Acest document reprezintă un instrument de documentare, iar instituțiile nu își asumă responsabilitatea pentru conținutul său.

►**B**

DECIZIA COMISIEI

din 29 noiembrie 2001

de modificare a regulamentului său de procedură

[notificată cu numărul C(2001) 3031]

(2001/844/CE, CECO, Euratom)

(JO L 317, 3.12.2001, p. 1)

Astfel cum a fost modificată prin:

		Jurnalul Oficial		
		NR.	Pagina	Data
►**M1**	Decizia 2005/94/CE, Euratom Comisiei din 3 februarie 2005	L 31	66	4.2.2005
►**M2**	Decizia 2006/70/CE, Euratom Comisiei din 31 ianuarie 2006	L 34	32	7.2.2006
►**M3**	Decizia 2006/548/CE, Euratom Comisiei din 2 august 2006	L 215	38	5.8.2006
►**M4**	Regulamentul (UE) nr. 519/2013 al Comisiei din 21 februarie 2013	L 158	74	10.6.2013

▼B

DECIZIA COMISIEI

din 29 noiembrie 2001

de modificare a regulamentului său de procedură

[notificată cu numărul C(2001) 3031]

(2001/844/CE, CECO, Euratom)

COMISIA COMUNITĂȚILOR EUROPENE,

având în vedere Tratatul de instituire a Comunității Europene, în special articolul 218 alineatul (2),

având în vedere Tratatul de instituire a Comunității Europene a Cărbunelui și Oțelului, în special articolul 16,

având în vedere Tratatul de instituire a Comunității Europene a Energiei Atomice, în special articolul 131,

având în vedere Tratatul privind Uniunea Europeană, în special articolul 28 alineatul (1) și articolul 41 alineatul (1),

DECIDE:

Articolul 1

Dispozițiile Comisiei în materie de securitate, al căror text este anexat la prezenta decizie, se adaugă la regulamentul de procedură al Comisiei, ca anexă.

Articolul 2

Prezenta decizie intră în vigoare la data publicării în *Jurnalul Oficial al Comunităților Europene*.

Se aplică de la 1 decembrie 2001.

▼B

ANEXĂ

DISPOZIȚIILE COMISIEI ÎN MATERIE DE SECURITATE

Întrucât:

(1) Pentru a dezvolta activitățile Comisiei în domenii care necesită un anumit nivel de confidențialitate, este necesar să se înființeze un sistem global de securitate aplicabil Comisiei, celorlalte instituții, organisme, birouri și agenții instituite în temeiul sau în conformitate cu Tratatul CE sau cu Tratatul privind Uniunea Europeană, statelor membre, precum și oricărui alt destinatar al unor informații clasificate ale Uniunii Europene, denumite în continuare „informații clasificate UE”.

(2) Pentru a asigura eficiența sistemului de securitate astfel instituit, Comisia va pune informațiile clasificate UE doar la dispoziția organismelor externe care oferă garanții privind adoptarea tuturor măsurilor necesare aplicării unor norme strict echivalente cu prezentele dispoziții.

(3) Prezentele dispoziții sunt adoptate fără a aduce atingere Regulamentului nr. 3 din 31 iulie 1958 de punere în aplicare a articolului 24 din Tratatul de instituire a Comunității Europene a Energiei Atomice [1], Regulamentului (CE) nr. 1588/90 al Consiliului din 11 iunie 1990 privind transmiterea către Biroul Statistic al Comunităților Europene a datelor aflate sub incidența confidențialității statistice [2] și Deciziei C (95) 1510 final a Comisiei din 23 noiembrie 1995 privind protecția sistemelor informatice.

(4) Sistemul de securitate al Comisiei se bazează pe principiile prevăzute în Decizia 2001/264/CE a Consiliului din 19 martie 2001 de adoptare a regulamentului de securitate al Consiliului [3] în vederea asigurării bunei funcționări a procesului decizional al Uniunii.

(5) Comisia subliniază importanța asocierii, dacă este cazul, a celorlalte instituții la normele și standardele de confidențialitate care sunt necesare pentru protejarea intereselor Uniunii și ale statelor sale membre.

(6) Comisia recunoaște necesitatea creării propriului concept de securitate, ținând cont de toate elementele de securitate și de caracterul specific al Comisiei ca instituție.

(7) Prezentele dispoziții sunt adoptate fără a aduce atingere articolul 255 din tratat și Regulamentului (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei [4].

▼M2

(8) Prezentele dispoziții nu aduc atingere articolului 286 din tratat, nici Regulamentului (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și libera circulație a acestor date.

▼B

Articolul 1

Normele Comisiei privind securitatea sunt prezentate în anexă.

---

[1] JO L 17, 6.10.1958, p. 406/58.
[2] JO L 151, 15.6.1990, p. 1.
[3] JO L 101, 11.4.2001, p. 1.
[4] JO L 145, 31.5.2001, p. 43.

▼B

Articolul 2

(1) Membrul Comisiei responsabil cu probleme de securitate adoptă măsurile necesare pentru a asigura, la prelucrarea informațiilor clasificate ale UE, că normele menționate în articolul 1 sunt respectate în cadrul Comisiei de către funcționari și de către ceilalți angajați, precum și de către personalul detașat la Comisie, dar și în interiorul tuturor sediilor Comisiei, inclusiv în reprezentanțele și birourile din Uniune și în delegațiile sale din țări terțe, ori de către contractanții externi ai Comisiei.

▼M3

Atunci când un contract sau o înțelegere privind subvențiile între Comisie și un contractant extern sau un beneficiar implică prelucrarea de informații clasificate UE în spațiile contractantului sau ale beneficiarului, măsurile corespunzătoare care trebuie luate de contractantul extern sau beneficiarul respectiv pentru a asigura respectarea, în cadrul prelucrării informațiilor clasificate UE, a normelor menționate la articolul 1 fac parte integrantă din contract sau din înțelegerea privind subvențiile.

▼B

(2) Statele membre, celelalte instituții, organisme, birouri și agenții instituite în temeiul sau în conformitate cu tratatele pot primi informații clasificate UE cu condiția ca acestea să asigure, la prelucrarea informațiilor clasificate UE, respectarea, în cadrul serviciilor și al sediilor lor, a unor norme strict echivalente cu cele menționate la articolul 1, în special de către:

(a) membrii reprezentanțelor permanente ale statelor membre la Uniunea Europeană, precum și de către membrii delegațiilor naționale care participă la reuniunile Comisiei sau ale organelor sale sau la alte activități ale Comisiei;

(b) alți membri ai administrațiilor naționale ale statelor membre care prelucrează informații clasificate UE, indiferent dacă aceștia lucrează pe teritoriul statelor membre sau în străinătate;

(c) contractanții externi și personalul detașat care prelucrează informații clasificate UE.

Articolul 3

Statele terțe, organizațiile internaționale și alte organisme pot primi informații clasificate UE cu condiția ca acestea să asigure, la prelucrarea acestor informații, respectarea unor norme strict echivalente cu cele menționate la articolul 1.

Articolul 4

În respectarea principiilor de bază și a standardelor minime de securitate cuprinse în partea I din anexă, membrul Comisiei însărcinat cu probleme de securitate poate lua măsuri în conformitate cu partea II din anexă.

Articolul 5

De la data punerii lor în aplicare, prezentele dispoziții înlocuiesc:

(a) Decizia C (94) 3282 a Comisiei din 30 noiembrie 1994 privind măsurile de securitate aplicabile informațiilor clasificate furnizate sau transmise în legătură cu activitățile Uniunii Europene;

(b) Decizia C (99) 423 a Comisiei din 25 februarie 1999 privind procedurile prin care funcționarii și alți angajați ai Comisiei Europene pot fi autorizați să aibă acces la informațiile clasificate deținute de Comisie.

▼B

Articolul 6

De la data punerii în aplicare a prezentelor dispoziții, toate informațiile clasificate deținute de Comisie până la această dată, cu excepția datelor clasificate ale Euratom:

(a) dacă au fost create de Comisie, sunt considerate reclasificate implicit ca „►**M1** RESTREINT UE ◄”, cu excepția cazului în care autorul lor decide să le clasifice altfel până la 31 ianuarie 2002. În acest caz, autorul informează toți destinatarii documentului respectiv;

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

▼B

ANEXĂ

NORME PRIVIND SECURITATEA

Cuprins

PARTEA I: PRINCIPII DE BAZĂ ŞI STANDARDE MINIME DE SECURITATE

1. INTRODUCERE
2. PRINCIPII GENERALE
3. FUNDAMENTELE SECURITĂŢII
4. PRINCIPIILE SECURITĂŢII INFORMAŢIEI
4.1. **Obiective**
4.2. **Definiţii**
4.3. **Clasificare**
4.4. **Obiectivele măsurilor de securitate**
5. ORGANIZAREA SECURITĂŢII
5.1. **Standarde minime comune**
5.2. **Organizare**
6. SECURITATEA PERSONALULUI
6.1. **Autorizarea personalului**
6.2. **Registre privind autorizarea personalului**
6.3. **Instruirea personalului în domeniul securităţii**
6.4. **Responsabilităţile conducerii**
6.5. **Statutul de securitate a personalului**
7. SECURITATEA FIZICĂ
7.1. **Nevoia de protecţie**
7.2. **Verificare**
7.3. **Securitatea clădirilor**
7.4. **Planuri de urgenţă**
8. SECURITATEA INFORMAŢIILOR
9. PROTECŢIA ÎMPOTRIVA SABOTAJULUI ŞI A ALTOR FORME DE DISTRUGERE INTENŢIONATĂ
10. COMUNICAREA DE INFORMAŢII CLASIFICATE UNOR STATE TERŢE SAU UNOR ORGANIZAŢII INTERNAŢIONALE

PARTEA II ORGANIZAREA SECURITĂŢII ÎN CADRUL COMISIEI

11. MEMBRUL COMISIEI ÎNSĂRCINAT CU PROBLEME DE SECURITATE
12. GRUPUL CONSULTATIV PENTRU POLITICA DE SECURITATE A COMISIEI
13. COMITETUL DE SECURITATE AL COMISIEI
14. ►M2 DIRECŢIA PENTRU SECURITATE A COMISIEI ◄
15. INSPECŢII DE SECURITATE
16. CLASIFICĂRI, IDENTIFICATORI ŞI MĂRCI DE SECURITATE
16.1. **Niveluri de clasificare**

▼B

16.2. **Identificatori de securitate**

16.3. **Mărci**

16.4. **Aplicarea clasificării**

16.5. **Aplicarea identificatorilor de securitate**

17. GESTIONAREA CLASIFICĂRII

17.1. **Generalități**

17.2. **Aplicarea clasificărilor**

17.3. **Declasarea și declasificarea**

18. SECURITATEA FIZICĂ

18.1. **Generalități**

18.2. **Cerințe de securitate**

18.3. **Măsuri de securitate fizică**

18.3.1. *Zone de securitate*

18.3.2. *Zonă administrativă*

18.3.3. *Controale la intrare și ieșire*

18.3.4. *Patrulări*

18.3.5. *Containere de securitate și seifuri*

18.3.6. *Dispozitive de închidere*

18.3.7. *Controlul cheilor și al combinațiilor*

18.3.8. *Dispozitive de detectare a intruziunilor*

18.3.9. *Echipamente aprobate*

18.3.10. *Protejarea fizică a copiatoarelor și faxurilor*

18.4. **Protecția împotriva vederii și ascultării clandestine**

18.4.1. *Protecția împotriva vederii*

18.4.2. *Protecția împotriva ascultării*

18.4.3. *Introducerea echipamentelor electronice și de înregistrare*

18.5. **Zone protejate tehnic**

19. NORME GENERALE PRIVIND PRINCIPIUL NEVOII DE A CUNOAȘTE ȘI AUTORIZĂRILE DE SECURITATE ALE PERSONALULUI UE

19.1. **Generalități**

19.2. **Norme specifice privind accesul la informațiile ►M1 TRES SECRET UE/EU TOP SECRET ◄**

19.3. **Norme specifice privind accesul la informații ►M1 SECRET UE ◄ și ►M1 CONFIDENTIEL UE ◄**

19.4. **Norme specifice privind accesul la informații ►M1 RESTREINT UE ◄**

19.5. **Transferuri**

19.6. **Instrucțiuni speciale**

▼B

20. PROCEDURĂ DE AUTORIZARE DE SECURITATE PENTRU FUNCȚIONARI ȘI ALȚI ANGAJAȚI AI COMISIEI

21. PREGĂTIREA, DISTRIBUIREA, TRANSMITEREA, SECURITATEA PERSONALĂ A CURIERILOR ȘI COPII SUPLIMENTARE, TRADUCERI ȘI EXTRASE ALE DOCUMENTELOR CLASIFICATE UE

21.1. **Pregătire**

21.2. **Distribuire**

21.3. **Transmiterea documentelor clasificate UE**

21.3.1. *Ambalare, confirmări de primire*

21.3.2. *Transmiterea în cadrul unei clădiri sau al unui grup de clădiri*

21.3.3. *Transmiterea în interiorul unei țări*

21.3.4. *Transmiterea de la un stat la altul*

21.3.5. *Transmiterea documentelor* ►M1 *RESTREINT UE* ◄

21.4. **Securitatea personală a curierilor**

21.5. **Mijloace electronice și alte mijloace de transmitere tehnică**

21.6. **Copii suplimentare, traduceri și extrase ale documentelor clasificate UE**

22. REGISTRATURI ICUE, REGRUPĂRI, VERIFICĂRI, ARHIVARE ȘI DISTRUGEREA ICUE

22.1. **Registraturi locale ICUE**

22.2. **Registratura** ►M1 **TRES SECRET UE/EU TOP SECRET** ◄

22.2.1. *Generalități*

22.2.2. *Registratura centrală* ►M1 *TRES SECRET UE/EU TOP SECRET* ◄

22.2.3. *Registraturi secundare* ►M1 *TRES SECRET UE/EU TOP SECRET* ◄

22.3. **Inventarieri, regrupări și verificări ale documentelor clasificate UE**

22.4. **Arhivarea informațiilor clasificate UE**

22.5. **Distrugerea documentelor clasificate UE**

22.6. **Distrugere în situații de urgență**

23. MĂSURI DE SECURITATE PENTRU REUNIUNI SPECIFICE ORGANIZATE ÎN AFARA SEDIILOR COMISIEI ȘI CARE IMPLICĂ INFORMAȚII CLASIFICATE UE.

23.1. **Generalități**

23.2. **Responsabilități**

23.2.1. ►M2 *Direcția pentru Securitate a Comisiei* ◄

23.2.2. *Ofițerul de securitate al reuniunii (MSO)*

23.3. **Măsuri de securitate**

23.3.1. *Zone de securitate*

23.3.2. *Permise*

23.3.3. *Controlul echipamentelor foto și audio*

▼B

23.3.4. *Verificarea servietelor, a computerelor portabile și a pachetelor*

23.3.5. *Securitatea tehnică*

23.3.6. *Documentele delegațiilor*

23.3.7. *Păstrarea în siguranță a documentelor*

23.3.8. *Inspectarea birourilor*

23.3.9. *Eliminarea deșeurilor clasificate UE*

24. ÎNCĂLCĂRI ALE SECURITĂȚII ȘI COMPROMITEREA INFORMAȚIILOR CLASIFICATE UE

24.1. **Definiții**

24.2. **Raportarea încălcărilor normelor de securitate**

24.3. **Acțiuni în justiție**

25. PROTECȚIA INFORMAȚIILOR CLASIFICATE UE PRELUCRATE ÎN SISTEME DE TEHNOLOGIA INFORMAȚIEI ȘI DE COMUNICAȚII

25.1. **Introducere**

25.1.1. *Generalități*

25.1.2. *Amenințări asupra sistemelor și vulnerabilitățile acestora*

25.1.3. *Principalul scop al măsurilor de securitate*

25.1.4. *Declarația privind cerințele de securitate specifice unui sistem (SSRS)*

25.1.5. *Moduri de operare de securitate*

25.2. **Definiții**

25.3. **Responsabilități în materie de securitate**

25.3.1. *Generalități*

25.3.2. *Autoritatea de acreditare de securitate (SAA)*

25.3.3. *Autoritatea INFOSEC (IA)*

25.3.4. *Proprietarul sistemelor tehnice (TSO)*

25.3.5. *Proprietarul informației (IO)*

25.3.6. *Utilizatori*

25.3.7. *Formarea INFOSEC*

25.4. **Măsuri de securitate fără caracter tehnic**

25.4.1. *Securitatea personalului*

25.4.2. *Securitatea fizică*

25.4.3. *Controlul accesului la un sistem*

25.5. **Măsuri tehnice de securitate**

25.5.1. *Securitatea informațiilor*

25.5.2. *Controlul și contabilizarea informațiilor*

25.5.3. *Manipularea și controlul suporturilor informatice de stocare mobile*

▼B

25.5.4. *Declasificarea și distrugerea suporturilor informatice de stocare*

25.5.5. *Securitatea comunicațiilor*

25.5.6. *Securitatea privind instalarea și radiațiile*

25.6. **Securitatea în cursul prelucrării**

25.6.1. *Proceduri de operare de securitate (SecOP)*

25.6.2. *Gestionarea protecției/configurației produselor software*

25.6.3. *Verificarea prezenței unor produse software dăunătoare (malicious software) sau a unor viruși informatici*

25.6.4. *Întreținere*

25.7. **Achiziții**

25.7.1. *Generalități*

25.7.2. *Acreditare*

25.7.3. *Evaluare și certificare*

25.7.4. *Verificarea sistematică a caracteristicilor de securitate pentru acreditarea continuă*

25.8. **Utilizare temporară sau ocazională**

25.8.1. *Securitatea microcomputerelor/computerelor personale*

25.8.2. *Utilizarea de echipamente IT private pentru activități oficiale ale Comisiei*

25.8.3. *Utilizarea de echipamente IT aparținând contractanților sau furnizate de un stat pentru activitățile oficiale ale Comisiei*

26. COMUNICAREA DE INFORMAȚII CLASIFICATE UE UNOR STATE TERȚE SAU UNOR ORGANIZAȚII INTERNAȚIONALE

26.1.1. *Principii care reglementează comunicarea de informații clasificate UE*

26.1.2. *Niveluri*

26.1.3. *Acorduri de securitate*

APENDICELE 1: **Comparație între clasificările naționale de securitate**

APENDICELE 2: **Ghid practic de clasificare**

APENDICELE 3: **Linii directoare pentru comunicarea de informații clasificate UE unor state terțe sau unor organizații internaționale: Nivelul 1 de cooperare**

APENDICELE 4: **Linii directoare pentru comunicarea de informații clasificate UE unor state terțe sau unor organizații internaționale: Nivelul 2 de cooperare**

APENDICELE 5: **Linii directoare pentru comunicarea de informații clasificate UE unor state terțe sau unor organizații internaționale: Nivelul 3 de cooperare**.

APENDICELE 6: **Lista abrevierilor**

▼B

PARTEA I: PRINCIPII DE BAZĂ ŞI STANDARDE MINIME DE SECURITATE

1. INTRODUCERE

Prezentele dispoziţii stabilesc principiile de bază şi standardele minime de securitate care trebuie respectate în mod adecvat de către Comisie în toate punctele sale de lucru precum şi de către toţi destinatarii ICUE, astfel încât să se asigure securitatea şi să existe certitudinea stabilirii unui standard comun de protecţie.

2. PRINCIPII GENERALE

Politica de securitate a Comisiei face parte integrantă din politica sa de gestionare internă generală şi, prin urmare, se bazează pe principiile care reglementează politica sa generală.

Aceste principii includ legalitatea, transparenţa, răspunderea şi subsidiaritatea (proporţionalitatea).

Legalitatea indică necesitatea de a menţine strict în cadrul legal executarea funcţiilor de securitate şi necesitatea de a respecta cerinţele legale. De asemenea, înseamnă că responsabilităţile din domeniul securităţii trebuie să se bazeze pe dispoziţiile legale adecvate. Se aplică integral dispoziţiile din Statutul funcţionarilor, în special articolul 17 privind obligaţia de discreţie a personalului în ceea ce priveşte informaţiile Comisiei şi titlul său VI privind măsurile disciplinare. În fine, acest principiu înseamnă că încălcările normelor de securitate în domeniile de responsabilitate ale Comisiei trebuie tratate în conformitate cu politica Comisiei privind acţiunile disciplinare şi cu politica sa de cooperare cu statele membre în domeniul dreptului penal.

Transparenţa indică nevoia de claritate în ceea ce priveşte toate normele şi dispoziţiile de securitate, de echilibru între diversele servicii şi diversele domenii (securitatea fizică faţă de protecţia informaţiilor etc.) şi nevoia unei politici coerente şi structurate de conştientizare a securităţii. Transparenţa defineşte, de asemenea, nevoia unor orientări scrise clare în punerea în aplicare a măsurilor de securitate.

Răspunderea înseamnă că responsabilităţile din domeniul securităţii vor fi clar definite. În plus, indică nevoia de a testa periodic corecta executare a acestor responsabilităţi.

Subsidiaritatea, sau proporţionalitatea, înseamnă că securitatea este organizată la cel mai jos nivel posibil şi cât mai aproape posibil de Direcţiunile Generale şi de serviciile Comisiei. Subsidiaritatea înseamnă, de asemenea, că activităţile de securitate se limitează la elementele pentru care se justifică cu adevărat. În fine, acest principiu înseamnă că măsurile de securitate sunt proporţionale cu interesele care trebuie protejate şi cu ameninţările reale sau potenţiale care planează asupra acestor interese, permiţând o apărare care să determine cât mai puţine perturbări posibile.

3. FUNDAMENTELE SECURITĂŢII

Fundamentele unei bune securităţi sunt:

(a) în cadrul fiecărui stat membru, o organizaţie naţională de securitate însărcinată cu:

1. colectarea şi înregistrarea informaţiilor privind spionajul, sabotajul, terorismul sau activităţile subversive şi

2. furnizarea către guvern şi, prin intermediul acestuia, către Comisie, de informaţii şi sfaturi privind natura ameninţărilor la adresa securităţii şi mijloacele de protecţie împotriva acestora;

▼B

(b) în cadrul fiecărui stat membru și în cadrul Comisiei, o autoritate tehnică INFOSEC (IA) însărcinată cu colaborarea cu autoritatea de securitate în cauză pentru a furniza informații și sfaturi privind amenințările tehnice la adresa securității și mijloacele de protecție împotriva acestora;

(c) colaborarea periodică între departamentele guvernamentale și serviciile competente din cadrul instituțiilor europene pentru a stabili și a recomanda, după caz:

1. persoanele, informațiile și resursele care trebuie protejate și

2. standardele comune de protecție;

(d) cooperarea strânsă între ►M2 Direcția pentru Securitate a Comisiei ◄ și serviciile de securitate ale altor instituții europene și cu Biroul de securitate al NATO (NOS).

4. PRINCIPIILE SECURITĂȚII INFORMAȚIEI

4.1. **Obiective**

Securitatea informațiilor are următoarele obiective principale:

(a) salvgardarea informațiilor clasificate UE (ICUE) împotriva spionajului, compromiterii sau divulgării neautorizate;

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

(c) salvgardarea sediilor Comisiei care adăpostesc informații UE împotriva sabotajelor și a actelor intenționate de deteriorare;

(d) în caz de eșec, evaluarea daunelor cauzate, limitarea consecințelor acestora și adoptarea măsurilor necesare de remediere.

4.2. **Definiții**

În sensul prezentelor norme:

(a) termenul „informații clasificate UE” (ICUE) înseamnă orice informație sau material a cărui divulgare neautorizată ar putea cauza prejudicii de diverse niveluri la adresa intereselor UE sau la adresa unuia sau a mai multora dintre statele sale membre, indiferent dacă informația în cauză provine din cadrul UE sau este primită de la state membre, state terțe sau organizații internaționale;

(b) termenul „document” înseamnă orice scrisoare, notă, proces verbal, raport, memorandum, semnal/mesaj, schiță, fotografie, diapozitiv, film, hartă, grafic, plan, caiet, șablon, indigo, bandă de mașină de scris sau de imprimantă, bandă magnetică, casetă, disc de computer, CD-ROM sau alt suport fizic pe care se înregistrează informații;

(c) termenul „material” înseamnă un „document” conform definiției de la litera (b), precum și orice alt element de echipament, deja fabricat sau în curs de fabricație;

(d) termenul „nevoie de a cunoaște” înseamnă necesitatea unui angajat individual de a avea acces la informații clasificate UE pentru a putea îndeplini o funcție sau o sarcină;

(e) „autorizație” înseamnă o decizie a ►M2 directorul Direcției pentru securitate a Comisiei ◄ de a permite accesul unei persoane la ICUE până la un anumit nivel, pe baza rezultatului pozitiv al unei examinări de securitate (procedură de abilitare), efectuată de o autoritate națională de securitate în temeiul legislației naționale;

▼B

(f) termenul „clasificare” înseamnă alocarea unui nivel adecvat de securitate informațiilor a căror divulgare neautorizată ar putea cauza prejudicii de diverse niveluri la adresa intereselor Comisiei și ale statelor membre;

(g) termenul „declasare” (déclassement) înseamnă o reducere a nivelului de clasificare;

(h) termenul „declasificare” (déclassification) înseamnă anularea oricărei clasificări;

(i) termenul „autoritate de origine” înseamnă autorul, autorizat corespunzător, al unui document clasificat; în cadrul Comisiei, șefii de departamente pot autoriza personalul din subordine să elaboreze ICUE;

(j) termenul „departamente ale Comisiei” înseamnă departamentele și serviciile Comisiei, inclusiv cabinetele, din toate punctele de lucru, inclusiv Centrul comun de cercetare, reprezentanțele și birourile din Uniune și delegațiile din țările terțe.

4.3. **Clasificare**

(a) În ceea ce privește confidențialitatea, este nevoie de atenție și experiență pentru selectarea informațiilor și a materialelor care trebuie protejate și pentru evaluarea gradului de protecție necesar. Este foarte important ca nivelul de protecție să corespundă gradului de securitate al informației sau al materialului care trebuie protejat. Pentru a asigura buna circulație a informațiilor, se iau măsuri pentru a evita atât clasificarea excesivă, cât și clasificarea insuficientă.

(b) Sistemul de clasificare este un instrument de aplicare a acestor principii; un sistem similar de clasificare se aplică pentru planificarea și organizarea măsurilor de luptă împotriva spionajului, sabotajului, terorismului și a altor amenințări, astfel încât să se asigure cel mai înalt grad de protecție celor mai importante sedii care adăpostesc informații clasificate și celor mai sensibile puncte din interiorul acestora.

(c) Responsabilitatea pentru clasificarea informațiilor îi revine exclusiv autorității de origine a informațiilor în cauză.

(d) Nivelul de clasificare poate fi bazat exclusiv pe conținutul informațiilor în cauză.

(e) Dacă mai multe informații sunt grupate împreună, nivelul de clasificare care trebuie aplicat grupului este cel puțin egal cu nivelul cel mai înalt de clasificare. Unui grup de informații i se poate, totuși, aloca o clasificare mai înaltă decât cea a părților sale componente.

(f) Clasificările sunt alocate doar atunci când este necesar și pentru cât timp este necesar.

4.4. **Obiectivele măsurilor de securitate**

Măsurile de securitate:

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

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

▼B

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

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

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

5. ORGANIZAREA SECURITĂȚII

5.1. **Standarde minime comune**

Comisia asigură respectarea unor standarde minime comune de securitate de către toți destinatarii ICUE, din cadrul instituției și care țin de competența sa, de exemplu de către toate departamentele și toți contractanții săi, astfel încât să existe certitudinea că informațiile clasificate UE transmise sunt prelucrate cu aceleași precauții. Aceste standarde minime includ criteriile de autorizare a personalului și procedurile de protecție a informațiilor clasificate UE.

Comisia permite accesul organismelor externe la ICUE doar cu condiția ca acestea să asigure, la prelucrarea ICUE, respectarea unor dispoziții cel puțin strict echivalente cu aceste standarde minime.

▼M3

Aceste standarde minimale se aplică, de asemenea, atunci când Comisia conferă, prin contract sau înțelegere privind subvențiile, entităților industriale sau altor entități sarcini care implică, necesită și/sau conțin informații clasificate UE; aceste standarde minimale comune sunt cuprinse în secțiunea 27 din partea II.

▼B

5.2. **Organizare**

În cadrul Comisiei, securitatea este organizată la două niveluri:

(a) la nivelul Comisiei în ansamblu, există un Birou de securitate al Comisiei cu o autoritate de acreditare de securitate (SAA), care acționează și ca autoritate Crypto (CrA), și ca autoritate TEMPEST, și cu o autoritate INFOSEC (IA), și una sau mai multe registraturi centrale ICUE, fiecare cu unul sau mai mulți ofițeri de control ai registraturii (RCO);

(b) la nivelul departamentelor Comisiei, sunt însărcinați cu securitatea unul sau mai mulți ofițeri locali de securitate (LSO), unul sau mai mulți ofițeri centrali de securitate informatică (CISO), ofițeri locali de securitate informatică (LISO) și registraturi locale ale informațiilor clasificate UE cu unul sau mai mulți ofițeri de control ai registraturii;

(c) organele centrale de securitate furnizează organelor locale de securitate instrucțiuni operaționale.

6. SECURITATEA PERSONALULUI

6.1. **Autorizarea personalului**

Toate persoanele care trebuie să aibă acces la informații clasificate ►M1 CONFIDENTIEL UE ◄ sau de nivel superior trebuie să fie evaluate în mod adecvat, înainte de autorizarea accesului. O evaluare similară este necesară pentru persoanele ale căror sarcini implică operarea tehnică sau întreținerea sistemelor informatice și de comunicare care conțin informații clasificate. Această evaluare este concepută astfel încât să determine dacă persoanele în cauză:

(a) sunt de o loialitate de necontestat;

▼B

(b) dau dovadă de un caracter și de o discreție care nu pun la îndoială integritatea lor în utilizarea informațiilor clasificate sau

(c) pot fi vulnerabile la presiuni externe sau din alte surse.

În procedura de evaluare se acordă o atenție specială persoanelor:

(d) cărora urmează să le fie permis accesul la informații ►M1 TRES SECRET UE/EU TOP SECRET ◄;

(e) care ocupă posturi implicând accesul periodic la un volum semnificativ de informații ►M1 SECRET UE ◄;

(f) ale căror sarcini le conferă accesul special la sisteme informatice și de comunicații securizate și care oferă astfel posibilitatea de a accesa în mod neautorizat volume mari de informații clasificate UE sau de a compromite grav misiunea prin acte de sabotaj tehnic.

În cazurile prevăzute la literele (d), (e) și (f), se utilizează în cea mai mare măsură posibilă tehnica de investigare a antecedentelor.

În cazul în care persoane care nu au „nevoia de a cunoaște” urmează a fi angajate în condiții care le-ar putea permite accesul la informații clasificate UE (de exemplu, mesageri, agenți de securitate, personal de întreținere și curățenie etc.), aceștia sunt în prealabil supuși unei evaluări adecvate în ceea ce privește securitatea.

6.2. **Registre privind autorizarea personalului**

Toate departamentele Comisiei care utilizează informații clasificate UE sau care adăpostesc sisteme informatice sau de comunicații securizate țin un registru al autorizațiilor acordate personalului propriu. Fiecare autorizație este verificată ori de câte ori este necesar pentru a se asigura că este adecvată funcției pe care o ocupă persoana în cauză; autorizația este reverificată cu prioritate ori de câte ori apar indicii noi care arată că menținerea persoanei în cauză într-un post care permite accesul la informații clasificate nu mai este compatibilă cu interesele de securitate. Ofițerul local de securitate al departamentului Comisiei ține registrul autorizațiilor din domeniul aflat sub controlul său.

6.3. **Instruirea personalului în domeniul securității**

Toți membrii personalului care ocupă posturi în cadrul cărora pot avea acces la informații clasificate sunt instruiți complet, la preluarea postului și la intervale regulate, cu privire la securitatea necesară și procedurile pentru asigurarea acesteia. Membrii personalului în cauză trebuie să certifice în scris faptul că au citit și că înțeleg pe deplin dispozițiile curente de securitate.

6.4. **Responsabilitățile conducerii**

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

6.5. **Statutul de securitate al personalului**

Se instituie proceduri care să permită, în momentul în care se obțin informații nefavorabile privind o anumită persoană, a determina dacă persoana în cauză ocupă un post care necesită accesul la informații clasificate sau dacă are acces la sisteme informatice sau de comunicații securizate și a informa ►M2 Direcția pentru Securitate a Comisiei ◄. Dacă se stabilește că această persoană constituie un risc de securitate, ea este exclusă sau îndepărtată de la sarcinile în cadrul cărora ar putea pune în pericol securitatea.

▼B

7. SECURITATEA FIZICĂ

7.1. **Nevoia de protecție**

Nivelul măsurilor de securitate fizică care trebuie aplicate pentru a asigura protecția informațiilor clasificate UE este proporțional cu clasificarea și volumul informațiilor și materialelor deținute și cu amenințarea la care acestea sunt expuse. Toți cei care dețin informații clasificate UE aplică practici uniforme privind clasificarea informațiilor în cauză și respectă standarde comune de protecție în ceea ce privește păstrarea, transmiterea și distrugerea informațiilor și materialelor care trebuie protejate.

7.2. **Verificare**

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

7.3. **Securitatea clădirilor**

Clădirile care adăpostesc informații clasificate UE sau sisteme informatice sau de comunicații securizate sunt protejate împotriva accesului neautorizat. Natura protecției asigurate informațiilor clasificate, de exemplu ferestre cu gratii, încuietori pentru uși, paznici la intrări, sisteme automate de control al accesului, verificări și patrule de securitate, sisteme de alarmă, sisteme de detectare a efracțiilor și câini de pază, depinde de:

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

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

(c) natura fizică și amplasarea clădirii.

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

7.4. **Planuri de urgență**

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

8. SECURITATEA INFORMAȚIILOR

Securitatea informațiilor (INFOSEC) se referă la identificarea și aplicarea măsurilor de securitate pentru protejarea informațiilor clasificate UE prelucrate, stocate sau transmise prin sisteme de comunicații, informatice sau prin alte sisteme electronice împotriva pierderii, accidentale sau intenționate, a caracterului confidențial, a integrității sau a disponibilității. Se adoptă măsuri adecvate pentru a preveni accesul unor utilizatori neautorizați la informații clasificate UE, pentru a preveni refuzarea accesului unor utilizatori autorizați la informații clasificate UE și pentru a preveni coruperea, modificarea neautorizată sau ștergerea informațiilor clasificate UE.

▼B

9. PROTECȚIA ÎMPOTRIVA SABOTAJULUI ȘI A ALTOR FORME DE DISTRUGERE INTENȚIONATĂ

Precauțiile fizice pentru protecția instalațiilor importante care adăpostesc informații clasificate reprezintă cele mai bune mijloace de protecție și securitate împotriva sabotajului și a distrugerii intenționate; doar autorizarea personalului nu reprezintă un substitut eficient. Organismului național competent îi revine sarcina de a furniza informații privind acțiuni de spionaj, sabotaj, terorism și alte activități subversive.

10. COMUNICAREA DE INFORMAȚII CLASIFICATE UNOR STATE TERȚE SAU UNOR ORGANIZAȚII INTERNAȚIONALE

Decizia de a comunica unui stat terț sau unei organizații internaționale informații clasificate UE emise de Comisie este adoptată de colegiul membrilor Comisiei. Dacă autoritatea de origine a informațiilor a căror comunicare este solicitată nu este Comisia, aceasta din urmă obține în prealabil consimțământul autorității de origine. Dacă autoritatea de origine nu poate fi stabilită, Comisia își asumă responsabilitatea acesteia.

În cazul în care Comisia primește informații clasificate din partea unor state terțe, a unor organizații internaționale sau din partea altor terți, informațiilor în cauză li se acordă o protecție adecvată clasificării lor și echivalentă cu standardele stabilite în prezentele dispoziții pentru informațiile clasificate UE sau cu standarde mai ridicate solicitate de partea terță care comunică informațiile în cauză. Se pot organiza verificări reciproce.

Principiile menționate anterior se aplică în conformitate cu dispozițiile detaliate din partea II secțiunea 26 și din apendicele 3, 4 și 5.

PARTEA II: ORGANIZAREA SECURITĂȚII ÎN CADRUL COMISIEI

11. MEMBRUL COMISIEI ÎNSĂRCINAT CU PROBLEME DE SECURITATE

Membrul Comisiei însărcinat cu probleme de securitate:

(a) pune în aplicarea politica de securitate a Comisiei;

(b) analizează problemele de securitate care îi sunt adresate de Comisie și organismele sale competente;

(c) examinează problemele care implică modificări ale politicii de securitate a Comisiei, în strânsă colaborare cu autoritățile naționale pentru securitate (sau alte autorități competente) ale statelor membre (denumite în continuare „ANS”).

Membrul Comisiei însărcinat cu probleme de securitate are, în special, următoarele responsabilități:

(a) să coordoneze toate problemele de securitate legate de activitățile Comisiei;

(b) să adreseze autorităților desemnate ale statelor membre solicitări pentru eliberarea de către ANS a unor autorizații de securitate pentru personalul angajat în cadrul Comisiei în conformitate cu secțiunea 20;

(c) să investigheze sau să solicite investigarea oricărei scurgeri de informații clasificate UE care, conform dovezilor *prima facie*, a avut loc în cadrul Comisiei;

(d) să solicite autorităților de securitate competente inițierea investigațiilor în cazul în care aparent a avut loc o scurgere de informații în afara Comisiei și să coordoneze investigațiile în cazul în care sunt implicate mai multe autorități de securitate;

(e) să efectueze verificări periodice ale dispozițiilor de securitate destinate protecției informațiilor clasificate UE;

▼B

(f) să mențină o legătură strânsă cu toate autoritățile de securitate implicate pentru a realiza coordonarea generală a securității;

(g) să revizuiască continuu politica și procedurile de securitate ale Comisiei și, după caz, să elaboreze recomandările adecvate. În această privință, membrul Comisiei însărcinat cu probleme de securitate prezintă Comisiei planul anual de inspecție elaborat de ►M2 Direcția pentru Securitate a Comisiei ◄.

12. GRUPUL CONSULTATIV PENTRU POLITICA DE SECURITATE A COMISIEI

Se instituie un Grup consultativ pentru politica de securitate a Comisiei. Grupul este format din membrul Comisiei însărcinat cu probleme de securitate sau delegatul acestuia, care asigură președinția grupului, și din reprezentanți ai ANS din fiecare stat membru. Pot fi invitați, de asemenea, reprezentanți ai altor instituții europene. De asemenea, pot fi invitați să participe la reuniuni reprezentanți ai agențiilor descentralizate ale CE și UE relevante, atunci când se discută aspecte care îi privesc.

Grupul consultativ pentru politica de securitate a Comisiei se reunește la cererea președintelui sau a oricăruia dintre membrii săi. Grupul are sarcina de a examina și evalua toate problemele de securitate relevante și de a prezenta recomandări Comisiei, după caz.

▼M2

13. COMITETUL DE SECURITATE AL COMISIEI

Se instituie un Comitet de securitate al Comisiei. Acesta este format din directorul general al Administrației și Personalului, care este președintele comitetului, un membru din cabinetul comisarului responsabil cu probleme de securitate, un membru din cabinetul președintelui, secretarul general adjunct care prezidează grupul de gestionare a crizelor, directorii generali ai Serviciului Juridic, ai Direcției Generale Relații Externe, ai Direcției Generale Justiție, Libertate și Securitate, ai Centrului Comun de Cercetare, ai Direcției Generale pentru Informatică și ai Serviciului de Audit Intern și directorul Direcției pentru Securitate a Comisiei, sau reprezentanții acestora. Pot fi invitați și alți funcționari ai Comisiei. Atribuția comitetului este aceea de a evalua măsurile de securitate din cadrul Comisiei și de a face recomandări în acest domeniu către membrul Comisiei responsabil cu probleme de securitate.

▼B

14. ►M2 DIRECȚIA PENTRU SECURITATE A COMISIEI ◄

Pentru a îndeplini sarcinile menționate în secțiunea 11, membrul Comisiei însărcinat cu probleme de securitate are la dispoziția sa ►M2 Direcția pentru Securitate a Comisiei ◄ în vederea coordonării, supravegherii și punerii în aplicare a măsurilor de securitate.

►M2 Directorul Direcției pentru Securitate a Comisiei ◄ este consilierul principal în probleme de securitate al membrului Comisiei însărcinat cu probleme de securitate, acesta deținând funcția de secretar al Grupului consultativ pentru probleme de securitate. În această privință, acesta conduce lucrările de actualizare a reglementărilor de securitate și coordonează măsurile de securitate cu autoritățile competente ale statelor membre și, după caz, cu organizațiile internaționale cu care Comisia a încheiat acorduri de securitate. În acest scop, el acționează ca ofițer de legătură.

►M2 Directorul Direcției pentru Securitate a Comisiei ◄ este responsabil cu acreditarea sistemelor și rețelelor IT din cadrul Comisiei. ►M2 Directorul Direcției pentru Securitate a Comisiei ◄ decide, de comun acord cu ANS competentă, în privința acreditării sistemelor și rețelelor IT care implică Comisia, pe de o parte, și orice alt destinatar al informațiilor clasificate UE, pe de altă parte.

▼B

15. INSPECȚII DE SECURITATE

►M2 Direcția pentru Securitate a Comisiei ◄ efectuează inspecții periodice privind dispozițiile de securitate pentru protecția informațiilor clasificate UE.

►M2 Direcția pentru Securitate a Comisiei ◄ poate fi asistat în îndeplinirea sarcinilor sale de serviciile de securitate ale altor instituții UE care dețin ICUE sau de Autoritățile naționale de securitate ale statelor membre ([1]).

La cererea unui stat membru, ANS a statului membru în cauză poate efectua o inspecție a ICUE în cadrul Comisiei, împreună și de comun acord cu ►M2 Direcția pentru Securitate a Comisiei ◄.

16. CLASIFICĂRI, IDENTIFICATORI ȘI MĂRCI DE SECURITATE

16.1. **Niveluri de clasificare** ([2])

Informațiile sunt clasificate la următoarele niveluri (a se vedea, de asemenea, apendicele 2):

►M1 TRES SECRET UE/EU TOP SECRET ◄: această clasificare se aplică doar informațiilor și materialelor a căror divulgare neautorizată ar putea cauza prejudicii extrem de grave intereselor esențiale ale Uniunii Europene sau ale unuia sau mai multora dintre statele sale membre.

►M1 SECRET UE ◄: această clasificare se aplică doar informațiilor și materialelor a căror divulgare neautorizată ar putea cauza prejudicii grave intereselor esențiale ale Uniunii Europene sau ale unuia sau mai multora dintre statele sale membre.

►M1 CONFIDENTIEL UE ◄: această clasificare se aplică doar informațiilor și materialelor a căror divulgare neautorizată ar putea dăuna intereselor esențiale ale Uniunii Europene sau ale unuia sau mai multora dintre statele sale membre.

►M1 RESTREINT UE ◄: această clasificare se aplică doar informațiilor și materialelor a căror divulgare neautorizată ar putea dezavantaja interesele Uniunii Europene sau ale unuia sau mai multora dintre statele sale membre.

Nu sunt permise alte clasificări.

16.2. **Identificatori de securitate**

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

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

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

16.3. **Mărci**

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

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

([1]) Fără a aduce atingere Convenției de la Viena din 1961 privind relațiile diplomatice și Protocolului privind privilegiile și imunitățile Comunităților Europene din 8 aprilie 1965.

([2]) A se vedea un tabel comparativ al clasificărilor de securitate ale UE, NATO, UEO și ale statelor membre în apendicele 1.

▼B

Marca PESA se aplică pe documentele și copiile documentelor privind securitatea și apărarea Uniunii sau a unuia sau mai multora dintre statele sale membre sau privind gestionarea militară sau nemilitară a situațiilor de criză.

16.4. **Aplicarea clasificării**

Clasificarea se aplică după cum urmează:

(a) pe documentele ►M1 RESTREINT UE ◄, prin mijloace mecanice sau electronice;

(b) pe documentele ►M1 CONFIDENTIEL UE ◄, prin mijloace mecanice, manual sau prin tipărire pe hârtie înregistrată și ștampilată în prealabil;

(c) pe documentele ►M1 SECRET UE ◄ și ►M1 TRES SECRET UE/EU TOP SECRET ◄, prin mijloace mecanice sau manual.

16.5. **Aplicarea identificatorilor de securitate**

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

17. GESTIONAREA CLASIFICĂRII

17.1. **Generalități**

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

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

Funcționarii și alți angajați ai Comisiei clasifică, declasează sau declasifică informațiile conform instrucțiunilor primite de la șeful de departament sau cu acordul acestuia.

Procedurile detaliate pentru prelucrarea documentelor clasificate au fost astfel concepute încât să asigure că acestea fac obiectul unei protecții adecvate a informațiilor pe care le conțin.

Numărul de persoane autorizate să emită documente ►M1 TRES SECRET UE/EU TOP SECRET ◄ este păstrat la minimum, iar numele persoanelor în cauză sunt înscrise pe o listă întocmită de ►M2 Direcția pentru Securitate a Comisiei ◄.

17.2. **Aplicarea clasificărilor**

Clasificarea unui document este determinată de nivelul de sensibilitate al conținutului său, în conformitate cu definiția din secțiunea 16. Este importantă utilizarea corectă și cu moderație a clasificării. Acest lucru este valabil în special pentru clasificarea ►M1 TRES SECRET UE/EU TOP SECRET ◄.

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

Apendicele 2 conține un ghid practic de clasificare.

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

▼B

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

Accesul public este în continuare reglementat de Regulamentul (CE) nr. 1049/2001.

17.3. **Declasarea și declasificarea**

Documentele clasificate UE pot fi declasate sau declasificate doar cu permisiunea autorității de origine și, dacă este necesar, după discuții cu alte părți interesate. Declasarea sau declasificarea se confirmă în scris. Autoritatea de origine trebuie să comunice modificarea destinatarilor documentelor, iar aceștia din urmă trebuie să informeze eventualii destinatari ulteriori, cărora le-au transmis documentele în cauză sau copii ale acestora, cu privire la modificare.

Dacă este posibil, autoritățile de origine specifică pe documentele clasificate o dată, o perioadă sau un eveniment de la care conținutul poate fi declasat sau declasificat. Altfel, acestea revizuiesc documentele cel târziu o dată la cinci ani pentru a asigura necesitatea menținerii clasificării inițiale.

18. SECURITATEA FIZICĂ

18.1. **Generalități**

Principalele obiective ale măsurilor de securitate fizică sunt prevenirea accesului oricărei persoane neautorizate la informații și/sau materiale clasificate UE, prevenirea furtului sau degradării echipamentelor sau a altor bunuri și prevenirea hărțuirii sau a oricărui alt tip de agresiune asupra personalului, a altor angajați și a vizitatorilor.

18.2. **Cerințe de securitate**

Toate sediile, zonele, clădirile, sălile, sistemele informatice și de comunicații etc. în care sunt păstrate și/sau prelucrate informații și materiale clasificate UE sunt protejate prin măsuri adecvate de securitate fizică.

La determinarea nivelului de securitate fizică necesar, se ține cont de toți factorii relevanți, precum:

(a) clasificarea informațiilor și/sau a materialelor;

(b) volumul și forma (de exemplu, pe suport de hârtie, pe suport informatic) ale informațiilor deținute;

(c) amenințarea evaluată local venită din partea serviciilor de informații care au ca țintă UE, statele membre și/sau alte instituții sau părți terțe care dețin informații clasificate UE, în special acte de sabotaj, terorism și alte activități subversive și/sau criminale.

Măsurile de securitate fizică aplicate sunt concepute pentru:

(a) a împiedica orice intrare frauduloasă sau prin forță a unui intrus;

(b) a descuraja, a împiedica și a detecta acțiunile personalului neloial;

(c) a împiedica accesul la informațiile clasificate UE al persoanelor care nu sunt motivate de nevoia de a cunoaște.

▼B

18.3. **Măsuri de securitate fizică**

18.3.1. *Zone de securitate*

Zonele în care sunt prelucrate și stocate informații clasificate ►M1 CONFIDENTIEL UE ◄ sau de nivel superior sunt organizate și structurate astfel încât să corespundă uneia dintre următoarele categorii:

(a) zonă de securitate de clasa I: o zonă în care informațiile clasificate ►M1 CONFIDENTIEL UE ◄ sau de nivel superior sunt prelucrate și stocate astfel încât intrarea în zonă constituie, în practică, acces la informații clasificate. O astfel de zonă necesită:

(i) un perimetru clar definit și protejat în care sunt controlate toate intrările și ieșirile;

(ii) un sistem de control al intrărilor, care permite doar accesul persoanelor verificate adecvat și special autorizate pentru accesul în zonă;

(iii) specificarea clasificării informațiilor păstrate în mod normal în zonă, adică a informațiile la care intrarea conferă acces;

(b) zonă de securitate de clasa II: o zonă în care informațiile clasificate ►M1 CONFIDENTIEL UE ◄ sau de nivel superior sunt prelucrate și stocate astfel încât pot fi protejate de accesul unor persoane neautorizate prin intermediul unor controale interne, de exemplu sedii care adăpostesc servicii în care sunt prelucrate și stocate de obicei informații clasificate ►M1 CONFIDENTIEL UE ◄ sau de nivel superior. O astfel de zonă necesită:

(i) un perimetru clar definit și protejat în care sunt controlate toate intrările și ieșirile;

(ii) un sistem de control al intrărilor care permite accesul fără însoțitor doar în cazul persoanelor verificate adecvat și special autorizate să intre în zonă. Pentru orice alte persoane, se prevăd însoțitori sau controale echivalente, pentru a preveni accesul neautorizat la informații clasificate UE sau intrarea necontrolată în zone supuse inspecțiilor tehnice de securitate.

Zonele care nu sunt ocupate de personal de serviciu 24 de ore din 24 sunt inspectate imediat după programul normal de lucru pentru a asigura protecția adecvată a informațiilor clasificate UE.

18.3.2. *Zonă administrativă*

O zonă de securitate de clasa I sau II poate fi înconjurată sau precedată de o zonă administrativă cu un nivel de securitate inferior. O astfel de zonă necesită un perimetru definit în mod vizibil care se permită verificarea personalului și a vehiculelor. În astfel de zone, se prelucrează și se stochează doar informații clasificate ►M1 RESTREINT UE ◄ și informații neclasificate.

18.3.3. *Controale la intrare și ieșire*

Intrările în zonele de securitate de clasa I și II și ieșirile din aceste zone sunt controlate printr-un sistem de permise sau de identificare personală aplicabil întregului personal care lucrează în mod normal în aceste zone. De asemenea, se instituie un sistem de verificare a vizitatorilor destinat să împiedice accesul neautorizat la informațiile clasificate UE. Sistemele de permise pot fi însoțite de sisteme de identificare automată, care sunt considerate o suplimentare a pazei, și nu un înlocuitor integral al acesteia. O modificare a evaluării amenințării poate conduce la o întărire a măsurilor de control la intrare și ieșire, de exemplu pe parcursul vizitei unor persoane importante.

▼B

18.3.4. *Patrulări*

În afara programului normal de lucru, au loc patrulări în zonele de securitate de clasa I și II pentru a asigura protecția bunurilor UE împotriva compromiterii, deteriorării sau pierderii. Frecvența patrulărilor va fi determinată în funcție de condițiile locale, dar, orientativ, acestea trebuie să aibă loc o dată la două ore.

18.3.5. *Containere de securitate și seifuri*

Pentru stocarea informațiilor clasificate UE se utilizează trei clase de containere:

— clasa A: containere aprobate la nivel național pentru stocarea informațiilor ►M1 TRES SECRET UE/EU TOP SECRET ◄ din zonele de securitate de clasa I și II;

— clasa B: containere aprobate la nivel național pentru stocarea informațiilor ►M1 SECRET UE ◄ și ►M1 CONFIDENTIEL UE ◄ din zonele de securitate de clasa I și II;

— clasa C: mobilier de birou destinat exclusiv stocării informațiilor ►M1 RESTREINT UE ◄.

Pentru seifurile instalate în zone de securitate de clasa I sau II și pentru toate zonele de securitate de clasa I în care informații clasificate ►M1 CONFIDENTIEL UE ◄ sau de nivel superior sunt păstrate pe rafturi deschise sau sunt prezentate pe grafice, hărți etc., pereții, podelele și plafoanele, ușa (ușile) cu încuietori trebuie să fie certificate de către o SAA ca oferind o protecție echivalentă clasei de containere de securitate aprobate pentru stocarea informațiilor având aceeași clasificare.

18.3.6. *Dispozitive de închidere*

Dispozitivele de închidere utilizate pentru containerele de securitate și seifurile în care sunt stocate informații clasificate UE respectă următoarele standarde:

— grupa A: aprobate la nivel național pentru containere de clasa A;

— grupa B: aprobate la nivel național pentru containere de clasa B;

— grupa C: destinate exclusiv pentru mobilierul de birou de clasa C.

18.3.7. *Controlul cheilor și al combinațiilor*

Cheile de la containerele de securitate nu se scot din clădirile Comisiei. Combinațiile de la containerele de securitate trebuie memorate de persoanele care au nevoie să le cunoască. Pentru situațiile de urgență, ofițerul local de securitate al departamentului în cauză al Comisiei trebuie să dețină chei de rezervă și câte o înregistrare scrisă a fiecărei combinații; acestea din urmă se păstrează în plicuri separate opace, sigilate. Cheile de lucru, cheile de rezervă de securitate și combinațiile se păstrează în containere de securitate separate. Aceste chei și combinații trebuie să beneficieze de o protecție cel puțin la fel de strictă ca și materialele la care asigură accesul.

Cunoașterea combinațiilor de la containerele de securitate este limitată la cât mai puține persoane posibil. Combinațiile sunt modificate:

(a) la primirea unui nou container;

(b) la orice modificare de personal;

(c) în caz de compromitere, reală sau suspectată;

(d) de preferință la intervale de șase luni și cel puțin o dată la douăsprezece luni.

▼B

18.3.8. *Dispozitive de detectare a intruziunilor*

Dacă pentru protejarea informațiilor clasificate UE se utilizează sisteme de alarmă, televiziune cu circuit închis sau alte dispozitive electrice, se asigură o sursă de alimentare cu electricitate în caz de urgență, pentru a asigura funcționarea continuă a sistemului în cazul întreruperii sursei principale de alimentare cu electricitate. O altă cerință de bază este ca o defecțiune de funcționare sau o încercare de neutralizare a sistemelor în cauză să declanșeze o alarmă sau un alt avertisment fiabil personalului de supraveghere.

18.3.9. *Echipamente aprobate*

►**M2** Direcția pentru Securitate a Comisiei ◄ menține liste actualizate cu tipurile și modelele de echipamente de securitate pe care le-a aprobat pentru protecția informațiilor clasificate UE în diverse circumstanțe și condiții specifice. ►**M2** Direcția pentru Securitate a Comisiei ◄ întocmește aceste liste, *inter alia*, pe baza informațiilor furnizate de ANS.

18.3.10. *Protejarea fizică a copiatoarelor și faxurilor*

Copiatoarele și faxurile sunt protejate fizic în măsura necesară pentru a asigura utilizarea lor exclusivă de către personalul autorizat în scopul stocării informațiilor clasificate și controlarea adecvată a tuturor produsele clasificate.

18.4. **Protecția împotriva vederii și ascultării clandestine**

18.4.1. *Protecția împotriva vederii*

Se adoptă toate măsurile necesare, ziua și noaptea, pentru a asigura că informațiile clasificate UE nu sunt văzute, nici măcar accidental, de persoane neautorizate.

18.4.2. *Protecția împotriva ascultării*

Serviciile sau zonele în care se discută în mod regulat despre informații clasificate ►**M1** SECRET UE ◄ sunt protejate împotriva tentativelor de ascultare clandestină activă sau pasivă, dacă acest lucru este impus de riscuri. Responsabilitatea evaluării riscurilor unor astfel de tentative revine Biroului de securitate al Comisiei după consultarea ANS, dacă este necesar.

18.4.3. *Introducerea echipamentelor electronice și de înregistrare*

Nu este permisă introducerea de telefoane mobile, calculatoare personale, dispozitive de înregistrare, aparate foto și alte dispozitive electronice sau de înregistrare în zonele de securitate sau în zonele protejate tehnic fără acordul prealabil al șefului Biroului de securitate al Comisiei.

Pentru a determina măsurile de protecție care trebuie adoptate în sediile sensibile la ascultarea clandestină pasivă (de exemplu, izolarea pereților, a ușilor, a plafoanelor și a podelelor, măsurarea radiațiilor compromițătoare) și la ascultarea clandestină activă (de exemplu, căutarea de microfoane), ►**M2** Direcția pentru Securitate a Comisiei ◄ poate solicita asistența unor experți din cadrul ANS.

În mod similar, atunci când circumstanțele impun acest lucru, echipamentele de telecomunicații și echipamentele electrice și electronice de birou, de orice tip, utilizate în cursul unor reuniuni la nivel ►**M1** SECRET UE ◄ sau superior pot fi verificate de către specialiști în securitate tehnică ai ANS, la cererea șefului Biroului de securitate al Comisiei.

▼B

18.5. **Zone protejate tehnic**

Anumite zone pot fi desemnate ca zone protejate tehnic. Se efectuează o verificare specială la intrare. Aceste zone sunt păstrate închise printr-o metodă aprobată atunci când nu sunt ocupate, iar toate cheile sunt considerate chei de securitate. Astfel de zone sunt supuse unor inspecții fizice periodice, care se efectuează, de asemenea, după orice intrare neautorizată, reală sau suspectată.

Se întocmește un inventar detaliat al echipamentelor și mobilierului pentru a monitoriza mișcarea acestora. Într-o astfel de zonă nu se poate introduce nici o piesă de mobilier sau nici un echipament înainte ca acestea să fi fost supuse unei verificări atente de către personalul de securitate special pregătit, cu scopul de a detecta eventualele dispozitive de ascultare. În general, instalarea liniilor de comunicații în zonele protejate tehnic nu este permisă fără autorizarea prealabilă a autorității competente.

19. NORME GENERALE PRIVIND PRINCIPIUL NEVOII DE A CUNOAȘTE ȘI AUTORIZĂRILE DE SECURITATE ALE PERSONALULUI UE

19.1. **Generalități**

Accesul la informațiile clasificate UE este autorizat doar persoanelor care au o „nevoie de a cunoaște” pentru a-și îndeplini sarcinile sau misiunile. Accesul la informațiile clasificate ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ și ►M1 CONFIDENTIEL UE ◄ este autorizat doar persoanelor care dețin o autorizare de securitate adecvată.

Responsabilitatea pentru determinarea „nevoii de a cunoaște” revine departamentului în cadrul căruia urmează a fi angajată persoana în cauză.

Responsabilitatea de a solicita autorizarea pentru personalul propriu revine fiecărui departament.

Ca urmare, se emite un „certificat personal de securitate UE” care menționează nivelul informațiilor clasificate la care persoana autorizată poate avea acces și data expirării.

Un certificat personal de securitate UE pentru o anumită clasificare poate permite accesul deținătorului la informații cu un nivel inferior de clasificare.

Alte persoane decât funcționarii sau alți angajați, precum contractanții externi, experții sau consultanții, cu care poate fi necesar a discuta despre informații clasificate UE sau cărora poate fi necesar a li se arăta astfel de informații trebuie să dețină o autorizare personală de securitate UE în ceea ce privește informațiile clasificate UE și trebuie să fie informate cu privire la responsabilitatea lor în domeniul securității.

Accesul public este în continuare reglementat de Regulamentul (CE) nr. 1049/2001.

19.2. **Norme specifice privind accesul la informațiile ►M1 TRES SECRET UE/EU TOP SECRET ◄**

Toate persoanele care urmează să aibă acces la informații ►M1 TRES SECRET UE/EU TOP SECRET ◄ sunt, în prealabil, verificate pentru accesul la astfel de informații.

Toate persoanele care trebuie să aibă acces la informații ►M1 TRES SECRET UE/EU TOP SECRET ◄ sunt desemnate de către membrul Comisiei însărcinat cu probleme de securitate, iar numele acestor persoane sunt înscrise în registrul ►M1 TRES SECRET UE/EU TOP SECRET ◄ adecvat. ►M2 Direcția pentru Securitate a Comisiei ◄ creează și ține acest registru.

▼B

Înainte de a avea acces la informații ►M1 TRES SECRET UE/EU TOP SECRET ◄, toate persoanele semnează un certificat prin care confirmă că au fost informate în privința procedurilor de securitate ale Comisiei și că înțeleg pe deplin responsabilitatea specială ce le revine în salvgardarea informațiilor ►M1 TRES SECRET UE/EU TOP SECRET ◄, precum și consecințele pe care normele UE și dispozițiile naționale legislative sau administrative le prevăd pentru divulgarea, intenționată sau din neglijență, de informații clasificate unor persoane neautorizate.

În cazul persoanelor care au acces la informații ►M1 TRES SECRET UE/EU TOP SECRET ◄ la reuniuni etc., ofițerul de control competent al serviciului sau organului în cadrul căruia sunt angajate persoanele în cauză notifică organismului care organizează reuniunea faptul că persoanele în cauză dețin autorizații în acest sens.

Numele tuturor persoanelor care nu mai sunt angajate în funcții care necesită accesul la informații ►M1 TRES SECRET UE/EU TOP SECRET ◄ sunt eliminate de pe lista ►M1 TRES SECRET UE/EU TOP SECRET ◄. În plus, persoanelor în cauză li se atrage din nou atenția asupra responsabilităților speciale care le revin în salvgardarea informațiilor ►M1 TRES SECRET UE/EU TOP SECRET ◄. Persoanele în cauză semnează, de asemenea, o declarație prin care se angajează să nu utilizeze și să nu transmită informațiile ►M1 TRES SECRET UE/EU TOP SECRET ◄ pe care le dețin.

19.3. **Norme specifice privind accesul la informații ►M1 SECRET UE ◄ și ►M1 CONFIDENTIEL UE ◄**

Toate persoanele care urmează să aibă acces la informații ►M1 SECRET UE ◄ și ►M1 CONFIDENTIEL UE ◄ sunt, în prealabil, verificate în măsura adecvată.

Toate persoanele care urmează să aibă acces la informații ►M1 SECRET UE ◄ și ►M1 CONFIDENTIEL UE ◄ trebuie să cunoască dispozițiile adecvate de securitate și consecințele neglijenței.

În cazul persoanelor care au acces la informații ►M1 SECRET UE ◄ și ►M1 CONFIDENTIEL UE ◄ la reuniuni etc., ofițerul de securitate al organismului în cadrul căruia sunt angajate persoanele în cauză notifică organismului care organizează reuniunea faptul că persoanele în cauză dețin autorizații în acest sens.

19.4. **Norme specifice privind accesul la informații ►M1 RESTREINT UE ◄**

Persoanele care au acces la informații ►M1 RESTREINT UE ◄ vor fi avertizate în privința prezentelor norme de securitate și a consecințelor neglijenței.

19.5. **Transferuri**

Când un membru al personalului este transferat dintr-un post care implică utilizarea de materiale clasificate UE, registratura trebuie să supravegheze transferul adecvat al materialelor în cauză de la vechiul la noul funcționar.

Când un membru al personalului este transferat pe un alt post care implică utilizarea de materiale clasificate UE, ofițerul local de securitate instruiește persoana în cauză în mod corespunzător.

19.6. **Instrucțiuni speciale**

Se impune ca persoanele care trebuie să utilizeze informații clasificate UE să fie atenționate, la preluarea funcțiilor lor și ulterior periodic, în privința:

(a) pericolelor pe care le prezintă la adresa securității conversațiile indiscrete;

(b) precauțiilor care trebuie luate în relațiile cu presa și cu reprezentanții grupurilor de interese speciale;

▼B

(c) amenințării reprezentate de activitățile serviciilor de informații care au drept țintă UE și statele sale membre în ceea ce privește informațiile clasificate și activitățile UE;

(d) obligației de a raporta imediat autorităților de securitate competente orice demers sau manevră care generează suspiciuni privind activități de spionaj sau orice situație neobișnuită care are legătură cu securitatea.

Toate persoanele expuse în mod normal unor contacte frecvente cu reprezentanți ai țărilor ale căror servicii de informații au drept țintă UE sau statele sale membre în ceea ce privește informațiile clasificate și activitățile UE sunt informate în privința tehnicilor cunoscute ca fiind utilizate de diverse servicii de informații.

Nu există dispoziții de securitate în cadrul Comisiei referitoare la călătoriile private către orice destinație ale personalului autorizat să aibă acces la informații clasificate UE. Totuși, ►M2 Direcția pentru Securitate a Comisiei ◄ informează funcționarii și alți angajați aflați sub responsabilitatea sa cu privire la reglementările în materie de călătorii sub incidența cărora ar putea intra.

20. PROCEDURĂ DE AUTORIZARE DE SECURITATE PENTRU FUNCȚIONARI ȘI ALȚI ANGAJAȚI AI COMISIEI

(a) Doar funcționarii, alți angajați ai Comisiei sau persoanele care lucrează în cadrul Comisiei care, prin natura sarcinilor lor sau pentru cerințe de serviciu, trebuie să cunoască sau să utilizeze informații clasificate deținute de Comisie au acces la astfel de informații.

(b) Pentru a avea acces la informații clasificate „►M1 TRES SECRET UE/EU TOP SECRET ◄”, „►M1 SECRET UE ◄” și „►M1 CONFIDENTIEL UE ◄”, persoanele menționate la litera (a) anterioară trebuie să fi fost autorizate în conformitate cu procedura menționată la literele (c) și (d) din prezenta secțiune.

(c) Autorizațiile se acordă doar persoanelor care au fost supuse unei verificări de securitate de către autoritățile naționale competente ale statelor membre (ANS) în conformitate cu procedura menționată la literele (i)–(n).

(d) ►M2 Directorul Direcției pentru Securitate a Comisiei ◄ este responsabil cu acordarea autorizațiilor menționate la literele (a), (b) și (c).

(e) Acesta acordă autorizația după obținerea avizului emis de autoritățile naționale competente ale statelor membre pe baza verificării de securitate efectuate în conformitate cu literele (i)–(n).

(f) ►M2 Direcția pentru Securitate a Comisiei ◄ păstrează o listă actualizată a tuturor posturilor sensibile, furnizată de departamentele competente ale Comisiei, și a tuturor persoanelor cărora li s-a acordat o autorizație (temporară).

(g) Autorizația, valabilă pe o perioadă de cinci ani, nu poate depăși durata funcțiilor în temeiul cărora este acordată. Autorizația poate fi reînnoită în conformitate cu procedura menționată la litera (e).

(h) Autorizația este retrasă de ►M2 directorul Direcției pentru Securitate a Comisiei ◄ în cazul în care acesta consideră că există motive justificate în acest sens. Orice decizie de retragere a unei autorizații este notificată persoanei în cauză, care poate solicita să fie audiată de ►M2 directorul Direcției pentru Securitate a Comisiei ◄ și de autoritatea națională competentă.

▼B

(i) Verificarea de securitate se efectuează cu sprijinul persoanei vizate și la cererea șefului Biroului de securitate al Comisiei. Autoritatea națională competentă pentru verificare este cea a statului membru al cărui cetățean este persoana supusă autorizării. În cazul în care persoana în cauză nu este cetățean al unui stat membru al UE, ►M2 directorul Direcției pentru Securitate a Comisiei ◄ va solicita efectuarea unei verificări de securitate de către statul membru al UE în care persoana în cauză își are domiciliul sau reședința uzuală.

(j) În cadrul procedurii de verificare, persoana în cauză trebuie să completeze un formular cu informații personale.

(k) ►M2 Directorul Direcției pentru Securitate a Comisiei ◄ specifică în cererea sa tipul și nivelul informațiilor clasificate care vor fi puse la dispoziția persoanei în cauză, astfel încât autoritățile naționale competente să poată efectua procesul de verificare și să emită un aviz cu privire la nivelul de autorizare adecvat pentru a fi acordat persoanei în cauză.

(l) Întregul proces de verificare de securitate și rezultatele obținute sunt supuse reglementărilor relevante în vigoare în statul membru în cauză, inclusiv cele privind căile de apel.

(m) Dacă autoritățile naționale competente ale statului membru emit un aviz pozitiv, ►M2 directorul Direcției pentru Securitate a Comisiei ◄ poate acorda autorizația persoanei în cauză.

(n) Un aviz negativ emis de autoritățile naționale competente este notificat persoanei în cauză, care poate solicita să fie audiată de ►M2 directorul Direcției pentru Securitate a Comisiei ◄. În cazul în care consideră că acest lucru este necesar, ►M2 directorul Direcției pentru Securitate a Comisiei ◄ poate solicita autorităților naționale competente orice clarificări suplimentare pe care acestea le pot furniza. Dacă avizul negativ este confirmat, nu se acordă autorizația.

(o) Toate persoanele autorizate în sensul literelor (d) și (e) primesc, în momentul acordării autorizației și ulterior periodic, toate instrucțiunile necesare privind protecția informațiilor clasificate și mijloacele prin care se asigură această protecție. Persoanele în cauză semnează o declarație prin care confirmă primirea instrucțiunilor și se angajează să le respecte.

(p) ►M2 Directorul Direcției pentru Securitate a Comisiei ◄ ia toate măsurile necesare pentru punerea în aplicare a prezentei secțiuni, în special în ceea ce privește normele care reglementează accesul la lista persoanelor autorizate.

(q) În mod excepțional și în funcție de necesitățile serviciului, ►M2 directorul Direcției pentru Securitate a Comisiei ◄ poate acorda, după notificarea autorităților naționale competente și cu condiția ca acestea să nu răspundă în termen de o lună, autorizări temporare pentru o perioadă de maximum 6 luni, până la finalizarea verificării menționate la litera (i).

(r) Autorizările provizorii și temporare astfel acordate nu permit accesul la informații ►M1 TRES SECRET UE/EU TOP SECRET ◄; accesul la aceste informații este limitat doar la funcționarii care au fost efectiv supuși unei verificări cu rezultate pozitive, în conformitate cu litera (i). Până la finalizarea verificării, funcționarii care trebuie să fie autorizați pentru nivelul ►M1 TRES SECRET UE/EU TOP SECRET ◄ pot fi autorizați, temporar și provizoriu, să acceseze informații clasificate până la nivelul ►M1 SECRET UE ◄, inclusiv.

▼B

21. PREGĂTIREA, DISTRIBUIREA, TRANSMITEREA, SECURITATEA PERSONALĂ A CURIERILOR ŞI COPII SUPLIMENTARE, TRADUCERI ŞI EXTRASE ALE DOCUMENTELOR CLASIFICATE UE

21.1. **Pregătire**

1. Clasificările UE se aplică conform menţiunilor din secţiunea 16, iar pentru documentele ►M1 CONFIDENTIEL UE ◄ şi de nivel superior clasificările apar centrat în partea de sus şi de jos a fiecărei pagini, toate paginile fiind numerotate. Fiecare document clasificat UE poartă un număr de referinţă şi o dată. În cazul documentelor ►M1 TRES SECRET UE/EU TOP SECRET ◄ şi ►M1 SECRET UE ◄, acest număr de referinţă apare pe fiecare pagină. Dacă acestea trebuie distribuite în mai multe exemplare, fiecare dintre ele poartă un număr de exemplar, care apare pe prima pagină, împreună cu numărul total de pagini. Toate anexele şi documentele însoţitoare sunt enumerate pe prima pagină a unui document clasificat ►M1 CONFIDENTIEL UE ◄ sau de nivel superior.

2. Documentele clasificate ►M1 CONFIDENTIEL UE ◄ şi de nivel superior sunt dactilografiate, traduse, stocate, fotocopiate, înregistrate pe suport magnetic sau pe microfilm doar de către persoane care au primit autorizaţia de a accesa informaţii clasificate UE cel puţin până la clasificarea de securitate adecvată a documentului în cauză.

3. Dispoziţiile care reglementează elaborarea computerizată a documentelor clasificate sunt prevăzute în secţiunea 25.

21.2. **Distribuire**

1. Informaţiile clasificate UE se distribuie doar persoanelor care au nevoie să le cunoască şi care deţin autorizarea de securitate adecvată. Autoritatea de origine specifică destinatarii iniţiali.

2. Documentele ►M1 TRES SECRET UE/EU TOP SECRET ◄ sunt difuzate prin registraturi ►M1 TRES SECRET UE/EU TOP SECRET ◄ (a se vedea secţiunea 22.2). În cazul mesajelor ►M1 TRES SECRET UE/EU TOP SECRET ◄, registratura competentă poate autoriza şeful centrului de comunicaţii să realizeze numărul de copii specificat în lista destinatarilor.

3. Documentele clasificate ►M1 SECRET UE ◄ şi de nivel inferior pot fi redistribuite de către destinatarul iniţial altor destinatari pe baza nevoii de a cunoaşte. Totuşi, autorităţile de origine menţionează clar orice restricţii pe care doreşte să le impună. Ori de câte ori sunt impuse astfel de restricţii, destinatarii pot redistribui documentele doar cu aprobarea autorităţilor de origine.

4. La intrarea într-o DG sau într-un serviciu sau la ieşirea dintr-o DG sau dintr-un serviciu, orice document clasificat ►M1 CONFIDENTIEL UE ◄ sau de nivel superior este înregistrat de registratura locală ICUE a departamentului în cauză. Elementele care trebuie înregistrate (referinţe, data şi, dacă este cazul, numărul exemplarului) trebuie să permită identificarea documentelor şi trebuie să fie înregistrate într-un registru sau pe un suport informatic special protejat (a se vedea secţiunea 22.1).

21.3. **Transmiterea documentelor clasificate UE**

21.3.1. *Ambalare, confirmări de primire*

1. Documentele clasificate ►M1 CONFIDENTIEL UE ◄ şi de nivel superior se transmit în plicuri duble, opace şi rezistente. Plicul interior este marcat cu clasificarea de securitate UE adecvată, precum şi, dacă este posibil, cu toate elementele privind funcţia şi adresa destinatarului.

▼B

2. Doar un ofițer de control al registraturii (a se vedea secțiunea 22.1) sau înlocuitorul acestuia poate deschide plicul interior și confirma primirea documentelor pe care le conține, cu excepția cazului în care plicul este adresat unei anumite persoane. În acest caz, registratura competentă (a se vedea secțiunea 22.1) înregistrează sosirea plicului și doar persoana căreia îi este adresat poate deschide plicul interior și confirma primirea documentelor pe care le conține.

3. În plicul interior este introdus un formular de confirmare de primire. Confirmarea de primire, care nu se clasifică, menționează numărul de referință, data și numărul exemplarului documentului, dar niciodată subiectul acestuia.

4. Plicul interior este introdus într-un plic exterior care este marcat cu un număr de colet, pentru confirmarea primirii. Clasificarea de securitate nu apare în nici un caz pe plicul exterior.

5. Pentru documentele clasificate ►**M1** CONFIDENTIEL UE ◄ și de nivel superior, curierii și mesagerii obțin confirmări de primire corespunzătoare numerelor de colet.

21.3.2. *Transmiterea în cadrul unei clădiri sau al unui grup de clădiri*

În cadrul unei clădiri sau al unui grup de clădiri, documentele clasificate pot fi transportate într-un plic sigilat marcat doar cu numele destinatarului, cu condiția ca plicul să fie transportat de o persoană autorizată la nivelul de clasificare a documentelor.

21.3.3. *Transmiterea în interiorul unei țări*

1. În interiorul unei țări, documentele ►**M1** TRES SECRET UE/EU TOP SECRET ◄ trebuie transmise doar prin intermediul unui serviciu oficial de mesagerie sau prin persoane autorizate să aibă acces la informații ►**M1** TRES SECRET UE/EU TOP SECRET ◄.

2. Ori de câte ori se utilizează un serviciu de mesagerie pentru transmiterea unui document ►**M1** TRES SECRET UE/EU TOP SECRET ◄ în afara unei clădiri sau a unui grup de clădiri, se respectă dispozițiile privind ambalarea și confirmarea de primire prevăzute în prezentul capitol. Serviciile de livrare trebuie să dețină un personal adecvat, astfel încât să asigure că pachetele care conțin documente ►**M1** TRES SECRET UE/EU TOP SECRET ◄ rămân permanent sub supravegherea directă a unui funcționar responsabil.

3. În mod excepțional, documentele ►**M1** TRES SECRET UE/EU TOP SECRET ◄ pot fi transportate de alți funcționari decât mesagerii în afara unei clădiri sau a unui grup de clădiri pentru utilizare locală la reuniuni și discuții, cu condiția ca:

   (a) purtătorul să dețină autorizația de a accesa documentele ►**M1** TRES SECRET UE/EU TOP SECRET ◄ în cauză;

   (b) modul de transport să respecte normele care reglementează transmiterea documentelor ►**M1** TRES SECRET UE/EU TOP SECRET ◄;

   (c) funcționarul să nu lase în nici un caz nesupravegheate documentele ►**M1** TRES SECRET UE/EU TOP SECRET ◄;

   (d) să se ia măsuri pentru ca lista documentelor astfel transportate să fie păstrată în registratura ►**M1** TRES SECRET UE/EU TOP SECRET ◄ care deține documentele și să fie înregistrată într-un registru și verificată față de înregistrare la returnarea acestora.

4. Într-o anumită țară, documentele ►**M1** SECRET UE ◄ și ►**M1** CONFIDENTIEL UE ◄ pot fi expediate fie prin poștă, dacă acest mod de trimitere este permis de reglementările naționale și este în conformitate cu prevederile reglementărilor în cauză, fie prin serviciu de mesagerie, fie prin intermediul unor persoane autorizate să aibă acces la informații clasificate UE.

▼B

5. Pe baza acestor norme, ►M2 Direcția pentru Securitate a Comisiei ◄ va elabora instrucțiuni privind personalul care transportă documente clasificate UE. Purtătorul trebuie să citească și să semneze aceste instrucțiuni. În special, instrucțiunile subliniază faptul că, în nici un caz, documentele nu pot:

   (a) ieși din posesia purtătorului, cu excepția cazului în care se află în siguranță în conformitate cu prevederile secțiunii 18;

   (b) fi lăsate nesupravegheate în mijloace de transport în comun sau în autoturisme sau în locuri precum restaurante sau hoteluri; documentele nu pot fi păstrate în seifuri la hoteluri sau nu pot rămâne nesupravegheate în camere de hotel;

   (c) fi citite în locuri publice precum avioane sau trenuri.

21.3.4. *Transmiterea de la un stat la altul*

1. Materialele clasificate ►M1 CONFIDENTIEL UE ◄ și de nivel superior se transmit prin servicii de curier UE diplomatic sau militar.

2. Cu toate acestea, poate fi autorizat transportul de către o persoană al materialelor clasificate ►M1 SECRET UE ◄ sau ►M1 CONFIDENTIEL UE ◄ dacă dispozițiile privind transportul sunt de natură să asigure faptul că materialele în cauză nu pot intra în posesia unor persoane neautorizate.

3. Membrul Comisiei însărcinat cu probleme de securitate poate autoriza transportul de către persoane dacă nu sunt disponibili curieri diplomatici sau militari sau dacă utilizarea unor astfel de curieri ar determina o întârziere care ar periclita operațiunile UE, iar materialul în cauză este solicitat de urgență de destinatar. ►M2 Direcția pentru Securitate a Comisiei ◄ va elabora instrucțiuni care reglementează transportul internațional al materialelor clasificate până la nivelul ►M1 SECRET UE ◄, inclusiv, de către alte persoane decât curierii diplomatici sau militari. Instrucțiunile prevăd că:

   (a) purtătorul deține autorizația de securitate adecvată;

   (b) toate materialele astfel transportate sunt înregistrate de departamentul adecvat sau de registratura adecvată;

   (c) pachetele sau genții care conțin materiale UE poartă un sigiliu oficial pentru a împiedica sau descuraja inspecția vamală, precum și etichete de identificare cu instrucțiuni pentru găsitor;

   (d) purtătorul deține un certificat de curier și/sau un ordin de misiune recunoscut de toate statele membre, prin care este autorizat să transporte pachetul astfel identificat;

   (e) dacă transportul se face pe cale terestră, nu se tranzitează nici un stat nemembru al UE și nu se trece nici o frontieră a unui astfel de stat, cu excepția cazului în care statul expeditor obține o garanție specifică din partea statului în cauză;

   (f) dispozițiile de călătorie ale purtătorului referitoare la destinații, traseele urmate și mijloacele de transport utilizate respectă normele UE sau – dacă dispozițiile naționale privind aceste aspecte sunt mai stricte – dispozițiile în cauză;

   (g) materialele nu trebuie să iasă din posesia purtătorului, cu excepția cazului în care sunt păstrate în conformitate cu dispozițiile privind păstrarea în siguranță prevăzute în secțiunea 18;

   (h) materialele nu trebuie să fie lăsate nesupravegheate în mijloace de transport în comun sau în autoturisme sau în locuri precum restaurante sau hoteluri; materialele nu trebuie depuse în seifuri la hoteluri sau nu trebuie lăsate nesupravegheate în camere de hotel;

   (i) dacă materialele transportate conțin documente, acestea nu trebuie citite în locuri publice (de exemplu în avioane, trenuri etc.).

▼B

4. Persoana desemnată să transporte materialele clasificate trebuie să citească și să semneze instrucțiuni de securitate care conțin cel puțin instrucțiunile enumerate anterior și procedurile care trebuie urmate într-o situație de urgență sau în cazul în care pachetul care conține materialele clasificate face obiectul unui control efectuat de funcționarii vamali sau de funcționarii de securitate dintr-un aeroport.

21.3.5. *Transmiterea documentelor* ►M1 *RESTREINT UE* ◄

Nu sunt prevăzute dispoziții speciale privind transmiterea documentelor ►M1 RESTREINT UE ◄, cu excepția faptului că transmiterea trebuie să asigure că documentele nu pot intra în posesia unor persoane neautorizate.

21.4. **Securitatea personală a curierilor**

Toți curierii și mesagerii angajați pentru transportul de documente ►M1 SECRET UE ◄ și ►M1 CONFIDENTIEL UE ◄ fac obiectul unei verificări de securitate adecvate.

21.5. **Mijloace electronice și alte mijloace de transmitere tehnică**

1. Măsurile de securitate a comunicațiilor sunt destinate să asigure transmiterea în siguranță a informațiilor clasificate UE. Normele aplicabile transmiterii de informații clasificate UE sunt prezentate în secțiunea 25.

2. Doar centrele de comunicații, rețelele și/sau terminalele și sistemele acreditate pot transmite informații clasificate ►M1 CONFIDENTIEL UE ◄ și ►M1 SECRET UE ◄.

21.6. **Copii suplimentare, traduceri și extrase ale documentelor clasificate UE**

1. Doar autoritatea de origine poate autoriza copierea sau traducerea documentelor ►M1 TRES SECRET UE/EU TOP SECRET ◄.

2. În cazul în care persoane neautorizate la nivelul ►M1 TRES SECRET UE/EU TOP SECRET ◄ au nevoie de informații care, deși sunt incluse într-un document ►M1 TRES SECRET UE/EU TOP SECRET ◄, nu sunt clasificate la acest nivel, șeful registraturii ►M1 TRES SECRET UE/EU TOP SECRET ◄ (a se vedea secțiunea 22.2) poate fi autorizat să realizeze numărul necesar de extrase din documentul în cauză. În același timp, acesta ia măsurile necesare pentru a asigura că extrasele în cauză primesc o clasificare de securitate adecvată.

3. Documentele clasificate ►M1 SECRET UE ◄ și de nivel inferior pot fi reproduse și traduse de către destinatar, în cadrul prezentelor dispoziții de securitate și cu condiția respectării stricte a principiului nevoii de a cunoaște. Măsurile de securitate aplicabile documentului original se aplică și reproducerilor și/sau traducerilor documentului în cauză.

22. REGISTRATURI ICUE, REGRUPĂRI, VERIFICĂRI, ARHIVARE ȘI DISTRUGEREA ICUE

22.1. **Registraturi locale ICUE**

1. În cadrul Comisiei, în fiecare departament, în funcție de necesități, una sau multe registraturi locale ICUE sunt însărcinate cu înregistrarea, reproducerea, transmiterea, arhivarea și distrugerea documentelor clasificate ►M1 SECRET UE ◄ și ►M1 CONFIDENTIEL UE ◄.

2. În cazul în care un departament nu dispune de o registratură locală ICUE, registratura locală ICUE a Secretariatului General va acționa ca registratură ICUE a departamentului respectiv.

3. Registraturile locale ICUE se subordonează șefului de departament, de la care își primesc instrucțiunile. Șeful acestor registraturi este ofițerul de control al registraturii (RCO).

▼B

4. Acestea sunt supuse supravegherii ofițerului local de securitate în ceea ce privește dispozițiile referitoare la prelucrarea documentelor ICUE și respectarea măsurilor corespunzătoare de securitate.

5. Funcționarii angajați în registraturile locale ICUE sunt autorizați să aibă acces la ICUE în conformitate cu secțiunea 20.

6. Sub autoritatea șefului competent de departament, registraturile locale ICUE:

   (a) gestionează operațiunile privind înregistrarea, reproducerea, traducerea, transmiterea, expedierea și distrugerea informațiilor în cauză;

   (b) actualizează registrul privind informațiile clasificate;

   (c) chestionează periodic emitenții cu privire la necesitatea de a menține clasificarea informațiilor.

7. Registraturile locale ICUE țin un registru conținând următoarele date:

   (a) data elaborării informațiilor clasificate;

   (b) nivelul de clasificare;

   (c) data expirării clasificării;

   (d) numele și departamentul emitentului;

   (e) destinatarul sau destinatarii, cu număr de ordine;

   (f) subiectul;

   (g) numărul;

   (h) numărul de exemplare distribuite;

   (i) date privind elaborarea de inventare ale informațiilor clasificate prezentate departamentului;

   (j) registrul privind declasarea și declasificarea informațiilor clasificate.

8. Normele generale prevăzute în secțiunea 21 se aplică registraturilor locale ICUE ale Comisiei, cu excepția eventualelor modificări aduse de normele specifice prevăzute în prezenta secțiune.

22.2. **Registratura ►M1 TRES SECRET UE/EU TOP SECRET ◄**

22.2.1. *Generalități*

1. O registratură centrală ►M1 TRES SECRET UE/EU TOP SECRET ◄ asigură înregistrarea, prelucrarea și difuzarea documentelor ►M1 TRES SECRET UE/EU TOP SECRET ◄ în conformitate cu prezentele dispoziții de securitate. Șeful registraturii ►M1 TRES SECRET UE/EU TOP SECRET ◄ este ofițerul de control al registraturii ►M1 TRES SECRET UE/EU TOP SECRET ◄.

2. Registratura centrală ►M1 TRES SECRET UE/EU TOP SECRET ◄ acționează ca autoritate principală de primire și de expediere în cadrul Comisiei, în relația cu alte instituții europene, cu statele membre, cu organizațiile internaționale și cu statele terțe cu care Comisia a încheiat acorduri privind procedurile de securitate pentru schimbul de informații clasificate.

3. Dacă este necesar, se instituie registraturi secundare, însărcinate cu gestionarea internă a documentelor ►M1 TRES SECRET UE/EU TOP SECRET ◄; acestea păstrează înregistrări actualizate privind circulația fiecărui document care intră în responsabilitatea registraturii secundare.

▼B

4. Registraturile secundare ►M1 TRES SECRET UE/EU TOP SECRET ◄ sunt instituite în conformitate cu secțiunea 22.2.3 ca răspuns la nevoi pe termen lung și sunt atașate unei registraturi centrale ►M1 TRES SECRET UE/EU TOP SECRET ◄. În cazul unei necesități de consultare doar temporară și ocazională a documentelor ►M1 TRES SECRET UE/EU TOP SECRET ◄, aceste documente pot fi comunicate fără instituirea unei registraturi secundare ►M1 TRES SECRET UE/EU TOP SECRET ◄, cu condiția să se prevadă norme care să asigure că acestea rămân sub controlul registraturii ►M1 TRES SECRET UE/EU TOP SECRET ◄ adecvate și că sunt respectate toate măsurile de securitate fizică și cele privind personalul.

5. Registraturile secundare nu pot transmite documente ►M1 TRES SECRET UE/EU TOP SECRET ◄ direct altor registraturi secundare ale aceleiași registraturi centrale ►M1 TRES SECRET UE/EU TOP SECRET ◄ fără aprobarea expresă a acesteia din urmă.

6. Toate schimburile de documente ►M1 TRES SECRET UE/EU TOP SECRET ◄ între registraturi secundare care nu aparțin aceleiași registraturi centrale au loc prin intermediul registraturilor centrale ►M1 TRES SECRET UE/EU TOP SECRET ◄.

22.2.2. *Registratura centrală* ►M1 *TRES SECRET UE/EU TOP SECRET* ◄

În calitate de ofițer de control, șeful registraturii centrale ►M1 TRES SECRET UE/EU TOP SECRET ◄ are ca responsabilități:

(a) transmiterea documentelor ►M1 TRES SECRET UE/EU TOP SECRET ◄ în conformitate cu dispozițiile definite în secțiunea 21.3;

(b) păstrarea unei liste cu toate registraturile secundare ►M1 TRES SECRET UE/EU TOP SECRET ◄ subordonate, împreună cu numele și semnăturile ofițerilor de control desemnați și ale adjuncților lor autorizați;

(c) păstrarea confirmărilor de primire de la registraturi pentru toate documentele ►M1 TRES SECRET UE/EU TOP SECRET ◄ distribuite de registratura centrală;

(d) ținerea unui registru al documentelor ►M1 TRES SECRET UE/EU TOP SECRET ◄ deținute și distribuite;

(e) păstrarea unei liste actualizate a tuturor registraturilor centrale ►M1 TRES SECRET UE/EU TOP SECRET ◄ cu care corespondează în mod normal, împreună cu numele și semnăturile ofițerilor de control desemnați și ale adjuncților lor autorizați;

(f) salvgardarea fizică a tuturor documentelor ►M1 TRES SECRET UE/EU TOP SECRET ◄ deținute în cadrul registraturii în conformitate cu reglementările prevăzute în secțiunea 18.

22.2.3. *Registraturi secundare* ►M1 *TRES SECRET UE/EU TOP SECRET* ◄

În calitate de ofițer de control, șeful unei registraturi secundare ►M1 TRES SECRET UE/EU TOP SECRET ◄ are ca responsabilități:

(a) transmiterea documentelor ►M1 TRES SECRET UE/EU TOP SECRET ◄ în conformitate cu dispozițiile prevăzute în secțiunea 21.3;

(b) păstrarea unei liste actualizate cu toate persoanele autorizate să aibă acces la informațiile ►M1 TRES SECRET UE/EU TOP SECRET ◄ aflate sub controlul său;

(c) distribuirea documentelor ►M1 TRES SECRET UE/EU TOP SECRET ◄ în conformitate cu instrucțiunile autorității de origine și pe baza nevoii de a cunoaște, după ce a verificat, în prealabil, că destinatarul deține autorizarea de securitate adecvată;

(d) ținerea unui registru actualizat al tuturor documentelor ►M1 TRES SECRET UE/EU TOP SECRET ◄ deținute și distribuite sub controlul său sau care au fost transmise altor registraturi ►M1 TRES SECRET UE/EU TOP SECRET ◄ și păstrarea tuturor confirmărilor de primire corespunzătoare;

▼B

(e) păstrarea unei liste actualizate a registraturilor ►M1 TRES SECRET UE/EU TOP SECRET ◄ cu care este autorizat să facă schimb de documente ►M1 TRES SECRET UE/EU TOP SECRET ◄, împreună cu numele și semnăturile ofițerilor de control și ale adjuncților autorizați ai acestora;

(f) salvgardarea fizică a tuturor documentelor ►M1 TRES SECRET UE/EU TOP SECRET ◄ deținute în cadrul registraturii secundare în conformitate cu normele prevăzute în secțiunea 18.

22.3. **Inventarieri, regrupări și verificări ale documentelor clasificate UE**

1. În fiecare an, fiecare registratură ►M1 TRES SECRET UE/EU TOP SECRET ◄ menționată în prezenta secțiune efectuează o inventariere detaliată a documentelor ►M1 TRES SECRET UE/EU TOP SECRET ◄. Un document este considerat ca fiind inventariat dacă registratura constată existența fizică a documentului sau deține o confirmare de primire de la registratura ►M1 TRES SECRET UE/EU TOP SECRET ◄ căreia i-a fost trimis documentul, un certificat de distrugere a documentului sau o instrucțiune de declasare sau declasificare a documentului în cauză. Registraturile ►M1 TRES SECRET UE/EU TOP SECRET ◄ transmit rezultatele inventarelor anuale membrului Comisiei însărcinat cu probleme de securitate, până cel târziu la data de 1 aprilie a fiecărui an.

2. Registraturile secundare ►M1 TRES SECRET UE/EU TOP SECRET ◄ transmit rezultatele inventarului lor anual registraturii centrale căreia i se subordonează, la o dată specificată de aceasta din urmă.

3. Documentele clasificate UE de un nivel inferior celui ►M1 TRES SECRET UE/EU TOP SECRET ◄ sunt supuse unor verificări interne în conformitate cu instrucțiunile membrului Comisiei însărcinat cu probleme de securitate.

4. Aceste operațiuni oferă oportunitatea de a obține punctul de vedere al deținătorilor cu privire la:

   (a) posibilitatea de a declasa sau de a declasifica anumite documente;

   (b) documentele care trebuie distruse.

22.4. **Arhivarea informațiilor clasificate UE**

1. ICUE se păstrează în condiții care respectă toate cerințele relevante enumerate în secțiunea 18.

2. Pentru a minimiza problemele de păstrare, ofițerii de control ai tuturor registraturilor sunt autorizați să microfilmeze documentele ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ și ►M1 CONFIDENTIEL UE ◄ sau să le înregistreze pe un suport magnetic sau optic în scopul arhivării, cu condiția ca:

   (a) procesul de microfilmare/arhivare să fie efectuat de persoane care dețin autorizare pentru nivelul de clasificare adecvat corespunzător;

   (b) microfilmul/suportul de arhivare să beneficieze de același grad de securitate ca și documentele originale;

   (c) microfilmarea/arhivarea oricărui document ►M1 TRES SECRET UE/EU TOP SECRET ◄ să fie semnalată autorității de origine;

   (d) rolele de film sau alte tipuri de suport să conțină doar documente cu aceeași clasificare ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ sau ►M1 CONFIDENTIEL UE ◄;

▼B

(e) microfilmarea/arhivarea unui document ►M1 TRES SECRET UE/EU TOP SECRET ◄ sau ►M1 SECRET UE ◄ să fie indicată clar în registrul utilizat pentru inventarul anual;

(f) documentele originale care au fost microfilmate sau arhivate pe un alt suport să fie distruse, în conformitate cu normele prevăzute în secțiunea 22.5.

3. De asemenea, prezentele norme se aplică oricărei alte forme de arhivare autorizată, de exemplu pe suport electromagnetic sau disc optic.

22.5. **Distrugerea documentelor clasificate UE**

1. Pentru a evita acumularea inutilă a documentelor clasificate UE, cele care sunt considerate de șeful departamentului care le deține ca fiind perimate și excedentare ca număr sunt distruse de îndată ce e posibil, în modurile următoare:

(a) documentele ►M1 TRES SECRET UE/EU TOP SECRET ◄ sunt distruse doar de registratura centrală responsabilă de acestea. Fiecare document distrus este înscris într-un certificat de distrugere, semnat de ofițerul de control ►M1 TRES SECRET UE/EU TOP SECRET ◄ și de ofițerul care este martor la distrugere, acesta din urmă fiind autorizat ►M1 TRES SECRET UE/EU TOP SECRET ◄. Registrul include o mențiune în acest sens;

(b) registratura păstrează certificatele de distrugere, împreună cu fișele de distribuție, timp de zece ani. Se transmit copii autorității de origine sau registraturii centrale corespunzătoare doar la cererea expresă a acestora;

(c) documentele ►M1 TRES SECRET UE/EU TOP SECRET ◄, inclusiv toate deșeurile clasificate provenite din elaborarea documentelor ►M1 TRES SECRET UE/EU TOP SECRET ◄, precum copii distruse, ciorne, note dactilografiate, dischete sunt distruse, sub supravegherea unui ofițer de control al registraturii ►M1 TRES SECRET UE/EU TOP SECRET ◄, prin ardere, transformare în pastă, tăiere în fâșii sau printr-o altă modalitate de mărunțire în fragmente neidentificabile și care nu permit reconstituirea.

2. Documentele ►M1 SECRET UE ◄ sunt distruse de registratura responsabilă cu documentele în cauză, sub supravegherea unei persoane deținând o autorizare de securitate, folosind unul dintre procedeele indicate la punctul 1 litera (c). Documentele ►M1 SECRET UE ◄ distruse sunt înregistrate în certificate de distrugere semnate care urmează a fi păstrate de registratură, împreună cu formularele de distribuire, timp de cel puțin trei ani.

3. Documentele ►M1 CONFIDENTIEL UE ◄ sunt distruse de registratura responsabilă cu documentele în cauză, sub supravegherea unei persoane deținând o autorizare de securitate, folosind unul dintre procedeele indicate la punctul 1 litera (c). Distrugerea acestora se înregistrează în conformitate cu instrucțiunile membrului Comisiei însărcinat cu probleme de securitate.

4. Documentele ►M1 RESTREINT UE ◄ sunt distruse de registratura responsabilă cu documentele în cauză sau de utilizator, în conformitate cu instrucțiunile membrului Comisiei însărcinat cu probleme de securitate.

22.6. **Distrugere în situații de urgență**

1. Departamentele Comisiei elaborează planuri bazate pe condițiile locale pentru a asigura salvgardarea materialelor clasificate UE într-o situație de criză, inclusiv, dacă este necesar, planuri pentru distrugere și evacuare de urgență. Departamentele emit instrucțiunile considerate necesare pentru a preveni accesul unor persoane neautorizate la informații clasificate UE.

▼B

2. Măsurile luate pentru salvgardarea și/sau distrugerea materialelor ►M1 SECRET UE ◄ și ►M1 CONFIDENTIEL UE ◄ într-o situație de criză nu afectează, în nici un caz, salvgardarea sau distrugerea materialelor ►M1 TRES SECRET UE/EU TOP SECRET ◄, inclusiv a echipamentelor de codificare, care trebuie să aibă prioritate față de toate celelalte sarcini.

3. Măsurile care trebuie adoptate pentru salvgardarea și distrugerea echipamentelor de codificare într-o situație de urgență sunt reglementate de instrucțiuni specifice.

4. Instrucțiunile trebuie să fie disponibile la fața locului într-un plic sigilat. Mijloacele/instrumentele de distrugere trebuie să fie disponibile.

23. MĂSURI DE SECURITATE PENTRU REUNIUNI SPECIFICE ORGANIZATE ÎN AFARA SEDIILOR COMISIEI ȘI CARE IMPLICĂ INFORMAȚII CLASIFICATE UE

23.1. **Generalități**

În cazul în care reuniunile Comisiei sau alte reuniuni importante sunt organizate în afara sediilor Comisiei și dacă acest lucru este justificat de cerințele speciale de securitate privind sensibilitatea ridicată a problemelor sau informațiilor abordate, se iau măsurile de securitate descrise în continuare. Aceste măsuri se referă doar la protecția informațiilor clasificate UE; pot fi planificate, de asemenea, alte măsuri de securitate.

23.2. **Responsabilități**

23.2.1. ►M2 *Direcția pentru Securitate a Comisiei* ◄

►M2 Direcția pentru Securitate a Comisiei ◄ cooperează cu autoritățile competente ale statului membru pe al cărui teritoriu se desfășoară reuniunea (statul membru gazdă), pentru a asigura securitatea reuniunilor Comisiei sau a altor reuniuni importante și pentru securitatea delegaților și a personalului acestora. În ceea ce privește protecția de securitate, ►M2 Direcția pentru Securitate a Comisiei ◄ se asigură, în special, că:

(a) se elaborează planuri pentru rezolvarea amenințărilor la adresa securității și a incidentelor legate de securitate, măsurile în cauză vizând, în special, păstrarea în siguranță a documentelor clasificate UE în birouri;

(b) se iau măsuri pentru a asigura eventualul acces la sistemul de comunicații al Comisiei pentru recepția și transmiterea de mesaje clasificate UE. Statului membru gazdă i se solicită să asigure, dacă este necesar, accesul la sisteme securizate de telefonie.

►M2 Direcția pentru Securitate a Comisiei ◄ acționează în calitate de consilier de securitate pentru pregătirea reuniunii; acesta trebuie să fie reprezentat la reuniune pentru a ajuta și a sfătui, dacă este cazul, ofițerul de securitate al reuniunii (MSO) și delegațiile.

Fiecare delegație la o reuniune trebuie să desemneze un ofițer de securitate, care este însărcinat cu rezolvarea problemelor de securitate din cadrul delegației proprii și cu menținerea legăturii cu ofițerul de securitate al reuniunii, precum și cu reprezentantul Biroului de securitate al Comisiei, dacă este necesar.

23.2.2. *Ofițerul de securitate al reuniunii (MSO)*

Se desemnează un ofițer de securitate al reuniunii, însărcinat cu pregătirea generală și controlul măsurilor generale interne de securitate, precum și cu coordonarea cu celelalte autorități de securitate implicate. Măsurile luate de MSO se referă, în general, la:

(a) măsurile de protecție la locul de desfășurare a reuniunii pentru a asigura că aceasta are loc fără incidente care ar putea compromite securitatea informațiilor clasificate UE care ar putea fi utilizate la reuniune;

▼B

(b) verificarea personalului căruia îi este permis accesul la locul de desfășurare a reuniunii, în zonele delegațiilor și în sălile de conferință și verificarea eventualelor echipamente;

(c) coordonarea permanentă cu autoritățile competente ale statului membru gazdă și cu ►M2 Direcția pentru Securitate a Comisiei ◄;

(d) includerea în dosarul reuniunii a unor instrucțiuni de securitate care țin cont în mod adecvat de cerințele prevăzute în prezentele norme de securitate și a oricăror instrucțiuni de securitate considerate necesare.

23.3. **Măsuri de securitate**

23.3.1. *Zone de securitate*

Se instituie următoarele zone de securitate:

(a) o zonă de securitate de clasa II, formată dintr-o sală de redactare, birourile și echipamentele de reproducere ale Comisiei, precum și birourile delegațiilor, dacă este cazul;

(b) o zonă de securitate de clasa I, formată din sala de conferință și cabinele interpreților și ale inginerilor de sunet;

(c) zone administrative, care includ zona destinată presei și sectoarele rezervate pentru administrație, servirea mesei și cazare, precum și zona din imediata apropiere a centrului de presă și a locului de desfășurare a reuniunii.

23.3.2. *Permise*

MSO oferă ecusoane adecvate, în funcție de necesitățile delegațiilor. Dacă este cazul, se poate face o diferențiere în ceea ce privește accesul în diferite zone de securitate.

Instrucțiunile de securitate pentru reuniune prevăd ca toate persoanele implicate să își poarte permanent și la vedere ecusoanele în locul de desfășurare a reuniunii, astfel încât să poată fi verificate de personalul de securitate, dacă este cazul.

În afara participanților care dețin ecusoane, sunt admise la locul de desfășurare a reuniunii cât mai puține persoane posibil. MSO permite delegațiilor naționale să primească vizitatori în cursul reuniunii doar la cererea acestora. Vizitatorilor trebuie să li se ofere un ecuson de vizitator. Se completează un formular de vizită care indică numele vizitatorului și numele persoanei vizitate. Vizitatorii sunt însoțiți în permanență de un agent de securitate sau de persoana vizitată. Formularul de vizită este purtat de însoțitor, care îl înapoiază, împreună cu ecusonul de vizitator, personalului de securitate în momentul în care vizitatorul părăsește locul reuniunii.

23.3.3. *Controlul echipamentelor foto și audio*

Într-o zonă de securitate de clasa I nu pot fi introduse aparate foto sau de înregistrare, cu excepția echipamentelor introduse de fotografii și de inginerii de sunet autorizați corespunzător de MSO.

23.3.4. *Verificarea servietelor, a computerelor portabile și a pachetelor*

Purtătorii de ecusoane cărora le este permis accesul într-o zonă de securitate pot introduce în mod normal la locul reuniunii servietele și computerele lor portabile (doar cu sursă proprie de alimentare) fără efectuarea unei verificări. În ceea ce privește pachetele pentru delegații, acestea din urmă pot accepta livrarea pachetelor, care sunt fie inspectate de ofițerul de securitate al delegației, fie sunt verificate cu echipamente speciale, fie sunt deschise de personalul de securitate pentru inspectare. Dacă MSO consideră că este necesar, pot fi prevăzute măsuri mai stricte pentru inspectarea servietelor și a pachetelor.

▼B

23.3.5. *Securitatea tehnică*

O echipă de securitate tehnică poate asigura securitatea tehnică a sălii și, de asemenea, supravegherea electronică în timpul reuniunii.

23.3.6. *Documentele delegațiilor*

Delegațiile sunt responsabile cu transportul documentelor clasificate UE la și de la reuniuni. De asemenea, ele sunt responsabile cu verificarea și securitatea documentelor în cauză în timpul utilizării lor în spațiile care le sunt alocate. Poate fi solicitat ajutorul statelor membre gazdă pentru transportul documentelor clasificate la și de la locul de desfășurare a reuniunii.

23.3.7. *Păstrarea în siguranță a documentelor*

În cazul în care Comisia sau delegațiile nu au posibilitatea de a-și păstra documentele clasificate în conformitate cu standardele aprobate, ele pot încredința documentele în cauză, într-un plic sigilat și în schimbul unei confirmări de primire, ofițerului de securitate al reuniunii, astfel încât acesta din urmă să poată păstra documentele în conformitate cu standardele aprobate.

23.3.8. *Inspectarea birourilor*

Ofițerul de securitate al reuniunii organizează inspectarea birourilor Comisiei și ale delegațiilor la sfârșitul fiecărei zile de lucru pentru a asigura păstrarea în siguranță a tuturor documentelor clasificate UE. În cazul în care este periclitată siguranța documentelor, ofițerul de securitate al reuniunii ia măsurile necesare.

23.3.9. *Eliminarea deșeurilor clasificate UE*

Toate deșeurile sunt considerate ca fiind clasificate UE, iar pentru eliminarea acestora sunt puse la dispoziția Comisiei și a delegațiilor coșuri pentru deșeuri de hârtie sau pungi. Înainte de părăsirea spațiilor alocate, Comisia și delegațiile predau deșeurile ofițerului de securitate al reuniunii, care asigură distrugerea lor conform normelor.

La sfârșitul reuniunii, toate documentele deținute de Comisie sau de delegații, dar care nu mai sunt necesare, sunt considerate deșeuri. Înainte de ridicarea măsurilor de securitate adoptate pentru reuniune, spațiile alocate Comisiei și delegațiilor sunt cercetate atent. În măsura posibilului, documentele pentru care s-a semnat o confirmare de primire sunt distruse în conformitate cu secțiunea 22.5.

24. ÎNCĂLCĂRI ALE SECURITĂȚII ȘI COMPROMITEREA INFORMAȚIILOR CLASIFICATE UE

24.1. **Definiții**

O încălcare a securității apare ca urmare a unui act sau a unei omisiuni contrare unei dispoziții de securitate a Comisiei care ar putea pune în pericol sau compromite informații clasificate UE.

Compromiterea informațiilor clasificate UE survine în cazul în care informațiile în cauză ajung, integral sau parțial, în posesia unor persoane neautorizate, adică persoane care nu dețin nici autorizarea adecvată de securitate, nici nevoia de a cunoaște necesară, sau în cazul în care există posibilitatea ca un astfel de eveniment să fi avut loc.

Informațiile clasificate UE pot fi compromise ca urmare a neatenției, neglijenței sau indiscreției, precum și prin activitățile serviciilor care au ca țintă UE sau statele sale membre în ceea ce privește informațiile clasificate și activitățile UE sau ale unor organizații subversive.

24.2. **Raportarea încălcărilor normelor de securitate**

Toate persoanele care trebuie să prelucreze informații clasificate UE sunt instruite complet cu privire la responsabilitățile ce le revin în acest domeniu. Ele raportează imediat orice încălcare a securității de care au cunoștință.

▼B

În cazul în care ofițerul local de securitate sau ofițerul de securitate al reuniunii descoperă sau este informat despre o încălcare a securității în privința informațiilor clasificate UE sau despre pierderea sau dispariția unor materiale clasificate UE, acesta acționează imediat pentru:

(a) a salva dovezile;

(b) a stabili faptele;

(c) a evalua și a reduce daunele cauzate;

(d) a preveni repetarea faptelor;

(e) a notifica autorităților competente efectele încălcării securității.

În acest context, sunt furnizate următoarele informații:

(i) o descriere a informațiilor în cauză, inclusiv clasificarea, referința, numărul exemplarului, data, autoritatea de origine, subiectul și sfera documentului;

(ii) o scurtă descriere a circumstanțelor încălcării securității, inclusiv data și perioada în care informația a fost expusă compromiterii;

(iii) o declarație specificând dacă autoritatea de origine a fost sau nu informată.

Imediat ce îi este notificată posibilitatea ca o astfel de încălcare a securității să fi survenit, fiecare autoritate de securitate are sarcina de a raporta imediat acest lucru Biroului de securitate al Comisiei.

Cazurile care implică informații ►**M1** RESTREINT UE ◄ trebuie raportate doar dacă prezintă caracteristici neobișnuite.

Când este informat despre o încălcare a securității, membrul Comisiei însărcinat cu probleme de securitate:

(a) anunță autoritatea de origine care a furnizat informațiile clasificate în cauză;

(b) solicită autorităților de securitate competente inițierea unei investigații;

(c) coordonează anchetele în cazurile în care sunt implicate mai multe autorități de securitate;

(d) obține un raport privind circumstanțele încălcării, data sau perioada în care a avut loc și a fost descoperită, cu o descriere detaliată a conținutului și clasificării materialelor implicate. Se precizează, de asemenea, daunele cauzate intereselor UE sau ale unuia sau mai multora dintre statele sale membre și acțiunile întreprinse pentru a preveni repetarea încălcării.

Autoritatea de origine informează destinatarii și furnizează instrucțiunile adecvate.

24.3. **Acțiuni în justiție**

Orice persoană care este răspunzătoare de compromiterea informațiilor clasificate UE este pasibilă de sancțiuni disciplinare în conformitate cu reglementările relevante, în special titlul VI din Statutul funcționarilor. Sancțiunile în cauză nu aduc atingere oricărei acțiuni ulterioare în justiție.

Dacă este cazul, pe baza raportului menționat în secțiunea 24.2, membrul Comisiei însărcinat cu probleme de securitate face demersurile necesare pentru a permite autorităților naționale competente inițierea procedurilor penale.

▼B

25. PROTECȚIA INFORMAȚIILOR CLASIFICATE UE PRELUCRATE ÎN SISTEME DE TEHNOLOGIA INFORMAȚIEI ȘI DE COMUNICAȚII

25.1. **Introducere**

25.1.1. *Generalități*

Politica de securitate și cerințele în acest domeniu se aplică tuturor sistemelor și rețelelor informatice și de comunicații (denumite în continuare sisteme) care prelucrează informații clasificate ►**M1** CONFIDENTIEL UE ◄ și de nivel superior. Acestea se aplică ca o completare la Decizia C (95) 1510 final a Comisiei din 23 noiembrie 1995 privind protecția sistemelor informatice.

Sistemele care prelucrează informații ►**M1** RESTREINT UE ◄ necesită, de asemenea, măsuri de securitate pentru a proteja confidențialitatea informațiilor în cauză. Toate sistemele necesită măsuri de securitate pentru protejarea integrității și disponibilității sistemelor în cauză și ale informațiilor pe care le conțin.

Politica de securitate IT aplicată de Comisie include următoarele elemente:

— face parte integrantă din securitate în general și completează toate elementele de securitate a informațiilor, securitate a personalului și securitate fizică;

— repartizarea responsabilităților între proprietarii de sisteme tehnice, proprietarii de ICUE stocate sau prelucrate în sisteme tehnice, specialiștii în securitate IT și utilizatori;

— descrierea principiilor și cerințelor de securitate pentru fiecare sistem IT;

— aprobarea principiilor și cerințelor respective de către o autoritate desemnată;

— luarea în considerare a amenințărilor și a vulnerabilităților specifice din domeniul IT.

25.1.2. *Amenințări asupra sistemelor și vulnerabilitățile acestora*

O amenințare poate fi definită ca o posibilitate de compromitere accidentală sau deliberată a securității. În cazul sistemelor, o astfel de compromitere implică pierderea uneia sau multora dintre proprietățile de confidențialitate, integritate și disponibilitate. O vulnerabilitate poate fi definită ca o slăbiciune sau o lipsă de control care ar putea facilita sau permite concretizarea unei amenințări împotriva unui bun sau a unei ținte specifice.

Informațiile clasificate și neclasificate UE prelucrate în sisteme într-o formă concentrată concepută pentru recuperare, comunicare și utilizare rapide sunt vulnerabile la multe amenințări. Acestea includ accesul la informații de către utilizatori neautorizați sau, invers, interzicerea accesului utilizatorilor autorizați. De asemenea, există riscul divulgării neautorizate, al coruperii, al modificării și al ștergerii informațiilor. Mai mult, echipamentele complexe și uneori fragile sunt costisitoare și deseori dificil de reparat sau de înlocuit rapid.

25.1.3. *Principalul scop al măsurilor de securitate*

Principalul scop al măsurilor de securitate prevăzute în prezenta secțiunea este de a asigura protecția împotriva divulgării neautorizate a informațiilor clasificate UE (pierderea confidențialității) și împotriva pierderii integrității și disponibilității informațiilor. Pentru realizarea unei protecții adecvate de securitate a unui sistem care prelucrează informații clasificate UE, standardele adecvate de securitate convențională sunt specificate de ►**M2** Direcția pentru Securitate a Comisiei ◄, împreună cu procedurile și tehnicile de securitate adecvate concepute special pentru fiecare sistem.

▼B

25.1.4. *Declarația privind cerințele de securitate specifice unui sistem (SSRS)*

Pentru toate sistemele care prelucrează informații clasificate ►M1 CONFIDENTIEL UE ◄ și de nivel superior, o declarație privind cerințele de securitate specifice sistemului trebuie elaborată de proprietarul sistemului tehnic (TSO, a se vedea secțiunea 25.3.4) și proprietarul informațiilor (a se vedea secțiunea 25.3.5), dacă este cazul, cu contribuția și asistența personalului responsabil cu proiectul și ale Biroului de securitate al Comisiei (în calitate de autoritate INFOSEC–IA, a se vedea secțiunea 25.3.3), declarație care trebuie aprobată de autoritatea de acreditare de securitate (SAA, a se vedea secțiunea 25.3.2).

De asemenea, este necesară o SSRS în cazul în care autoritatea de acreditare de securitate (SAA) consideră ca fiind esențiale disponibilitatea și integritatea informațiilor ►M1 RESTREINT UE ◄ sau ale celor neclasificate.

SSRS este formulată în prima etapă de concepere a proiectului și este dezvoltată și extinsă pe măsură ce proiectul evoluează, îndeplinind diverse roluri în diferitele etape din ciclul de viață al proiectului și al sistemului.

25.1.5. *Moduri de operare de securitate*

Toate sistemele care prelucrează informații clasificate ►M1 CONFIDENTIEL UE ◄ și de nivel superior sunt acreditate să funcționeze în unul sau, în cazul în care acest lucru este justificat de cerințe în diferite perioade de timp, în mai multe dintre următoarele moduri de operare de securitate sau în echivalentul național al acestora:

(a) exclusiv;

(b) prioritar și

(c) multinivel.

25.2. **Definiții**

„Acreditare” înseamnă autorizarea și aprobarea acordate unui sistem de a prelucra informații clasificate UE în mediul său de operare.

Notă:

Acreditarea trebuie efectuată după punerea în aplicare a tuturor procedurilor adecvate de securitate și atingerea unui nivel suficient de protecție a resurselor sistemului. Acreditarea trebuie acordată, în mod normal, pe baza SSRS, inclusiv a următoarelor elemente:

(a) o declarație privind obiectivul acreditării sistemului: în special, nivelul (nivelurile) de clasificare a informațiilor care urmează a fi prelucrate și modul (modurile) de operare de securitate propus (propuse) pentru sistem sau rețea;

(b) elaborarea unei analize a riscului de gestionare pentru identificarea amenințărilor și vulnerabilităților și a măsurilor de prevenire a acestora;

(c) procedurile de operare de securitate (SecOP) cu o descriere detaliată a operațiunilor propuse (de exemplu, moduri, servicii care urmează a fi furnizate), inclusiv o descriere a caracteristicilor de securitate ale sistemului care stau la baza acreditării;

(d) planul de punere în aplicare și de menținere a caracteristicilor de securitate;

(e) planul pentru testarea, evaluarea și certificarea vizând securitatea inițială și ulterioară a sistemului sau a rețelei și

(f) certificarea, dacă este necesară, împreună cu alte elemente de acreditare.

▼B

„Ofițerul central de securitate informatică” (CISO) înseamnă funcționarul dintr-un serviciu central IT care coordonează și supervizează măsurile de securitate pentru sistemele organizate în mod centralizat.

„Certificare” înseamnă emiterea unei declarații oficiale, justificată de o analiză independentă a desfășurării și a rezultatelor unei evaluări, a măsurii în care un sistem îndeplinește cerința de securitate sau în care un produs de securitate informatică îndeplinește cerințele de securitate definite în prealabil.

„Securitatea comunicațiilor” (COMSEC) înseamnă aplicarea de măsuri de securitate telecomunicațiilor pentru a împiedica persoanele neautorizate să obțină informații de valoare prin deținerea și studierea mesajelor comunicate sau pentru a asigura autenticitatea acestor mesaje.

Notă:

Măsurile în cauză includ securitatea mijloacelor de codificare, a transmisiilor și a emisiilor, precum și securitatea fizică, a procedurilor, a personalului, a documentelor și securitatea informatică.

„Securitatea informatică” (COMPUSEC) înseamnă aplicarea caracteristicilor de securitate hardware, firmware și software unui sistem computerizat pentru a-l proteja împotriva divulgării neautorizate, manipulării, modificării/ștergerii informațiilor sau blocării accesului sau pentru a preveni aceste amenințări.

„Produs de securitate informatică” înseamnă un element generic de securitate informatică care este destinat a fi încorporat într-un sistem IT pentru a fi utilizat la creșterea sau asigurarea confidențialității, integrității sau disponibilității informațiilor prelucrate.

„Modul exclusiv de operare de securitate” înseamnă un mod de operare în care TOATE persoanele care au acces la sistem sunt autorizate la cel mai înalt nivel de clasificare a informațiilor prelucrate în cadrul sistemului și au o nevoie comună de a cunoaște TOATE informațiile prelucrate în cadrul sistemului.

Note:

1. Nevoia comună de a cunoaște indică faptul că nu este obligatoriu ca prin caracteristicile de securitate informatică să se asigure separarea informațiilor în cadrul sistemului.

2. Alte caracteristici de securitate (de exemplu aspecte fizice, aspecte privind personalul și procedurile) îndeplinesc cerințele stabilite pentru cel mai înalt nivel de clasificare și pentru toate categoriile de informații prelucrate în cadrul sistemului.

„Evaluare” înseamnă examinarea tehnică detaliată, efectuată de autoritatea competentă, a aspectelor de securitate ale unui sistem, ale unui produs de codificare sau ale unui produs de securitate informatică.

Note:

1. Evaluarea investighează prezența funcționalității de securitate necesare și absența efectelor secundare compromițătoare ale acestei funcționalități și analizează incoruptibilitatea acestei funcționalități.

2. Evaluarea determină măsura în care sunt îndeplinite cerințele de securitate ale unui sistem sau caracteristicile pretinse de securitate ale unui produs de securitate informatică și stabilește nivelul de asigurare al sistemului sau al echipamentului de codificare sau funcția de încredere a produsului de securitate informatică.

„Proprietarul informației” (IO) înseamnă autoritatea (șeful de departament) care are responsabilitatea creării, prelucrării și utilizării informațiilor, inclusiv în ceea ce privește decizia referitoare la persoanele care pot avea acces la informațiile în cauză.

▼B

„Securitatea informațiilor” (INFOSEC) înseamnă aplicarea de măsuri de securitate pentru a proteja informațiile prelucrate, stocate sau transmise prin sisteme informatice, de comunicații și prin alte sisteme electronice împotriva pierderii, accidentale sau intenționate, a confidențialității, integrității sau disponibilității și pentru a preveni pierderea integrității și disponibilității sistemelor.

„Măsurile INFOSEC” includ măsurile de securitate informatică, a transmisiilor, a emisiilor și a mijloacelor de codificare și măsurile de detectare, documentare și contracarare a amenințărilor la adresa informațiilor și a sistemelor.

„Zonă IT” înseamnă o zonă care conține unul sau mai multe computere, unitățile lor locale periferice și de stocare, unitățile de control și echipamentele de rețea și de comunicații care le sunt rezervate.

Notă:

Această zonă nu include o zonă separată în care sunt amplasate echipamente periferice la distanță sau terminale/posturi de lucru, chiar dacă acestea sunt conectate la echipamente din zona IT.

„Rețea IT” înseamnă organizarea, dispersată geografic, a unor sisteme IT interconectate pentru schimburi de date care include componentele sistemelor IT interconectate și interfața acestora cu rețele de date sau de comunicații care le completează.

Note:

1. O rețea IT poate utiliza serviciile uneia sau mai multor rețele de comunicații interconectate pentru schimburi de date; mai multe rețele IT pot utiliza serviciile unei rețele comune de comunicații.

2. O rețea IT este denumită „locală” dacă interconectează mai multe computere din același amplasament.

„Caracteristicile de securitate ale rețelei IT” includ caracteristicile de securitate ale fiecărui sistem IT care face parte din rețea împreună cu componentele și caracteristicile suplimentare asociate direct rețelei (de exemplu, comunicații în rețea, mecanisme și proceduri de identificare de securitate și de etichetare, controale de acces, programe și piste de urmărire) necesare pentru a asigura informațiilor clasificate un nivel acceptabil de protecție.

„Sistem IT” înseamnă ansamblul de echipamente, metode și proceduri și, dacă este necesar, de personal organizat în vederea realizării funcțiilor de prelucrate a informațiilor.

Note:

1. Acesta reprezintă un ansamblu de mijloace, configurate pentru prelucrarea informațiilor în cadrul sistemului.

2. Astfel de sisteme pot fi utilizate pentru funcții de consultare, comandă, control, comunicații, aplicații științifice sau administrative, inclusiv prelucrare de texte.

3. Limitele unui sistem sunt în general determinate ca fiind elementele aflate sub controlul unui singur TSO.

4. Un sistem IT poate conține subsisteme, dintre care unele sunt ele însele sisteme IT.

▼B

„Caracteristicile de securitate ale sistemului IT” includ toate funcțiile, calitățile și caracteristicile hardware/firmware/software; procedurile de operare, procedurile de responsabilizare și controalele de acces, zona IT, zona terminalelor/posturilor de lucru la distanță, normele de gestionare, structura și dispozitivele fizice, controalele asupra personalului și comunicațiilor necesare pentru a asigura informațiilor clasificate prelucrate în sistemul IT un nivel acceptabil de protecție.

„Ofițerul local de securitate informatică” (LISO) înseamnă funcționarul dintr-un departament al Comisiei care este însărcinat să coordoneze și să supravegheze măsurile de securitate din domeniul său.

„Modul de operare de securitate multinivel” înseamnă un mod de operare în care NU TOATE persoanele care accesează sistemul au autorizare pentru cel mai înalt nivel de clasificare al informațiilor prelucrate în cadrul sistemului și NU TOATE persoanele care au acces la sistem au o nevoie comună de a cunoaște pentru informațiile prelucrate în cadrul sistemului.

Note:

1. Acest mod de operare permite, simultan, prelucrarea unor informații având niveluri diferite de clasificare și a unor informații de diferite categorii.

2. Faptul că nu toate persoanele sunt autorizate la cele mai înalte niveluri, asociat cu absența unei nevoi comune de a cunoaște, arată că sunt necesare caracteristici de securitate informatică care să asigure accesul selectiv la informații și separarea acestora în cadrul sistemului.

„Zonă de terminale/posturi de lucru la distanță” înseamnă o zonă, separată de o zonă IT, care conține anumite echipamente informatice, dispozitivele lor periferice locale sau terminalele/posturile de lucru și echipamentele asociate de comunicații.

„Procedura de operare de securitate” înseamnă procedurile elaborate de proprietarul sistemelor tehnice care definesc principiile ce trebuie respectate în domeniul securității, procedurile de operare care trebuie urmate și responsabilitățile personalului.

„Modul de operare de securitate prioritar” înseamnă un mod de operare în care TOATE persoanele care au acces la sistem sunt autorizate la cel mai înalt nivel de clasificare a informațiilor prelucrate în cadrul sistemului, dar NU TOATE persoanele care au acces la sistem au o nevoie comună de a cunoaște pentru informațiile prelucrate în cadrul sistemului.

Note:

1. Absența unei nevoi comune de a cunoaște arată că sunt necesare caracteristici de securitate informatică care să asigure accesul selectiv la informații și separarea acestora în cadrul sistemului.

2. Alte caracteristici de securitate (de exemplu aspecte fizice, aspecte privind personalul și procedurile) îndeplinesc cerințele stabilite pentru cel mai înalt nivel de clasificare și pentru toate categoriile de informații prelucrate în cadrul sistemului.

3. Toate informațiile prelucrate sau disponibile în cadrul unui sistem în acest mod de operare, împreună cu rezultatele obținute, sunt protejate ca aparținând, potențial, categoriei de informații și celui mai înalt nivel de clasificare al informațiilor prelucrate, până în momentul în care se stabilește altfel, cu excepția cazului în care se poate atașa un nivel acceptabil de încredere unei funcții de etichetare existente.

▼B

O „declarație privind cerințele de securitate specifice unui sistem” (SSRS) este o declarație completă și explicită a principiilor de securitate care trebuie respectate și a cerințelor detaliate de securitate care trebuie îndeplinite. Ea se bazează pe politica de securitate a Comisiei și pe o evaluare a riscurilor sau este impusă de parametri precum mediul de operare, cel mai scăzut nivel de autorizare de securitate a personalului, cel mai ridicat nivel de clasificare a informațiilor prelucrate, modul de operare de securitate sau cerințele utilizatorilor. SSRS face parte integrantă din documentația de proiect prezentată autorităților competente pentru aprobarea tehnică, bugetară și de securitate. În forma sa finală, SSRS reprezintă o declarație completă a ceea ce înseamnă securitatea sistemului.

„Proprietarul sistemelor tehnice” (TSO) înseamnă autoritatea care are responsabilitatea creării, întreținerii, operării și închiderii unui sistem.

Contramăsuri „Tempest” înseamnă măsuri de securitate destinate să protejeze echipamentele și infrastructurile de comunicații împotriva compromiterii informațiilor clasificate prin emisii electromagnetice neintenționate și prin conductivitate.

25.3. **Responsabilități în materie de securitate**

25.3.1. *Generalități*

Responsabilitățile consultative ale Grupului consultativ pentru politica de securitate a Comisiei, definite în secțiunea 12, includ chestiuni INFOSEC. Grupul își organizează activitățile astfel încât să poate oferi sfaturi specializate privind chestiunile menționate anterior.

►**M2** Direcția pentru Securitate a Comisiei ◄ este însărcinat cu emiterea dispozițiilor detaliate INFOSEC, pe baza dispozițiilor prezentului capitol.

În cazul unor probleme privind securitatea (incidente, încălcări etc.), ►**M2** Direcția pentru Securitate a Comisiei ◄ adoptă măsuri imediate.

►**M2** Direcția pentru Securitate a Comisiei ◄ dispune de o unitate INFOSEC.

25.3.2. *Autoritatea de acreditare de securitate (SAA)*

►**M2** Directorul Direcției pentru Securitate a Comisiei ◄ reprezintă autoritatea de acreditare de securitate (SAA) a Comisiei. SAA are responsabilități în domeniul general al securității și în domeniile specializate ale INFOSEC, în domeniul securității comunicațiilor, al securității Crypto și al securității Tempest.

SAA este însărcinată să asigure conformitatea sistemelor cu politica de securitate a Comisiei. Una dintre sarcinile sale este aceea de a acorda aprobarea unui sistem de a prelucra informații clasificate UE până la un anumit nivel de clasificare în mediul său de operare.

Jurisdicția SAA a Comisiei include toate sistemele care operează în sediile de lucru ale Comisiei. În momentul în care diverse componente ale unui sistem intră sub jurisdicția SAA a Comisiei și a altor SAA, toate părțile implicate pot desemna un comitet comun de acreditare sub coordonarea SAA a Comisiei.

25.3.3. *Autoritatea INFOSEC (IA)*

Șeful unității INFOSEC a Biroului de securitate al Comisiei reprezintă autoritatea INFOSEC a Comisiei. Autoritatea INFOSEC are sarcinile:

— de a furniza SAA consultanță și asistență tehnică;

— de a contribui la elaborarea SSRS;

▼B

— de a revizui SSRS pentru a asigura conformitatea cu prezentele norme de securitate și cu politicile INFOSEC și cu documentele privind arhitectura;

— de a participa la grupurile/comitetele de acreditare în funcție de necesități și de a prezenta SAA o recomandare INFOSEC privind acreditarea;

— de a sprijini activitățile de formare și instruire INFOSEC;

— de a furniza consultanță tehnică în investigarea incidentelor privind INFOSEC;

— de a elabora linii directoare tehnice pentru a asigura doar utilizarea de software autorizat.

25.3.4. *Proprietarul sistemelor tehnice (TSO)*

Responsabilitatea punerii în aplicare și a operării controalelor și caracteristicilor speciale de securitate ale unui sistem aparține proprietarului sistemului, proprietarul sistemelor tehnice (TSO). Pentru sistemele deținute la nivel central, este desemnat un ofițer central de securitate informatică (CISO). Fiecare departament desemnează, după caz, un ofițer local de securitate informatică (LISO). Responsabilitatea unui TSO include elaborarea de proceduri de operare de securitate (SecOP) și se extinde, pe durata ciclului de viață al unui sistem, de la etapa de concepere a proiectului la oprirea definitivă.

TSO specifică standardele și practicile de securitate care trebuie îndeplinite de furnizorul sistemului.

TSO poate delega o parte din responsabilitățile sale, dacă este cazul, unui ofițer local de securitate informatică. O singură persoană poate exercita diversele funcții INFOSEC.

25.3.5. *Proprietarul informației (IO)*

Proprietarul informației (IO) este responsabil de ICUE (și alte informații) care urmează a fi introduse, prelucrate și produse în sistemele tehnice. Acesta definește cerințele pentru accesul la aceste informații din cadrul sistemelor. El poate delega această responsabilitate unui gestionar de informații sau unui gestionar de bază de date din domeniul său.

25.3.6. *Utilizatori*

Toți utilizatorii au responsabilitatea de a asigura că acțiunile lor nu afectează negativ securitatea sistemului pe care îl utilizează.

25.3.7. *Formarea INFOSEC*

Instruirea și formarea INFOSEC sunt disponibile întregului personal care are nevoie de acestea.

25.4. **Măsuri de securitate fără caracter tehnic**

25.4.1. *Securitatea personalului*

Utilizatorii sistemului sunt autorizați și au nevoia de a cunoaște, corespunzător clasificării și conținutului informațiilor prelucrate în cadrul sistemului lor specific. Pentru accesul la anumite echipamente și informații specifice securității sistemelor este necesară o autorizație specială emisă în conformitate cu procedurile Comisiei.

SAA desemnează toate posturile sensibile și specifică nivelul de autorizare și supervizare necesar pentru întregul personal care ocupă aceste posturi.

Sistemele sunt specificate și concepute într-un mod care să faciliteze alocarea de sarcini și responsabilități personalului, astfel încât să se prevină situațiile în care o singură persoană deține toate cunoștințele și întregul control asupra punctelor cheie ale securității sistemului.

▼B

Un funcționar autorizat sau un alt angajat nu trebuie să se afle niciodată singur în zonele IT și în zonele de terminale/posturi de lucru la distanță în care securitatea sistemului poate fi modificată.

Setările de securitate ale unui sistem sunt modificate doar de către cel puțin două persoane autorizate care lucrează împreună.

25.4.2. *Securitatea fizică*

Zonele IT și zonele de terminale/posturi de lucru la distanță (definite în secțiunea 25.2) în care sunt prelucrate prin mijloace IT informații clasificate ►M1 CONFIDENTIEL UE ◄ și de nivel superior sau în care este posibil accesul potențial la astfel de informații sunt desemnate ca zone de securitate UE de clasa I sau II, după caz.

25.4.3. *Controlul accesului la un sistem*

Toate informațiile și materialele care asigură controlul asupra accesului la un sistem sunt protejate prin măsuri corespunzătoare celui mai înalt nivel de clasificare și categoriei informațiilor la care pot asigura accesul.

Când nu mai sunt utilizate în acest scop, informațiile și materialele de control al accesului sunt distruse în conformitate cu dispozițiile secțiunii 25.5.4.

25.5. **Măsuri tehnice de securitate**

25.5.1. *Securitatea informațiilor*

Autorității de origine a informațiilor îi revine sarcina de a identifica și de a clasifica toate documentele purtătoare de informații, indiferent dacă acestea au forma unui produs pe suport de hârtie sau pe suport informatic. Clasificarea este marcată, în partea de sus și în cea de jos, pe fiecare pagină a unui produs pe suport de hârtie. Produsul, indiferent dacă este pe suport de hârtie sau pe suport informatic, este clasificat la cel mai înalt nivel de clasificare a informațiilor utilizate pentru producerea lui. Modul de operare al unui sistem poate influența, de asemenea, clasificarea produselor sistemului în cauză.

Departamentelor Comisiei și deținătorilor de informații ale Comisiei le revine sarcina de a analiza problemele privind agregarea elementelor individuale ale informațiilor și deducțiile care pot fi făcute prin corelarea elementelor, precum și de a determina dacă o clasificare superioară este sau nu adecvată pentru ansamblul informațiilor.

Faptul că informațiile pot fi un cod abreviat, un cod de transmitere sau orice formă de reprezentare binară nu asigură o protecție de securitate și, prin urmare, nu ar trebui să influențeze clasificarea informațiilor.

Atunci când informațiile sunt transferate dintr-un sistem în altul, informațiile sunt protejate în cursul transferului și în sistemul destinatar într-o manieră adaptată clasificării și categoriei inițiale a informațiilor.

Toate suporturile informatice de stocare sunt tratate într-un mod corespunzător celei mai înalte clasificări a informațiilor stocate sau etichetei suportului și sunt protejate în mod adecvat în orice moment.

Suporturile informatice de stocare reutilizabile folosite pentru înregistrarea de informații clasificate UE păstrează cea mai înaltă clasificare pentru care au fost utilizate, până în momentul în care informațiile în cauză sunt declasate sau declasificare corespunzător, iar suportul este reclasificat în consecință sau până în momentul în care suportul este declasificat sau distrus în conformitate cu o procedură aprobată de SAA (a se vedea punctul 25.5.4).

▼B

25.5.2. *Controlul și contabilizarea informațiilor*

Accesul la informații clasificate ►M1 SECRET UE ◄ și de nivel superior este înscris în registre automate (piste de urmărire) sau manuale. Aceste registre sunt păstrate în conformitate cu prezentele norme de securitate.

Produsele clasificate UE păstrate în zona IT pot fi tratate ca un singur element clasificat și nu trebuie înregistrate, cu condiția ca materialele să fie identificate, marcate cu clasificarea corespunzătoare și controlate în mod adecvat.

Dacă produsul este generat de un sistem care prelucrează informații clasificate UE, iar apoi este transmis unei zone de terminale/posturi de lucru la distanță dintr-o zonă IT, se instituie proceduri aprobate de SAA pentru controlul și înregistrarea produsului. Pentru informații ►M1 SECRET UE ◄ și de nivel superior, aceste proceduri includ instrucțiuni specifice pentru contabilizarea informațiilor.

25.5.3. *Manipularea și controlul suporturilor informatice de stocare mobile*

Toate suporturile informatice de stocare mobile clasificate ►M1 CONFIDENTIEL UE ◄ și de nivel superior sunt tratate ca materiale clasificate, cu aplicarea normelor generale. Mijloacele adecvate de identificare și clasificare trebuie să fie adaptate caracteristicilor fizice ale suporturilor, pentru a permite recunoașterea clară a acestora.

Utilizatorilor le revine responsabilitatea de a asigura stocarea informațiilor clasificate UE pe suporturi având marcajul și protecția de securitate adecvate. Se instituie proceduri pentru a asigura că, pentru toate nivelurile de informații UE, înregistrarea informațiilor pe suporturi informatice de stocare se efectuează în conformitate cu prezentele norme de securitate.

25.5.4. *Declasificarea și distrugerea suporturilor informatice de stocare*

Suporturile informatice de stocare utilizate pentru înregistrarea de informații clasificate UE pot fi declasate sau declasificate în conformitate cu o procedură care urmează a fi aprobată de SAA.

Suporturile informatice de stocare pe care au fost înregistrate informații ►M1 TRES SECRET UE/EU TOP SECRET ◄ sau informații dintr-o categorie specială nu sunt declasificate și reutilizate.

Dacă suporturile informatice de stocare nu pot fi declasificate sau nu sunt reutilizabile, acestea sunt distruse în conformitate cu procedura menționată anterior.

25.5.5. *Securitatea comunicațiilor*

►M2 Directorul Direcției pentru Securitate a Comisiei ◄ reprezintă autoritatea Crypto.

Dacă informațiile clasificate UE sunt transmise pe cale electromagnetică, se aplică măsuri speciale pentru protejarea confidențialității, integrității și disponibilității acestor transmisii. SAA stabilește cerințele pentru protejarea transmisiilor împotriva detectării și interceptării. Informațiile transmise printr-un sistem de comunicații sunt protejate conform cerințelor de confidențialitate, integritate și disponibilitate.

Dacă sunt necesare metode de codificare pentru asigurarea confidențialității, integrității și disponibilității, metodele în cauză și produsele asociate sunt aprobate în mod expres în acest scop de SAA în calitate de autoritate Crypto.

▼B

În timpul transmisiei, confidențialitatea informațiilor clasificate ►M1 SECRET UE ◄ și de nivel superior este protejată prin metode sau produse de codificare aprobate de membrul Comisiei însărcinat cu probleme de securitate după consultarea Grupului consultativ pentru politica de securitate a Comisiei. În cursul transmisiei, confidențialitatea informațiilor clasificate ►M1 CONFIDENTIEL UE ◄ sau ►M1 RESTREINT UE ◄ este protejată prin metode sau produse de codificare aprobate de autoritatea Crypto a Comisiei după consultarea Grupului consultativ pentru politica de securitate a Comisiei.

Normele detaliate aplicabile transmisiei de informații clasificate UE figurează în instrucțiuni specifice de securitate aprobate de ►M2 Direcția pentru Securitate a Comisiei ◄ după consultarea Grupului consultativ pentru politica de securitate a Comisiei.

În condiții excepționale de operare, informațiile clasificare ►M1 RESTREINT UE ◄, ►M1 CONFIDENTIEL UE ◄ și ►M1 SECRET UE ◄ pot fi transmise în clar, cu condiția ca fiecare transmisie să fie autorizată în mod expres de proprietarul informațiilor și să fie înregistrată corespunzător de acesta. Aceste condiții excepționale sunt următoarele:

(a) în situații iminente sau reale de criză, de conflict sau de război;

(b) când viteza de transmisie este de o importanță extremă, când nu sunt disponibile mijloace de codificare și se estimează că informațiile transmise nu pot fi exploatate la timp, ceea ce ar influența negativ operațiunile.

Un sistem trebuie să aibă capacitatea de a interzice categoric accesul la informațiile clasificate UE la nivelul unuia sau tuturor terminalelor sale sau posturilor sale de lucru la distanță, dacă este cazul, fie prin deconectare fizică, fie prin caracteristici specifice de software aprobate de SAA.

25.5.6. *Securitatea privind instalarea și radiațiile*

Instalarea inițială a sistemelor și orice modificare semnificativă a acestora sunt specificate astfel încât instalarea să fie efectuată de instalatori deținând autorizarea de securitate sub supravegherea permanentă a personalului calificat tehnic care deține autorizarea pentru accesul la informații clasificate UE la nivelul echivalent celui mai înalt nivel de clasificare al informațiilor pe care sistemul trebuie să le stocheze și să le prelucreze.

Sistemele care prelucrează informații clasificate ►M1 CONFIDENTIEL UE ◄ și de nivel superior sunt protejate astfel încât securitatea lor să nu poate fi amenințată de emanații sau de o conductivitate compromițătoare, ale căror studiu și control sunt denumite „Tempest”.

Contramăsurile Tempest sunt revizuite și aprobate de autoritatea Tempest (a se vedea punctul 25.3.2).

25.6. **Securitatea în cursul prelucrării**

25.6.1. *Proceduri de operare de securitate (SecOP)*

Procedurile de operare de securitate (SecOP) definesc principiile care trebuie adoptate în ceea ce privește problemele de securitate, procedurile de operare care trebuie urmate și responsabilitățile personalului. SecOP sunt elaborate sub responsabilitatea proprietarului sistemelor tehnice (TSO).

25.6.2. *Gestionarea protecției/configurației produselor software*

Protecția de securitate a programelor de aplicații se determină mai degrabă pe baza unei evaluări a clasificării de securitate a programului în sine decât pe baza clasificării informațiilor pe care trebuie să le prelucreze. Versiunile de software utilizate sunt verificate la intervale regulate pentru a asigura integritatea și corecta funcționare a acestora.

▼B

Versiunile noi sau modificate de software nu sunt utilizate pentru prelucrarea de informații clasificate UE decât după verificarea lor de către TSO.

25.6.3. *Verificarea prezenței unor produse software dăunătoare sau a unor viruși informatici*

În conformitate cu cerințele SAA, se efectuează periodic verificări privind prezența unor produse software dăunătoare sau a unor viruși informatici.

Toate suporturile informatice de stocare care sosesc la Comisie sunt verificate pentru detectarea prezenței unor produse software dăunătoare sau a unor viruși informatici, înainte de a fi introduse într-un sistem.

25.6.4. *Întreținere*

Contractele și procedurile pentru întreținerea periodică și la cerere a sistemelor pentru care s-a elaborat o SSRS specifică cerințele și dispozițiile pentru personalul de întreținere și echipamentele asociate care pătrund într-o zonă IT.

Cerințele sunt menționate clar în SSRS, iar procedurile sunt menționate clar în SecOP. Operațiunile de întreținere efectuate de contractant pentru care sunt necesare proceduri de diagnosticare cu acces de la distanță sunt permise doar în cazuri excepționale, sub control strict de securitate și doar cu aprobarea SAA.

25.7. **Achiziții**

25.7.1. *Generalități*

Orice produs de securitate care urmează a fi utilizat cu sistemul care face obiectul achiziției fie a fost evaluat și certificat, fie face în prezent obiectul unei evaluări și certificări de către un organism adecvat de evaluare și certificare al unuia dintre statele membre UE conform unor criterii recunoscute pe plan internațional (precum Criteriile comune pentru evaluarea securității tehnologiei informației, cf. ISO 15408). Pentru obținerea aprobării CCAC sunt necesare proceduri speciale.

Pentru a decide dacă echipamentele, în special suporturile informatice de stocare, trebuie închiriate și nu achiziționate se ține cont de faptul că astfel de echipamente, după ce au fost utilizate pentru prelucrarea de informații clasificate UE, nu pot părăsi un mediu securizat în mod adecvat fără a fi mai întâi declasificate cu aprobarea SAA, obținerea acestei aprobări nefiind întotdeauna posibilă.

25.7.2. *Acreditare*

Înainte de prelucra informații clasificate UE, toate sistemele pentru care trebuie elaborată o SSRS sunt acreditate de SAA pe baza informațiilor furnizate în SSRS, SecOP și alte documente relevante. Subsistemele și terminalele/posturile de lucru la distanță sunt acreditate ca parte componentă a tuturor sistemelor la care sunt conectate. În cazul în care un sistem deservește atât Comisia, cât și alte organizații, Comisia și autoritățile relevante de securitate se pun de acord în privința acreditării.

Procesul de acreditare se poate desfășura în conformitate cu o strategie de acreditare adecvată unui anumit sistem și definită de SAA.

25.7.3. *Evaluare și certificare*

În anumite situații, înainte de acreditare, caracteristicile de securitate hardware, firmware și software ale unui sistem sunt evaluate și certificate în privința capacității de salvgardare a informațiilor la nivelul de clasificare avut în vedere.

Cerințele de evaluare și certificare sunt incluse în planificarea sistemului și sunt specificate clar în SSRS.

▼B

Procesul de evaluare și certificare este efectuat în conformitate cu liniile directoare aprobate, de către personal calificat tehnic, autorizat adecvat și acționând în numele TSO.

Echipele pot fi asigurate de o anumită autoritate de evaluare și certificare a unui stat membru desemnat sau de reprezentanții desemnați ai acesteia, de exemplu un contractant competent și autorizat.

Nivelul proceselor de evaluare și certificare implicate poate fi redus (de exemplu implicând doar aspecte privind integrarea) în cazul în care sistemele se bazează pe produse de securitate informatică existente evaluate și certificate la nivel național.

25.7.4. *Verificarea sistematică a caracteristicilor de securitate pentru acreditarea continuă*

TSO elaborează proceduri de control sistematic pentru a asigura că toate caracteristicile de securitate ale sistemului sunt încă valabile.

Tipurile de modificări care ar conduce la reacreditare sau care necesită aprobarea prealabilă a SAA sunt identificate și menționate clar în SSRS. După orice modificare, reparație sau defecțiune care ar fi putut afecta caracteristicile de securitate ale sistemului, TSO veghează la efectuarea unei verificări pentru a se asigura funcționarea corectă a caracteristicilor de securitate. Acreditarea continuă a sistemului depinde, în mod normal, de realizarea cu succes a acestor verificări.

Toate sistemele în cadrul cărora s-au aplicat caracteristici de securitate sunt inspectate sau revizuite periodic de către SAA. Pentru sistemele care prelucrează informații ►**M1** TRES SECRET UE/EU TOP SECRET ◄, inspecțiile se efectuează cel puțin o dată pe an.

25.8. **Utilizare temporară sau ocazională**

25.8.1. *Securitatea microcomputerelor/computerelor personale*

Microcomputerele/computerele personale (PC) cu discuri fixe (sau alte suporturi de stocare cu memorie remanentă), funcționând fie în mod autonom, fie în rețea, și dispozitivele informatice portabile (de exemplu, PC-uri portabile și calculatoare electronice mici portabile) cu discuri dure fixe sunt considerate suporturi informatice de stocare în același sens ca și dischetele sau alte suporturi informatice de stocare mobile.

Aceste echipamente beneficiază de un nivel de protecție, în ceea ce privește accesul, prelucrarea, stocarea și transportul, corespunzător celei mai înalte clasificări a informațiilor stocate sau prelucrate vreodată (până la declasarea sau declasificarea acestora în conformitate cu procedurile aprobate).

25.8.2. *Utilizarea de echipamente IT private pentru activități oficiale ale Comisiei*

Pentru prelucrarea informațiilor clasificate UE, este interzisă utilizarea de suporturi informatice de stocare mobile, software și hardware IT private (de exemplu, PC-uri și dispozitive informatice portabile) cu capacități de stocare.

Nu se introduc produse hardware și software și suporturi private într-o zonă de securitate de clasa I sau II în care sunt prelucrate informații clasificate UE fără autorizația scrisă a Șefului Biroului de securitate al Comisiei. Această autorizație se poate acorda doar din motive tehnice în cazuri excepționale.

▼B

25.8.3. *Utilizarea de echipamente IT aparținând contractanților sau furnizate de un stat pentru activitățile oficiale ale Comisiei*

►M2 Directorul Direcției pentru Securitate a Comisiei ◄ poate permite utilizarea de echipamente IT și de produse software aparținând contractanților pentru realizarea activităților oficiale ale Comisiei în cadrul organizațiilor. De asemenea, poate fi permisă utilizarea de echipamente IT și produse software furnizate de un stat; în acest caz, echipamentele IT sunt introduse în inventarul adecvat al Comisiei. În orice caz, dacă echipamentele IT urmează a fi folosite pentru prelucrarea de informații clasificate UE, SAA este consultată pentru ca elementele INFOSEC aplicabile utilizării echipamentelor în cauză să fie luate în considerare i puse în aplicare în mod adecvat.

26. COMUNICAREA DE INFORMAȚII CLASIFICATE UE UNOR STATE TERȚE SAU UNOR ORGANIZAȚII INTERNAȚIONALE

26.1.1. *Principii care reglementează comunicarea de informații clasificate UE*

Colegiul membrilor Comisiei decide în privința comunicării de informații clasificate UE unor state terțe sau unor organizații internaționale pe baza:

— naturii și conținutului informațiilor în cauză;

— nevoii de a cunoaște a destinatarilor;

— aprecierii avantajelor pentru UE.

Se va solicita acordul autorității de origine a informațiilor clasificate UE care urmează a fi comunicate.

Aceste decizii se iau de la caz la caz, în funcție de:

— nivelul de cooperare dorit cu statele terțe sau organizațiile internaționale în cauză;

— încrederea care le poate fi acordată – care rezultă din nivelul de securitate care s-ar aplica informațiilor confidențiale UE comunicate statelor și organizațiilor în cauză și din compatibilitatea dintre normele aplicabile în statele sau organizațiile în cauză și cele aplicate în UE. Grupul consultativ pentru politica de securitate a Comisiei furnizează Comisiei avizul său tehnic în privința acestui aspect.

Acceptarea de informații clasificate UE de către state terțe sau organizații internaționale implică o asigurare că informațiile în cauză nu vor fi utilizate pentru alte scopuri decât cele care au motivat comunicarea sau schimbul de informații și că ele vor beneficia de protecția solicitată de Comisie.

26.1.2. *Niveluri*

După ce a decis că informațiile clasificate pot fi comunicate unui anumit stat membru sau unei organizații internaționale sau pot face obiectul unui schimb de informații cu acestea, Comisia decide asupra nivelului de cooperare care este posibil. Acesta depinde, în special, de politica și de reglementările de securitate aplicate de statul sau organizația în cauză.

Există trei niveluri de cooperare:

Nivelul 1

Cooperare cu state terțe sau organizații internaționale ale căror politică și reglementări de securitate sunt foarte apropiate de cele ale UE.

Nivelul 2

Cooperare cu state terțe sau organizații internaționale ale căror politică și reglementări de securitate sunt sensibil diferite de cele ale UE.

▼B

Nivelul 3

Cooperare ocazională cu state terțe sau organizații internaționale ale căror politică și reglementări de securitate nu pot fi evaluate.

Fiecare nivel de cooperare determină procedurile și dispozițiile de securitate aplicabile, detaliate în apendicele 3, 4, și 5.

26.1.3. *Acorduri de securitate*

După ce a decis că sunt necesare, permanent sau pe termen lung, schimburi de informații clasificate între Comisie și state terțe sau alte organizații internaționale, Comisia încheie „acorduri privind procedurile de securitate pentru schimbul de informații clasificate" cu acestea, definind scopul cooperării și normele reciproce privind protecția informațiilor comunicate.

În cazul cooperării ocazionale de nivelul 3, ale cărei durată și scop sunt limitate prin definiție, un simplu memorandum de înțelegere care definește natura informațiilor clasificate ce fac obiectul schimbului și obligațiile reciproce privind informațiile în cauză poate înlocui „acordul privind procedurile de securitate pentru schimbul de informații clasificate", cu condiția ca nivelul de clasificare al informațiilor să nu fie mai mare decât ►M1 RESTREINT UE ◄.

Proiectele de acorduri privind procedurile de securitate și de memorandumuri de înțelegere sunt discutate de Grupul consultativ privind politica de securitate a Comisiei înainte de a fi prezentate Comisiei pentru adoptarea unei decizii.

Membrul Comisiei însărcinat cu probleme de securitate solicită asistența necesară din partea ANS ale statelor membre pentru a asigura că informațiile care urmează a fi comunicate sunt utilizate și protejate în conformitate cu dispozițiile acordurilor privind procedurile de securitate sau ale memorandumurilor de înțelegere.

▼M3

27. STANDARDE MINIMALE COMUNE PRIVIND SECURITATEA INDUSTRIALĂ

27.1. **Introducere**

Prezenta secțiune se ocupă de aspecte de securitate ale activităților industriale care sunt proprii negocierii și atribuirii contractelor sau înțelegerilor privind subvențiile, precum și executării de către entități industriale sau alte entități a acestor contracte sau înțelegeri privind subvențiile, în cadrul cărora sunt conferite sarcini care implică, necesită și/sau cuprind informații clasificate UE, inclusiv comunicarea acestor informații clasificate UE sau accesul la acestea în cursul procedurilor de achiziții publice și de cerere de oferte (perioada de depunere a ofertelor și de negocieri precontractuale).

27.2. **Definiții**

În sensul acestor standarde minimale comune, se aplică următoarele definiții:

(a) „contract clasificat": orice contract sau înțelegere privind subvențiile pentru furnizarea de produse, execuția de lucrări, punerea la dispoziție de imobile sau prestarea de servicii, a căror executare necesită sau implică accesul la informații clasificate UE sau crearea de astfel de informații;

(b) „contract de subcontrare clasificat": un contract încheiat de un contractant sau de beneficiarul unei subvenții cu un alt contractant (adică subcontractantul) pentru furnizarea de produse, execuția de lucrări, punerea la dispoziție de imobile sau prestarea de servicii, a căror executare necesită sau implică accesul la informații clasificate UE sau crearea de astfel de informații;

(c) „contractant": un operator economic sau o entitate juridică având capacitatea juridică de a încheia contracte sau de a fi beneficiarul unei subvenții;

▼M3

(d) „autoritate de securitate desemnată (ASD)”: o autoritate responsabilă în fața autorității naționale de securitate (ANS) a unui stat membru UE, a cărei responsabilitate constă în a comunica entităților industriale sau altor entități politica națională în toate domeniile având legătură cu securitatea industrială și în a furniza orientări și asistență pentru punerea sa în aplicare. Funcția de ASD poate fi exercitată de ANS;

(e) „autorizație de securitate pentru incinte (ASI)”: o decizie administrativă luată de o ANS/ASD conform căreia, din punct de vedere al securității, o instalație poate asigura o protecție adecvată informațiilor clasificate UE la un nivel stabilit de clasificare a securității, iar personalul său, care are nevoie de acces la informațiile clasificate UE, posedă o autorizație de securitate corespunzătoare și a fost informat cu privire la cerințele de securitate necesare pentru a accede la informațiile clasificate UE și a le proteja;

(f) „entitate industrială sau altă entitate”: un contractant sau un subcontractant angajat în furnizarea de bunuri, executarea de lucrări sau prestarea de servicii, inclusiv entități industriale, comerciale, de prestare de servicii, științifice, de cercetare, de învățământ sau de dezvoltare;

(g) „securitate industrială”: aplicarea măsurilor și a procedurilor de protecție pentru a preveni, identifica și recupera pierderea sau compromiterea informațiilor clasificate UE tratate de un contractant sau un subcontractant în cadrul negocierilor (pre)contractuale și al contractelor clasificate;

(h) „autoritate națională de securitate (ANS)”: autoritatea administrativă a unui stat membru UE, a cărei responsabilitate finală o reprezintă protecția informațiilor clasificate UE în cadrul acelui stat membru;

(i) „nivel general de clasificare a securității unui contract”: determinarea clasificării securității întregului contract sau a întregii înțelegeri privind subvențiile, pe baza clasificării informațiilor și/sau a materialelor care trebuie sau pot fi produse, comunicate sau accesate în temeiul oricărui element al contractului global sau al înțelegerii globale privind subvențiile. Nivelul general de clasificare a securității unui contract nu poate fi mai scăzut decât clasificarea cea mai ridicată a unuia din elementele sale, dar poate fi mai ridicat din cauza efectului de agregare;

(j) „clauzele privind securitatea (CS)”: un set de condiții contractuale speciale, întocmit de autoritatea contractantă, care face parte integrantă dintr-un contract clasificat care implică acces la informații clasificate UE sau producerea de astfel de informații și care stabilește cerințele de securitate sau acele elemente ale contractului clasificat care trebuie să fie protejate din motive de securitate;

(k) „ghid de clasificare pe criteriul securității (GCCS)”: un document care descrie elementele unui program, contract sau înțelegere privind subvențiile care sunt clasificate și precizează nivelurile de clasificare a securității aplicabile. GCCS poate fi extins pe toată durata programului, contractului sau înțelegerii privind subvențiile, iar elementele informațiilor pot fi reclasificate sau declasificate. GCCS trebuie să facă parte din CS.

27.3. **Organizare**

(a) Comisia poate conferi, prin contract clasificat, entităților industriale sau altor entități înregistrate într-un stat membru sarcini care implică, necesită și/sau cuprind informații clasificate UE;

(b) Comisia se asigură că toate cerințele care decurg din aceste standarde minimale sunt respectate atunci când sunt atribuite contractele clasificate;

(c) Comisia implică autoritatea sau autoritățile naționale de securitate competente în scopul aplicării acestor standarde minimale în materie de securitate industrială. Autoritățile naționale de securitate pot atribui aceste sarcini uneia sau mai multor ASD;

▼M3

(d) responsabilitatea pentru protejarea informațiilor clasificate UE în cadrul entităților industriale sau al altor entități revine în ultimă instanță conducerii acestor entități;

(e) ori de câte ori este atribuit un contract sau un contract de subcontractare clasificat care se încadrează în domeniul de aplicare al acestor standarde minimale, Comisia și/sau ANS/ASD, după caz, vor notifica, fără întârziere, ANS/ASD din statul membru în care este înregistrat contractantul sau subcontractantul.

27.4. **Contracte clasificate și decizii de atribuire**

(a) Clasificarea pe criteriul securității a contractelor sau a înțelegerilor privind subvențiile trebuie să țină seama de următoarele principii:

— Comisia determină, după caz, aspectele contractului clasificat care necesită protecție și clasificarea de securitate corespunzătoare; atunci când face acest lucru, ea trebuie să ia în considerare clasificarea de securitate inițială atribuită de autoritatea de origine informațiilor create înainte de atribuirea contractului clasificat;

— nivelul general de clasificare a contractului nu poate fi mai scăzut decât clasificarea cea mai ridicată a unuia din elementele sale;

— informațiile clasificate UE create în cadrul activităților contractuale sunt clasificate în conformitate cu ghidul de clasificare pe criteriul securității;

— după caz, Comisia este responsabilă de modificarea nivelului general de clasificare a contractului sau de clasificare a securității oricăruia din elementele sale, prin consultare cu autoritatea de origine, și de informarea tuturor părților interesate;

— informațiile clasificate comunicate contractantului sau subcontractantului sau create în cadrul unei activități contractuale nu trebuie să fie utilizate în alte scopuri decât cele prevăzute de contractul clasificat și nu trebuie divulgate terților fără consimțământul scris prealabil din partea autorității de origine.

(b) Comisia și ANS/ASD a statelor membre respective au responsabilitatea de a se asigura că subcontractanții și contractanții cărora li s-au atribuit contracte clasificate care implică informații clasificate „CONFIDENTIEL UE” sau peste acest nivel iau toate măsurile corespunzătoare pentru protejarea acestor informații clasificate UE care le sunt comunicate sau pe care aceștia le creează în momentul executării contractului clasificat în conformitate cu actele cu putere de lege și actele administrative naționale. Nerespectarea cerințelor de securitate poate avea ca rezultat rezilierea contractului clasificat.

(c) Toate entitățile industriale sau alte entități care participă la contractele clasificate care implică acces la informații clasificate „CONFIDENTIEL UE” sau peste acest nivel trebuie să dețină o ASI națională. Această autorizație este eliberată de ANS/ASD a statului membru pentru a confirma că o instalație poate asigura și garanta o protecție corespunzătoare a securității informațiilor clasificate UE la nivelul de clasificare corespunzător.

(d) Atunci când este atribuit un contract clasificat, responsabilul cu securitatea instalației (RSI) desemnat de conducerea contractantului sau a subcontractantului are ca atribuție să solicite o autorizație de securitate pentru personal (ASP) pentru toate persoanele angajate în entități industriale sau alte entități înregistrate într-un stat membru UE și ale căror funcții necesită ca acestea să aibă acces la informații clasificate „CONFIDENTIEL UE” sau peste acest nivel care fac obiectul unui contract clasificat; această autorizație este eliberată de ANS/ASD a statului membru respectiv în conformitate cu reglementările sale naționale.

▼M3

(e) Contractele clasificate trebuie să includă CS, astfel cum sunt definite la 27.2 (j). CS trebuie să cuprindă GCCS.

(f) Înainte de inițierea unei proceduri negociate pentru un contract clasificat, Comisia va contacta ANS/ASD a statului membru în care sunt înregistrate entitățile industriale sau alte entități interesate pentru a obține confirmarea că acestea dețin o ASI valabilă și corespunzătoare nivelului de clasificare a securității contractului.

(g) Autoritatea contractantă nu trebuie să atribuie un contract clasificat unui operator economic selectat înainte de a fi primit o ASI valabilă.

(h) Cu excepția cazurilor în care actele cu putere de lege și actele administrative naționale ale statelor membre impun acest lucru, o ASI nu este necesară pentru contractele care implică informații clasificate „RESTREINT UE”.

(i) Invitațiile de participare privind contracte clasificate trebuie să cuprindă o dispoziție care prevede că un operator economic care nu prezintă o ofertă sau care nu este selectat este obligat să restituie toate documentele într-un termen specificat.

(j) Poate fi necesar pentru contractanți să negocieze contracte de subcontractare clasificate cu subcontractanți la diferite niveluri. Este responsabilitatea contractantului de a asigura ca toate activitățile de subcontractare să fie întreprinse în conformitate cu standardele minimale comune cuprinse în prezenta secțiune. Cu toate acestea, contractantul nu trebuie să transmită informații sau materiale clasificate UE unui subcontractant fără consimțământul scris prealabil din partea autorității de origine.

(k) Condițiile în care un contractant poate subcontracta activități trebuie să fie definite în ofertă sau în cererea de oferte, precum și în contractul clasificat. Nici un contract de subcontractare nu poate fi atribuit entităților înregistrate într-un stat care nu este membru UE fără autorizarea scrisă expresă din partea Comisiei.

(l) Pe toată durata contractului clasificat, respectarea tuturor dispozițiilor sale în materie de securitate va fi monitorizată de Comisie, împreună cu ANS/ASD competente. Orice incidente legate de securitate sunt raportate, în conformitate cu dispozițiile prevăzute de partea II secțiunea 24 din prezentele norme în materie de securitate. Orice modificare sau retragere a unei ASI este comunicată de îndată Comisiei și oricărei alte ANS/ASD căreia i-a fost notificată.

(m) Atunci când un contract clasificat sau un contract de subcontractare clasificat este reziliat, Comisia și/sau ANS/ASD, după caz, vor notifica fără întârziere ANS/ASD din statul membru în care este înregistrat contractantul sau subcontractantul.

(n) Standardele minimale comune cuprinse în prezenta secțiune continuă să fie respectate, iar contractanții și subcontractanții păstrează confidențialitatea informațiilor clasificate după rezilierea sau expirarea contractului clasificat sau a contractului de subcontractare clasificat.

(o) Dispoziții specifice pentru distrugerea informațiilor clasificate la sfârșitul contractului clasificat vor fi prevăzute de CS sau de alte dispoziții relevante care conțin cerințe de securitate.

(p) Obligațiile și condițiile prevăzute de prezenta secțiune se aplică *mutatis mutandis* procedurilor de acordare a subvențiilor prin decizie și, în special, beneficiarilor unor astfel de subvenții. Decizia de acordare a subvenției enunță toate obligațiile beneficiarilor.

▼M3

27.5. **Vizite**

Vizitele efectuate de personalul Comisiei în contextul contractelor clasificate la entități industriale sau alte entități din statele membre care execută contracte clasificate UE trebuie organizate cu ANS/ASD competentă. Vizitele efectuate de angajați ai entităților industriale sau ai altor entități în cadrul unui contract clasificat UE trebuie să fie organizate între ANS/ASD competente. Cu toate acestea, ANS/ASD implicate într-un contract clasificat UE pot conveni asupra unei proceduri prin care vizitele efectuate de angajați ai entităților industriale sau ai altor entități pot fi organizate direct.

27.6. **Transmiterea și transportul informațiilor clasificate UE**

(a) În ceea ce privește transmiterea informațiilor clasificate UE, se aplică dispozițiile prevăzute în partea II secțiunea 21 din prezentele norme în materie de securitate. Pentru completarea acestor dispoziții, se vor aplica orice proceduri existente în vigoare între statele membre.

(b) Transportul internațional de materiale clasificate UE referitoare la contracte clasificate se efectuează în conformitate cu procedurile naționale ale statului membru. În momentul examinării măsurilor în materie de securitate pentru transportul internațional, se vor aplica următoarele principii:

— securitatea este asigurată în fiecare etapă a transportului și în toate împrejurările, de la punctul de origine până la destinația finală;

— gradul de protecție acordat unui lot se determină în funcție de nivelul de clasificare cel mai ridicat al materialului conținut;

— se obține o ASI, după caz, pentru societățile care asigură transportul. În acest caz, personalul care manipulează lotul trebuie să primească o autorizație de securitate în conformitate cu standardele minimale comune cuprinse în prezenta secțiune;

— traseele sunt, în măsura posibilului, directe și sunt parcurse cât mai rapid, în funcție de circumstanțe;

— ori de câte ori posibil, rutele de transport ar trebui să treacă numai prin state membre UE. Rutele care trec prin state care nu sunt membre UE nu sunt utilizate decât cu autorizarea din partea ANS/ASD atât a statului expeditorului, cât și al destinatarului;

— înaintea oricărui transfer de material clasificat UE, se elaborează un plan de transport de către expeditor, care este aprobat de ANS/ASD corespunzătoare.

▼M1

Apendicele 1

TABEL COMPARATIV AL CLASIFICĂRILOR DE SECURITATE NAȚIONALĂ

Clasificare UE	TRES SECRET UEEU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Clasificare UEO	FOCAL TOP SECRET	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Clasificare Euratom	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Clasificare NATO	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
Belgia	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Republica Cehă	Přísn tajné	Tajné	Důvěrné	Vyhrazené
Danemarca	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Germania	Streng geheim	Geheim	VS ([1]) — Vertraulich	VS — Nur für den Dienstgebrauch
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
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 ([2])	Secret Défense	Confidentiel Défense	

▼M4

Croația	Vrlo tajno	Tajno	Povjerljivo	Ograničeno

▼M1

Irlanda	Top Secret	Secret	Confidential	Restricted
Italia	Segretissimo	Segreto	Riservatissimo	Riservato
Cipru	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
Letonia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lituania	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo

▼**M1**

Luxemburg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Ungaria	Szigorúan titkos !	Titkos !	Bizalmas !	Korlátozott terjesztésű !
Malta	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Țările de Jos	Stg ([3]). Zeer Geheim	Stg. Geheim	Stg. Confidentieel	Departementaal-vertrouwelijk
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polonia	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalia	Muito Secreto	Secreto	Confidencial	Reservado
Slovenia	Strogo tajno	Tajno	Zaupno	SVN Interno
Slovacia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finlanda	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Suedia	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Regatul Unit	Top Secret	Secret	Confidential	Restricted

([1]) VS = Verschlusssache.
([2]) The classificationTrès secret défense, which covers governmental priority issues, may only be changed with the Prime Minister's authorisation.
([3]) Stg = staatsgeheim.

▼B

Apendicele 2

GHID PRACTIC DE CLASIFICARE

Prezentul ghid este orientativ și nu poate fi interpretat ca modificând dispozițiile de fond prevăzute în secțiunile 16, 17, 20 și 21.

Clasificare	Când	Cine	Aplicare	Declasare/declasificare/distrugere	
				Cine	Când
►**M1** TRES SECRET UE/EU TOP SECRET ◄: Această clasificare se aplică doar informațiilor și materialelor a căror divulgare neautorizată ar putea cauza prejudicii extrem de grave intereselor esențiale ale Uniunii Europene sau ale unuia sau mai multora dintre statele sale membre [16.1].	Compromiterea bunurilor clasificate ►**M1** TRES SECRET UE/EU TOP SECRET ◄ ar risca: — să amenințe direct stabilitatea internă a UE sau a unuia sau mai multora dintre statele sale membre sau țărilor prietene — să aducă prejudicii extrem de grave relațiilor cu guverne prietene — să conducă direct la pierderea multor vieți omenești — să aducă prejudicii extrem de grave eficienței operaționale sau securității forțelor armate ale statelor membre sau ale altor contribuabili sau eficienței continue a operațiunilor de securitate sau de informații extrem de valoroase — să provoace daune grave pe termen lung economiei UE sau a statelor membre.	Persoane autorizate corespunzător (autorități de origine), directori generali, șefi de servicii [17.1] Autoritățile de origine specifică o dată, o perioadă sau un eveniment de la care conținutul poate fi declasat sau declasificat. [16.2] În celelalte cazuri, ele revizuiesc documentele cel târziu o dată la cinci ani, pentru a se asigura că rămâne necesară clasificarea inițială [17.3].	Clasificarea ►**M1** TRES SECRET UE/EU TOP SECRET ◄ se aplică pe documentele ►**M1** TRES SECRET UE/EU TOP SECRET ◄, dacă este cazul, împreună cu un identificator de securitate și/sau un marcaj de apărare – PESA, prin mijloace mecanice sau manual [16.4, 16.5, 16.3]. Clasificările UE și identificatorii de securitate apar central în partea de sus și de jos a fiecărei pagini, fiecare pagină fiind numerotată. Fiecare document are marcat un număr de referință și o dată; acest număr de referință apare pe fiecare pagină. Dacă trebuie să fie distribuite în mai multe exemplare, fiecare dintre acestea este marcat cu numărul exemplarului, care apare pe prima pagină, împreună cu numărul total de pagini. Toate anexele și documentele însoțitoare sunt menționate pe prima pagină [21.1].	Decizia de declasificare sau declasare aparține exclusiv autorității de origine, care informează asupra modificării orice destinatar ulterior căruia i-a trimis documentul sau o copie a acestuia [17.3]. Documentele ►**M1** TRES SECRET UE/EU TOP SECRET ◄ sunt distruse de registratura centrală sau de registratura secundară responsabilă de ele. Fiecare document distrus este menționat într-un certificat de distrugere, semnat de ofițerul de control ►**M1** TRES SECRET UE/EU TOP SECRET ◄ și de ofițerul care este martor la distrugere, care este autorizat ►**M1** TRES SECRET UE/EU TOP SECRET ◄. Se face o mențiune în acest sens în registru. Registratura păstrează certificatele de distrugere, împreună cu fișele de distribuție, timp de 10 ani [22.5].	Copiile excedentare și documentele care nu mai sunt necesare trebuie distruse [22.5]. Documentele ►**M1** TRES SECRET UE/EU TOP SECRET ◄, inclusiv orice deșeu clasificat rezultat din pregătirea documentelor ►**M1** TRES SECRET UE/EU TOP SECRET ◄, precum copii distruse, ciorne, note dactilografiate și indigouri, sunt distruse sub supravegherea unui ofițer de control ►**M1** TRES SECRET UE/EU TOP SECRET ◄, prin ardere, transformare în pastă, tăiere în fâșii sau printr-o altă modalitate de mărunțire în fragmente neidentificabile și care nu permit reconstituirea [22.5].

▼B

Clasificare	Când	Cine	Aplicare	Declasare/declasificare/distrugere	
				Cine	Când
►M1 SECRET UE ◄: Această clasificare se aplică doar informațiilor și materialelor a căror divulgare neautorizată ar putea cauza prejudicii grave intereselor esențiale ale Uniunii Europene sau ale unuia sau mai multora dintre statele sale membre [16.1].	Compromiterea bunurilor clasificate ►M1 SECRET UE ◄ ar risca: — să provoace tensiuni internaționale — să dăuneze grav relațiilor cu guverne prietene — să amenințe direct viața sau să prejudicieze grav ordinea publică sau securitatea sau libertatea persoanelor — să cauzeze prejudicii grave eficienței operaționale sau securității forțelor armate ale statelor membre sau ale altor contribuabili sau eficienței continue a operațiunilor de securitate și de informații extrem de valoroase — să provoace daune materiale substanțiale intereselor financiare, monetare, economice și comerciale ale UE sau ale unuia dintre statele sale membre.	Persoane autorizate corespunzător (autorități de origine), directori generali, șefi de servicii [17.1]. Autoritățile de origine specifică o dată, o perioadă de la care conținutul poate fi declasat sau declasificat. [16.2]. În celelalte cazuri, ele revizuiesc documentele cel târziu o dată la cinci ani, pentru a asigura că rămâne necesară clasificarea inițială [17.3].	Clasificarea ►M1 SECRET UE ◄ se aplică pe documentele ►M1 SECRET UE ◄, dacă este cazul, împreună cu un identificator de securitate și/sau un marcaj de apărare – PESA, prin mijloace mecanice sau manual [16.4, 16.5, 16.3]. Clasificările UE și identificatorii de securitate apar central în partea de sus și de jos a fiecărei pagini, fiecare pagină fiind numerotată. Fiecare document are marcat un număr de referință și o dată; acest număr de referință apare pe fiecare pagină. Dacă trebuie să fie distribuite în mai multe exemplare, fiecare dintre acestea este marcat cu numărul exemplarului, care apare pe prima pagină, împreună cu numărul total de pagini. Toate anexele și documentele însoțitoare sunt menționate pe prima pagină [21.1].	Decizia de declasificare sau declasare aparține exclusiv autorității de origine, care informează asupra modificării orice destinatar ulterior căruia i-a trimis documentul sau o copie a acestuia [17.3]. Documentele ►M1 SECRET UE ◄ sunt distruse de registratura responsabilă de documentele în cauză, sub supravegherea unei persoane deținând o autorizare de securitate. Documentele ►M1 SECRET UE ◄ distruse sunt menționate în certificate de distrugere semnate, păstrate de registratură, împreună cu formularele de distrugere, timp de cel puțin trei ani [22.5].	Copiile excedentare și documentele care nu mai sunt necesare trebuie distruse [22.5]. Documentele ►M1 SECRET UE ◄, inclusiv toate deșeurile clasificate rezultate din pregătirea documentelor ►M1 SECRET UE ◄, precum copii distruse, ciorne, note dactilografiate și indigouri, sunt distruse prin ardere, transformare în pastă, tăiere în fâșii sau printr-o altă modalitate de mărunțire în fragmente neidentificabile și care nu permit reconstituirea [22.5].
►M1 CONFIDENTIEL UE ◄:	Compromiterea bunurilor clasificate ►M1 CONFIDENTIEL UE ◄ ar risca: — să provoace daune importante relațiilor diplomatice, adică să determine proteste oficiale sau alte sancțiuni;	Persoane autorizate (autorități de origine), directori generali și șefi de servicii [17.1].	Clasificarea ►M1 CONFIDENTIEL UE ◄ se aplică pe documentele ►M1 CONFIDENTIEL UE ◄, iar dacă este cazul, se introduce un identificator de securitate și/sau un marcaj de apărare – PESA, prin mijloace mecanice sau manual sau prin imprimare pe hârtie marcată în prealabil, înregistrată [16.4, 16.5, 16.3].	Decizia de declasificare sau declasare aparține exclusiv autorității de origine, care informează asupra modificării orice destinatar ulterior căruia i-a trimis documentul sau o copie a acestuia [17.3].	Copiile excedentare și documentele care nu mai sunt necesare trebuie distruse [22.5].

▼B

Clasificare	Când	Cine	Aplicare	Declasare/declasificare/distrugere	
				Cine	Când
Această clasificare se aplică informațiilor și materialelor a căror divulgare neautorizată ar putea dăuna intereselor esențiale ale Uniunii Europene sau ale unuia sau mai multora dintre statele sale membre [16.1].	— să prejudicieze securitatea sau libertatea persoanelor; — să cauzeze prejudicii eficienței operaționale sau securității forțelor armate ale statelor membre sau ale altor contribuabili sau eficienței operațiunilor valoroase de securitate și de informații; — să submineze substanțial viabilitatea financiară a unor organizații importante; — să obstrucționeze anchetarea sau să faciliteze comiterea unor infracțiuni grave; — să fie împotriva intereselor financiare, monetare, economice și comerciale ale UE sau ale statelor membre; — să obstrucționeze grav dezvoltarea sau funcționarea unor politici importante ale UE; — să conducă la încetarea sau la subminarea în vreun fel a activităților importante ale UE.	Autoritățile de origine specifică o dată sau o perioadă de la care conținutul poate fi declasat sau declasificat. În celelalte cazuri, ele revizuiesc documentele cel târziu o dată la cinci ani, pentru a se asigura că rămâne necesară clasificarea inițială [17.3].	Clasificările UE apar central în partea de sus și de jos a fiecărei pagini, fiecare pagină fiind numerotată. Fiecare document are marcat un număr de referință și o dată. Toate anexele și documentele însoțitoare sunt menționate pe prima pagină [21.1].	Documentele ►M1 CONFIDENTIEL UE ◄ sunt distruse de registratura responsabilă de documentele în cauză, sub supravegherea unei persoane deținând o autorizare. Distrugerea lor se înregistrează în conformitate cu reglementările naționale și, în cazul agențiilor descentralizate ale Comisiei sau ale UE, în conformitate cu instrucțiunile ►M2 membrul Comisiei responsabil cu probleme de securitate ◄ [22.5].	Documentele ►M1 CONFIDENTIEL UE ◄, inclusiv toate deșeurile clasificate rezultate din pregătirea documentelor ►M1 CONFIDENTIEL UE ◄, precum copii distruse, ciorne, note dactilografiate și indigouri, sunt distruse prin ardere, transformare în pastă, tăiere în fâșii sau printr-o altă modalitate de mărunțire în fragmente neidentificabile și care nu permit reconstituirea [22.5].

▼B

Clasificare	Când	Cine	Aplicare	Declasare/declasificare/distrugere	
				Cine	Când
►M1 RESTREINT UE ◄: Această clasificare se aplică informațiilor și materialelor a căror divulgare neautorizată ar putea dezavantaja interesele UE sau ale unuia sau mai multora dintre statele sale membre [16.1].	Compromiterea bunurilor clasificate ►M1 RESTREINT UE ◄ ar risca: — să afecteze negativ relațiile diplomatice — să provoace suferințe semnificative persoanelor — să îngreuneze menținerea eficienței operaționale sau a securității forțelor armate ale statelor membre sau ale altor contribuabili — să cauzeze pierderi financiare sau să faciliteze câștiguri nejustificate sau avantaje unor persoane sau societăți — să încalce angajamente asumate corespunzător de a păstra confidențialitatea informațiilor furnizate de părți terțe — să încalce restricții statutare privind divulgarea informațiilor — să obstrucționeze anchetarea sau să faciliteze comiterea de infracțiuni — să dezavantajeze UE sau statele membre în negocieri comerciale sau politice — să obstrucționeze dezvoltarea sau funcționarea politicilor UE — să submineze buna gestionare a UE și a activităților sale	Persoane autorizate (autorități de origine), directori generali, șefi de servicii [17.1]. Autoritățile de origine specifică o dată, o perioadă sau un eveniment de la care conținutul poate fi declasat sau declasificat [16.2]. În celelalte cazuri, ele revizuiesc documentele cel târziu o dată la cinci ani, pentru a se asigura că rămâne necesară clasificarea inițială [17.3].	Clasificarea ►M1 RESTREINT UE ◄ se aplică pe documentele ►M1 RESTREINT UE ◄, dacă este cazul, împreună cu un identificator de securitate și/sau un marcaj de apărare – PESA, prin mijloace mecanice sau electronice [16.4, 16.5, 16.3]. Clasificările UE și identificatorii de securitate apar central în partea de sus a fiecărei pagini, fiecare pagină fiind numerotată. Fiecare document are marcat un număr de referință și o dată [21.1].	Decizia de declasificare sau declasare aparține exclusiv autorității de origine, care informează asupra modificării orice destinatar ulterior căruia i-a trimis documentul sau o copie a acestuia [17.3]. Documentele ►M1 RESTREINT UE ◄ sunt distruse de registratura responsabilă de documentele în cauză sau de utilizator, conform instrucțiunilor ►M2 membrul Comisiei responsabil cu probleme de securitate ◄ [22.5].	Copiile excedentare și documentele care nu mai sunt necesare trebuie distruse [22.5].

▼B

Apendicele 3

Linii directoare pentru comunicarea de informații clasificate UE unor state terțe sau unor organizații internaționale: Nivelul 1 de cooperare

PROCEDURI

1. Competența de a comunica informații clasificate UE unor țări care nu sunt membre ale Uniunii Europene sau altor organizații internaționale, ale căror politică și reglementări de securitate sunt comparabile cu cele ale UE, aparține colegiului membrilor Comisiei.

2. Până la încheierea unui acord de securitate, membrul Comisiei însărcinat cu probleme de securitate are competența de a examina solicitările de comunicare a unor informații clasificate UE.

3. În acest sens, acesta:

   — solicită avizul autorităților de origine ale ICUE care urmează a fi comunicate;

   — stabilește contactele necesare cu organismele de securitate ale țărilor sau ale organizațiilor internaționale beneficiare pentru a verifica dacă politica și reglementările de securitate ale acestora sunt de natură să garanteze protecția informațiilor clasificate comunicate în conformitate cu prezentele dispoziții de securitate;

   — solicită avizul Grupului consultativ pentru politica de securitate a Comisiei cu privire la încrederea care poate fi acordată statelor sau organismelor internaționale beneficiare.

4. Membrul Comisiei însărcinat cu probleme de securitate transmite Comisiei solicitarea și avizul Grupului consultativ pentru politica de securitate a Comisiei pentru adoptarea unei decizii.

DISPOZIȚII DE SECURITATE CARE TREBUIE APLICATE DE BENEFICIARI

5. Membrul Comisiei însărcinat cu probleme de securitate notifică statelor sau organizațiilor internaționale beneficiare decizia Comisiei de autorizare a comunicării informațiilor clasificate UE.

6. Decizia de comunicare intră în vigoare doar în momentul în care beneficiarii oferă o garanție scrisă prin care se angajează:

   — să nu utilizeze informațiile pentru alte scopuri decât cele convenite;

   — să protejeze informațiile în conformitate cu prezentele dispoziții de securitate, în special cu normele specifice prevăzute în continuare.

7. Personal

   (a) Numărul funcționarilor care au acces la informațiile clasificate UE este strict limitat, pe baza principiului nevoii de a cunoaște, la persoanele ale căror sarcini necesită acest acces.

   (b) Toți funcționarii și cetățenii care sunt autorizați să aibă acces la informații clasificate ►**M1** CONFIDENTIEL UE ◄ sau de nivel superior dețin fie un certificat de securitate pentru nivelul adecvat, fie o autorizare de securitate echivalentă, acestea fiind emise de guvernului propriului stat.

8. Transmiterea documentelor

   (a) Procedurile practice de transmitere a documentelor se decid prin acord. Până la încheierea unui astfel de acord, se aplică dispozițiile secțiunii 21. Acordul prevede, în special, registraturile către care sunt transmise informațiile clasificate UE.

▼B

(b) Dacă informațiile clasificate a căror comunicare este autorizată de Comisie includ informații ►M1 TRES SECRET UE/EU TOP SECRET ◄, statul sau organizația internațională beneficiare înființează o registratură centrală UE și, dacă este necesar, registraturi secundare UE. Aceste registraturi aplică dispoziții strict echivalente cu cele din secțiunea 22 a prezentelor dispoziții de securitate.

9. Înregistrare

De îndată ce o registratură primește un document UE clasificat ►M1 CONFIDENTIEL UE ◄ sau de nivel superior, aceasta înscrie documentul într-un registru special al organizației, cu coloane pentru data primirii, informații privind documentul (data, numărul de referință și numărul exemplarului), clasificarea acestuia, titlul, numele sau funcția destinatarului, data transmiterii confirmării de primire și data la care documentul este înapoiat autorității de origine UE sau la care este distrus.

10. Distrugere

(a) Documentele clasificate UE sunt distruse în conformitate cu instrucțiunile prevăzute în secțiunea 22 din prezentele dispoziții de securitate. Pentru documentele ►M1 SECRET UE ◄ și ►M1 TRES SECRET UE/EU TOP SECRET ◄, se trimit copii ale certificatelor de distrugere registraturii UE care a transmis documentele.

(b) Documentele clasificate UE se includ în planurile de distrugere de urgență ale propriilor documente clasificate ale beneficiarului.

11. Protecția documentelor

Se iau toate măsurile pentru a preveni accesul persoanelor neautorizate la informații clasificate UE.

12. Copii, traduceri și extrase

Un document clasificat ►M1 CONFIDENTIEL UE ◄ sau ►M1 SECRET UE ◄ nu se fotocopiază, nu se traduce și nu se fac extrase din astfel de documente fără autorizarea șefului organizației de securitate în cauză, care înregistrează și verifică traducerile, copiile sau extrasele și aplică ștampilele necesare.

Reproducerea sau traducerea unui document ►M1 TRES SECRET UE/EU TOP SECRET ◄ este autorizată doar de către autoritatea de origine, care specifică numărul de copii autorizate; dacă nu se poate determina autoritatea de origine, solicitarea este adresată Serviciului de securitate al Comisiei.

13. Încălcări ale securității

Dacă a avut loc sau se suspectează o încălcare a securității care implică un document clasificat UE, se iau imediat următoarele măsuri, sub rezerva încheierii unui acord de securitate:

(a) se efectuează o investigație pentru stabilirea circumstanțelor încălcării securității;

(b) se anunță ►M2 Direcția pentru Securitate a Comisiei ◄, autoritatea națională de securitate competentă și autoritatea de origine sau se precizează clar că aceasta din urmă nu a fost notificată, în cazul în care nu s-a luat această măsură;

(c) se iau măsuri pentru a reduce efectele încălcării securității;

(d) se reanalizează și se pun în aplicare măsuri pentru a preveni repetarea încălcării;

(e) se pun în aplicare măsurile recomandate de ►M2 Direcția pentru Securitate a Comisiei ◄ pentru a preveni repetarea încălcării.

▼B

14. Inspecții

►M2 Direcția pentru Securitate a Comisiei ◄ este autorizat, în temeiul unui acord încheiat cu statele sau cu organizațiile internaționale în cauză, să efectueze o evaluare a eficienței măsurilor de protecție a informațiilor clasificate UE și comunicate.

15. Rapoarte

Sub rezerva încheierii unui acord de securitate, atâta timp cât deține informații clasificate UE, statul sau organizația internațională prezintă un raport anual, până la o dată specificată în momentul emiterii autorizației de comunicare a informațiilor, care confirmă respectarea prezentelor dispoziții de securitate.

▼B

Apendicele 4

Linii directoare pentru comunicarea de informații clasificate UE unor state terțe sau unor organizații internaționale: Nivelul 2 de cooperare

PROCEDURI

1. Competența de a comunica informații clasificate UE unor state terțe sau unor organizații internaționale a căror politică și reglementări de securitate sunt semnificativ diferite de cele ale UE aparține autorității de origine. Competența de a comunica ICUE create în cadrul Comisiei aparține colegiului membrilor Comisiei.

2. În principiu, comunicarea se limitează la informații clasificate până la nivelul ►M1 SECRET UE ◄, inclusiv; ea exclude informațiile clasificate protejate prin identificatori sau marcaje de securitate speciale.

3. Până la încheierea unui acord de securitate, membrul Comisiei însărcinat cu probleme de securitate are competența de a examina solicitările de comunicare a unor informații clasificate UE.

4. În acest sens, acesta:

   — solicită avizul autorităților de origine ale ICUE care urmează a fi comunicate;

   — stabilește contactele necesare cu organismele de securitate ale statelor sau organizațiilor internaționale beneficiare pentru a obține informații despre politica și reglementările de securitate ale acestora și, în special, pentru a întocmi un tabel comparativ al clasificărilor aplicabile în UE și în statul sau organizația în cauză;

   — convoacă o reuniune a Grupului consultativ pentru politica de securitate a Comisiei sau, printr-o procedură silențioasă, dacă este cazul, interoghează autoritățile naționale de securitate ale statelor membre pentru a obține avizul Grupului consultativ pentru politica de securitate a Comisiei.

5. Avizul Grupului consultativ pentru politica de securitate a Comisiei se referă la următoarele elemente:

   — încrederea care poate fi acordată statelor sau organizațiilor internaționale beneficiare în vederea evaluării riscurilor de securitate asumate de UE sau de statele sale membre;

   — o evaluare a capacității beneficiarului de a proteja informațiile clasificate comunicate de UE;

   — propuneri privind procedurile practice de prelucrare a informațiilor clasificate UE (furnizarea unor versiuni expurgate ale unui text, de exemplu) și a documentelor transmise (păstrarea sau ștergerea mențiunilor privind clasificarea UE, marcaje specifice etc.);

   — declasarea sau declasificarea înainte de comunicarea informațiilor către țările sau organizațiile internaționale beneficiare.

6. Membrul Comisiei însărcinat cu probleme de securitate transmite Comisiei solicitarea și avizul Grupului consultativ pentru politica de securitate a Comisiei pentru adoptarea unei decizii.

NORME DE SECURITATE CARE TREBUIE APLICATE DE BENEFICIARI

7. Membrul Comisiei însărcinat cu probleme de securitate notifică statelor sau organizațiilor internaționale beneficiare decizia Comisiei de autorizare a comunicării informațiilor clasificate UE și restricțiile sale.

▼B

8. Decizia de comunicare intră în vigoare doar în momentul în care beneficiarii oferă o garanție scrisă prin care se angajează:

   — să nu utilizeze informațiile pentru alte scopuri decât cele convenite;

   — să protejeze informațiile în conformitate cu dispozițiile prevăzute de Comisie.

9. Se aplică următoarele norme de protecție, cu excepția cazului în care Comisia, după obținerea avizului tehnic al Grupului consultativ pentru politica de securitate a Comisiei, decide aplicarea unei proceduri speciale pentru prelucrarea informațiilor clasificate UE (ștergerea mențiunii clasificării UE, marcaje speciale etc.).

10. Personal

   (a) Numărul funcționarilor care au acces la informațiile clasificate UE este strict limitat, pe baza principiului nevoii de a cunoaște, la persoanele ale căror sarcini impun acest acces.

   (b) Toți funcționarii și cetățenii care sunt autorizați să aibă acces la informații clasificate comunicate de Comisie dețin o autorizație sau o atestare națională de securitate care le permite accesul, la un nivel adecvat echivalent cu cel din UE, conform definițiilor din tabelul comparativ.

   (c) Aceste autorizații sau atestări naționale de securitate sunt transmise ►M2 directorul Direcției pentru Securitate a Comisiei ◄ spre informare.

11. Transmiterea documentelor

   Procedurile practice de transmitere a documentelor sunt decise prin acord. Până la încheierea unui astfel de acord, se aplică dispozițiile secțiunii 21. Acordul prevede, în special, registraturile către care sunt transmise informațiile clasificate UE și adresele exacte la care sunt expediate documentele, precum și serviciile poștale sau de curierat utilizate pentru transmiterea informațiilor clasificate UE.

12. Înregistrarea la primire

   ANS a statutului destinatar sau echivalentul său care primește în numele guvernului informațiile clasificate transmise de Comisie sau biroul de securitate al organizației internaționale destinatare deschide un registru special pentru înregistrarea informațiilor clasificate UE la primirea acestora. Registrul conține coloane care indică data primirii, informații privind documentul (data, numărul de referință și numărul exemplarului), clasificarea acestuia, titlul, numele sau funcția destinatarului, data transmiterii confirmării de primire și data la care documentul este înapoiat la UE sau la care este distrus.

13. Înapoierea documentelor

   Atunci când înapoiază Comisiei un document clasificat, destinatarul procedează conform indicațiilor de la punctul „Transmiterea documentelor” menționat anterior.

14. Protecție

   (a) Când nu sunt utilizate, documentele sunt păstrate într-un container de securitate care este aprobat pentru păstrarea de materiale clasificate la nivel național având aceeași clasificare. Pe container este indicat conținutul acestuia, care este accesibil doar persoanelor autorizate să prelucreze informații clasificate UE. Dacă se utilizează închizătoare cu combinații, combinația este cunoscută doar de funcționarii statului sau ai organizației în cauză care au autorizare de acces la informațiile clasificate UE păstrate în container; combinația este schimbată o dată la șase luni, sau mai devreme în caz de transfer al unui funcționar, în caz de retragere a autorizării de securitate a unuia dintre funcționarii care cunosc combinația sau în cazul în care există riscul compromiterii.

▼B

(b) Documentele clasificate UE sunt scoase din containerul de securitate doar de către funcționarii care au autorizare de acces la informații clasificate UE și nevoia de a cunoaște. Aceștia trebuie să păstreze în siguranță documentele în cauză atâta timp cât le au în posesie și, în special, să asigure că nici o persoană neautorizată nu are acces la documente. De asemenea, ei trebuie să se asigure că documentele sunt păstrate într-un container de securitate după ce nu le mai consultă și în afara programului de lucru.

(c) Un document clasificat ►M1 CONFIDENTIEL UE ◄ sau de nivel superior nu se fotocopiază și nu se fac extrase din astfel de documente fără autorizarea Biroului de securitate al Comisiei.

(d) Se definește procedura pentru distrugerea rapidă și totală a documentelor în situații de urgență, procedura fiind confirmată de ►M2 Direcția pentru Securitate a Comisiei ◄.

15. Securitatea fizică

(a) Atunci când nu sunt utilizate, containerele de securitate folosite pentru păstrarea documentelor clasificate UE se țin în permanență închise.

(b) În cazul în care este necesar ca personalul de întreținere sau de curățenie să pătrundă sau să lucreze într-o încăpere în care există astfel de containere de securitate, persoanele în cauză sunt însoțite întotdeauna de un membru al serviciului de securitate al statului sau al organizației sau de un funcționar însărcinat special cu supravegherea securității încăperii.

(c) În afara programului normal de lucru (noaptea, la sfârșit de săptămână sau în zilele libere), containerele de securitate care conțin documente clasificate UE sunt protejate fie prin pază, fie printr-un sistem automat de alarmă.

16. Încălcări ale securității

Dacă a avut loc sau se suspectează o încălcare a securității care implică un document clasificat UE, se iau imediat următoarele măsuri:

(a) se prezintă imediat un raport Biroului de securitate al Comisiei sau ANS a statului membru care a luat inițiativa de a transmite documentele (și o copie Biroului de securitate al Comisiei);

(b) se efectuează o investigație, la finalizarea căreia se prezintă un raport complet serviciului de securitate [a se vedea litera (a) anterioară]. Ulterior, se iau măsurile necesare pentru remedierea situației.

17. Inspecții

►M2 Direcția pentru Securitate a Comisiei ◄ este autorizat, în temeiul unui acord încheiat cu statele sau cu organizațiile internaționale respective, să efectueze o evaluare a eficienței măsurilor de protecție a informațiilor clasificate UE și comunicate.

18. Rapoarte

Sub rezerva încheierii unui acord de securitate, atâta timp cât deține informații clasificate UE, statul sau organizația internațională prezintă un raport anual, până la o dată specificată în momentul emiterii autorizației de comunicare a informațiilor, care confirmă respectarea prezentelor dispoziții de securitate.

▼B

Apendicele 5

Linii directoare pentru comunicarea de informații clasificate UE unor state terțe sau unor organizații internaționale: Nivelul 3 de cooperare

PROCEDURI

1. Din când în când, Comisia poate decide să coopereze, în anumite circumstanțe speciale, cu state sau organizații care nu pot oferi garanțiile impuse de prezentele norme de securitate, această cooperare putând necesita comunicarea de informații clasificate UE.

2. Competența de a comunica informații clasificate UE unor state terțe sau unor organizații internaționale ale căror politică și reglementări de securitate sunt semnificativ diferite de cele ale UE aparține autorității de origine. Competența de a comunica ICUE create în cadrul Comisiei aparține colegiului membrilor Comisiei.

   În principiu, comunicarea se limitează la informații clasificate până la nivelul ►M1 SECRET UE ◄, inclusiv; ea exclude informațiile clasificate protejate prin identificatori sau marcaje de securitate speciale.

3. Comisia analizează oportunitatea comunicării informațiilor clasificate, evaluează nevoia beneficiarului de a cunoaște și decide în privința naturii informațiilor clasificate care pot fi comunicate.

4. Dacă decizia Comisiei este favorabilă, membrul Comisiei însărcinat cu probleme de securitate:

   — solicită avizele autorităților de origine ale ICUE care urmează a fi comunicate;

   — convoacă o reuniune a Grupului consultativ pentru politica de securitate a Comisiei sau, printr-o procedură silențioasă, dacă este cazul, interoghează autoritățile naționale de securitate ale statelor membre pentru a obține avizul Grupului consultativ pentru politica de securitate a Comisiei.

5. Avizul Grupului consultativ pentru politica de securitate a Comisiei se referă la următoarele elemente:

   (a) o evaluare a riscurilor în materie de securitate asumate de UE și de statele sale membre;

   (b) nivelul de clasificare a informațiilor care pot fi comunicate;

   (c) declasarea sau declasificarea înainte de comunicarea informațiilor;

   (d) procedurile de prelucrare a documentelor care trebuie transmise (a se vedea punctul următor);

   (e) metodele posibile de transmitere (utilizarea serviciilor poștale publice, a sistemelor de telecomunicații publice sau securizate, a unor genți diplomatice, a unor curieri autorizați etc.).

6. Documentele transmise statelor și organizațiilor care intră sub incidența prezentului apendice sunt pregătite, în principiu, fără a se indica o referință privind originea sau clasificarea UE. Grupul consultativ pentru politica de securitate a Comisiei poate recomanda:

   — utilizarea unui marcaj special sau a unui nume de cod;

   — utilizarea unui sistem specific de clasificare care să facă legătura între caracterul sensibil al informațiilor, măsurile de control care trebuie aplicate de beneficiar și modalitățile de transmitere a documentelor.

▼B

7. ►M2 membrul Comisiei responsabil cu probleme de securitate ◄ le transmite Comisiei avizul Grupului consultativ pentru politica de securitate a Comisiei în vederea adoptării unei decizii.

8. După ce Comisia a aprobat comunicarea informațiilor clasificate UE și procedurile practice de punere în aplicare, ►M2 Direcția pentru Securitate a Comisiei ◄ stabilește contactele necesare cu serviciul de securitate al statului sau al organizației în cauză pentru a facilita aplicarea măsurilor de securitate avute în vedere.

9. Membrul Comisiei însărcinat cu probleme de securitate informează statele membre în privința naturii și clasificării informațiilor, enumerând organizațiile și țările cărora le pot fi comunicate acestea, conform deciziei Comisiei.

10. ►M2 Direcția pentru Securitate a Comisiei ◄ ia toate măsurile necesare pentru a facilita o eventuală evaluare ulterioară a daunelor și revizuirea procedurilor.

Ori de câte ori sunt modificate condițiile de cooperare, Comisia reexaminează problema.

DISPOZIȚII DE SECURITATE CARE TREBUIE APLICATE DE BENEFICIARI

11. Membrul Comisiei însărcinat cu probleme de securitate notifică statelor sau organizațiilor internaționale beneficiare decizia Comisiei de autorizare a comunicării informațiilor clasificate UE, împreună cu normele detaliate de protecție propuse de Grupul consultativ pentru politica de securitate a Comisiei și aprobate de Comisie.

12. Decizia intră în vigoare doar în momentul în care beneficiarii oferă o garanție scrisă prin care se angajează:

— să nu utilizeze informațiile pentru alte scopuri decât cooperarea decisă de Comisie;

— să asigure informațiilor protecția impusă de Comisie.

13. Transmiterea documentelor

(a) Procedurile practice pentru transmiterea documentelor sunt stabilite de comun acord de către ►M2 Direcția pentru Securitate a Comisiei ◄ și serviciile de securitate ale statelor sau organizațiilor internaționale destinatare. Acestea specifică, în special, adresele exacte la care trebuie transmise documentele.

(b) Documentele clasificate ►M1 CONFIDENTIEL UE ◄ și de nivel superior sunt transmise în plicuri duble. Plicul interior este marcat cu ștampila specifică sau cu numele de cod convenit și poartă o mențiune a clasificării speciale aprobate pentru document. Fiecărui document clasificat i se atașează un formular de confirmare de primire. Formularul de confirmare de primire, care nu este el însuși clasificat, menționează doar informații despre document (referința, data, numărul exemplarului) și limba documentului, dar nu și titlul acestuia.

(c) Plicul interior este introdus apoi într-un plic exterior, care este marcat cu un număr de colet pentru confirmarea primirii. Pe plicul exterior nu se menționează clasificarea de securitate.

(d) Curierilor li se înmânează întotdeauna o confirmare de primire menționând numărul coletului.

▼B

14. Înregistrarea la primire

ANS a statutului destinatar sau echivalentul său în stat care primește în numele guvernului informațiile clasificate transmise de Comisie sau biroul de securitate al organizației internaționale destinatare deschide un registru special pentru înregistrarea informațiilor clasificate UE la primirea acestora. Registrul conține coloane care indică data primirii, informații privind documentul (data, numărul de referință și numărul exemplarului), clasificarea acestuia, titlul, numele sau funcția destinatarului, data la care s-a transmis confirmarea de primire și data la care documentul este înapoiat la UE sau la care este distrus.

15. Utilizarea și protecția informațiilor clasificate care fac obiectul schimburilor

(a) Informațiile de nivelul ►M1 SECRET UE ◄ sunt prelucrate de funcționari desemnați în acest scop, autorizați să aibă acces la informații care au această clasificare. Acestea sunt păstrate în dulapuri de securitate de bună calitate care pot fi deschise doar de persoanele care sunt autorizate să aibă acces la informațiile pe care le conțin. Zonele în care sunt amplasate aceste dulapuri se păzesc în permanență și se instituie un sistem de verificare pentru a asigura că este permis doar accesul persoanelor autorizate. Informațiile de nivelul ►M1 SECRET UE ◄ sunt transmise prin curier diplomatic, prin servicii poștale securizate sau telecomunicații securizate. Un document ►M1 SECRET UE ◄ poate fi copiat doar cu acordul scris al autorității de origine. Toate copiile sunt înregistrate și monitorizate. Pentru toate operațiunile referitoare la documentele ►M1 SECRET UE ◄ se emit confirmări.

(b) Informațiile ►M1 CONFIDENTIEL UE ◄ sunt prelucrate de funcționari desemnați corespunzător, autorizați să fie informați în privința subiectului acestora. Documentele se păstrează în dulapuri de securitate încuiate, în zone controlate.

Informațiile ►M1 CONFIDENTIEL UE ◄ sunt transmise prin curier diplomatic, servicii poștale militare și telecomunicații securizate. Organismul destinatar poate face copii, numărul și distribuția acestora fiind înregistrate în registre speciale.

(c) Informațiile ►M1 RESTREINT UE ◄ se prelucrează în locuri care nu sunt accesibile personalului neautorizat și se păstrează în containere încuiate. Documentele pot fi transmise prin servicii poștale publice, ca trimiteri recomandate, în plicuri duble și, în situații de urgență în cursul unor operațiuni, prin sisteme publice de telecomunicații neprotejate. Destinatarii pot face copii.

(d) Informațiile neclasificate nu necesită măsuri speciale de protecție și pot fi transmise prin servicii poștale și sisteme de telecomunicații publice. Destinatarii pot face copii.

16. Distrugere

Documentele care nu mai sunt necesare se distrug. În cazul documentelor ►M1 RESTREINT UE ◄ și ►M1 CONFIDENTIEL UE ◄, se face o mențiune adecvată în registrele speciale. În cazul documentelor ►M1 SECRET UE ◄ se întocmesc certificate de distrugere, semnate de două persoane martore la distrugerea lor.

17. Încălcări ale normelor de securitate

Dacă sunt compromise informații ►M1 CONFIDENTIEL UE ◄ sau ►M1 SECRET UE ◄ sau există suspiciuni de compromitere, ANS a statului sau șeful securității organizației efectuează o anchetă privind circumstanțele compromiterii. ►M2 Direcția pentru Securitate a Comisiei ◄ este notificat cu privire la rezultatele anchetei. Se adoptă măsurile necesare pentru remedierea procedurilor sau metodelor inadecvate de păstrare dacă acestea au condus la compromiterea informațiilor.

▼B

Apendicele 6

LISTA ABREVIERILOR

CCAC	Comitet consultativ pentru achiziții și contracte
CrA	Autoritate Crypto
CISO	Ofițer central de securitate informatică
COMPUSEC	Securitate informatică
COMSEC	Securitatea comunicațiilor
CSO	►M2 Direcția pentru Securitate a Comisiei ◄
PESA	Politica europeană de securitate și apărare
ICUE	Informații clasificate UE
IA	Autoritate INFOSEC
INFOSEC	Securitatea informațiilor
IO	Proprietarul informației
ISO	Organizația Internațională pentru Standardizare
IT	Tehnologia informațiilor
LISO	Ofițer local de securitate informatică
LSO	Ofițer local de securitate
MSO	Ofițer de securitate al reuniunii
ANS	Autoritatea națională de securitate
PC	Computer personal
RCO	Ofițer de control al registraturii
SAA	Autoritate de acreditare de securitate
SecOP	Proceduri de operare de securitate
SSRS	Declarație privind cerințele de securitate specifice unui sistem
TA	Autoritate Tempest
TSO	Proprietarul sistemelor tehnice

▼M3

ASD	autoritate de securitate desemnată
ASI	autorizație de securitate pentru incinte
RSI	responsabilul cu securitatea instalației
ASP	autorizație de securitate pentru personal
CS	clauzele privind securitatea
GCCS	ghid de clasificare pe criteriul securității