de risc, inclusiv evaluarea, tratarea, acceptarea și comunicarea;

14. „Statutul funcționarilor" înseamnă Statutul funcționarilor Uniunii Europene și Regimul aplicabil celorlalți agenți ai Uniunii Europene, stabilite prin Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului ([1]);

15. „amenințare" înseamnă o cauză potențială a unui incident nedorit care poate aduce prejudicii unei organizații sau oricăruia dintre sistemele pe care aceasta le folosește. Astfel de amenințări pot fi accidentale sau deliberate (rău intenționate) și sunt caracterizate prin elemente amenințătoare, ținte potențiale și metode de atac;

16. „vulnerabilitate" înseamnă un punct slab de orice natură care poate fi exploatat de una sau mai multe amenințări. Vulnerabilitatea poate fi o omisiune sau se poate referi la un punct slab în cadrul controalelor, din punctul de vedere al rigurozității, exhaustivității sau omogenității acestora, și poate fi de ordin tehnic, procedural, fizic, organizațional sau operațional.

Articolul 2

Obiect și domeniu de aplicare

(1) Prezenta decizie stabilește principiile de bază și standardele minime de securitate pentru protecția IUEC.

(2) Prezenta decizie se aplică tuturor serviciilor Comisiei și în toate incintele acesteia.

(3) În pofida oricăror indicații specifice cu privire la anumite categorii de personal, prezenta decizie se aplică membrilor Comisiei, personalului Comisiei care intră în domeniul de aplicare al Statutului funcționarilor și al condițiilor de angajare a altor agenți ai Comunităților Europene, experților naționali detașați (END) pe lângă Comisie, întreprinderilor prestatoare de servicii și angajaților acestora, stagiarilor și tuturor persoanelor cărora le este permis accesul în clădirile Comisiei sau la alte bunuri ale acesteia ori accesul la informațiile tratate de Comisie.

(4) Dispozițiile prezentei decizii se aplică fără a aduce atingere Deciziei 2002/47/CE, CECO, Euratom a Comisiei și Deciziei 2004/563/CE, Euratom a Comisiei.

Articolul 3

Definiția IUEC, a clasificărilor și a marcajelor de securitate

(1) „Informații clasificate ale Uniunii Europene" (IUEC) înseamnă orice informații sau materiale desemnate ca atare printr-o clasificare de securitate a UE, a căror divulgare neautorizată ar putea cauza prejudicii de diferite grade intereselor Uniunii Europene sau ale unuia ori mai multor state membre.

(2) IUEC sunt clasificate la unul dintre următoarele niveluri:

(a) TRES SECRET UE/EU TOP SECRET: informații și materiale a căror divulgare neautorizată ar putea aduce prejudicii deosebit de grave intereselor esențiale ale Uniunii Europene sau ale unuia ori mai multor state membre;

(b) SECRET UE/EU SECRET: informații și materiale a căror divulgare neautorizată ar putea aduce prejudicii grave intereselor esențiale ale Uniunii Europene sau ale unuia ori mai multor state membre;

(c) CONFIDENTIEL UE/EU CONFIDENTIAL: informații și materiale a căror divulgare neautorizată ar putea aduce prejudicii intereselor esențiale ale Uniunii Europene sau ale unuia ori mai multor state membre;

(d) RESTREINT UE/EU RESTRICTED: informații și materiale a căror divulgare neautorizată ar putea fi în defavoarea intereselor Uniunii Europene sau ale unuia ori mai multor state membre.

(3) IUEC afișează un marcaj de clasificare de securitate, în conformitate cu alineatul (2). IUEC pot avea marcaje suplimentare, care, fără a fi marcaje de securitate, sunt destinate să indice domeniul de activitate la care se referă, să identifice emitentul, să limiteze distribuirea, să restrângă utilizarea sau să precizeze dacă pot fi comunicate.

([1]) Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului din 29 februarie 1968 de instituire a Statutului funcționarilor comunităților europene și a Regimului aplicabil celorlalți agenți ai acestor comunități, precum și a unor dispoziții speciale aplicabile temporar funcționarilor Comisiei (JO L 56, 4.3.1968, p. 1).

Articolul 4

Gestionarea clasificărilor

(1) Fiecare membru al Comisiei și fiecare departament al acesteia se asigură că IUEC pe care le produc sunt clasificate corespunzător, identificate în mod clar ca IUEC și că nivelul de clasificare al acestora este menținut doar atât timp cât este necesar.

(2) Fără a aduce atingere articolului 26 de mai jos, IUEC nu sunt clasificate la un nivel de securitate inferior sau declasificate și niciun marcaj al clasificării de securitate menționat la articolul 3 alineatul (2) nu este modificat sau eliminat fără acordul prealabil scris al emitentului.

(3) Atunci când este cazul, se adoptă, în conformitate cu articolul 60 de mai jos, norme de punere în aplicare referitoare la gestionarea IUEC, inclusiv un ghid practic de clasificare.

Articolul 5

Protecția informațiilor clasificate

(1) IUEC sunt protejate în conformitate cu prezenta decizie și cu normele de punere în aplicare a acesteia.

(2) Deținătorul oricărei informații UE clasificate este responsabil de protecția acesteia, în conformitate cu prezenta decizie și cu normele sale de punere în aplicare, cu respectarea normelor prevăzute în capitolul 4 de mai jos.

(3) În cazul în care statele membre introduc în structurile sau rețelele Comisiei informații clasificate care conțin un marcaj național de clasificare de securitate, Comisia protejează informațiile respective în conformitate cu cerințele aplicabile IUEC de nivel echivalent, astfel cum se precizează în tabelul de echivalență a clasificărilor de securitate din anexa I.

(4) Un volum total de IUEC poate justifica un nivel de protecție corespunzător unei clasificări superioare celei a elementelor sale individuale.

Articolul 6

Managementul riscului de securitate

(1) Măsurile de securitate pentru protejarea IUEC pe durata ciclului lor de viață sunt proporționale, în special, cu clasificarea de securitate a acestora, forma și volumul informațiilor sau al materialelor, amplasarea și construcția clădirilor care adăpostesc IUEC și evaluarea locală a amenințării reprezentate de activități rău-intenționate și/sau infracționale, inclusiv spionaj, sabotaj și terorism.

(2) Planurile de urgență iau în considerare necesitatea protejării IUEC în situații de urgență, pentru a împiedica accesul neautorizat, divulgarea sau pierderea integrității ori a disponibilității.

(3) Toate serviciile includ în planurile de asigurare a continuității activității măsuri de prevenire și de recuperare destinate reducerii la minimum a impactului erorilor sau incidentelor majore survenite în timpul gestionării și păstrării IUEC.

Articolul 7

Punerea în aplicare a prezentei decizii

(1) Atunci când acest lucru este necesar, în conformitate cu articolul 60 de mai jos, se adoptă norme de punere în aplicare menite să completeze sau să sprijine prezenta decizie.

(2) Departamentele Comisiei iau toate măsurile necesare care intră în sfera lor de responsabilitate pentru a se asigura că, atunci când IUEC sau orice alte informații clasificate sunt gestionate ori păstrate, se aplică prezenta decizie și normele de punere în aplicare corespunzătoare.

(3) Măsurile de securitate luate pentru punerea în aplicare a prezentei decizii trebuie să respecte principiile de securitate din cadrul Comisiei prevăzute la articolul 3 din Decizia (UE, Euratom) 2015/443.

(4) Directorul general al DG Resurse Umane și Securitate înființează Autoritatea de securitate a Comisiei în cadrul Direcției Generale Resurse Umane și Securitate. Autoritatea de securitate a Comisiei îndeplinește responsabilitățile care îi sunt atribuite prin prezenta decizie și prin normele de punere în aplicare a acesteia.

(5) În cadrul fiecărui departament al Comisiei, ofițerul local de securitate (LSO), menționat la articolul 20 din Decizia (UE, Euratom) 2015/443 privind securitatea în cadrul Comisiei, îndeplinește următoarele responsabilități generale în materie de protecție a IUEC, în conformitate cu prezenta decizie, în strânsă cooperare cu Direcția Generală Resurse Umane și Securitate:

(a) gestionarea cererilor privind acordarea de autorizații de securitate pentru personal;

(b) contribuția la formarea în materie de securitate și la informările de conștientizare;

(c) supervizarea ofițerului de control al registraturii (RCO) din cadrul departamentului;

(d) raportarea cu privire la încălcările securității și compromiterea IUEC;

(e) păstrarea cheilor de rezervă și a unei evidențe scrise a fiecărei combinații de cifruri;

(f) asumarea altor sarcini legate de protecția IUEC sau definite în normele de punere în aplicare.

Articolul 8

Încălcări ale securității și compromiterea IUEC

(1) O încălcare a securității are loc în urma unei fapte sau omisiuni a unei persoane care contravine normelor de securitate stabilite în prezenta decizie și în normele de punere în aplicare a acesteia.

(2) Compromiterea IUEC are loc atunci când, în urma unei încălcări a securității, acestea au fost divulgate, integral sau parțial, unor persoane neautorizate.

(3) Orice încălcare sau suspiciune de încălcare a securității este raportată imediat Autorității de securitate a Comisiei.

(4) În cazul în care se cunoaște sau există motive întemeiate să se presupună că au fost compromise sau pierdute IUEC, se desfășoară o investigație privind securitatea în conformitate cu articolul 13 din Decizia (UE, Euratom) 2015/443.

(5) Se iau toate măsurile corespunzătoare pentru:

(a) a informa emitentul;

(b) a asigura investigarea cazului de către membri ai personalului care nu sunt implicați în mod direct în încălcare, pentru a stabili faptele;

(c) a evalua eventualele prejudicii aduse intereselor Uniunii sau ale statelor membre;

(d) a lua măsuri adecvate pentru a împiedica repetarea situației; precum și

(e) a notifica autorităților competente acțiunea întreprinsă.

(6) Orice persoană responsabilă de încălcarea normelor de securitate prevăzute în prezenta decizie poate fi pasibilă de acțiuni disciplinare, în conformitate cu Statutul funcționarilor. Orice persoană responsabilă de compromiterea sau pierderea unor informații de tip IUEC este pasibilă de acțiuni disciplinare și/sau în justiție, în conformitate cu actele cu putere de lege, normele și reglementările aplicabile.

CAPITOLUL 2

SECURITATEA PERSONALULUI

Articolul 9

Definiții

În sensul prezentului capitol, se aplică definițiile următoare:

1. „autorizație de acces la IUEC” înseamnă o decizie a Autorității de securitate a Comisiei, luată pe baza unei asigurări date de o autoritate competentă a unui stat membru, conform căreia unui funcționar, unui alt agent al Comisiei sau unui expert național detașat, odată ce s-a stabilit că este necesar ca persoana în cauză să aibă cunoștință de astfel de informații și cu condiția ca acesta să fi fost informat corespunzător cu privire la responsabilitățile sale, îi poate fi acordat accesul la IUEC până la un nivel precizat (CONFIDENTIEL UE/EU CONFIDENTIAL sau superior) și până la o anumită dată; se consideră că persoana astfel descrisă deține „autorizația de securitate”;

2. „autorizare de securitate pentru personal" înseamnă aplicarea unor măsuri prin care se garantează că accesul la IUEC este acordat numai în persoanelor care:

   (a) au nevoie să le cunoască;

   (b) au primit autorizație de securitate pentru nivelul corespunzător, dacă este cazul; precum și

   (c) au fost informate cu privire la responsabilitățile care le revin;

3. „acordarea autorizării de securitate personalului" (ASP) înseamnă o declarație a unei autorități competente a unui stat membru făcută după finalizarea unei investigații de securitate efectuate de autoritățile competente ale unui stat membru, care certifică faptul că unei persoane îi poate fi acordat accesul la IUEC până la un nivel precizat (CONFIDENTIEL UE/EU CONFIDENTIAL sau superior) și până la o anumită dată, cu condiția să se fi stabilit necesitatea de a cunoaște în cazul său și ca persoana în cauză să fi fost informată în mod corespunzător cu privire la responsabilitățile sale;

4. „certificare a autorizării de securitate a personalului" (CASP) înseamnă un certificat eliberat de o autoritate competentă care stabilește că o persoană deține un certificat de securitate valabil sau o autorizare de securitate valabilă eliberată de Autoritatea de securitate a Comisiei și care indică nivelul IUEC la care este permis accesul persoanei respective (CONFIDENTIEL UE/EU CONFIDENTIAL sau superior), perioada de valabilitate a certificatului sau a autorizării de securitate corespunzătoare și data expirării certificatului în cauză;

5. „investigație de securitate" înseamnă procedurile de investigare întreprinse de autoritatea competentă a unui stat membru, în conformitate cu actele cu putere de lege și normele administrative naționale din statul membru în cauză, pentru a obține asigurarea că nu există elemente defavorabile care ar putea să împiedice o persoană să beneficieze de un certificat de securitate la un nivel precizat (CONFIDENTIEL UE/EU CONFIDENTIAL) sau la un nivel superior.

Articolul 10

Principii de bază

(1) Unei persoane i se acordă accesul la IUEC numai după parcurgerea următoarelor etape:

1. a fost stabilită necesitatea de a cunoaște a acesteia;

2. persoana în cauză a fost instruită cu privire la normele de securitate pentru protecția IUEC și cu privire la standardele și orientările relevante în materie de securitate și a confirmat că a luat cunoștință de responsabilitățile care îi revin cu privire la protecția informațiilor de acest tip;

3. pentru accesul la informații clasificate la nivelul CONFIDENTIEL UE/EU ONFIDENTIAL și la un nivel superior, persoana în cauză a primit autorizarea de securitate pentru nivelul corespunzător sau este autorizată într-un alt mod corespunzător în temeiul funcțiilor deținute în conformitate cu actele cu putere de lege și normele administrative naționale.

(2) Toate persoanele ale căror atribuții pot necesita accesul la IUEC de nivel CONFIDENTIEL UE/EU CONFIDENTIAL sau de un nivel superior primesc autorizarea de securitate pentru nivelul corespunzător înainte de a primi acces la respectivele IUEC. Persoana în cauză consimte în scris să se supună procedurii prevăzute pentru acordarea autorizării de securitate personalului. În caz contrar, persoana în cauză nu poate primi un post, funcții sau atribuții care presupun accesul la informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL ori la un nivel superior.

(3) Se elaborează proceduri de acordare a autorizării de securitate personalului, pentru a stabili dacă o persoană poate avea acces la IUEC, ținându-se seama de loialitatea și onestitatea acesteia și de încrederea pe care o inspiră.

(4) Loialitatea, onestitatea și încrederea inspirată de o persoană în scopul acordării autorizării de securitate pentru accesul la informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL ori la un nivel superior sunt stabilite prin intermediul unei investigații privind securitatea efectuate de autoritățile competente ale unui stat membru în conformitate cu actele cu putere de lege și normele administrative naționale.

(5) Autoritatea de securitate a Comisiei răspunde în mod exclusiv de asigurarea legăturii cu autoritățile naționale de securitate („ANS") sau cu alte autorități naționale competente în contextul tuturor aspectelor legate de permisiunea de securitate. Toate contactele dintre serviciile Comisiei și personalul acestora cu ANS și alte autorități competente au loc prin intermediul Autorității de securitate a Comisiei.

Articolul 11

Procedura de autorizare de securitate

(1) Fiecare director general sau șef de serviciu din cadrul Comisiei identifică, în cadrul departamentului său, posturile ai căror titulari au nevoie să obțină acces la informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL ori la un nivel superior pentru a-și îndeplini atribuțiile și, prin urmare, trebuie să primească autorizarea de securitate.

(2) De îndată ce se știe că o persoană va fi numită într-un post care necesită accesul la informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL ori la un nivel superior, ofițerul local de securitate (LSO) al departamentului în cauză al Comisiei informează Autoritatea de securitate a Comisiei, care îi transmite persoanei interesate chestionarul aferent procedurii de acordare a unui certificat de securitate emis de ANS a statului membru al cărui cetățean este persoana care a fost numită pe un post în cadrul instituțiilor europene. Persoana în cauză consimte în scris să se supună procedurii prevăzute pentru acordarea autorizării de securitate și să trimită Autorității de securitate a Comisiei, în cel mai scurt termen, chestionarul completat.

(3) Odată ce este completat, chestionarul aferent procedurii de acordare a autorizării de securitate este transmis de Autoritatea de securitate a Comisiei către ANS a statului membru a cărui cetățenie o deține persoana care a fost numită pe un post în cadrul instituțiilor europene, solicitând efectuarea unei investigații de securitate privind nivelul IUEC la care va trebui să i se acorde accesul persoanei respective.

(4) În cazul în care Autoritatea de securitate a Comisiei intră în posesia unor informații relevante pentru o investigație de securitate referitoare la o persoană care a solicitat o autorizare de securitate, Autoritatea de securitate a Comisiei, acționând în conformitate cu actele cu putere de lege și normele administrative relevante, notifică acest lucru ANS competente.

(5) La încheierea investigației de securitate și cât mai curând posibil după ce ANS i-a adus la cunoștință evaluarea sa generală cu privire la rezultatele investigației de securitate, Autoritatea de securitate a Comisiei:

(a) poate acorda persoanei în cauză o autorizație de acces la IUEC și poate autoriza accesul la IUEC la nivelul relevant și până la dată indicată de persoana respectivă, dar fără ca această durată să depășească 5 ani, în cazul în care investigația de securitate stabilește cu certitudine că nu se cunosc elemente defavorabile care ar pune la îndoială loialitatea, onestitatea și încrederea inspirate de persoana în cauză;

(b) în cazul în care investigația de securitate nu are drept rezultat obținerea unei astfel de garanții, în conformitate cu actele cu putere de lege și normele administrative relevante, notifică acest lucru persoanei în cauză, care poate solicita să fie audiată de Autoritatea de securitate a Comisiei, care, la rândul său, poate solicita ANS competente orice clarificare suplimentară pe care aceasta din urmă o poate oferi în conformitate cu actele cu putere de lege și normele administrative naționale. Dacă rezultatul investigației de securitate este confirmat, nu se acordă autorizația de acces la IUEC.

(6) Investigația de securitate și rezultatele obținute sunt supuse actelor cu putere de lege și normelor administrative relevante în vigoare în statul membru în cauză, inclusiv celor privind căile de atac. Deciziile Autorității de securitate a Comisiei pot face obiectul unor căi de atac, în conformitate cu Statutul funcționarilor.

(7) Comisia acceptă autorizația de acces la IUEC acordată de orice altă instituție, alt organ sau altă agenție a Uniunii, cu condiția ca aceasta să fie în continuare valabilă. Autorizațiile vor acoperi orice funcție deținută de persoana în cauză în cadrul Comisiei. Instituția, organul sau agenția Uniunii în care își preia funcția persoana respectivă va informa ANS relevantă cu privire la schimbarea angajatorului.

(8) Dacă o persoană nu își începe activitatea în termen de 12 luni de la notificarea rezultatului investigației de securitate Autorității de securitate a Comisiei sau dacă intervine o pauză de 12 luni în exercitarea atribuțiilor sale, perioadă în care persoana în cauză nu a fost angajată în cadrul Comisiei sau al oricărei alte instituții, al oricărui alt organ ori al oricărei alte agenții a Uniunii sau nu a ocupat un post în cadrul administrației naționale a unui stat membru, Autoritatea de securitate a Comisiei prezintă această chestiune ANS competente, pentru a obține confirmarea că permisiunea de securitate rămâne valabilă și pertinentă.

(9) În cazul în care Autoritatea de securitate a Comisiei intră în posesia unor informații privind faptul că o persoană care deține o autorizare de securitate valabilă prezintă un risc legat de securitate, autoritatea de securitate, acționând în conformitate cu actele cu putere de lege și dispozițiile administrative relevante, notifică acest lucru ANS competente.

(10) În cazul în care o ANS notifică Autorității de securitate a Comisiei retragerea unei garanții acordate în conformitate cu alineatul (5) litera (a) unei persoane care deține o autorizație valabilă de acces la IUEC, Autoritatea de securitate a Comisiei poate solicita ANS orice clarificare pe care aceasta din urmă o poate oferi în conformitate cu actele cu putere de lege și dispozițiile administrative naționale. În cazul în care informațiile nefavorabile sunt confirmate de ANS relevantă, persoanei respective i se retrage autorizarea de securitate și i se interzice accesul la IUEC și la funcțiile în cadrul cărora ar putea avea acces la acestea sau ar putea compromite securitatea.

(11) Orice decizie de a retrage sau de a suspenda o autorizație de acces la IUEC deținută de orice persoană căreia i se aplică prezenta decizie și, după caz, motivele care stau la baza unei astfel de decizii, îi sunt comunicate persoanei în cauză, care poate solicita să fie audiată de Autoritatea de securitate a Comisiei. Informațiile puse la dispoziție de o ANS sunt supuse actelor cu putere de lege și dispozițiilor administrative relevante în vigoare în statul membru în cauză. Deciziile adoptate în acest context de Autoritatea de securitate a Comisiei pot face obiectul unor căi de atac, în conformitate cu Statutul funcționarilor.

(12) Departamentele Comisiei se asigură că experții naționali detașați pe lângă acestea care ocupă posturi ce necesită autorizarea de securitate pentru accesul la IUEC prezintă, înainte de a-și prelua funcția, o ASP valabilă sau o confirmare valabilă privind deținerea autorizării de securitate a personalului („CASP"), în conformitate cu actele cu putere de lege și dispozițiile administrative naționale, către Autoritatea de securitate a Comisiei, care, pe această bază, va acorda o autorizare de securitate pentru accesul la IUEC până la nivelul echivalent celui menționat în permisiunea națională de securitate, autorizare a cărei valabilitate maximă acoperă durata exercitării funcției în cauză.

Accesul la IUEC al persoanelor autorizate în mod corespunzător în temeiul funcțiilor deținute

(13) Membrii Comisiei care au acces la IUEC prin natura funcțiilor deținute în temeiul tratatului sunt informați despre obligațiile de securitate care le revin cu privire la protecția IUEC.

Evidențele referitoare la permisiunile de securitate și la autorizările de securitate

(14) Autoritatea de securitate a Comisiei păstrează evidențe ale permisiunilor și autorizărilor de securitate acordate în vederea accesului la IUEC în conformitate cu prezenta decizie. Evidențele respective conțin cel puțin detalii cu privire la nivelul IUEC la care este permis accesul persoanei, data la care a fost eliberată permisiunea de securitate și durata valabilității acesteia.

(15) Autoritatea de securitate a Comisiei poate elibera o CASP care indică nivelul IUEC la care este permis accesul persoanei respective (CONFIDENTIEL UE/EU CONFIDENTIAL sau superior), perioada de valabilitate a autorizației corespunzătoare de acces la IUEC și data expirării certificării în cauză.

Reînnoirea autorizărilor de securitate

(16) După acordarea inițială a autorizărilor de securitate și dacă persoana a lucrat neîntrerupt în cadrul Comisiei Europene sau al altei instituții, altui organ ori altei agenții a Uniunii și are nevoie de accesul permanent la IUEC, autorizarea de securitate pentru accesul la IUEC este reexaminată în vederea revalidării, în general la intervale de maximum cinci ani cu începere de la data comunicării rezultatului ultimei investigații de securitate pe care s-a bazat.

(17) Autoritatea de securitate a Comisiei poate prelungi valabilitatea autorizării de securitate existente cu maximum 12 luni, dacă nu s-au primit informații defavorabile din partea ANS relevante sau a oricărei alte autorități naționale competente în termen de două luni de la data transmiterii cererii de revalidare și a chestionarului prevăzut pentru acordarea autorizării de securitate. Dacă, la sfârșitul acestei perioade de 12 luni, ANS relevantă sau orice altă autoritate națională competentă nu a comunicat avizul său Autorității de securitate a Comisiei, persoanei în cauză îi sunt încredințate atribuții care nu necesită o autorizare de securitate.

Articolul 12

Informări cu privire la autorizarea de securitate

(1) După ce au participat la informările referitoare la autorizarea de securitate organizate de Autoritatea de securitate a Comisiei, toate persoanele care au primit autorizarea de securitate confirmă în scris faptul că au înțeles obligațiile care le revin în legătură cu protecția IUEC, precum și consecințele compromiterii IUEC. Autoritatea de securitate a Comisiei ține evidența acestor confirmări scrise.

(2) Toate persoanele autorizate să aibă acces la IUEC sau care trebuie să gestioneze IUEC primesc, inițial, informații cu privire la pericolele la adresa securității, sunt informate periodic despre acestea și trebuie să raporteze imediat Autorității de securitate a Comisiei orice abordare sau activitate pe care o consideră suspectă sau neobișnuită.

(3) Toate persoanele care încetează să aibă atribuții care necesită acces la IUEC sunt informate asupra obligațiilor care le revin în ceea ce privește protecția continuă a IUEC și, dacă este cazul, confirmă acest lucru în scris.

Articolul 13

Autorizările temporare de securitate

(1) În împrejurări excepționale, în cazuri de interes de serviciu justificate în mod corespunzător și în așteptarea finalizării unei investigații de securitate complete, Autoritatea de securitate a Comisiei poate acorda unei persoane o autorizație temporară de acces la IUEC pentru o funcție specifică, după consultarea ANS a statului membru al cărei cetățean este persoana respectivă și cu condiția să se cunoască rezultatul verificărilor preliminare efectuate cu privire la existența unor eventuale informații defavorabile, fără a aduce atingere dispozițiilor referitoare la reînnoirea permisiunilor de securitate. Astfel de autorizații temporare de acces la IUEC sunt valabile pe o perioadă maximă de șase luni care nu poate fi reînnoită și nu permit accesul la informații clasificate la nivelul TRES SECRET UE/EU TOP SECRET.

(2) După ce au fost informate în conformitate cu articolul 12 alineatul (1), toate persoanele cărora li s-a acordat o autorizație temporară confirmă în scris faptul că au înțeles obligațiile ce le revin cu privire la protecția IUEC, precum și consecințele compromiterii IUEC. Autoritatea de securitate a Comisiei ține evidența acestor confirmări scrise.

Articolul 14

Participarea la reuniunile clasificate organizate de Comisie

(1) Prin intermediul LSO sau al organizatorului reuniunii, departamentele Comisiei responsabile de organizarea de reuniuni la care sunt discutate informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior informează Autoritatea de securitate a Comisiei, cu suficient timp înainte, cu privire la datele, orele, locul și participanții la aceste reuniuni.

(2) Sub rezerva dispozițiilor de la articolul 11 alineatul (13), persoanele desemnate să participe la reuniuni organizate de Comisie în cadrul cărora se discută informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior pot participa numai după confirmarea statutului lor în ceea ce privește permisiunea de securitate sau autorizarea de securitate. Accesul la astfel de reuniuni clasificate le este refuzat persoanelor care nu au prezentat Autorității de securitate a Comisiei o CASP sau o altă dovadă a autorizării de securitate ori participanților din cadrul Comisiei care nu sunt titulari ai unei autorizări de securitate.

(3) Înainte de organizarea unei reuniuni clasificate, organizatorul responsabil de reuniune sau LSO al departamentului Comisiei care organizează reuniunea le solicită participanților externi să prezinte Autorității de securitate a Comisiei o CASP sau o altă dovadă a autorizării de securitate. Autoritatea de securitate a Comisiei îl informează pe LSO sau pe organizatorul reuniunii în legătură cu CASP sau cu o altă dovadă a ASP primite. După caz, se poate folosi o listă centralizată de nume, cuprinzând dovada relevantă a autorizării de securitate.

(4) În cazul în care Autoritatea de securitate a Comisiei este informată de autoritățile competente că unei persoane ale cărei atribuții impun participarea la reuniuni organizate de Comisie i s-a retras ASP Autoritatea de securitate a Comisiei îl informează LSO al departamentului Comisiei responsabil de organizarea reuniunii.

Articolul 15

Acces potențial la IUEC

Curierii, gardienii și escortele dețin autorizări de securitate de nivel corespunzător sau fac obiectul unor investigații adecvate în conformitate cu actele cu putere de lege și dispozițiile administrative naționale, sunt informați cu privire la procedurile de securitate privind protecția IUEC și sunt instruiți în legătură cu obligațiile de protecție a acestor informații care le sunt încredințate.

CAPITOLUL 3

SECURITATEA FIZICĂ CE VIZEAZĂ PROTEJAREA INFORMAȚIILOR CLASIFICATE

Articolul 16

Principii de bază

(1) Măsurile de securitate fizică sunt concepute astfel încât să împiedice accesul disimulat sau forțat al vreunui intrus, să descurajeze, să împiedice și să detecteze acțiunile neautorizate și să permită stabilirea unei distincții între membrii personalului în ceea ce privește accesul acestora la IUEC, pe baza principiului necesității de a cunoaște. Aceste măsuri sunt stabilite pe baza unui proces de management al riscului, în conformitate cu dispozițiile prezentei decizii și cu normele de punere în aplicare a acesteia.

(2) Măsurile de securitate fizică urmăresc îndeosebi să împiedice accesul neautorizat la IUEC și sunt concepute astfel încât:

(a) să asigure gestionarea și păstrarea IUEC într-un mod adecvat;

(b) să permită stabilirea unei distincții între membrii personalului în ceea ce privește accesul la IUEC, pe baza necesității de a cunoaște a acestora și, după caz, a autorizării lor de securitate;

(c) să descurajeze, să împiedice și să detecteze acțiunile neautorizate; precum și

(d) să împiedice sau să întârzie accesul clandestin sau forțat al intrușilor.

(3) Se instituie măsuri de securitate fizică pentru toate incintele, clădirile, birourile, sălile și alte spații în care sunt gestionate sau păstrate IUEC, inclusiv spațiile în care sunt amplasate sistemele informatice și de comunicații menționate la capitolul 5.

(4) Zonele în care sunt păstrate IUEC clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior sunt instituite ca zone securizate în conformitate cu prezentul capitol și omologate de Autoritatea de securitate a Comisiei.

(5) În vederea protecției IUEC de la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau de la un nivel superior se utilizează numai echipamente sau dispozitive aprobate de Autoritatea de securitate a Comisiei.

Articolul 17

Cerințe și măsuri de securitate fizică

(1) Măsurile de securitate fizică sunt selectate pe baza unei evaluări a amenințărilor efectuate de Autoritatea de securitate a Comisiei, în consultare, atunci când este cazul, cu alte departamente ale Comisiei, alte instituții, agenții sau organe ale Uniunii și/sau cu autoritățile competente din statele membre. Comisia aplică un proces de management al riscurilor pentru protejarea IUEC în incintele sale, pentru a asigura aplicarea unui nivel de protecție fizică proporțional cu riscul evaluat. Procesul de management al riscurilor ține seama de toți factorii relevanți, în special de:

(a) nivelul de clasificare al IUEC;

(b) forma și volumul IUEC, având în vedere faptul că, pentru volume mari de IUEC sau o compilație de IUEC, poate fi necesară aplicarea unor măsuri de protecție mai stricte;

(c) mediul înconjurător și structura clădirilor sau a spațiilor în care sunt amplasate IUEC; precum și

(d) evaluarea amenințării reprezentate de serviciile secrete care au drept țintă Uniunea, instituțiile, organele sau agențiile acesteia ori statele membre și de sabotaje, acte teroriste, activități subversive sau alte activități infracționale.

(2) Autoritatea de securitate a Comisiei, prin aplicarea conceptului apărării în profunzime, stabilește combinația corespunzătoare de măsuri de securitate fizică ce trebuie implementate. În acest sens, Autoritatea de securitate a Comisiei elaborează standarde, norme și criterii minime, stabilite în normele de punere în aplicare.

(3) Autoritatea de securitate a Comisiei este autorizată să efectueze controale la intrare și la ieșire, pentru a descuraja introducerea neautorizată de materiale sau sustragerea neautorizată a IUEC din incinte sau clădiri.

(4) Atunci când există riscul să se omită fie și accidental, anumite IUEC, departamentele relevante ale Comisiei iau măsuri adecvate, astfel cum sunt definite de Autoritatea de securitate a Comisiei, pentru a contracara acest risc.

(5) În ceea ce privește clădirile noi, cerințele de securitate fizică și specificațiile funcționale ale acestora se definesc, cu acordul Autorității de securitate a Comisiei, ca parte integrantă a planificării și proiectării obiectivelor. Pentru clădirile existente, cerințele de securitate fizică sunt puse în aplicare în conformitate cu standardele, normele și criteriile minime stabilite în normele de aplicare.

Articolul 18

Echipamente destinate protecției fizice a IUEC

(1) Pentru protecția fizică a IUEC, se instituie două tipuri de zone protejate fizic:

(a) zone administrative; și

(b) zone securizate (inclusiv zonele securizate din punct de vedere tehnic).

(2) Autoritatea de acreditare în materie de securitate a Comisiei stabilește o zonă care îndeplinește cerințele pentru a fi desemnată drept zonă administrativă, zonă securizată sau zonă securizată din punct de vedere tehnic.

(3) Pentru zonele administrative:

(a) se instituie un perimetru delimitat în mod vizibil, care permite verificarea persoanelor și, dacă este posibil, a vehiculelor;

(b) accesul neînsoțit este permis numai persoanelor autorizate în mod corespunzător de Autoritatea de securitate a Comisiei sau de orice altă autoritate competentă; și

(c) orice alte persoane sunt însoțite în permanență sau sunt supuse unor controale echivalente.

(4) Pentru zonele securizate:

(a) se instituie un perimetru delimitat în mod vizibil și protejat, în care toate intrările și ieșirile sunt controlate prin intermediul unui permis sau al unui sistem de recunoaștere personală;

(b) accesul neînsoțit este permis numai persoanelor care posedă certificatul de securitate și aprobarea specifică de a intra în zona respectivă, acordate pe baza necesității de a cunoaște a acestora;

(c) orice alte persoane sunt însoțite în permanență sau sunt supuse unor controale echivalente.

(5) Atunci când accesul într-o zonă securizată este echivalent, practic, cu accesul direct la informațiile clasificate aflate în zona respectivă, se aplică următoarele cerințe suplimentare:

(a) nivelul cel mai înalt de clasificare de securitate a informațiilor păstrate în mod normal în zonă este indicat în mod clar;

(b) toți vizitatorii au nevoie de o autorizație specifică pentru a intra în zona respectivă, sunt escortați în permanență și dețin un certificat de securitate adecvat, cu excepția cazului în care sunt instituite măsuri care fac imposibil accesul la IUEC.

(6) Zonele securizate protejate împotriva interceptării audio sunt desemnate drept zone securizate din punct de vedere tehnic. Se aplică următoarele cerințe suplimentare:

(a) aceste zone sunt echipate cu un sistem de detectare a intruziunilor (SDI), sunt încuiate atunci când nu sunt ocupate și păzite atunci când sunt ocupate. Toate cheile sunt gestionate în conformitate cu articolul 20;

(b) toate persoanele și materialele care intră în zonele respective sunt controlate;

(c) aceste zone sunt inspectate cu regularitate din punct de vedere fizic și/sau tehnic, în conformitate cu cerințele Autorității de securitate a Comisiei. De asemenea, astfel de inspecții sunt efectuate în urma accesului neautorizat sau a suspiciunii de acces neautorizat; și

(d) aceste zone nu sunt prevăzute cu linii de comunicații, telefoane sau alte dispozitive de comunicare și echipamente electrice ori electronice neautorizate.

(7) În pofida alineatului (6) litera (d), înainte de a fi utilizate în zone în care se desfășoară reuniuni sau se lucrează cu informații cu nivelul de clasificare SECRET UE/EU SECRET sau un nivel superior acestuia și în cazul în care amenințarea la adresa IUEC este evaluată ca fiind semnificativă, toate dispozitivele de comunicare și echipamentele electrice și electronice de orice tip sunt examinate, mai întâi, de Autoritatea de securitate a Comisiei, astfel încât nicio informație inteligibilă să nu poată fi transmisă în mod accidental sau ilicit prin intermediul unor asemenea echipamente în afara perimetrului zonei securizate.

(8) Acolo unde este cazul, zonele securizate care nu sunt ocupate de personal de serviciu 24 de ore/zi sunt inspectate după încheierea programului normal de lucru și la intervale aleatorii în afara acestuia, cu excepția cazului în care este instalat un SDI.

(9) Zonele securiza și zone securizate din punct de vedere tehnic pot fi create, în mod temporar, într-o zonă administrativă, în scopul unei reuniuni clasificate sau în orice alt scop similar.

(10) LSO al departamentului în cauză al Comisiei elaborează proceduri operaționale de securitate (SecOP) pentru fiecare zonă securizată aflată sub răspunderea sa, proceduri care prevăd, în conformitate cu dispozițiile prezentei decizii și cu normele de aplicare a acesteia:

(a) nivelul IUEC care pot fi gestionate sau păstrate în zona respectivă;

(b) măsurile de supraveghere și de protecție care trebuie asigurate;

(c) persoanele autorizate să aibă acces neînsoțite la zona respectivă pe baza necesității de a cunoaște și a autorizării de securitate;

(d) după caz, procedurile privind escortările sau protecția IUEC în cazul autorizării accesului oricăror altor persoane în zona respectivă;

(e) orice alte măsuri și proceduri relevante.

(11) În cadrul zonelor securizate se construiesc camere tezaur. Pereții, pardoseala, tavanele, ferestrele și ușile cu încuietori sunt aprobate de Autoritatea de securitate a Comisiei și oferă o protecție echivalentă celei garantate de un container de securitate aprobat pentru păstrarea IUEC de același nivel de clasificare.

Articolul 19

Măsuri de protecție fizică pentru gestionarea și păstrarea IUEC

(1) IUEC clasificate RESTREINT UE/EU RESTRICTED pot fi gestionate:

(a) într-o zonă securizată;

(b) într-o zonă administrativă, cu condiția ca IUEC să fie protejate împotriva accesului persoanelor neautorizate; sau

(c) în afara unei zone securizate sau a unei zone administrative, cu condiția ca deținătorul să transporte IUEC în conformitate cu articolul 31 și să se fi angajat să respecte măsurile compensatorii stabilite în normele de punere în aplicare, pentru a se asigura că IUEC sunt protejate împotriva accesului persoanelor neautorizate.

(2) IUEC clasificate RESTREINT UE/EU RESTRICTED sunt păstrate în mobilier de birou încuiat în mod corespunzător, într-o zonă administrativă sau o zonă securizată. Aceste informații pot fi păstrate, în mod temporar, în afara unei zone securizate sau a unei zone administrative, cu condiția ca deținătorul să se fi angajat să respecte măsurile compensatorii stabilite în normele de punere în aplicare.

(3) IUEC clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET pot fi gestionate:

(a) într-o zonă securizată;

(b) într-o zonă administrativă, cu condiția ca IUEC să fie protejate împotriva accesului persoanelor neautorizate; sau

(c) în afara unei zone securizate sau a unei zone administrative, cu condiția ca deținătorul:

(i) să se fi angajat să respecte măsurile compensatorii stabilite în normele de punere în aplicare, astfel încât IUEC să fie protejate împotriva accesului persoanelor neautorizate;

(ii) să mențină IUEC în permanență sub controlul său personal; și

(iii) în cazul documentelor în format tipărit, să fi informat registratura competentă în această privință.

(4) IUEC clasificate CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET sunt păstrate într-o zonă securizată, într-un container de securitate sau o cameră tezaur.

(5) IUEC clasificate TRES SECRET UE/EU TOP SECRET sunt gestionate într-o zonă securizată, instituită și întreținută de Autoritatea de securitate a Comisiei și acreditată la acest nivel de autoritatea de acreditare în materie de securitate a Comisiei.

(6) IUEC clasificate TRES SECRET UE/EU TOP SECRET sunt păstrate într-o zonă securizată, acreditată la acest nivel de autoritatea de acreditare în materie de securitate a Comisiei, într-una din următoarele condiții:

(a) într-un container de securitate conform dispozițiilor articolului 18, beneficiind de unul sau mai multe dintre următoarele controale suplimentare:

1. protecție continuă sau controale efectuate de membrii personalului de securitate sau de serviciu posesori ai unui certificat de securitate;

2. un SDI aprobat și personal de securitate de intervenție;

sau

(b) într-o cameră tezaur echipată cu SDI și personal de securitate de intervenție.

Articolul 20

Gestionarea cheilor și a combinațiilor de cifruri utilizate pentru protecția IUEC

(1) Normele de punere în aplicare trebuie să prevadă proceduri de gestionare a cheilor și a combinațiilor de cifruri pentru birouri, încăperi, camere tezaur și containere de securitate, în conformitate cu articolul 60 de mai jos. Aceste proceduri sunt menite să împiedice accesul neautorizat.

(2) Combinațiile de cifruri sunt memorate de cel mai mic număr de persoane posibil care trebuie să le cunoască. Combinațiile de cifruri pentru containerele de securitate și camerele tezaur în care sunt păstrate IUEC sunt schimbate:

(a) la primirea unui nou container;

(b) ori de câte ori se schimbă personalul care cunoaște cifrul;

(c) ori de câte ori s-a produs o compromitere sau există suspiciunea unei compromiteri;

(d) în cazul în care una dintre încuietori a făcut obiectul unei operații de întreținere sau a fost reparată; și

(e) cel puțin la fiecare 12 luni.

CAPITOLUL 4

MANAGEMENTUL INFORMAȚIILOR CLASIFICATE ALE UE

Articolul 21

Principii de bază

(1) Toate documentele IUEC ar trebui să fie gestionate în conformitate cu politica aplicată de Comisie în ceea ce privește gestionarea documentelor și, prin urmare, ar trebui să fie înregistrate, clasate, conservate, și, în cele din urmă, eliminate, incluse în eșantioane sau transferate la arhivele istorice în conformitate cu lista comună de păstrare a dosarelor Comisiei Europene.

(2) Din motive de securitate, informațiile clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior sunt înregistrate înainte de a fi distribuite, precum și la primire. Informațiile clasificate TRES SECRET UE/EU TOP SECRET sunt înregistrate în registre speciale.

(3) În cadrul Comisiei, se înființează un sistem de registraturi IUEC în conformitate cu dispozițiile articolului 27.

(4) Departamentele și incintele Comisiei unde sunt gestionate sau păstrate IUEC sunt supuse unor inspecții periodice întreprinse de Autoritatea de securitate a Comisiei.

(5) IUEC sunt transmise între serviciile și incintele situate în afara zonelor protejate fizic după cum urmează:

(a) ca regulă generală, IUEC sunt transmise prin mijloace electronice protejate prin intermediul unor produse criptografice aprobate în conformitate cu capitolul 5;

(b) în situațiile în care nu se utilizează mijloacele menționate la litera (a), IUEC sunt transportate:

(i) fie pe suport electronic (de ex. stickuri memorie USB, CD-uri, hard diskuri) protejat prin intermediul unor produse criptografice aprobate în conformitate cu capitolul 5; fie

(ii) în toate celelalte cazuri, astfel cum se prevede în normele de punere în aplicare.

Articolul 22

Clasificări și marcaje

(1) Informațiile se clasifică atunci când este necesară protecția confidențialității lor, în conformitate cu articolul 3 alineatul (1).

(2) Emitentul IUEC are responsabilitatea de a stabili nivelul de clasificare de securitate, în conformitate cu normele de punere în aplicare, standardele și orientările relevante cu privire la clasificare, și de a efectua diseminarea inițială a informațiilor.

(3) Nivelul de clasificare al IUEC se stabilește în conformitate cu articolul 3 alineatul (2) și cu normele de punere în aplicare relevante.

(4) Clasificarea de securitate este indicată în mod clar și corect, indiferent dacă IUEC se prezintă sub formă tipărită, orală, electronică sau sub orice altă formă.

(5) Anumite părți dintr-un document (și anume pagini, paragrafe, secțiuni, anexe, documente însoțitoare sau atașate) pot necesita atribuirea unor niveluri diferite de clasificare și trebuie marcate în mod corespunzător, inclusiv în cazul în care sunt stocate în format electronic.

(6) 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. La compilarea unor informații din surse diferite, produsul final este reexaminat pentru a i se stabili nivelul general de clasificare de securitate, deoarece poate necesita o clasificare superioară celei atribuite părților sale componente.

(7) În măsura posibilului, documentele care conțin porțiuni cu niveluri de clasificare diferite sunt structurate astfel încât porțiunile cu niveluri de clasificare diferite să poată fi identificate și separate cu ușurință, dacă este necesar.

(8) Nivelul de clasificare al scrisorilor sau al notelor care însoțesc documente clasificate trebuie să fie același cu cel mai ridicat nivel al documentelor atașate. Emitentul indică clar, printr-un marcaj adecvat, nivelul de clasificare pe care scrisorile sau notele îl vor avea după ce vor fi separate de documentele atașate, de exemplu:

CONFIDENTIEL UE/EU CONFIDENTIAL

Fără anexă/anexe RESTREINT UE/EU RESTRICTED

Articolul 23

Marcaje

În afară de marcajele clasificărilor de securitate stabilite la articolul 3 alineatul (2), IUEC pot prezenta marcajele suplimentare, precum:

(a) un element de identificare care desemnează emitentul;

(b) orice avertismente, coduri sau acronime care precizează domeniul de activitate la care se referă documentul, un anumit tip de distribuire bazat pe necesitatea de a cunoaște sau restricții privind utilizarea;

(c) marcaje de comunicare;

(d) după caz, data sau evenimentul specific în urma căruia poate scădea nivelul de clasificare al documentului sau acesta poate fi declasificat.

Articolul 24

Marcaje de clasificare abreviate

(1) Pentru a indica nivelul de clasificare al anumitor paragrafe dintr-un text, pot fi utilizate marcaje de clasificare abreviate standardizate. Abrevierile nu înlocuiesc marcajele de clasificare complete.

(2) În interiorul documentelor UE clasificate pot fi utilizate următoarele abrevieri standard, pentru a indica nivelul de clasificare al unor secțiuni sau porțiuni de text care nu depășesc o pagină:

TRES SECRET UEEU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Articolul 25

Crearea IUEC

(1) La crearea unui document UE clasificat:

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

(b) fiecare pagină este numerotată;

(c) documentul conține un număr de înregistrare și un subiect care, în sine, nu reprezintă informație clasificată, cu excepția cazului în care acesta este marcat ca atare;

(d) documentul este datat;

(e) documentele clasificate la nivelul SECRET UE/EU SECRET sau la un nivel superior poartă un număr de exemplar pe fiecare pagină, în cazul în care acestea urmează să fie distribuite în mai multe exemplare.

(2) În cazul în care există IUEC cărora nu li se poate aplica alineatul (1), se iau alte măsuri corespunzătoare în conformitate cu normele de punere în aplicare.

Articolul 26

Reducerea nivelului de clasificare și declasificarea IUEC

(1) Cu ocazia elaborării documentului, emitentul indică, atunci când acest lucru este posibil, dacă poate fi redus nivelul de clasificare al informațiilor UE clasificate sau dacă acestea pot fi declasificate la o anumită dată sau în urma unui anumit eveniment.

(2) Fiecare departament al Comisiei reexaminează în mod periodic IUEC emise de acesta, pentru a evalua necesitatea menținerii nivelului de clasificare. Normele de punere în aplicare prevăd un sistem de reexaminare, cel puțin o dată la cinci ani,.a nivelului de clasificare al IUEC înregistrate pe care le-a emis în cadrul Comisiei. O astfel de reexaminare nu este necesară în cazul în care emitentul a indicat de la început că trebuie să se reducă nivelul de clasificare al informațiilor sau că acestea trebuie declasificate în mod automat, iar informațiile au fost marcate în consecință.

(3) Informațiile clasificate la nivelul „RESTREINT UE/EU RESTRICTED” care au drept autor Comisia vor fi considerate declasificate în mod automat după treizeci de ani, în conformitate cu Regulamentul (CEE, Euratom) nr. 354/83 al Consiliului, astfel cum a fost modificat prin Regulamentul (CE, Euratom) nr. 1700/2003 al Consiliului ([1]).

Articolul 27

Sistemul de registraturi IUEC din cadrul Comisiei

(1) Fără a aduce atingere articolului 52 alineatul (5) de mai jos, în cadrul fiecărui departament al Comisiei în care sunt gestionate sau stocate IUEC la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET se identifică o registratură IUEC locală responsabilă, astfel încât IUEC să fie gestionate în conformitate cu prezenta decizie.

(2) Registratura IUEC gestionată de Secretariatul General este registratura IUEC centrală a Comisiei. Acesta acționează în calitate de:

— registratură IUEC locală a Secretariatului General al Comisiei;

— registratură IUEC pentru cabinetele membrilor Comisiei, cu excepția cazului în care acestea dispun de o registratură IUEC locală desemnat în mod expres;

— registratură IUEC pentru direcțiile generale sau serviciile care nu dispun de o registratură IUEC locală;

— principal punct de intrare și de ieșire pentru toate informațiile clasificate la nivelul RESTREINT UE/EU RESTRICTED și până la SECRET UE/EU SECRET, inclusiv informațiile schimbate de Comisie și serviciile acesteia cu state terțe și organizații internaționale și, atunci când acest lucru este prevăzut prin acorduri specifice, pentru alte instituții, agenții și organe ale Uniunii.

(3) În cadrul Comisiei, Autoritatea de securitate a Comisiei desemnează o registratură care să funcționeze ca autoritate centrală de primire și de expediere a informațiilor clasificate TRES SECRET UE/EU TOP SECRET. Dacă acest lucru este necesar, pot fi desemnate registraturi subordonate care să gestioneze informațiile respective în scopul înregistrării.

(4) Registraturile subordonate nu pot transmite documente clasificate TRES SECRET UE/EU TOP SECRET în mod direct către alte registraturi subordonate aceleiași registraturi centrale TRES SECRET UE/EU TOP SECRET sau în exterior, fără aprobarea expresă și scrisă a acestuia din urmă.

(5) Registraturile IUEC sunt concepute ca zone securizate, astfel cum sunt definite în capitolul 3, și sunt acreditate de către autoritatea de acreditare în materie de securitate (AAS) a Comisiei.

Articolul 28

Ofițerul de control al registraturii

(1) Fiecare registratură IUEC este gestionate de un ofițer de control al registraturii („RCO”).

(2) RCO trebuie să posede permisiunea de securitate corespunzătoare.

(3) RCO este supervizat de LSO din cadrul departamentului respectiv al Comisiei în ceea ce privește aplicarea dispozițiilor referitoare la gestionarea documentelor IUEC și respectarea normelor, a standardelor și a orientărilor de securitate relevante.

(4) În cadrul responsabilităților sale de gestionare a registraturii IUEC care i-au fost încredințate, RCO exercită următoarele atribuții generale în conformitate cu prezenta decizie și cu normele de punere în aplicare, standardele și orientările relevante:

— gestionează operațiunile legate de înregistrarea, păstrarea, reproducerea, traducerea, transmiterea, expedierea și distrugerea sau transferul la serviciul arhivelor istorice al IUEC;

— verifică periodic necesitatea menținerii clasificării informațiilor;

— preia orice alte atribuții legate de protecția IUEC definite în normele de punere în aplicare.

Articolul 29

Înregistrarea IUEC din motive de securitate

(1) În sensul prezentei decizii, înregistrarea din motive de securitate (denumită în continuare „înregistrarea”) înseamnă aplicarea unor proceduri care permit înregistrarea ciclului de viață al IUEC, inclusiv diseminarea lor.

([1]) Regulamentul (CE, Euratom) nr. 1700/2003 al Consiliului din 22 septembrie 2003 de modificare a Regulamentului (CEE, Euratom) nr. 354/83 privind deschiderea către public a arhivelor istorice ale Comunității Economice Europene și Comunității Europene a Energiei Atomice (JO L 243, 27.9.2003, p. 1).

(2) Toate informațiile sau materialele clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL și la un nivel superior sunt înregistrate în registre speciale ori de câte ori sunt recepționate sau diseminate de o entitate organizațională.

(3) În cazul în care ICUE sunt gestionate sau stocate cu ajutorul unui sistem informatice și de comunicații (SIC), procedurile de înregistrare pot fi efectuate prin procese care au loc chiar în cadrul respectivului SIC.

(4) Dispoziții mai detaliate privind înregistrarea IUEC în scopuri de securitate sunt prevăzute în normele de punere în aplicare.

Articolul 30

Copierea și traducerea documentelor clasificate ale UE

(1) Documentele TRES SECRET UE/EU TOP SECRET nu pot fi copiate sau traduse decât cu acordul scris prealabil al emitentului.

(2) În cazul în care emitentul documentelor clasificate la nivelul SECRET UE/EU SECRET și la un nivel inferior nu a impus restricții de copiere sau traducere, aceste documente pot fi copiate sau traduse conform instrucțiunilor deținătorului.

(3) Măsurile de securitate aplicabile documentului original se aplică copiilor și traducerilor acestuia.

Articolul 31

Transportul IUEC

(1) Transportul IUEC se desfășoară astfel încât aceste informații să fie protejate împotriva divulgării neautorizate pe durata transportului.

(2) Transportul IUEC respectă măsurile de protecție prevăzute, care:

— sunt proporționale cu nivelul de clasificare al IUEC transportate; și

— sunt adaptate la condițiile specifice transportului, în special în funcție de faptul dacă ICUE sunt transportate:

  — în interiorul unei clădiri a Comisiei sau al unui grup autonom de clădiri ale Comisiei;

  — între clădiri ale Comisiei situate în același stat membru;

  — în Uniune;

  — din Uniune către teritoriul unui stat terț; și

  — sunt adaptate la caracteristicile și forma IUEC.

(3) Aceste măsuri de protecție sunt prevăzute într-o formă detaliată în normele de punere în aplicare sau, în cazul proiectelor și programelor menționate la articolul 42, ca parte integrantă a instrucțiunilor de securitate relevante ale programului sau proiectului în cauză (ISP).

(4) Normele de aplicare sau ISP includ dispoziții proporționale cu nivelul de clasificare al IUEC, în ceea ce privește:

— tipul de transport, precum transportul personal, transportul prin curier diplomatic sau militar, transportul prin intermediul serviciilor poștale sau al serviciilor de curierat comercial;

— modul de prezentare al IUEC;

— contramăsurile tehnice pentru IUEC transportate pe suporturi electronice;

— orice altă măsură procedurală, fizică sau electronică;

— procedurile de înregistrare;

— recurgerea la personalul de securitate autorizat.

(5) În cazul în care IUEC sunt transportate pe suporturi electronice și fără a aduce atingere articolului 21 alineatul (5), măsurile de protecție prevăzute în normele de punere în aplicare relevante pot fi completate cu contramăsuri tehnice adecvate aprobate de Autoritatea de securitate a Comisiei, astfel încât riscul pierderii sau compromiterii lor să fie redus la minimum.

Articolul 32

Distrugerea IUEC

(1) Documentele UE clasificate care nu mai sunt necesare pot fi distruse, ținându-se seama de reglementările privind arhivele, de normele și regulamentele Comisiei referitoare la administrarea și arhivarea documentelor și în special de Lista comună de conservare a dosarelor la nivelul Comisiei.

(2) IUEC clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL și la un nivel superior sunt distruse de către RCO al registraturii IUEC responsabile la instrucțiunile deținătorului sau ale unei autorități competente. RCO actualizează registrele de evidență și alte informații de înregistrare în mod corespunzător.

(3) În ceea ce privește documentele clasificate SECRET UE/EU SECRET sau TRES SECRET UE/EU TOP SECRET, aceste operațiuni de distrugere sunt realizate de către RCO în prezența unui martor care deține un certificat de securitate de nivel cel puțin echivalent cu nivelul documentului distrus.

(4) Gestionarul și martorul, în cazul în care este necesară prezența acestuia din urmă, semnează un proces-verbal de distrugere, care este păstrat la registru. RCO al registraturii IUEC responsabile păstrează procesele-verbale de distrugere timp de cel puțin zece ani în cazul documentelor clasificate TRES SECRET UE/EU TOP SECRET și de cel puțin cinci ani în cazul documentelor clasificate CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET.

(5) Documentele clasificate, inclusiv cele clasificate RESTREINT UE/EU RESTRICTED, sunt distruse prin metode care urmează să fie definite în normele de punere în aplicare și care sunt conforme cu standardele relevante ale UE sau cu standarde echivalente.

(6) Suporturile informatice utilizate pentru stocarea IUEC sunt distruse în conformitate cu procedurile stabilite în normele de punere în aplicare.

Articolul 33

Distrugerea IUEC în situații de urgență

(1) Departamentele Comisiei care dețin IUEC elaborează planuri bazate pe condițiile locale pentru a asigura protecția, într-o situație de criză, a materialelor UE clasificate, inclusiv, dacă este necesar, planuri pentru distrugere și evacuare de urgență. Entitățile în cauză promulgă instrucțiuni considerate necesare pentru ca IUEC să nu parvină unor persoane neautorizate.

(2) Măsurile luate pentru protecția și/sau distrugerea, în situații de criză, a materialelor clasificate CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET nu afectează, în nici un caz, salvgardarea sau distrugerea materialelor clasificate TRES SECRET UE/EU TOP SECRET, inclusiv a echipamentelor de codificare, a căror tratare trebuie să aibă prioritate față de toate celelalte sarcini.

(3) În cazul unei urgențe, dacă există un risc iminent de divulgare neautorizată, IUEC sunt distruse de către deținător astfel încât să nu poată fi reconstituite în întregime sau parțial. Emitentul și registratura emitentă sunt informați cu privire la distrugerea de urgență a IUEC înregistrate.

(4) Dispoziții mai detaliate privind distrugerea IUEC sunt prevăzute în normele de punere în aplicare.

CAPITOLUL 5

PROTECȚIA INFORMAȚIILOR UE CLASIFICATE ÎN SISTEMELE INFORMATICE ȘI DE COMUNICAȚII (SIC)

Articolul 34

Principii de bază ale asigurării informațiilor

(1) Asigurarea informațiilor (AI) în domeniul sistemelor informatice și de comunicații reprezintă încrederea în faptul că aceste sisteme vor proteja informațiile pe care le gestionează și vor funcționa corespunzător, atunci când este necesar, sub controlul utilizatorilor legitimi.

(2) Printr-o asigurare eficace a informațiilor se garantează niveluri adecvate de:

Autenticitate: garanția faptului că informațiile sunt originale și provin de la surse de bună credință;

Disponibilitate: proprietatea informațiilor de a putea fi accesate și utilizate la cerere de către o entitate autorizată;

Confidențialitate: proprietatea informațiilor de a nu fi divulgate persoanelor, entităților sau proceselor neautorizate;

Integritate: proprietate care constă în garantarea acurateței și a exhaustivității activelor și a informațiilor;

Nerepudiere: capacitatea de a dovedi că o acțiune sau un eveniment a avut loc, astfel încât acțiunea sau evenimentul în cauză să nu poată fi negate ulterior.

(3) AI se bazează pe un proces de management al riscului.

Articolul 35

Definiții

În sensul prezentului capitol se folosesc următoarele definiții:

(a) „acreditare" înseamnă autorizarea și aprobarea oficiale acordate unui sistem informatic și de comunicații de către autoritatea de acreditare de securitate (AAS) pentru prelucrarea IUEC în mediul lor operațional, după validarea oficială a planului de securitate și punerea sa corectă în aplicare;

(b) „proces de acreditare" înseamnă măsurile și sarcinile necesare înainte de acreditarea de către autoritatea de acreditare în materie de securitate. Aceste măsuri și sarcini sunt specificate într-un proces de acreditare standard;

(c) „sistem informatic și de comunicații" (SIC) înseamnă un sistem care permite gestionarea informațiilor în format electronic. Un sistem informatic și de comunicații cuprinde toate mijloacele necesare pentru funcționarea sa, inclusiv infrastructura, organizarea, personalul și resursele informaționale;

(d) „risc rezidual" înseamnă riscul care persistă după punerea în aplicare a măsurilor de securitate, ținând seama de faptul că nu toate amenințările sunt contracarate și nu toate vulnerabilitățile pot fi eliminate;

(e) „risc" înseamnă posibilitatea ca o anumită amenințare să exploateze vulnerabilitățile interne și externe ale unei organizații sau ale oricăruia dintre sistemele pe care aceasta le utilizează și, în consecință, să cauzeze un prejudiciu organizației sau activelor sale corporale ori necorporale. Riscul se măsoară ținându-se cont, în același timp, de probabilitatea materializării amenințărilor și de impactul acestora.

(f) „acceptarea riscului" înseamnă decizia de a accepta, după tratarea riscului, existența în continuare a unui risc rezidual;

(g) „evaluarea riscului" constă în identificarea amenințărilor și a vulnerabilităților și în desfășurarea analizei de risc aferente, și anume a analizei de probabilitate și de impact;

(h) „comunicarea riscului" constă în sensibilizarea comunităților de utilizatori ai SIC cu privire la riscuri, în informarea autorităților de omologare cu privire la aceste riscuri și în raportarea lor către autoritățile operaționale;

(i) „tratarea riscului" constă în atenuarea, eliminarea sau reducerea riscului (prin măsuri adecvate de ordin tehnic, fizic, organizațional sau procedural), transferul riscului sau monitorizarea riscului.

Articolul 36

SIC care gestionează IUEC

(1) SIC gestionează IUEC în conformitate cu conceptul de AI.

(2) Pentru SIC care tratează ICUE, respectarea sistemelor de informare ale Comisiei, politica de securitate, astfel cum se menționează în Decizia C(2006) 3602 a Comisiei ([1]), implică faptul că:

(a) pentru punerea în aplicare a politicii privind sistemele de informare de securitate pe parcursul întregului ciclu de viață al sistemului de informare se aplică abordarea „planifică-execută-verifică-acționează";

(b) nevoile în materie de securitate trebuie să fie identificate prin intermediul unei evaluări a impactului asupra activității;

(c) sistemul de informare și datele pe care le conține trebuie să fie supuse unei clasificări formale a activelor;

([1]) Decizia C(2006) 3602 din 16 august 2006 privind securitatea sistemelor informatice utilizate de Comisia Europeană.

(d) trebuie să fie puse în aplicare toate măsurile de securitate obligatorii, astfel cum sunt stabilite de politica privind securitatea sistemelor de informații;

(e) trebuie să fie aplicat un proces de management al riscurilor, constând în următoarele etape: identificarea amenințărilor și a vulnerabilităților, evaluarea riscurilor, tratarea riscurilor, acceptarea riscurilor și comunicarea riscurilor;

(f) se definește, se pune în aplicare, se verifică și se revizuiește un plan de securitate care cuprinde politica de securitate și procedurile operaționale de securitate.

(3) Toți membrii personalului implicați în proiectarea, dezvoltarea, testarea, funcționarea, gestionarea sau utilizarea unui SIC care tratează ICUE aduc la cunoștința ASA toate posibilele deficiențe în materie de securitate, incidente, cazuri de încălcare sau de compromitere a securității care pot avea un impact asupra protecției SIC și/sau a IUEC pe care le conține acesta.

(4) În cazurile în care protecția IUEC este asigurată prin produse criptografice, acestea sunt aprobate după cum urmează:

(a) se preferă produselor care au fost aprobate de Consiliu sau de către secretarul general al Consiliului, în calitatea sa de autoritate de aprobare criptografică a Consiliului, la recomandarea Grupului de experți în materie de securitate al Comisiei;

(b) atunci când acest lucru este justificat din motive operaționale specifice, autoritatea de aprobare criptografică (AAC) a Comisiei poate, la recomandarea Grupului de experți în materie de securitate al Comisiei, să acorde derogări de la cerințele prevăzute la litera (a) și să acorde o aprobare provizorie pe o anumită perioadă.

(5) Pe durata transmiterii, prelucrării și stocării IUEC prin mijloace electronice, se folosesc produse criptografice aprobate. Fără a aduce atingere acestei cerințe, pot fi aplicate proceduri specifice în situații de urgență sau în cadrul unor configurații tehnice specifice, după ce s-a obținut o aprobare în acest sens din partea AAC.

(6) Se pun în aplicare măsuri de securitate pentru a proteja sistemele de comunicare și informare care tratează informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior împotriva compromiterii acestor informații prin emisii electromagnetice accidentale („măsuri de securitate TEMPEST"). Măsurile de securitate respective sunt proporționale cu riscul de exploatare și nivelul de clasificare a informațiilor.

(7) Autoritatea de securitate a Comisiei exercită următoarele funcții:

— autoritate AI (AAI);

— autoritatea de acreditare în materie de securitate (AAS);

— autoritate TEMPEST (AT);

— autoritatea de aprobare criptografică (AAC);

— autoritate de distribuție criptografică (ADC);

(8) Pentru fiecare sistem, Autoritatea de securitate a Comisiei numește autoritatea operațională AI.

(9) Responsabilitățile funcțiilor descrise la punctele 7 și 8 sunt definite în normele de aplicare.

Articolul 37

Acreditarea unui SIC care gestionează IUEC

(1) Toate SIC care gestionează IUEC sunt supuse unui proces de acreditare, pe baza principiilor AI, al căror nivel de detaliere trebuie să fie proporțional cu nivelul de protecție necesar.

(2) Procesul de acreditare include validarea formală de către AAS a Comisiei a planului de securitate pentru SIC în cauză pentru a obține asigurări cu privire la faptul că:

(a) procesul de management al riscurilor, astfel cum este menționat la articolul 36 alineatul (2), a fost pus în aplicare în mod adecvat;

(b) proprietarul de sistem a acceptat în mod conștient riscul rezidual; și

(c) s-a atins un nivel suficient de protecție a SIC și a IUEC gestionate în cadrul acestuia, în conformitate cu prezenta decizie.

(3) AAS a Comisiei eliberează o declarație de acreditare care stabilește nivelul maxim de clasificare a IUEC care pot fi gestionate în cadrul SCI, precum și clauzele și condițiile de funcționare corespunzătoare. Această dispoziție se aplică fără a aduce atingere sarcinilor încredințate Consiliului de acreditare de securitate definit la articolul 11 din Regulamentul nr. 512/2014 (UE) al Parlamentului European și al Consiliului ([1]).

(4) Un Consiliu mixt de acreditare în materie de securitate (CAS), care implică mai multe părți, este responsabil cu acreditarea SIC ale Comisiei. Acesta este alcătuit dintr-un reprezentant AAS al fiecărei părți implicate și este prezidat de un reprezentant AAS al Comisiei Europene.

(5) Procesul de acreditare constă într-o serie de sarcini care trebuie asumate de părțile implicate. Responsabilitatea pentru pregătirea dosarelor de acreditare și a documentației îi revine exclusiv proprietarului de sistem al SCI.

(6) Acreditarea intră în sfera de responsabilitate a AAS a Comisiei, care, în orice moment din ciclul de viață al SCI, are dreptul:

(a) de a solicita aplicarea unui proces de acreditare;

(b) de a audita sau inspecta SCI;

(c) în cazul în care condițiile de funcționare nu mai sunt îndeplinite, de a solicita definirea și implementarea efectivă a unui plan de îmbunătățire a securității într-un interval de timp bine definit, retrăgând, eventual, permisiunea de funcționare acordată pentru SIC în cauză până când condițiile de funcționare sunt din nou îndeplinite.

(7) Procesul de acreditare trebuie să fie stabilit printr-o normă privind procesul de acreditare pentru SIC care gestionează ICUE, care se adoptă în conformitate cu articolul 10 alineatul (3) din Decizia C (2006) 3602.

Articolul 38

Situații de urgență

(1) Fără a aduce atingere dispozițiilor de la prezentul capitol, procedurile specifice descrise în continuare pot fi aplicate într-o situație de urgență, cum ar fi înaintea sau în timpul unor crize, conflicte sau situații de război sau în cazul unor împrejurări operaționale excepționale.

(2) IUEC pot fi transmise prin intermediul unor produse criptografice aprobate pentru un nivel de clasificare inferior sau fără a fi criptate, cu consimțământul autorității competente, în cazul în care orice întârziere ar cauza un prejudiciu mult mai grav decât orice prejudiciu rezultat în urma divulgării materialului clasificat și dacă:

(a) expeditorul și destinatarul nu dispun de echipamentele de criptare necesare; și

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

(3) Informațiile clasificate transmise în împrejurările enunțate la alineatul (1) 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.

(4) Ulterior, se prezintă un raport în acest sens autorității competente și Grupului de experți în materie de securitate al Comisiei.

CAPITOLUL 6

SECURITATE INDUSTRIALĂ

Articolul 39

Principii de bază

(1) Securitatea industrială înseamnă aplicarea de măsuri în vederea asigurării protecției IUEC

(a) în cadrul contractelor clasificate, de către:

(i) candidați sau ofertanți pe parcursul licitației și al procedurii de contractare;

(ii) contractanți sau subcontractanți pe parcursul ciclului de viață al contractelor clasificate;

([1]) Regulamentul (UE) nr. 512/2014 al Parlamentului European și al Consiliului din 16 aprilie 2014 de modificare a Regulamentului (UE) nr. 912/2010 de instituire a Agenției GNSS European (JO L 150, 20.5.2014, p. 72).

(b) în cadrul acordurilor de grant clasificate, de către:

(i) solicitanți pe durata procedurilor de acordare de granturi;

(ii) beneficiari pe parcursul întregului ciclu de viață al acordurilor de grant clasificate.

(2) Astfel de contracte sau acorduri de grant nu implică accesul la informații clasificate TRES SECRET UE/EU TOP SECRET.

(3) Cu excepția unor dispoziții contrare, dispozițiile din prezentul capitol referitoare la contracte clasificate sau la contractanți se aplică și subcontractelor clasificate sau subcontractanților.

Articolul 40

Definiții

În sensul prezentului capitol, se aplică următoarele definiții:

(a) „contract clasificat" înseamnă un contract-cadru sau un contract, astfel cum este menționat în Regulamentul (CE, Euratom) nr. 1605/2002 al Consiliului ([1]), încheiat de Comisie sau de unul dintre departamentele acesteia cu un contractant pentru livrarea de bunuri mobile sau imobile, executarea de lucrări sau prestarea de servicii, a căror executare necesită sau implică crearea, gestionarea sau stocarea unor IUEC;

(b) „subcontract clasificat" înseamnă un contract încheiat de un contractant al Comisiei sau de unul dintre departamentele acesteia cu un alt contractant (respectiv, subcontractantul) pentru livrarea de bunuri mobile și imobile, executarea de lucrări sau prestarea de servicii, a căror executare necesită sau implică crearea, gestionarea sau stocarea unor IUEC;

(c) „acord de grant clasificat" înseamnă un acord prin care Comisia acordă un grant, astfel cum este menționat în partea I titlul VI din Regulamentul (CE, Euratom) nr. 1605/2002, a căror executare necesită sau implică crearea, gestionarea sau păstrarea unor IUEC;

(d) „autoritatea de securitate desemnată" (ASD) înseamnă o autoritate care răspunde în fața autorității naționale de securitate (ANS) a unui stat membru, însărcinată să comunice entităților industriale sau de alt tip politica națională în materie de securitate industrială, sub toate aspectele acesteia, și să ofere indicații și asistență pentru punerea în aplicare a acesteia. Atribuțiile ASD pot fi îndeplinite de ANS sau de orice altă autoritate competentă.

Articolul 41

Procedura aplicabilă contractelor sau acordurilor de grant clasificate

(1) Atunci când atribuie contracte sau acorduri de grant clasificate, fiecare departament al Comisiei, în calitate de autoritate contractantă, se asigură că standardele minime privind securitatea industrială prevăzute în prezentul capitol sunt menționate sau integrate în contract și că acestea sunt respectate.

(2) În sensul alineatului (1), serviciile competente din cadrul Comisiei solicită consiliere din partea Direcției Generale Resurse Umane și Securitate, și, în special, din partea Direcției Securitate și se asigură că modelele de contracte și subcontracte și modelele de acorduri de grant includ dispoziții care să reflecte principiile de bază și standardele minime referitoare la protecția IUEC ce trebuie respectate de către contractanți și subcontractanți și, respectiv, de către beneficiarii acordurilor de grant.

(3) Comisia cooperează strâns cu ANS, ADS sau cu orice altă autoritate competentă a statelor membre în cauză.

(4) În cazul în care o autoritate contractantă intenționează să inițieze o procedură care are drept scop încheierea unui contract sau a unui acord de grant clasificat, autoritatea în cauză va solicita consiliere din partea Autorității de securitate a Comisiei cu privire la aspecte legate de caracterul clasificării și de elementele clasificate ale procedurii, pe durata tuturor etapelor acesteia.

(5) În cadrul normelor de punere în aplicare privind securitatea industrială se stabilesc, după consultarea Grupului de experți în materie de securitate al Comisiei, formulare și modele de contracte și subcontracte clasificate, acorduri de grant clasificate, anunțuri de participare, orientări privind împrejurările în care certificatele de securitate industrială (CSI) sunt obligatorii, instrucțiuni de securitate pentru program/proiect (ISP), anexe de securitate (AS), vizite, precum și transmiterea și transportul IUEC în cadrul contractelor clasificate sau al acordurilor de grant clasificate.

([1]) Regulamentul (CE, Euratom) nr. 1605/2002 al Consiliului din 25 iunie 2002 privind Regulamentul financiar aplicabil bugetului general al Comunităților Europene (JO L 248, 16.9.2002, p. 1).

(6) Comisia poate încheia contracte sau acorduri de grant clasificate prin care încredințează sarcini care implică sau necesită accesul la IUEC ori gestionarea sau păstrarea acestora de către operatori economici înregistrați într-un stat membru sau într-un stat terț cu care a fost încheiat un acord sau un acord administrativ în conformitate cu capitolul 7 din prezenta decizie.

Articolul 42

Elementele de securitate din cadrul unui contract clasificat sau al unui acord de grant clasificat

(1) Contractele sau acordurile de grant clasificate includ următoarele elemente de securitate:

Instrucțiuni de securitate pentru program sau proiect (ISP)

(a) „Instrucțiuni de securitate pentru program sau proiect" (ISP) înseamnă o listă de proceduri de securitate care sunt aplicate unui anumit program sau proiect în scopul standardizării procedurilor de securitate. Lista poate fi revizuită pe parcursul programului sau al proiectului.

(b) Direcția Generală Resurse Umane și Securitate elaborează o serie de ISP generice, iar departamentele Comisiei care răspund de programe sau proiecte ce presupun gestionarea sau păstrarea IUEC pot elabora, atunci când este cazul, ISP specifice, care se bazează pe ISP generice.

(c) Se elaborează ISP specifice în special pentru programele și proiectele care se caracterizează printr-un domeniu de aplicare ce prezintă o importanță, o amploare sau o complexitate deosebite ori prin multitudinea și/sau diversitatea contractanților, a beneficiarilor și a altor parteneri și părți interesate implicate, de exemplu în ceea ce privește statutul lor juridic. ISP specifice sunt elaborate de departamentul (departamentele) Comisiei care gestionează programul sau proiectul în cauză, în strânsă cooperare cu Direcția Generală Resurse Umane și Securitate.

(d) Direcția Generală Resurse Umane și Securitate prezintă Grupului de experți în materie de securitate al Comisiei, spre avizare, atât ISP generice, cât și ISP specifice.

Anexa de securitate

(a) „Anexa de securitate" (AS) înseamnă un set de condiții contractuale speciale, emis de autoritatea contractantă, care este parte integrantă a oricărui contract clasificat ce implică accesul la IUEC sau crearea de IUEC și care identifică cerințele de securitate sau elementele din cadrul contractului care necesită protecție de securitate.

(b) Cerințele de securitate specifice contractului sunt descrise într-o AS. Atunci când este cazul, AS cuprinde „Ghidul clasificărilor de securitate" (GCS) și este parte integrantă a contractului sau a subcontractului clasificat ori a acordului de grant clasificat.

(c) AS cuprinde dispozițiile prin care se solicită contractantului și/sau beneficiarului să respecte standardele minime prevăzute în prezenta decizie. Autoritatea contractantă se asigură că AS precizează că nerespectarea acestor standarde minime poate constitui un motiv suficient pentru rezilierea contractului sau a acordului de grant.

(2) Atât ISP, cât și AS cuprind un GCS cu titlu de element de securitate obligatoriu:

(a) „Ghid al clasificărilor de securitate" (GCS) înseamnă un document care descrie elementele clasificate ale unui program, proiect, contract sau acord de grant, precizând nivelurile aplicabile de clasificare de securitate. GCS poate fi extins pe toată durata programului, a proiectului, a contractului sau a acordului de grant, iar informațiile pot fi reclasificate sau declasificate; atunci când există un GCS, acesta face parte din AS.

(b) Înainte de a iniția o procedură de ofertare sau de a atribui un contract clasificat, departamentul relevant al Comisiei, în calitate de autoritate contractantă, stabilește clasificarea de securitate a tuturor informațiilor care urmează a fi puse la dispoziția candidaților și ofertanților sau a contractanților, precum și clasificarea de securitate a oricăror informații care urmează să fie create de contractant. În acest sens, departamentul în cauză elaborează un GCS care urmează să fie folosit pentru executarea contractului, în conformitate cu prezenta decizie și cu normele de punere în aplicare a acesteia, după consultarea Autorității de securitate a Comisiei.

(c) Pentru a stabili clasificarea de securitate a diferitelor elemente ale unui contract clasificat, se aplică următoarele principii:

(i) la pregătirea unui GCS, departamentul Comisiei, în calitate de autoritate contractantă, ia în considerare toate aspectele de securitate relevante, inclusiv clasificarea de securitate acordată informațiilor furnizate și aprobate în vederea utilizării în scopul contractului de către emitentul informațiilor;

(ii) nivelul general de clasificare al contractului nu poate să fie mai scăzut decât cel mai ridicat nivel de clasificare al oricăruia dintre elementele sale; și

(iii) atunci când este cazul, autoritatea contractantă ia legătura, prin intermediul Autorității de securitate a Comisiei, cu ANS, ADS sau cu orice altă autoritate de securitate competentă a statelor membre, în cazul în care apar schimbări în ceea ce privește clasificarea informațiilor create de contractanți sau furnizate acestora în cursul executării contractului sau în cazul oricăror modificări ulterioare ale GCS.

Articolul 43

Accesul la IUEC al personalului contractanților și al beneficiarilor

Autoritatea contractantă sau care acordă grantul se asigură că respectivul contract clasificat sau acord de grant clasificat conține dispoziții care să indice că personalul contractantului, al subcontractantului sau al beneficiarului care, pentru executarea contractului, a subcontractului sau a acordului de grant clasificat, solicită acces la IUEC, primește acces la IUEC numai în cazul în care:

(a) a primit o autorizare de securitate pentru nivelul corespunzător sau este autorizat într-un alt mod corespunzător odată ce a fost stabilită necesitatea de a cunoaște în cazul său;

(b) a fost instruit cu privire la normele și procedurile de securitate aplicabile pentru protecția IUEC și a confirmat că a luat cunoștință de responsabilitățile care îi revin în ceea ce privește protejarea acestor informații;

(c) a primit permisiunea de securitate la nivelul corespunzător pentru informațiile clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET din partea ANS, ADS sau a oricărei alte autorități competente.

Articolul 44

Autorizarea de securitate industrială

(1) „Autorizare de securitate industrială” (ASI) înseamnă o decizie administrativă a ANS, ADS sau a oricărei alte autorități de securitate competente conform căreia, în ceea ce privește securitatea, un obiectiv poate oferi un nivel de protecție adecvat IUEC clasificate la un anumit nivel de clasificare a securității.

(2) O ASI eliberată de ANS sau ADS ori de orice altă autoritate de securitate competentă a unui stat membru pentru a adeveri că, în conformitate cu actele cu putere de lege și dispozițiile administrative naționale, un operator economic poate proteja IUEC la nivelul de clasificare adecvat (CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET) în interiorul clădirilor sale este adresată Autorității de securitate a Comisiei, care o va transmite departamentului Comisiei care acționează în calitate de autoritate contractantă, înainte ca unui candidat, unui ofertant sau unui contractant ori unui solicitant sau beneficiar al unui grant să îi poată fi furnizate IUEC sau să i se acorde accesul la IUEC.

(3) Atunci când este cazul, autoritatea contractantă, prin intermediul Autorității de securitate a Comisiei, înștiințează ANS, ADS corespunzătoare sau orice altă autoritate de securitate competentă că executarea contractului necesită o ASI. Trebuie să se prezinte o ASI sau un CSP în cazul în care, pe parcursul procedurii de atribuire a achizițiilor sau de acordare a grantului, trebuie furnizate IUEC clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET.

(4) Autoritatea contractantă sau care acordă grantul nu atribuie un contract clasificat sau un acord de grant clasificat unui ofertant sau unui participant selectat înainte de a fi primit confirmarea eliberării unei ASI corespunzătoare, dacă o ASI este necesară, din partea ANS, a ADS sau a oricărei alte autorități de securitate competente a statului membru în care este înregistrat contractantul sau subcontractantul respectiv.

(5) Atunci când Autoritatea de securitate a Comisiei a fost notificată de către ANS, ADS sau de orice altă autoritate de securitate competentă emitentă a unei ASI în legătură cu orice modificări care afectează ASI în cauză, Autoritatea de securitate a Comisiei trebuie să informeze departamentul Comisiei care acționează în calitate de autoritate contractantă sau de autoritate care acordă grantul. În cazul subcontractelor, ANS, ADS sau orice altă autoritate de securitate competentă sunt informate în mod corespunzător.

(6) Retragerea unei ASI de către ANS, ADS relevantă sau de către orice altă autoritate de securitate competentă constituie un motiv suficient pentru ca autoritatea contractantă sau care acordă grantul să rezilieze un contract clasificat sau să excludă un candidat, un ofertant sau un solicitant din competiție. În modelele de contracte și de acorduri de grant care urmează să fie elaborate se include o dispoziție în acest sens.

Articolul 45

Dispoziții referitoare la contractele clasificate și la acordurile de grant clasificate

(1) În cazul în care unui candidat, unui ofertant sau unui solicitant îi sunt furnizate IUEC pe parcursul procedurii de atribuire a achizițiilor, procedura de ofertare sau cererea de propuneri cuprinde o dispoziție prin care candidatul, ofertantul sau solicitantul care nu prezintă o ofertă ori o propunere sau care nu este selectat,are obligația de a restitui, într-un termen specificat, toate documentele clasificate.

(2) Autoritatea contractantă sau autoritatea care acordă grantul înștiințează, prin intermediul Autorității de securitate a Comisiei, ANS, ADS competentă sau orice altă autoritate de securitate competentă în legătură cu faptul că a fost atribuit un contract clasificat sau un acord de grant clasificat, notificându-i totodată datele relevante, cum ar fi numele contractantului (contractanților) sau al beneficiarilor, durata contractului și nivelul maxim de clasificare.

(3) În cazul în care astfel de contracte sau de acorduri de grant sunt reziliate, autoritatea contractantă sau autoritatea care acordă grantul aduce această informație, prin intermediul Autorității de securitate a Comisiei, la cunoștința ANS, a ADS sau a oricărei alte autorități de securitate competente a statului membru în care este înregistrat contractantul sau beneficiarului grantului.

(4) În general, la rezilierea contractului clasificat sau a acordului de grant clasificat, contractantul sau beneficiarul grantului are obligația de a restitui autorității contractante sau care acordă grantul toate IUEC aflate în posesia sa.

(5) În AS se stabilesc dispoziții specifice privind distrugerea IUEC pe durata executării contractului clasificat sau a acordului de grant clasificat ori la rezilierea acestuia.

(6) În cazul în care contractantul sau beneficiarul grantului este autorizat să rețină IUEC după încetarea unui contract clasificat sau a unui acord de grant clasificat, standardele minime cuprinse în prezenta decizie sunt respectate în continuare, iar confidențialitatea IUEC este protejată de către contractant sau beneficiarul grantului.

Articolul 46

Dispoziții specifice referitoare la contractele clasificate

(1) Condițiile relevante pentru protecția IUEC pe care trebuie să le îndeplinească contractantul pentru a putea subcontracta sunt stabilite în procedura de ofertare și în contractul clasificat.

(2) Contractantul trebuie să obțină permisiunea autorității contractante înainte de a subcontracta oricare dintre părțile unui contract clasificat. Niciun subcontract care presupune accesul la IUEC nu poate fi atribuit subcontractanților înregistrați într-o țară terță, cu excepția cazului în care există un cadru normativ referitor la securitatea informațiilor, astfel cum se prevede la capitolul 7.

(3) 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.

(4) În ceea ce privește IUEC create sau gestionate de contractant, se consideră că emitentul acestora este Comisia, iar drepturile care îi revin emitentului sunt exercitate de autoritatea contractantă.

Articolul 47

Vizite legate de contractele clasificate

(1) În cazul în care un membru al personalului Comisiei sau al contractanților ori al beneficiarilor de granturi are nevoie de acces la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET în incintele celeilalte părți, în scopul executării unui contract clasificat sau a unui acord de grant clasificat, se organizează vizite în colaborare cu ANS, ADS sau cu orice altă autoritate de securitate competentă implicată. Autoritatea de securitate a Comisiei este informată cu privire la astfel de vizite. Cu toate acestea, în cadrul unor programe sau proiecte specifice, ANS, ADS sau orice altă autoritate de securitate competentă pot conveni, de asemenea, cu privire la o procedură care să permită organizarea în mod direct a unor astfel de vizite.

(2) Accesul vizitatorilor la IUEC legate de contractul clasificat se acordă pe baza deținerii unei permisiuni de securitate corespunzătoare și a respectării principiului necesității de a cunoaște.

(3) Vizitatorilor li se acordă accesul numai la IUEC legate de scopul vizitei.

(4) Dispoziții mai detaliate sunt prevăzute în normele de punere în aplicare.

(5) Respectarea dispozițiilor referitoare la vizitele întreprinse în legătură cu contractele clasificate, stabilite în prezenta decizie și în normele de punere în aplicare menționate la alineatul (4), este obligatorie.

Articolul 48

Transmiterea și transportul IUEC legate de contracte clasificate sau de acorduri de grant clasificate

(1) În ceea ce privește transmiterea IUEC prin mijloace electronice, se aplică dispozițiile relevante din capitolul 5 din prezenta decizie.

(2) În ceea ce privește transportul IUEC, se aplică dispozițiile relevante din capitolul 4 din prezenta decizie și din normele de punere în aplicare a acesteia, în conformitate cu actele cu putere de lege și dispozițiile administrative naționale.

(3) 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 și 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) înaintea oricărei deplasări transfrontaliere de materiale clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET, expeditorul întocmește un plan de transport aprobat de ANS, ADS sau de orice altă autoritate de securitate competentă implicată;

(d) transporturile se realizează, în măsura posibilului, pe rute directe și se finalizează cât mai rapid posibil, în funcție de împrejurări;

(e) atunci când este posibil, rutele de transport ar trebui să treacă numai prin state membre. Rutele care trec prin alte state decât statele membre ar trebui efectuate numai cu autorizația ANS/ADS sau a oricărei alte autorități de securitate competente atât din statul expeditorului, cât și din cel al destinatarului.

Articolul 49

Transferul IUEC către contractanții sau beneficiarii de granturi aflați în state terțe

IUEC sunt transferate contractanților sau beneficiarilor de granturi aflați în state terțe în conformitate cu măsurile de securitate convenite între Autoritatea de securitate a Comisiei, departamentul Comisiei în calitate de autoritate contractantă și ANS, ADS sau o altă autoritate de securitate competentă a țării terțe implicate în care este înregistrat contractantul sau beneficiarul grantului.

Articolul 50

Gestionarea informațiilor clasificate RESTREINT UE/EU RESTRICTED în contextul contractelor clasificate sau al acordurilor de grant clasificate

(1) Protecția informațiilor clasificate RESTREINT UE/EU RESTRICTED care sunt gestionate sau stocate în temeiul unor contracte clasificate sau al unor acorduri de grant clasificate se bazează pe principiile proporționalității și al rentabilității.

(2) Nu sunt necesare nicio ASI și niciun CSP în cadrul contractelor clasificate sau al acordurilor de grant clasificate care presupun gestionarea de informații clasificate la nivelul RESTREINT UE/EU RESTRICTED.

(3) Atunci când un contract sau un acord de grant prevede gestionarea unor informații clasificate RESTREINT UE/EU RESTRICTED într-un SIC gestionat de un contractant sau de beneficiarul unui grant, autoritatea contractantă sau care acordă grantul se asigură, după consultarea Autorității de securitate a Comisiei, că în contract sau în acordul de grant se specifică cerințele tehnice și administrative necesare în ceea ce privește acreditarea sau aprobarea SIC, care sunt proporționale cu riscul evaluat, luându-se în considerare toți factorii relevanți. Domeniul de aplicare al acreditării sau aprobării unui astfel de SIC este convenit de Autoritatea de securitate a Comisiei cu ANS sau ADS competentă.

CAPITOLUL 7

SCHIMBUL DE INFORMAȚII CLASIFICATE CU ALTE INSTITUȚII, AGENȚII, ORGANE ȘI OFICII ALE UNIUNII, CU STATELE MEMBRE, PRECUM ȘI CU STATE TERȚE ȘI ORGANIZAȚII INTERNAȚIONALE

Articolul 51

Principii de bază

(1) În cazul în care Comisia sau unul dintre departamentele sale stabilește că este necesar să facă schimb de IUEC cu o altă instituție, altă agenție, alt organ sau alt oficiu al Uniunii sau cu un stat terț ori cu o organizație internațională, se iau măsurile necesare în vederea instituirii unui cadru juridic sau administrativ adecvat în acest scop, care poate include acorduri privind securitatea informațiilor sau acorduri administrative încheiate în conformitate cu reglementările relevante.

(2) Fără a aduce atingere articolului 57, schimburile de IUEC cu o altă instituție, altă agenție, alt organ sau alt oficiu al Uniunii sau cu un stat terț ori cu o organizație internațională nu pot avea loc decât cu condiția instituirii unui astfel de cadru juridic sau administrativ adecvat și cu condiția să existe suficiente garanții cu privire la aplicarea de către instituția, agenția, organul sau oficiul Uniunii sau de către statul terț ori organizația internațională în cauză a unor principii de bază și standarde minime echivalente cu privire la protecția informațiilor clasificate ale UE.

Articolul 52

Schimbul de IUEC cu alte instituții, agenții, organe și oficii ale Uniunii

(1) Înainte de a încheia un acord administrativ privind schimbul de IUEC cu o altă instituție, altă agenție, alt organ sau alt oficiu al Uniunii, Comisia se asigură că instituția, agenția, organul sau oficiul Uniunii în cauză:

(a) aplică un cadru normativ privind protecția IUEC, care stabilește principii de bază și standarde minime echivalente cu cele stabilite în prezenta decizie și în normele de punere în aplicare a acesteia;

(b) aplică standarde și orientări de securitate cu privire la securitatea personalului, securitatea fizică, gestionarea IUEC și securitatea sistemelor informatice și de comunicații (SIC) care garantează un nivel echivalent de protecție a IUEC cu cel aplicat în cadrul Comisiei;

(c) marchează ca IUEC informațiile clasificate pe care le creează.

(2) Direcția Generală Resurse Umane și Securitate, în strânsă cooperare cu departamentele competente ale Comisiei, este serviciul responsabil în cadrul Comisiei pentru încheierea de acorduri administrative privind schimbul de IUEC cu alte instituții, agenții, organe sau oficii ale Uniunii.

(3) În general, acordurile administrative iau forma unui schimb de scrisori semnate de către directorul general al DG Resurse Umane și Securitate în numele Comisiei.

(4) Înainte de a încheia un acord administrativ privind schimbul de IUEC, Autoritatea de securitate a Comisiei efectuează o vizită de evaluare cu scopul de a analiza cadrul normativ privind protecția IUEC și de a verifica eficacitatea măsurilor puse în aplicare pentru protecția IUEC. Acordul administrativ intră în vigoare și schimburile de IUEC au loc numai dacă rezultatele acestei vizite de evaluare sunt satisfăcătoare, iar recomandările formulate în urma vizitei au fost respectate. Periodic, sunt organizate vizite de evaluare cu rol de monitorizare, în scopul de a se verifica dacă acordul administrativ este respectat și dacă măsurile de securitate în vigoare respectă în continuare principiile de bază și standardele minime convenite.

(5) În cadrul Comisiei, registratura IUEC gestionată de Secretariatul General constituie, în general, principalul punct de intrare și de ieșire în cadrul schimburilor de informații clasificate efectuate cu alte instituții, agenții, organe sau oficii ale Uniunii. Cu toate acestea, în cazul în care, din motive de securitate sau din motive organizaționale ori operaționale, în acest mod se asigură o protecție mai adecvată a IUEC, registraturile IUEC locale înființate în cadrul departamentelor Comisiei în conformitate cu prezenta decizie și cu normele de punere în aplicare a acesteia acționează ca punct de intrare și de ieșire pentru schimbul de informații clasificate referitoare la aspecte care țin de competența departamentelor în cauză ale Comisiei.

(6) Grupul de experți în materie de securitate al Comisiei este informat în legătură cu procesul încheierii unor acorduri administrative în temeiul alineatului (2).

Articolul 53

Schimbul de IUEC cu statele membre

(1) IUEC pot fi schimbate cu statele membre și comunicate acestora cu condiția ca statele membre să protejeze informațiile respective în conformitate cu cerințele aplicabile informațiilor clasificate care au o clasificare de securitate națională de nivel echivalent, astfel cum se indică în tabelul de echivalență a clasificărilor de securitate din anexa I.

(2) În cazul în care statele membre introduc în structurile sau rețelele Uniunii Europene informații clasificate care prezintă un marcaj național de clasificare a securității, Comisia protejează informațiile respective în conformitate cu cerințele aplicabile IUEC de nivel echivalent, astfel cum se precizează în tabelul de echivalență a clasificărilor de securitate din anexa I.

Articolul 54

Schimbul de IUEC cu state terțe și organizații internaționale

(1) În cazul în care Comisia consideră că există o necesitate de lungă durată privind schimbul de informații clasificate cu state terțe sau cu organizații internaționale, se iau măsurile necesare în vederea instituirii unui cadru juridic sau administrativ corespunzător în acest scop, care poate include acorduri privind securitatea informațiilor sau acorduri administrative încheiate în conformitate cu reglementările relevante.

(2) Acordurile privind securitatea informațiilor și acordurile administrative menționate la alineatul (1) conțin dispoziții menite să garanteze că, atunci când statele terțe sau organizațiile internaționale primesc IUEC, aceste informații beneficiază de protecția corespunzătoare nivelului lor de clasificare, pe baza unor standarde echivalente celor instituite prin prezenta decizie.

(3) Comisia poate încheia acorduri administrative în conformitate cu articolul 56 în cazul în care nivelul de clasificare a IUEC nu depășește, în general, nivelul RESTREINT UE/EU RESTRICTED.

(4) Acordurile administrative privind schimbul de informații clasificate menționate la alineatul (3) conțin dispoziții care garantează că, atunci când statele terțe sau organizațiile internaționale primesc IUEC, aceste informații beneficiază de protecția corespunzătoare nivelului lor de clasificare, pe baza unor standarde minime echivalente celor instituite prin prezenta decizie. Grupul de experți în materie de securitate al Comisiei este consultat cu privire la încheierea de acorduri privind securitatea informațiilor sau de acorduri administrative.

(5) Decizia de a comunica IUEC emise de Comisie către un stat terț sau o organizație internațională se ia de către departamentul Comisiei, în calitatea sa de emitent al IUEC în cadrul Comisiei, de la caz la caz, în funcție de caracterul și conținutul informațiilor respective, de necesitatea de a cunoaște a destinatarului lor și de avantajul pe care acest fapt l-ar prezenta pentru Uniune. În cazul în care Comisia nu este emitentul informațiilor clasificate a căror comunicare este solicitată sau al materialelor-sursă pe care aceste informații le-ar putea conține, departamentul Comisiei care deține informațiile clasificate în cauză trebuie să solicite, mai întâi, consimțământul scris al emitentului. În cazul în care emitentul nu poate fi identificat, departamentul Comisiei care deține respectivele informații clasificate își asumă această răspundere în locul emitentului, după consultarea Grupului de experți în materie de securitate al Comisiei.

Articolul 55

Acordurile privind securitatea informațiilor

(1) Acordurile privind securitatea informațiilor cu un stat terț sau cu organizații internaționale sunt încheiate în conformitate cu articolul 218 din TFUE.

(2) Acordurile privind securitatea informațiilor:

(a) stabilesc principiile de bază și standardele minime care reglementează schimbul de informații clasificate dintre Uniune și un stat terț sau o organizație internațională;

(b) prevăd măsuri tehnice de punere în aplicare care urmează a fi convenite între autoritățile de securitate competente ale instituțiilor și organismelor relevante ale Uniunii și autoritatea de securitate competentă a statului terț sau a organizației internaționale în cauză. Aceste măsuri țin seama în mod corespunzător de nivelul de protecție prevăzut de reglementările, structurile și procedurile existente în materie de securitate în statul terț sau în cadrul organizației internaționale în cauză;

(c) prevăd că, anterior schimbului de informații clasificate în temeiul acordului, trebuie să se verifice că destinatarul este în măsură să protejeze și să păstreze în mod corespunzător informațiile clasificate care îi sunt puse la dispoziție.

(3) Atunci când se stabilește că este necesar să se facă schimb de informații clasificate în conformitate cu articolul 51 alineatul (1), Comisia se consultă cu Serviciul European de Acțiune Externă, cu Secretariatul General al Consiliului și cu alte instituții și organe ale Uniunii, atunci când este cazul, pentru a decide dacă trebuie să se transmită o recomandare în conformitate cu articolul 218 alineatul (3) din TFUE.

(4) IUEC sunt schimbate prin mijloace electronice numai atunci când acest lucru este autorizat în mod explicit prin acordul privind securitatea informațiilor sau prin măsurile tehnice de punere în aplicare.

(5) În cadrul Comisiei, registratura IUEC gestionată de Secretariatul General constituie, în general, principalul punct de intrare și de ieșire în cadrul schimburilor de informații clasificate efectuate cu state terțe și organizații internaționale. Cu toate acestea, în cazul în care, din motive de securitate sau din motive organizaționale ori operaționale, în acest mod se asigură o protecție mai adecvată a IUEC, registraturile IUEC locale înființate în cadrul departamentelor Comisiei în conformitate cu prezenta decizie și cu normele de punere în aplicare a acesteia acționează ca punct de intrare și de ieșire pentru schimbul de informații clasificate referitoare la aspecte care țin de competența departamentelor în cauză ale Comisiei.

(6) Pentru a evalua eficacitatea reglementărilor, a structurilor și a procedurilor de securitate din statul terț sau din cadrul organizației internaționale interesate, Comisia ia parte la vizite de evaluare, în cooperare cu alte instituții, agenții sau organe ale Uniunii, de comun acord cu statul terț sau cu organizația internațională în cauză. Cu ocazia acestor vizite de evaluare se analizează:

(a) cadrul normativ aplicabil pentru protecția informațiilor clasificate;

(b) orice caracteristici specifice ale politicii de securitate și ale modului de organizare a securității în statul terț sau organizația internațională, care pot avea un impact asupra nivelului de clasificare al informațiilor care pot fi schimbate;

(c) măsurile și procedurile de securitate în vigoare; și

(d) procedurile privind autorizarea de securitate pentru nivelul de clasificare al IUEC care urmează să fie comunicate.

Articolul 56

Acorduri administrative

(1) În cazul în care, în contextul unui cadru politic sau juridic al Uniunii, există o necesitate pe termen lung privind schimbul de informații clasificate, în general, cel mult la nivelul RESTREINT UE/EU RESTRICTED. cu un stat terț sau cu o organizație internațională, dar Autoritatea de securitate a Comisiei, după consultarea Grupului de experți în materie de securitate al Comisiei, a stabilit îndeosebi că partea în cauză nu deține un sistem de securitate suficient de dezvoltat pentru a permite încheierea unui acord privind securitatea informațiilor, Comisia poate să încheie un acord administrativ cu autoritățile competente ale statului terț sau ale organizației internaționale în cauză.

(2) În general, astfel de acorduri administrative iau forma unui schimb de scrisori.

(3) Înainte de încheierea acordului se efectuează o vizită de evaluare. Grupul de experți în materie de securitate al Comisiei trebuie să fie informat cu privire la rezultatul vizitei de evaluare. În cazul în care intervin motive excepționale pentru schimbul urgent de informații clasificate, pot fi comunicate IUEC, cu condiția să se ia toate măsurile necesare pentru organizarea vizitei de evaluare cât mai curând.

(4) IUEC nu sunt schimbate prin mijloace electronice decât în cazul în care acest lucru este prevăzut în mod explicit în acordul administrativ.

Articolul 57

Comunicarea ad-hoc excepțională a IUEC

(1) În cazul în care nu este în vigoare niciun acord privind securitatea informațiilor sau un acord administrativ, iar Comisia sau unul dintre departamentele acesteia stabilește că există o necesitate cu caracter excepțional, în contextul unui cadru politic sau juridic al Uniunii, de a comunica IUEC unui stat terț sau unei organizații internaționale, Autoritatea de securitate a Comisiei verifică, în măsura posibilului, împreună cu autoritățile de securitate ale statului terț sau ale organizației internaționale în cauză că reglementările, structurile și procedurile de securitate ale statului sau organizației în cauză sunt astfel concepute încât garantează faptul că IUEC comunicate vor fi protejate la standarde la fel de stricte precum cele stabilite prin prezenta decizie.

(2) Decizia de a comunica IUEC către statul terț sau organizația internațională în cauză,, este adoptată de Comisie după consultarea Grupului de experți în materie de securitate al Comisiei, pe baza unei propuneri din partea membrului Comisiei responsabil în materie de securitate.

(3) În urma deciziei Comisiei de a comunica IUEC și sub rezerva consimțământului scris acordat în prealabil de către emitent, inclusiv de către emitenții materialelor-sursă pe care aceste informații le-ar putea conține, departamentul competent al Comisiei transmite informațiile în cauză, care prezintă un marcaj de comunicare ce indică statul terț sau organizația internațională destinatară. Înaintea sau în timpul comunicării efective, partea terță în cauză se angajează în scris să protejeze IUEC primite în conformitate cu principiile de bază și standardele minime stabilite în prezenta decizie.

CAPITOLUL 8

DISPOZIȚII FINALE

Articolul 58

Înlocuirea deciziei anterioare

Prezenta decizie abrogă și înlocuiește Decizia 2001/844/CE, CECO, Euratom a Comisiei ([1]).

Articolul 59

Informațiile clasificate create înainte de intrarea în vigoare a prezentei decizii

(1) Toate IUEC clasificate în conformitate cu Decizia 2001/844/CE, CECO, Euratom continuă să fie protejate în conformitate cu dispozițiile corespunzătoare ale prezentei decizii.

(2) Toate informațiile clasificate deținute de Comisie la data la care a intrat în vigoare Decizia 2001/844/CE, CECO, Euratom, cu excepția datelor clasificate ale Euratom:

(a) dacă au fost create de Comisie, se consideră în continuare că au fost reclasificate RESTREINT UE în mod automat, cu excepția cazului în care autorul lor a decis să le clasifice altfel până la 31 ianuarie 2002 și a informat toți destinatarii documentului respectiv;

(b) dacă au fost create de autori din afara Comisiei, își păstrează clasificarea inițială și, prin urmare, sunt tratate ca IUEC de nivel echivalent, cu excepția cazului în care autorul acceptă declasificarea sau declasarea lor.

Articolul 60

Norme de punere în aplicare și notificări de securitate

(1) Dacă este necesar, adoptarea normelor de punere în aplicare a prezentei decizii face obiectul unei decizii separate a Comisiei prin care este abilitat, în deplină conformitate cu regulamentul intern de procedură, membrul Comisiei responsabil în materie de securitate.

(2) După abilitarea sa, în urma deciziei susmenționate a Comisiei, membrul Comisiei responsabil în materie de securitate poate elabora notificări de securitate care să stabilească orientări în materie de securitate și cele mai bune practici, care intră în domeniul de aplicare al prezentei decizii și al normelor de punere în aplicare a acesteia.

(3) Comisia poate delega directorului Direcției Generale Resurse Umane și Securitate, pe baza unei decizii de delegare separate, în deplină conformitate cu regulamentul intern de procedură, sarcinile menționate la primul și al doilea paragraf din prezentul articol.

Articolul 61

Intrarea în vigoare

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

Adoptată la Bruxelles, 13 martie 2015.

Pentru Comisie

Președintele

Jean-Claude JUNCKER

([1]) Decizia 2001/844/CE a Comisiei din 29 noiembrie 2001 de modificare a regulamentului său de procedură (JO L 317, 3.12.2001, p. 1).

ANEXA I

ECHIVALENȚA CLASIFICĂRILOR DE SECURITATE

UE	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Euratom	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Belgia	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	nota (1) de mai jos
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Republica Cehă	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danemarca	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Germania	Streng geheim	Geheim	VS (2) – Vertraulich	VS – Nur für den Dienstgebrauch
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irlanda	Top Secret	Secret	Confidential	Restricted
Grecia	Άκρως Απόρρητο Abr.: ΑΑΠ	Απόρρητο Abr.: (ΑΠ)	Εμπιστευτικό Abr.: (ΕΜ)	Περιορισμένης Χρήσης Abr.: (ΠΧ)
Spania	Secreto	Reservado	Confidencial	Difusión Limitada
Franța	Très Secret Défense	Secret Défense	Confidentiel Défense	nota (3) de mai jos
Croația	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italia	Segretissimo	Segreto	Riservatissimo	Riservato
Cipru	Άκρως Απόρρητο Abr.: (ΑΑΠ)	Απόρρητο Abr.: (ΑΠ)	Εμπιστευτικό Abr.: (ΕΜ)	Περιορισμένης Χρήσης Abr.: (ΠΧ)
Letonia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lituania	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Ungaria	„Szigorúan titkos!”	„Titkos!”	„Bizalmas!”	„Korlátozott terjesztésű!”
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Țările de Jos	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polonia	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalia	Muito Secreto	Secreto	Confidencial	Reservado

UE	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
România	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenia:	Strogo tajno	Tajno	Zaupno	Interno
Slovacia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finlanda	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Suedia ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Regatul Unit	UK TOP SECRET	UK SECRET	Niciun echivalent ([5])	UK OFFICIAL – SENSITIVE

([1]) Diffusion restreinte/Beperkte Verspreiding nu reprezintă o clasificare de securitate în Belgia. Belgia gestionează și protejează informațiile clasificate ca „RESTREINT UE/EU RESTRICTED” într-un mod nu mai puțin strict decât standardele și procedurile descrise în normele de securitate ale Consiliului Uniunii Europene.

([2]) Germania: VS = Verschlusssache.

([3]) Franța nu folosește clasificarea „RESTREINT” în sistemul său național. Franța gestionează și protejează informațiile clasificate ca „RESTREINT UE/EU RESTRICTED” într-un mod nu mai puțin strict decât standardele și procedurile descrise în normele de securitate ale Consiliului Uniunii Europene.

([4]) Suedia: marcajele clasificărilor de securitate din rândul de sus sunt utilizate de autoritățile de apărare, iar marcajele din rândul de jos, de celelalte autorități.

([5]) Regatul Unit gestionează și protejează informațiile clasificate „CONFIDENTIEL UE/EU CONFIDENTIAL” în conformitate cu cerințele de protecție de securitate pentru categoria „UK SECRET”.

ANEXA II

LISTA ABREVIERILOR

Acronim	Sens
AC	autoritate criptografică
AAC	autoritate de aprobare criptografică
CCTV	televiziune cu circuit închis
ADMC	autoritate de distribuire a materialului criptografic
SCI	sisteme informatice și de comunicații care gestionează IUEC
ASD	autoritate de securitate desemnată
IUEC	informații UE clasificate
ASI	autorizare de securitate industrială
AI	asigurarea informațiilor
AAI	autoritate de asigurare a informațiilor
SDI	sisteme de detectare a intruziunilor
TI	tehnologia informației
LSO	ofițer local de securitate
ANS	autoritate națională de securitate
ASP	autorizare de securitate a personalului
CASP	certificare a autorizării de securitate a personalului
ISP	instrucțiuni de securitate pentru program/proiect
OCR	ofițer de control al registraturii
AAS	autoritate de acreditare în materie de securitate
AS	anexă de securitate
GCS	ghidul clasificărilor de securitate
SecOP	proceduri operaționale de securitate
AT	autoritate TEMPEST
TFUE	Tratatul privind funcționarea Uniunii Europene

ANEXA III

LISTA AUTORITĂȚILOR NAȚIONALE DE SECURITATE

BELGIA

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles/Brussel
Tel. secretariat: +32 25014542
Fax: +32 25014596
E-mail: nvo-ans@diplobel.fed.be

BULGARIA

State Commission on Information Security
90 Cherkovna Str.
1505 Sofia
Tel. +359 29333600
Fax: +359 29873750
E-mail: dksi@government.bg
Site internet: www.dksi.bg

REPUBLICA CEHĂ

Národní bezpečnostní úřad
(Autoritatea Națională de Securitate)
Na Popelce 2/16
150 06 Praha 56
Tel. +420 257283335
Fax: +420 257283110
E-mail: czech.nsa@nbu.cz
Site internet: www.nbu.cz

DANEMARCA

Politiets Efterretningstjeneste
(Serviciul Danez de Informații de Securitate)
Klausdalsbrovej 1
2860 Søborg
Tel. +45 33148888
Fax: +45 33430190

Forsvarets Efterretningstjeneste
(Serviciul Danez de Informații de Apărare)
Kastellet 30
2100 Copenhagen Ø
Tel. +45 33325566
Fax: +45 33931320

GERMANIA

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
11014 Berlin
Tel. +49 30186810
Fax: +49 30186811441
E-mail: oesIII3@bmi.bund.de

ESTONIA

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn
Tel. +372 7170113 0019, +372 7170117
Fax: +372 7170213
E-mail: nsa@mod.gov.ee

GRECIA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Τηλ.: +30 2106572045 (ώρες γραφείου)
+ 30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279; + 30 2106577612

Personalul general de apărare națională a Greciei
Direcția Sectorială Informații Militare
Direcția de Contrainformații de Securitate
GR-STG 1020 Holargos – Athens
Tel. +30 2106572045
+ 30 2106572009
Fax: +30 2106536279, +30 2106577612

SPANIA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid
Tel. +34 913725000
Fax: +34 913725808
E-mail: nsa-sp@areatec.com

FRANȚA

Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Paris 07 SP
Tel. +33 171758177
Fax: + 33 171758200

CROAȚIA

Office of the National Security Council
Croatian NSA
Jurjevska 34
HR-10000 Zagreb
Croația
Tel. +385 14681222
Fax: + 385 14686049
Website: www.uvns.hr

IRLANDA

National Security Authority
Department of Foreign Affairs
76-78 Harcourt Street
Dublin 2
Tel. +353 14780822
Fax: +353 14082959

ITALIA

Presidenza del Consiglio dei Ministri
D.I.S. – U.C.Se.
Via di Santa Susanna, 15
00187 Roma
Tel. +39 0661174266
Fax: +39 064885273

CIPRU

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministerul Apărării
Personalul militar al ministrului
Autoritatea Națională de Securitate (ANS)
4 Emanuel Roidi street
1432 Nicosia
Tel. +357 22807569, +357 22807643,
+357 22807764
Fax: +357 22302351
E-mail: cynsa@mod.gov.cy

LETONIA

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV-1001 Riga
Tel. +371 67025418
Fax: +371 67025454
E-mail: ndi@sab.gov.lv

LITUANIA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(Comisia de coordonare a protecției secretelor Republicii Lituania Autoritatea Națională de Securitate)
Gedimino 40/1
LT-01110 Vilnius
Tel. +370 706 66701, +370 706 66702
Fax: +370 706 66700
E-mail: nsa@vsd.lt

LUXEMBURG

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxemburg
Tel. +352 24782210 central
+ 352 24782253 direct
Fax: +352 24782243

UNGARIA

Nemzeti Biztonsági Felügyelet
(Autoritatea Națională de Securitate a Ungariei)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tel. +36 (1) 7952303
Fax: +36 (1) 7950344

Postal address:
H-1357 Budapest, PO Box 2
E-mail: nbf@nbf.hu
Website: www.nbf.hu

MALTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Tel. +356 21249844
Fax: +356 25695321

ȚĂRILE DE JOS

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Tel. +31 703204400
Fax: +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag
Tel. +31 703187060
Fax: +31 703187522

AUSTRIA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien
Tel. +43 1531152594
Fax: +43 1531152615
E-mail: ISK@bka.gv.at

POLONIA

Agencja Bezpieczeństwa Wewnętrznego – ABW
(Agenția de Securitate Internă)
2A Rakowiecka St.
00-993 Warszawa
Tel. +48 22 58 57 944
Fax: +48 22 58 57 443
E-mail: nsa@abw.gov.pl
Website: www.abw.gov.pl

PORTUGALIA

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Tel. +351 213031710
Fax: +351 213031711

ROMÂNIA

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA – ORNISS National Registry Office for Classified Information)
4 Mureș Street
012275 Bucharest
Tel. +40 212245830
Fax: +40 212240714
E-mail: nsa.romania@nsa.ro
Website: www.orniss.ro

SLOVENIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
SI-1000 Ljubljana
Tel. +386 14781390
Fax: +386 14781399
E-mail: gp.uvtp@gov.si

SLOVACIA

Národný bezpečnostný úrad
(Autoritatea Națională de Securitate)
Budatínska 30
P.O. Box 16
850 07 Bratislava
Tel. +421 268692314
Fax: +421 263824005
Website: www.nbusr.sk

FINLANDA

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Tel. 16055890
Fax: +358 916055140
E-mail: NSA@formin.fi

SUEDIA

Utrikesdepartementet
(Ministerul Afacerilor Externe)
SSSB
SE-103 39 Stockholm
Tel. +46 84051000
Fax: +46 87231176
E-mail: ud-nsa@foreign.ministry.se

REGATUL UNIT

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Tel. 1: +44 2072765649
Tel. 2: +44 2072765497
Fax: +44 2072765651
E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk