32001D0264

DECIZIA CONSILIULUI
din 19 martie 2001
de adoptare a regulamentului de securitate al Consiliului

(2001/264/CE)

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul de instituire a Comunității Europene și, în special, articolul 207 alineatul (3) al acestuia,

având în vedere Decizia 2000/396/CE, CECO, Euratom a Consiliului din 5 iunie 2000 de adoptare a Regulamentului de procedură al Consiliului [1] și, în special, articolul 24 al acestuia,

întrucât:

(1) Pentru a dezvolta activitățile Consiliului în domenii care necesită un anume nivel de confidențialitate, este necesar să se elaboreze un sistem general de securitate, care să cuprindă Consiliul, Secretariatul General al acestuia și statele membre.

(2) Acest sistem trebuie să cuprindă într-un singur text materiile vizate de toate deciziile și dispozițiile luate anterior în acest domeniu.

(3) Practic, cea mai mare parte a informațiilor ale UE, clasificate CONFIDENTIEL UE *[Confidențial UE]* și cu un nivel mai înalt de clasificare, vor privi politica comună de securitate și apărare.

(4) Pentru a asigura eficiența sistemului de securitate astfel creat, trebuie asociate statele membre la funcționarea sa, în acest sens acestea trebuie să ia măsurile naționale necesare pentru a asigura respectarea dispozițiilor prezentei decizii, în cazul în care autoritățile lor și funcționarii lor competenți lucrează cu informații clasificate ale UE.

(5) Consiliul salută intenția Comisiei de a introduce, până la data aplicării prezentei decizii, un sistem general în conformitate cu anexele prezentei decizii, în scopul de a asigura buna funcționare a procesului decizional în cadrul Uniunii.

(6) Consiliul subliniază importanța asocierii, dacă este cazul, a Parlamentului European și a Comisiei, la normele și la standardele de confidențialitate necesare pentru a proteja interesele Uniunii și ale statelor sale membre.

(7) Prezenta decizie se adoptă fără a aduce atingere articolul 255 din tratat și instrumentelor de aplicare a acestuia.

(8) Prezenta decizie se adoptă fără a aduce atingere practicilor existente în interiorul statelor membre în ceea ce privește informarea parlamentelor naționale ale acestora cu privire la activitățile Uniunii,

DECIDE:

Articolul 1

Se aprobă regulamentul de securitate al Consiliului, prevăzut în anexă.

Articolul 2

(1) Secretarul general/Înalt reprezentant ia măsurile potrivite pentru a asigura, la utilizarea informațiilor clasificate ale UE, respectarea regulamentului menționat la articolul 1, în cadrul Secretariatului General al Consiliului (în continuare numit „SGC") de către funcționarii și alți agenți ai SGC, de către contractanții externi ai SGC și personalul detașat la SGC, precum și în sediile Consiliului și în cadrul organismelor descentralizate ale UE [2].

[1] JO L 149, 23.6.2000, p. 21.

[2] A se vedea concluziile Consiliului din 10 noiembrie 2000.

(2) Statele membre iau măsurile potrivite, conform dispozițiilor naționale, pentru a asigura, la utilizarea informațiilor clasificate ale UE, respectarea regulamentului menționat la articolul 1, în cadrul serviciilor și sediilor acestora, de către:

(a) membrii reprezentanțelor permanente ale statelor membre pe lângă Uniunea Europeană, precum și de către membrii delegațiilor naționale care asistă la ședințele Consiliului sau ale organelor acestuia sau participă la alte activități ale Consiliului;

(b) alți membri ai administrațiilor naționale ale statelor membre, care utilizează informații clasificate ale UE, fie că activează pe teritoriul statelor membre sau în străinătate;

(c) contractanții externi ai statelor membre și personalul detașat, care utilizează informații clasificate ale UE.

Statele membre informează imediat SGC despre aceste măsuri.

(3) Măsurile menționate la alineatele (1) și (2) sunt luate înainte de 30 noiembrie 2001.

Articolul 3

Pentru a respecta principiile de bază și standardele minime de securitate, descrise în partea I a anexei, secretarul general/Înalt reprezentant poate lua măsuri în conformitate cu partea a II-a, secțiunea I, punctele 1 și 2 din anexă.

Articolul 4

Începând cu data punerii sale în aplicare, prezenta decizie înlocuiește:

(a) Decizia 98/319/CE a Consiliului din 27 aprilie 1998 privind procedurile prin care funcționarii și agenții Secretariatului General al Consiliului pot fi autorizați să aibă acces la informații clasificate deținute de către Consiliu [1];

(b) Decizia secretarului general/Înalt reprezentant din 27 iulie 2000 privind măsurile pentru protecția informațiilor clasificate care se aplică Secretariatului General al Consiliului [2];

(c) Decizia secretarului general al Consiliului nr. 433/97 din 22 mai 1997 privind procedura de verificare a funcționarilor însărcinați cu funcționarea rețelei Cortesy.

Articolul 5

(1) Prezenta decizie intră în vigoare la data publicării.

(2) Prezenta decizie se aplică de la 1 decembrie 2001.

Adoptată la Bruxelles, 19 martie 2001.

Pentru Consiliu

Președintele

A. LINDH

[1] JO L 140, 12.5.1998, p. 12.
[2] JO C 239, 23.8.2000, p. 1.

ANEXĂ

REGULAMENTUL DE SECURITATE AL CONSILIULUI UNIUNII EUROPENE

CUPRINS

Pagina

Anexe

PARTEA I

PRINCIPII DE BAZĂ ŞI STANDARDE MINIME DE SECURITATE

INTRODUCERE

1. Prezentul document definește principiile de bază și standardele minime de securitate pe care Consiliul, Secretariatul General al acestuia (în continuare numit „SGC"), statele membre și organismele descentralizate ale Uniunii Europene (în continuare numite „organisme descentralizate ale UE") trebuie să le respecte într-un mod corespunzător, astfel încât să asigure securitatea și astfel încât fiecare să poată avea certitudinea că este instituit un standard comun de protecție.

2. Prin „informații clasificate ale UE" se înțelege orice material și orice informație a căror divulgare neautorizată poate aduce diferite grade de atingere intereselor UE sau ale unuia sau mai multor state membre, fie că aceste informații își au originea în cadrul UE sau în statele membre, în state terțe sau în organizații internaționale.

3. În prezentul regulament, se înțelege prin:

   (a) „document": orice scrisoare, notă, raport, dare de seamă, memorandum, mesaj/semnal, schiță, fotografie, diapozitiv, film, hartă, tabel, plan, caiet de notițe, matriță, indigo, bandă de mașină de scris sau imprimantă, casetă, bandă magnetică, dischetă, CD-Rom sau alt suport material pe care sunt înregistrate informații;

   (b) „material": documentele definite la litera (a) de mai sus și orice element de echipament sau de armă, fabricat sau în curs de fabricație.

4. Securitatea are ca principale obiective:

   (a) protecția informațiilor clasificate ale UE împotriva spionajului, compromiterii sau divulgării neautorizate;

   (b) protecția informațiilor UE care fac obiectul comunicațiilor și care circulă prin sisteme și rețele de informații, împotriva amenințărilor la adresa integrității și disponibilității acestora;

   (c) protecția incintelor care adăpostesc informații UE împotriva tentativelor de sabotaj și a actelor intenționate de deteriorare;

   (d) în cazul unui eșec, evaluarea prejudiciului cauzat, limitarea consecințelor acestuia și adoptarea măsurilor necesare de corectare.

5. Un sistem eficient de securitate se bazează pe:

   (a) în cadrul fiecărui stat membru, o organizație națională de securitate care asigură:

      (i) colectarea și înregistrarea informațiilor privind activitățile de spionaj, sabotaj, terorism sau alte activități subversive și

      (ii) comunicarea către guvern și, prin intermediul acestuia din urmă, către Consiliu, a informațiilor cu privire la natura amenințărilor la adresa securității și a sfaturilor de protecție contra acestora;

   (b) în cadrul fiecărui stat membru și în cadrul SGC, o autoritate tehnică INFOSEC însărcinată să lucreze cu autoritatea responsabilă de securitate în cauză pentru a furniza informații cu privire la amenințările de ordin tehnic la adresa securității și sfaturi cu privire la mijloacele pentru protecția împotriva acestora;

   (c) colaborarea sistematică între serviciile și agențiile oficiale și serviciile competente ale SGC pentru a determina:

      (i) informațiile, resursele și incintele ce trebuie protejate și

      (ii) standardele comune de protecție

      și a emite, dacă este cazul, recomandări în această materie.

6. În ceea ce privește confidențialitatea, sunt necesare prudență și experiență în selectarea informațiilor și materialelor ce urmează a fi protejate și în evaluarea gradului de protecție ce trebuie asigurat. Acesta – și este vorba de un aspect fundamental – trebuie să fie corespunzător importanței care revine, din punct de vedere al securității, informațiilor și materialelor care trebuie protejate. Pentru a asigura buna circulație a informațiilor, trebuie luate măsuri pentru a evita supra-clasificarea. Sistemul de clasificare este instrumentul care permite aplicarea acestor principii; este necesară adoptarea unui sistem similar pentru planificarea și organizarea măsurilor de combatere a spionajului, sabotajului, terorismului și a altor amenințări, în așa fel încât să se acorde cea mai bună protecție celor mai importante incinte care adăpostesc informații clasificate și în interiorul acestor incinte, celor mai sensibile elemente.

PRINCIPII DE BAZĂ

7. **Măsurile de securitate trebuie:**

(a) să se aplice tuturor persoanelor care au acces la informații clasificate, la mijloacele de transmitere a informațiilor clasificate, tuturor sediilor unde există asemenea informații și instalațiilor importante;

(b) să fie concepute astfel încât să permită depistarea persoanelor al căror loc de muncă ar putea pune în pericol securitatea informațiilor clasificate și instalațiile importante care adăpostesc informații clasificate, precum și excluderea sau schimbarea locului acestora;

(c) să împiedice accesul oricărei persoane neautorizate la informații clasificate sau la instalații care conțin aceste informații;

(d) să permită asigurarea faptului că difuzarea informațiilor clasificate se bazează numai pe principiul necesității de a cunoaște, care stă la baza tuturor aspectelor securității;

(e) să permită asigurarea integrității (adică să împiedice alterarea sau modificarea sau distrugerea neautorizată) și disponibilitatea (adică să nu fie refuzat accesul persoanelor care au nevoie să consulte informațiile și care sunt autorizate să o facă) tuturor informațiilor, clasificate sau nu, în special informații stocate, prelucrate sau transmise pe cale electromagnetică.

ORGANIZAREA SECURITĂȚII

Standarde minime comune

8. Consiliul și fiecare stat membru trebuie să asigure faptul că toate serviciile administrative și/sau oficiale, celelalte instituții, organisme și contractanți ai UE respectă standardele minime comune de securitate, în așa fel încât există siguranța, în momentul comunicării unei informații clasificate a UE, că ea va fi prelucrată de toate aceste persoane cu aceleași măsuri de precauție. Aceste standarde minime trebuie să cuprindă criteriile care se aplică în cazul verificării personalului și măsurile ce trebuie luate pentru protecția informațiilor clasificate ale UE.

MĂSURI DE SECURITATE CU PRIVIRE LA PERSONAL

Autorizațiile de securitate

9. Orice persoană care trebuie să aibă acces la informații clasificate de nivelul CONFIDENTIEL UE *[Confidențial UE]* sau mai mare trebuie să dispună în prealabil de o autorizație de securitate corespunzătoare. O autorizație similară se cere și în cazul persoanelor ale căror funcții includ asigurarea funcționării și întreținerii tehnice a sistemelor de comunicare și informare ce conțin informații clasificate. Această autorizație trebuie să permită să se stabilească dacă:

(a) persoana în cauză este de o loialitate mai presus de orice îndoială;

(b) caracterul și discreția sa sunt de așa natură încât integritatea sa nu poate fi pusă la îndoială atunci când va avea acces la informații clasificate;

(c) ar putea ceda presiunilor care ar putea fi exercitate de surse externe sau de altă natură, de exemplu din cauza locului său anterior de reședință sau a contactelor sale din trecut, care ar putea constitui un risc pentru securitate.

Va trebui să se acorde o atenție specială procesului de autorizare a persoanelor:

(d) care trebuie să aibă acces la informații TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*;

(e) care ocupă locuri de muncă care necesită accesul regulat la numeroase informații SECRET UE;

(f) ale căror funcții le conferă un acces special la sistemele de comunicare sau de informare aferente unei misiuni esențiale și care au astfel posibilitatea de avea acces fără autorizație la un mare număr de informații clasificate UE sau de a compromite grav misiunea prin acțiuni de sabotaj tehnic.

În cazurile menționate la literele (d), (e) și (f) trebuie să se recurgă la maximum de metode de cercetare a antecedentelor.

10. În cazul în care o persoană care nu are în mod necesar nevoie să cunoască trebuie să fie angajată într-o funcție care poate să-i permită accesul la informații clasificate ale UE (de exemplu: mesager, agent de securitate, personal de întreținere și curățenie), aceasta va trebui să posede în prealabil autorizația corespunzătoare.

Registrele privind autorizațiile de securitate ale personalului

11. Orice serviciu, organism sau entitate care lucrează cu informații clasificate ale UE sau care adăpostește sisteme de comunicare și informare indispensabile unei misiuni trebuie să țină un registru privind autorizațiile acordate personalului său. Fiecare autorizație trebuie să fie verificată, în funcție de împrejurări, pentru a asigura conformitatea ei cu nivelurile de clasificare ale informațiilor și materialelor cu care va lucra beneficiarul ei; o nouă verificare se impune de fiecare dată când o nouă informație indică faptul că menținerea persoanei în cauză într-un post care permite accesul la informații clasificate nu mai corespunde securității. Registrul privind autorizațiile este ținut de responsabilul pentru securitate al serviciului, organismului sau entității în cauză.

Instructajul de securitate al personalului

12. Orice persoană care ocupă un post care îi poate permite accesul la informații clasificate trebuie să primească, la intrarea în funcțiune și, ulterior, periodic, un instructaj complet asupra măsurilor de securitate necesare și asupra procedurilor în vigoare în materie. Este util să se solicite tuturor acestor membri ai personalului să certifice în scris că au înțeles pe deplin normele de securitate care se aplică postului lor.

Răspunderea personalului de conducere

13. Personalului de conducere îi revine datoria de a ști care sunt membrii personalului care lucrează cu informații clasificate sau care au acces la sisteme de comunicare sau informare aferente unei misiuni esențiale, de a lua la cunoștință incidentele sau vulnerabilitățile evidente care pot avea repercusiuni pe planul securității și de a le semnala.

Statutul de securitate al personalului

14. Este necesară instituirea procedurilor care să permită, în cazul în care sunt comunicate informații defavorabile cu privire la o anumită persoană, să se determine dacă această persoană ocupă o funcție care necesită accesul la informații clasificate sau dacă ea are acces la sisteme de comunicare și informare aferente unei misiuni esențiale și să fie informate autoritățile competente. Dacă se constată că această persoană prezintă un risc de securitate, ea trebuie îndepărtată din funcțiile în care riscă să pună în pericol securitatea.

MĂSURI MATERIALE DE SECURITATE

Cerințe în materie de protecție

15. Gradul de securitate materială care trebuie aplicată pentru a asigura protecția informațiilor clasificate ale UE trebuie să fie proporțional cu nivelul de clasificare al informațiilor și materialelor deținute și cu volumul acestora, precum și cu pericolul la care sunt expuse. Trebuie evitată atât atribuirea unui nivel exesiv de clasificare, cât și a unui nivel subestimat de clasificare și trebuie revăzut periodic nivelul de clasificare atribuit. Toți deținătorii de informații clasificate ale UE trebuie să se conformeze unor reguli standardizate de clasificare și să respecte criterii de protecție uniforme cu privire la deținerea, transmiterea și distrugerea informațiilor și materialelor care trebuie protejate.

Controale

16. Înaintea de a lăsa fără supraveghere un sector care cuprinde informații clasificate ale UE, persoanele care le dețin trebuie să se asigure că acestea sunt în siguranță și că toate dispozitivele de securitate (încuietori, alarme etc.) sunt activate. În afara orelor de program trebuie să fie efectuate controale suplimentare de către alți agenți.

Securitatea clădirilor

17. Clădirile care adăpostesc informații clasificate ale UE sau sisteme de comunicare și informare indispensabile unei misiuni trebuie să fie protejate împotriva accesului persoanelor neautorizate. Natura acestei protecții (de exemplu ferestre cu gratii, uși care pot fi încuitate, prezența paznicilor la intrări, sisteme automate de control la intrare, inspecții și ronduri de securitate, sisteme de alarmă, sisteme de detectare a intrușilor și câini de pază) depinde de următorii parametri:

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

(b) calitatea mobilelor de securitate care adăpostesc aceste informații și materiale;

(c) caracteristicile tehnice și localizarea clădirii.

18. Natura protecției acordată sistemelor de comunicare și informare depinde de evaluarea valorii informațiilor și materialelor în cauză și de eventualele prejudicii în cazul compromiterii securității, de caracteristicile tehnice și de situația clădirii care adăpostește sistemul în cauză, precum și de amplasarea sistemului în clădire.

Planuri de urgență

19. Trebuie să se stabilească în avans planuri detaliate, care să protejeze informațiile clasificate în caz de urgență datorată situației locale sau naționale.

SECURITATEA SISTEMELOR DE INFORMARE (INFOSEC)

20. Securitatea sistemelor de informare (INFOSEC) se referă la identificarea și aplicarea măsurilor de securitate care permit protecția informațiilor prelucrate, stocate sau transmise prin sisteme de comunicare, de informare sau alte sisteme electronice împotriva atingerilor aduse confidențialității, integrității sau disponibilității acestor informații, indiferent dacă sunt accidentale sau intenționate. Trebuie să se ia măsuri preventive corespunzătoare pentru a împiedica accesul unor utilizatori neautorizați la informații ale UE, pentru a împiedica refuzul accesului la aceste informații unor utilizatori autorizați și pentru a împiedica alterarea, modificarea sau distrugerea neautorizată a informațiilor UE.

PROTECȚIA ÎMPOTRIVA SABOTAJULUI ȘI A ORICĂRUI ALT ACT INTENȚIONAT DE DETERIORARE

21. Măsurile materiale de precauție sunt mijloacele cele mai eficiente de a asigura securitatea și protecția instalațiilor importante care adăpostesc informații clasificate împotriva sabotajului sau oricărui alt act intenționat de deteriorare; numai verificarea personalului nu li se poate substitui eficient. Revine organismului național responsabil cu securitatea să strângă informațiile cu privire la activitățile de spionaj, de sabotaj, de terorism și alte acțiuni subversive.

COMUNICAREA INFORMAȚIILOR CLASIFICATE CĂTRE STATE TERȚE SAU CĂTRE ORGANIZAȚII INTERNAȚIONALE

22. Consiliul este competent să autorizeze comunicarea informațiilor clasificate ale UE emise de Consiliu către un stat terț sau către o organizație internațională. Dacă autoritatea emitentă a informațiilor care se comunică nu este Consiliul, acesta din urmă trebuie să solicite consimțământul acesteia. În cazul în care emitentul nu poate fi identificat, Consiliul își asumă răspunderea.

23. În cazul în care Consiliul primește informații clasificate de la state terțe, de la organizații internaționale sau de la alți terți, acestor informații li se va acorda protecția corespunzătoare clasificării lor și standardelor prevăzute de prezentul regulament pentru informațiile clasificate ale UE sau standardelor mai exigente care pot fi solicitate de terții care comunică aceste informații. Pot fi prevăzute controale reciproce.

24. Principiile menționate mai sus se aplică în conformitate cu normele metodologice prevăzute în partea II.

PARTEA II

SECȚIUNEA I

ORGANIZAREA SECURITĂȚII ÎN CADRUL CONSILIULUI UNIUNII EUROPENE

Secretarul general/Înalt reprezentant

1. Secretarul general/Înalt reprezentant:

   (a) pune în aplicare politica de securitate a Consiliului;

   (b) analizează problemele de securitate care îi sunt aduse la cunoștință de către Consiliu sau de autoritățile competente ale acestuia;

   (c) analizează problemele care implică modificări ale politicii de securitate a Consiliului, în strânsă legătură cu autoritățile naționale de securitate (sau cu alte autorități corespunzătoare) din statele membre (în continuare denumite „ANS"). Anexa 1 cuprinde o listă a acestor autorități.

2. Secretarul general/Înalt reprezentant are, în special, responsabilitatea:

   (a) de a coordona toate chestiunile de securitate aferente activităților Consiliului;

   (b) de a solicita elaborarea de către fiecare stat membru a unui registru central TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* și de a solicita, dacă este cazul, elaborarea acestuia în cadrul organismelor descentralizate ale UE;

   (c) de a solicita ANS din statele membre să furnizeze verificările de securitate cu privire la personalul angajat în cadrul SGC, în conformitate cu secțiunea VI;

   (d) de a investiga ori de a impune desfășurarea unei investigații în legătură cu orice scurgere de informații clasificate ale UE dacă, la prima vedere, indiciile arată că aceasta s-a produs în cadrul SGC sau în cadrul unuia din organismele descentralizate ale UE;

   (e) de a solicita autorităților de securitate competente să inițieze investigații în momentul în care scurgeri de informații clasificate ale UE par să se fi produs în afara SGC sau a organismelor descentralizate ale UE și de a-și coordona investigațiile atunci când în această acțiune este implicată mai mult de o singură autoritate de securitate;

   (f) de a analiza periodic, împreună și de comun acord cu ANS în cauză, dispozițiile adoptate pentru protejarea informațiilor clasificate în statele membre;

   (g) de a menține legături strânse cu toate autoritățile de securitate pentru a ajunge la o coordonare de ansamblu a securității;

   (h) de a reanaliza permanent organizarea și procedurile Consiliului privind securitatea și, după caz, de a pregăti recomandările corespunzătoare. În acest temei, acesta prezintă spre aprobare Consiliului planul anual de inspecție elaborat de Oficiul de Securitate al SGC.

Comitetul de securitate al Consiliului

3. Se instituie Comitetul de securitate. Acesta este format din reprezentanți ANS din fiecare stat membru. Acesta este prezidat de secretarul general/Înalt reprezentant sau de către delegatul acestuia. La reuniunile acestuia pot fi invitați să asiste și reprezentanți ai organismelor descentralizate ale UE, atunci când chestiunile dezbătute le privesc.

4. Comitetul de securitate se întrunește la chemarea Consiliului, la cererea secretarului general/Înalt reprezentant sau a unei ANS. Comitetul este competent să analizeze și să evalueze toate chestiunile de securitate legate de lucrările Consiliului și să îi prezinte recomandări Consiliului, după caz. În ceea ce privește activitățile SGC, Comitetul este împuternicit să adreseze recomandări secretarului general/Înalt reprezentant referitoare la chestiuni de securitate.

Oficiul de Securitate al Secretariatului General al Consiliului

5. Pentru a îndeplini responsabilitățile prevăzute la alineatele (1) și (2), secretarul general/Înalt reprezentant dispune de Oficiul de Securitate al SGC pentru coordonarea, supravegherea și îndeplinirea măsurilor de securitate.

6. Șeful Oficiului de Securitate al SGC este principalul consultant în probleme de securitate al secretarului general/Înalt reprezentant și este secretarul Comitetului de securitate. În acest temei, el conduce lucrările de actualizare a reglementărilor privind securitatea și coordonează măsurile de securitate cu autoritățile competente ale statelor membre și, după caz, cu organizațiile internaționale care au încheiat cu Consiliul acorduri de securitate. În acest sens, acesta îndeplinește rolul de persoană de legătură.

7. Șeful Oficiului de Securitate al SGC este responsabil cu acreditarea sistemelor și rețelelor TI din cadrul SGC. Șeful Oficiului de Securitate al SGC și ANS în cauză decid în comun, după caz, cu privire la acreditarea sistemelor și rețelelor TI ce implică SGC, statele membre, organismele descentralizate ale UE și/sau terți (state sau organizații internaționale).

Organismele descentralizate ale UE

8. Directorul fiecărui organism descentralizat al UE este responsabil pentru aplicarea normelor de securitate în cadrul organismului pe care îl conduce. În mod obișnuit, acesta însărcinează un membru al personalului organismului de a se ocupa de această materie. Membrul personalului este desemnat ca fiind responsabilul pentru probleme de securitate.

State membre

9. Fiecare stat membru desemnează un ANS care este responsabilă pentru securitatea informațiilor clasificate ale UE ([1]).

10. În cadrul administrației fiecărui stat membru, ANS este responsabilă de:

(a) menținerea securității informațiilor clasificate ale UE deținute în cadrul tuturor serviciilor, organismelor sau agențiilor naționale, publice sau private, pe teritoriul național și în străinătate;

(b) autorizarea elaborării unor registre TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* [această autoritate poate fi delegată controlorului competent pentru nivelul TRÈS SECRET UE/EU TOP SECRET - *(Strict secret UE)* al unui registru central];

(c) inspecția periodică a aranjamentelor de securitate destinate să asigure protecția informațiilor clasificate ale UE;

(d) asigurarea faptului că toți membrii personalului care sunt resortisanți ai acelui stat, precum și toți resortisanții străini angajați în servicii, organisme sau agenții naționale și care pot avea acces la informații clasificate TRÈS SECRET UE/EU TOP SECRET, SECRET UE *[Strict secret UE]* și CONFIDENTIEL UE *[Confidențial UE]* posedă o autorizare de securitate;

(e) elaborarea unor planuri de securitate considerate necesare pentru ca informațiile clasificate ale UE să nu ajungă la persoane neautorizate.

Inspecții reciproce cu privire la securitate

11. Oficiul de Securitate al SGC, împreună și de comun acord cu ANS ([2]) în cauză, efectuează inspecții periodice ale aranjamentelor de securitate stabilite pentru protecția informațiilor clasificate ale UE în interiorul SGC și al reprezentanțelor permanente ale statelor membre pe lângă Uniunea Europeană, precum și în incintele rezervate statelor membre în cadrul clădirilor Consiliului.

12. Oficiul de Securitate al SGC sau, la cererea secretarului general, ANS a statului membru gazdă efectuează inspecții periodice ale aranjamentelor de securitate stabilite pentru protecția informațiilor clasificate ale UE în cadrul organismelor descentralizate ale UE.

([1]) Vezi anexa 1 pentru lista reprezentanților ANS responsabile pentru securitatea informațiilor clasificate.

([2]) Fără a aduce atingere Convenției de la Viena din 1961 privind relațiile diplomatice.

SECȚIUNEA II

CLASIFICĂRI ȘI MARCĂRI

NIVELE DE CLASIFICARE ([1])

Informațiile se clasifică conform următoarelor nivele:

1. TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*: acest nivel de clasificare se aplică numai acelor informații și materiale a căror divulgare neautorizată poate aduce prejudicii deosebit de grave intereselor esențiale ale Uniunii Europene sau ale unuia ori mai multor state membre.

2. SECRET UE: acest nivel de clasificare se aplică numai acelor informații și materiale a căror divulgare neautorizată poate dăuna grav intereselor esențiale ale Uniunii Europene sau unuia ori mai multor state membre.

3. CONFIDENTIEL UE *[Confidențial UE]*: acest nivel de clasificare se aplică numai acelor informații și materiale a căror divulgare neautorizată poate dăuna intereselor esențiale ale Uniunii Europene sau ale unuia ori mai multor state membre.

4. RESTREINT UE *[Circulație restrânsă UE]*: acest nivel de clasificare se aplică numai acelor informații și materiale a căror divulgare neautorizată poate fi în dezavantajul intereselor Uniunii Europene sau ale unuia ori mai multor state membre.

MARCĂRI

5. Se poate folosi un marcaj restrictiv pentru specificarea domeniului acoperit de respectivul document sau pentru a indica distribuirea pe o anumită scară bazată pe necesitatea de a cunoaște.

6. Marcajul ESDP/PESD *[PESA]* se aplică pe documente și pe copiile referitoare la securitatea și apărarea Uniunii ori a unuia sau mai multor state membre sau referitoare la gestionarea militară și civilă a crizelor.

7. Anumite documente și, în special, cele referitoare la sistemele de tehnologie a informațiilor (TI), pot avea un marcaj adițional care să atragă după sine aplicarea unor măsuri suplimentare de securitate, în conformitate cu reglementarea corespunzătoare.

APLICAREA CLASIFICĂRILOR ȘI A MARCAJELOR

8. Clasificările și marcajele se aplică după cum urmează:

   (a) pe documente RESTREINT UE *[Circulație restrânsă UE]*, prin mijloace mecanice sau electronice;

   (b) pe documente CONFIDENTIEL UE *[Confidențial UE]*, prin mijloace mecanice, cu mâna, prin ștampilare sau înregistrare;

   (c) pe documente SECRET UE și TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*, prin mijloace mecanice sau cu mâna.

([1]) În anexa 2 se găsește un tabel comparativ cu nivelele de clasificare ale UE, NATO, UEO și ale statelor membre.

SECȚIUNEA III

ADMINISTRAREA CLASIFICĂRILOR

1. Informațiile se clasifică numai dacă acest lucru este necesar. Clasificarea se indică în mod clar și corect și se păstrează atât timp cât respectiva informație necesită protecție.

2. Clasificarea informațiilor și orice reducere a nivelului de clasificare sau orice declasificare ulterioară ([1]) revine numai autorității emitente a informațiilor.

   Funcționarii și alți agenți ai SGC clasifică, reduc nivelul de clasificare sau declasifică informații la instrucțiunile sau cu acordul directorului general.

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

4. Numărul persoanelor autorizate să emită documente TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* trebuie să fie unul minim, iar numele acestora trebuie înregistrate pe o listă întocmită de SGC, de fiecare stat membru și, după caz, de fiecare organism descentralizat al UE.

STABILIREA CLASIFICĂRII

5. Clasificarea unui document se face în funcție de gradul de sensibilitate al conținutului acestuia, în conformitate cu definițiile prevăzute în secțiunea II alineatele (1)-(4). Este important ca aplicarea unui anumit nivel de clasificare să fie făcută cu bună știință și cu măsură. Acest lucru se aplică în special pentru nivelul de clasificare TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*.

6. În stabilirea nivelului de clasificare ce urmează a fi atribuit unui document, autoritatea emitentă trebuie să țină seama de diferitele reguli de mai sus, înfrângând orice tendință de atribuire a unui nivel prea înalt sau prea scăzut de clasificare.

   Deși, la prima vedere, utilizarea unui nivel de clasificare mai important poate garanta documentului o mai mare protecție, recurgerea sistematică la atribuirea unor nivele de clasificare prea înalte poate antrena o pierdere a încrederii în ceea ce privește valoare sistemului de clasificare.

   Pe de altă parte, dorința de a evita anumite constrângeri ale protecției nu trebuie să conducă la atribuirea unui nivel de clasificare inferior al documentelor.

   Anexa 3 conține un ghid practic pentru atribuirea nivelurilor de clasificare.

7. Pagini, paragrafe, secțiuni, anexe dintr-un anume document sau la acesta pot necesita atribuirea unor niveluri diferite de clasificare și trebuie, în acest caz, să poarte mențiunea corespunzătoare. Nivelul de clasificare atribuit unui document ca întreg este acela al părții sale căreia i s-a atribuit nivelul de clasificare cel mai înalt.

8. Scrisorile sau notele care însoțesc documente anexate poartă nivelul de clasificare cel mai înalt care a fost atribuit acestora din urmă. Autoritatea emitentă indică în mod clar nivelul lor de clasificare în cazul în care sunt separate de anexele lor.

REDUCEREA NIVELULUI DE CLASIFICARE ȘI DECLASIFICAREA

9. Documentelor clasificate ale UE nu le poate fi redus nivelul de clasificare și nici nu pot fi declasificate decât cu permisiunea autorității emitente și, dacă este necesar, după consultarea celorlalte părți în cauză. Reducerea nivelului de clasificare și declasificarea se confirmă în scris. Instituția, statul membru, oficiul, organizația succesoare sau autoritatea superioară emitentă are responsabilitatea de a informa destinatarii cu privire la eventuale schimbări ale nivelului de clasificare; aceștia, la rândul lor, au responsabilitatea de a informa destinatarii succesivi cărora le-au transmis originalul documentului sau o copie a acestuia.

10. Dacă este posibil, autoritatea emitentă indică pe documentul clasificat data sau termenul începând cu care informațiilor pe care acesta le cuprinde li se va putea reduce nivelul de clasificare sau vor putea fi declasificate. În caz contrar, autoritatea emitentă reanalizează această chestiune la cel mult fiecare cinci ani pentru a se asigura că nivelul de clasificare atribuit inițial este necesar.

([1]) Reducerea nivelului de clasificare („downgrading") înseamnă trecerea unui document la un nivel inferior de clasificare; declasificarea („declassification") înseamnă eliminarea din orice sistem de clasificare.

SECȚIUNEA IV

SECURITATEA FIZICĂ

GENERALITĂȚI

1. Principalul obiectiv al măsurilor fizice de securitate îl constituie împiedicarea accesului persoanelor neautorizate la informațiile și/sau materialele clasificate ale UE.

CERINȚE DE SECURITATE

2. Este obligatorie protecția tuturor sediilor, zonelor, clădirilor, birourilor, încăperilor, sistemelor de informare și de comunicare etc. în care se stochează sau se lucrează cu informații și materiale clasificate ale UE, prin adoptarea unor măsuri corespunzătoare de securitate fizică.

3. Pentru stabilirea gradului de securitate fizică ce trebuie asigurat este necesar să se țină seama de toți factori relevanți și, în special, de:

   (a) nivelul de clasificare atribuit informațiilor și/sau materialelor;

   (b) cantitatea și forma informațiilor (de exemplu pe suport de hârtie sau pe suport informatic) deținute;

   (c) evaluarea locală a amenințării pe care o constituie serviciile de informații ce au drept țintă UE, statele membre și/sau alte instituții sau părți terțe care dețin informații clasificate ale UE, amenințare sub formă de sabotaj, terorism și alte acțiuni subversive și/sau criminale.

4. Măsurile fizice de securitate ce urmează a fi aplicate trebuie să fie concepute astfel încât:

   (a) să împiedice accesul disimulat sau forțat al vreunui intrus;

   (b) să descurajeze, să împiedice și să detecteze acțiunile personalului neloial (spionaj din interior);

   (c) să împiedice ca funcționarii și alți agenți ai SGC, ai serviciilor oficiale ale statelor membre și/sau ai altor instituții, ori terți cărora nu le este necesar să cunoască acced la informații clasificate ale UE.

MĂSURI FIZICE DE SECURITATE

Zone de securitate

5. Zonele, în care informațiile cu un nivel de clasificare CONFIDENTIEL UE *[Confidențial UE]* sau superior sunt prelucrate și păstrate trebuie să fie organizate în așa fel încât să corespundă uneia din următoarele categorii:

   (a) zona de securitate clasa I: o zonă în care informații de nivelul CONFIDENTIEL UE *[Confidențial UE]* sau mai înalt sunt prelucrate și conservate astfel încât accesul în această zonă echivalează practic cu accesul la aceste informații. O astfel de zonă impune:

      (i) un perimetru clar definit și protejat, unde toate intrările și ieșirile sunt controlate;

      (ii) existența unui sistem de control la intrare, care permite accesul numai persoanelor verificate în mod corespunzător și autorizate special în acest sens;

      (iii) specificarea nivelului de clasificare al informațiilor deținute în mod normal în zona respectivă, adică a acelor informații la care, prin intrarea în zona respectivă, se poate avea acces;

   (b) zona de securitate clasa a II-a: o zonă în care informații de nivelul CONFIDENTIEL UE *[Confidențial UE]* sau mai importante sunt prelucrate și conservate astfel încât pot fi protejate prin controale interne care împiedică orice persoană neautorizată să aibă acces la acestea; este vorba, de exemplu, de sedii ce adăpostesc birouri în care sunt prelucrate și conservate, de regulă, informații cu un nivel de clasificare CONFIDENTIEL UE *[Confidențial UE]* sau mai înalt. O astfel de zonă impune:

      (i) un perimetru clar definit și protejat, unde toate intrările și ieșirile sunt controlate;

      (ii) existența unui sistem de control la intrare, care nu permite intrarea neînsoțită decât a persoanelor verificate în mod corespunzător și autorizate special în acest sens. Pentru toate celelalte persoane este necesar să se prevadă un însoțitor sau controale echivalente care să le împiedice să aibe acces la informațiile clasificate ale UE și să pătrundă în zone supuse unor inspecții tehnice de securitate.

Acele zone care nu sunt ocupate de personalul de serviciu timp de 24 de ore sunt inspectate îndată după terminarea orelor de lucru pentru a se asigura faptul că informațiile clasificate ale UE sunt protejate în mod corespunzător.

Zona administrativă

6. O zonă de securitate de clasa I sau a II-a poate fi înconjurată sau precedată de o zonă administrativă mai puțin protejată, pentru care trebuie stabilit în mod vizibil un perimetru care permite controlul persoanelor și al vehiculelor. Numai informațiile de nivelul RESTREINT UE *[Circulație restrânsă UE]* pot fi prelucrate și păstrate în zonele administrative.

Controlul intrărilor și ieșirilor

7. Intrarea în zonele de securitate din clasa I și clasa a II-a este controlată printr-un sistem de permise sau de recunoaștere individuală, aplicabile personalului permanent. Se va elabora și un sistem pentru verificarea vizitatorilor pentru ca niciun acces neautorizat la informații clasificate ale UE să nu aibă loc. Sistemului bazat pe permise i se poate adăuga un sistem de recunoaștere automată, care trebuie înțeles, în acest caz, ca măsură complementară și nu ca pe un înlocuitor absolut al paznicilor. O schimbare în evaluarea amenințărilor poate atrage după sine o întărire a măsurilor de control la intrare și ieșire, de exemplu în timpul vizitei unor personalități de nivel înalt.

Rondurile

8. Pentru zonele de securitate din clasa I și clasa a II-a au loc ronduri în timpul orelor de lucru pentru a proteja bunurile UE împotriva compromiterii, pierderii sau deteriorării. Frecvența rondurilor se stabilește ținând seama de împrejurările locale, dar, de regulă, acestea au loc o dată la două ore.

Containerele de securitate și camerele speciale

9. Pentru păstrarea informațiilor clasificate ale UE se folosesc trei tipuri de containere:

— Clasa A: containere aprobate la nivel național pentru depozitarea informațiilor de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* în cadrul zonelor de securitate din clasa I și clasa II;

— Clasa B: containere aprobate la nivel național pentru depozitarea informațiilor de nivelul SECRET UE și CONFIDENTIEL UE *[Confidențial UE]* în cadrul zonelor de securitate din clasa I și clasa II;

— Clasa C: mobilă de birou potrivită doar pentru depozitarea informațiilor de nivelul RESTREINT UE *[Circulație restrânsă UE]*.

10. În ceea ce privește camerele speciale construite în cadrul zonelor de securitate din clasa I și clasa a II-a și pentru toate zonele din clasa I, unde informațiile de nivelul CONFIDENTIEL UE *[Confidențial UE]* sau mai importante sunt depozitate pe rafturi sau sunt expuse pe hărți, tabele etc., pereții, podelele și tavanele, ușile cu încuietorile respective sunt notificate de ANS ca oferind o protecție echivalentă cu clasa containerului de securitate aprobat pentru depozitarea informațiilor din aceeași clasificare.

Încuietorile

11. Încuietorile containerelor de securitate și camerelor speciale în care sunt depozitate informații clasificate ale UE trebuie să corespundă următoarelor standarde:

— Grupul A: aprobate la nivel național pentru containere din clasa A;

— Grupul B: aprobate la nivel național pentru containere din clasa B;

— Grupul C: potrivite doar pentru mobilă de birou clasa C.

Controlul cheilor și combinațiilor

12. Cheile containerelor de securitate nu pot fi scoase din clădire. Sistemul de combinații ale containerelor de securitate trebuie să fie memorate de persoanele care au nevoie să le cunoască. În scopuri urgente, responsabilul pentru probleme de securitate al organismului în cauză păstrează cheile de rezervă și transcrierea fiecărei combinații, păstrată separat în plicuri netransparente sigilate. Cheile, cheile de rezervă și plicurile cu combinații sunt păstrate în containere de securitate separate. Aceste chei și combinații sunt protejate la fel de riguros ca și materialul la care acestea permit accesul.

13. Combinațiile containerelor de securitate sunt cunoscute numai de numărul cel mai restrâns posibil de persoane. Combinațiile se modifică:

(a) la primirea unui nou container;

(b) cu ocazia oricărei schimbări de personal;

(c) în caz de compromitere a secretului informațiilor, reală sau bănuită;

(d) de preferință, la intervale de 6 luni și la cel puțin la fiecare 12 luni.

Dispozitivele de detectare a intruşilor

14. Atunci când sistemele de alarmă, camerele de luat vederi sau alte mecanisme electrice sunt folosite pentru a proteja informațiile clasificate ale UE, este obligatorie prevederea unor surse electrice suplimentare pentru a permite funcționarea continuă a sistemului în cazul întreruperii alimentării cu curent electric de la sursa principală. O altă cerință de bază este aceea ca orice funcționare greșită a acestor sisteme sau orice încercare de neutralizare a sistemelor arătate trebuie să declanșeze alarma sau să fie semnalată prin orice alt mijloc fiabil personalului de supraveghere.

Echipamente aprobate

15. ANS-urile mențin, din surse proprii sau bilaterale, liste la zi cu tipul și modelul echipamentelor de securitate acceptate pentru protecția directă și indirectă a informațiilor clasificate în diferite circumstanțe și condiții. Oficiul de Securitate al SGC menține o listă asemănătoare bazată, *inter alia*, pe informații furnizate de ANS-uri. Organismele descentralizate ale UE se consultă cu Oficiul de Securitate al SGC și, dacă este cazul, cu ANS a statului membru gazdă înaintea achiziționării unor astfel de echipamente.

Protecția fizică a faxurilor şi maşinilor de copiat

16. Faxurile și mașinile de copiat sunt protejate în măsura în care este necesar a se asigura faptul că numai personalul autorizat se poate folosi de acestea și că toate informațiile clasificate sunt supus unor controale corespunzătoare.

PROTECȚIA ÎMPOTRIVA VIZUALIZĂRII ȘI A INTERCEPTĂRILOR

Protecția împotriva vizualizării

17. Se iau toate măsurile pentru a se asigura faptul că informațiile clasificate ale UE nu sunt văzute, nici măcar în mod accidental, de persoane neautorizate.

Protecția împotriva interceptării

18. Birourile și zonele în care se dezbat în mod regulat informațiile clasificate ale UE trebuie protejate împotriva interceptărilor active și pasive în cazul în care riscul justifică aceasta. Evaluarea existenței unor astfel de riscuri constituie responsabilitatea autorității competente în materie de securitate, după consultarea cu ANS, dacă este necesar.

19. Pentru a determina măsurile de protecție ce urmează a fi luate în zonele sensibile împotriva interceptărilor pasive (de exemplu izolarea pereților, ușilor, podelelor și tavanelor, măsurarea posibilităților de compromitere a informațiilor respective) și a interceptărilor active (de exemplu căutarea microfoanelor), Oficiul de Securitate al SGC poate cere sprijinul experților ANS-urilor. Responsabilii pentru probleme de securitate ai organismelor descentralizate ale UE pot cere desfășurarea unor inspecții tehnice din partea Oficiului de Securitate al SGC și/sau asistență din partea experților ANS.

20. De asemenea, dacă este cazul, echipamentele de telecomunicații și echipamentele electronice și electrice de birou, de orice fel, utilizate în timpul reuniunilor la nivel de SECRET UE sau mai important, pot fi verificate de către specialiști tehnici de securitate din ANS-uri la cererea responsabilului competent pentru probleme de securitate.

ZONELE PROTEJATE DIN PUNCT DE VEDERE TEHNIC

21. Anumite zone pot fi concepute ca fiind zone protejate din punct de vedere tehnic. La intrarea în aceste zone are loc un control special. Aceste zone sunt păstrate închise printr-o metodă corespunzătoare atunci când nu sunt ocupate și toate cheile au regim de chei de securitate. Aceste zone sunt supuse unor inspecții fizice regulate; acest fapt are loc și ca urmare a oricărei intrări neautorizate sau a existenței suspiciunii în legătură cu o astfel de intrare.

22. Se va ține un inventar detaliat al mobilierului și echipamentelor pentru a fi monitorizate. În aceste zone nu se pot aduce nici un articol de mobilier sau echipament fără să fi fost înainte supus unor inspecții atente de către personal de securitate specializat, instruit pentru a putea detecta orice mecanisme de ascultare. De regulă, se evită instalarea liniilor de comunicație într-o astfel de zonă.

SECȚIUNEA V

NORME GENERALE PRIVIND PRINCIPIUL NECESITĂȚII DE A CUNOAȘTE ȘI AUTORIZĂRILE DE SECURITATE

1. Accesul la informații clasificate ale UE este autorizat doar pentru persoanele care au nevoie să cunoască respectivele informații pentru a-și îndeplini sarcinile de serviciu sau a-și duce la bun sfârșit misiunile. Accesul la informații de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*, SECRET UE sau CONFIDENTIEL UE *[Confidențial UE]* este autorizat doar pentru persoanele care posedă autorizarea de securitate corespunzătoare.

2. Responsabilitatea de a stabili cine are nevoie de anumite informații aparține SGC, organismelor descentralizat al UE și serviciului statului membru în care persoana în cauză își exercită funcțiile, ținându-se seama de necesitățile acestora din urmă.

3. Autorizarea de securitate este emisă de către angajatorul agentului în conformitate cu procedurile în materie. În ceea ce privește pe funcționarii SGC sau alți agenți, procedura verificării de securitate este descrisă în secțiunea VI.

   Această verificare are drept rezultat eliberarea unui certificat de securitate care arată nivelul informațiilor clasificate la care are acces persoana autorizată, precum și data expirării.

   Deținerea unui certificat de securitate pentru un anumit nivel de clasificare permite persoanei respective accesul la informații ce se află la un nivel mai jos.

4. Celelalte persoane, altele decât funcționarii și agenții SGC sau ai statelor membre, de exemplu membri, funcționari sau agenți ai instituțiilor UE, cu care este necesar să se examineze sau să se consulte informații clasificate ale UE, trebuie să posede o autorizație de securitate care să le permită accesul la informațiile clasificate ale UE și să fie instruiți în ceea ce privește responsabilitățile lor în materie de securitate. Aceeași regulă se aplică, în condiții similare, contractanților externi, experților și consultanților.

NORME SPECIALE PRIVIND ACCESUL LA INFORMAȚII DE NIVELUL TRÈS SECRET UE/EU TOP SECRET *[STRICT SECRET UE]*

5. Toate persoanele care urmează să aibă acces la informații clasificate de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* trebuie să fie supuse în prealabil unei proceduri de autorizare care să le permită accesul la aceste informații.

6. Toate persoanele cărora li se cere să aibă acces la informații clasificate de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* sunt numite de către șeful serviciului cărora îi aparțin, iar numele lor sunt păstrate în registrul special pentru informații clasificate de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*.

7. Înainte de a avea acces la informații clasificate de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*, toate persoanele semnează un certificat care atestă faptul că acestea au fost informate în legătură cu procedurile de securitate ale Consiliului și că înțeleg pe deplin responsabilitățile avute pentru protecția informațiilor clasificate de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* și consecințele prevăzute de normele UE și de actele cu putere de lege și normele administrative naționale în cazul în care respectivele informații ajung la persoane neautorizate, intenționat sau din neglijență.

8. În cazul persoanelor care au acces la informații de acest nivel cu ocazia diferitelor reuniuni, controlorul competent al serviciului sau organismului în cadrul căruia sunt angajate persoanele respective anunță serviciul care organizează reuniunea cu privire la faptul că persoanele respective au autorizația de a avea acces la informații de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*.

9. Numele tuturor persoanelor care nu mai lucrează cu informații de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* sunt eliminate de pe lista TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*. Acestor persoane li se atrage atenția cu privire la protecția acestui tip de informații. Respectivele persoane semnează o declarație prin care se obligă că nu vor utiliza sau divulga informațiile de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* de care au luat la cunoștință.

NORME SPECIALE PRIVIND ACCESUL LA INFORMAȚII DE NIVELUL SECRET UE ȘI CONFIDENTIEL UE *[CONFIDENȚIAL UE]*

10. Toate persoanele care urmează să aibă acces la informații de nivelul SECRET UE sau CONFIDENTIEL UE *[Confidențial UE]* trebuie să fie supuse în prealabil unei proceduri de autorizare corespunzătoare nivelului.

11. Toate persoanele care urmează să aibă acces la informații de nivelul SECRET UE sau CONFIDENTIEL UE *[Confidențial UE]* trebuie să cunoască normele de securitate și consecințele oricărei neglijențe.

12. În cazul persoanelor care au acces la acest tip de informații cu ocazia diferitelor reuniuni, responsabilul pentru probleme de securitate al organismului în cadrul căruia este angajată persoana în cauză anunță serviciul care organizează reuniunea că aceasta are autorizația de a avea acces la asemenea informații.

NORME SPECIALE PRIVIND ACCESUL LA INFORMAȚII DE NIVELUL RESTREINT UE *[CIRCULAȚIE RESTRÂNSĂ UE]*

13. Persoanele care au acces la informații de nivelul RESTREINT UE *[Circulație restrânsă UE]* sunt informate în legătură cu prezentele norme de securitate și cu consecințele oricărei neglijențe.

TRANSFERURI

14. Când un membru al personalului este transferat de la un post care implică prelucrarea de documente clasificate ale UE, registrul trebuie să se asigure că transferul documentelor de la persoana transferată la cea care îi ia locul se desfășoară cu respectarea reglementărilor în vigoare.

DISPOZIȚII SPECIALE

15. Persoanele cărora li se cere să lucreze cu informații clasificate ale UE trebuie să fie avertizați începând cu intrarea în funcție și, ulteriror, cu regularitate, cu privire la:

    (a) pericolele create pentru securitate din cauza unei conversații indiscrete;

    (b) precauțiile pe care trebuie să le ia în relația cu presa;

    (c) amenințarea prezentată de serviciile de spionaj a căror țintă o constituie UE și statele membre și care se interesează de informațiile clasificate și de activitățile UE;

    (d) obligația de a raporta imediat autorităților de securitate orice încercare sau activitate care ar putea trezi suspiciuni în legătură cu posibile activități de spionaj sau orice situații neobișnuite, care ar putea avea o legătură cu securitatea.

16. Toate persoanele expuse în mod obișnuit contactului frecvent cu reprezentanți ai țărilor ale căror servicii de spionaj au drept țintă UE și statele membre și care se interesează de informațiile clasificate și de activitățile UE sunt informați cu privire la tehnicile care sunt cunoscute ca fiind utilizate de diferitele servicii de informații.

17. Nu există reglementări de securitate ale Consiliului cu privire la călătoriile cu caracter personal, către orice destinație, întreprinse de personalul autorizat să aibă acces la informații clasificate ale UE. Cu toate acestea, autoritățile competente în materie de securitate îi vor informa pe funcționari și pe ceilalți agenți care se află sub autoritatea lor cu privire la reguli care se aplică în cazul călătoriilor, pe care aceștia ar trebui să le respecte. Responsabililor pentru probleme de securitate le revine răspunderea de a organiza, pentru membrii personalului, reuniuni de instructaj privind aceste dispoziții speciale.

SECȚIUNEA VI

PROCEDURA ACORDĂRII AUTORIZAȚIEI DE SECURITATE ÎN CAZUL FUNCȚIONARILOR ȘI AL ALTOR AGENȚI AI SGC

1. Au acces la informații clasificate doar funcționarii sau alți agenți ai SGC sau persoane care lucrează în cadrul SGC și care, prin natura serviciului și a sarcinilor de serviciu, au nevoie să ia la cunoștință informații clasificate deținute de Consiliu sau au nevoie să prelucreze aceste informații.

2. Pentru a avea acces la informațiile de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*, SECRET UE și CONFIDENTIEL UE *[Confidențial UE]*, persoanele la care se referă punctul 1 trebuie să fie autorizate în conformitate cu procedura prevăzută la punctele 4 și 5.

3. Autorizația este acordată numai persoanelor care au fost supuse unei anchete de securitate efectuate de autoritățile naționale competente ale statelor membre (ANS), în conformitate cu modalitățile prevăzute la punctele 6-10.

4. Autoritatea împuternicită să facă numiri (AIFN), în înțelesul articolul 2 primul paragraf din statutul personalului, este responsabilă cu eliberarea autorizațiilor prevăzute la punctele 1, 2 și 3.

   Autoritatea respectivă eliberează autorizația după obținerea avizului autorităților naționale competente ale statelor membre (ANS), pe baza anchetei de securitate efectuate în conformitate cu punctele 6-12.

5. Autorizația, valabilă pe o perioadă de 5 ani, nu poate să depășească durata sarcinilor pe baza cărora a fost eliberată. Aceasta poate fi reînnoită de către AIFN conform procedurii descrise la punctul 4.

   Autorizarea este retrasă de către AIFN când acest lucru se consideră necesar. Persoana în cauză este informată în legătură cu decizia de retragere a autorizării; respectiva persoană se poate cere să fie ascultată de către AIFN și de autoritatea națională competentă.

6. Ancheta de securitate urmărește să asigure că nu există obiecții pentru care o persoană să nu aibă acces la informațiile confidențiale deținute de către Consiliu.

7. Ancheta de securitate este efectuată, cu concursul persoanei în cauză și la cererea AIFN, de către autoritățile naționale competente ale statului membru al cărei resortisant este persoana. Dacă reședința persoanei se află pe teritoriul altui stat membru, autoritățile naționale în cauză se pot asigura de cooperarea autorităților statului de reședință.

8. În vederea anchetei, persoana în cauză este obligată să completeze un formular cu date personale.

9. AIFN specifică în cerere tipul și nivelul de clasificare al informațiilor de care persoana în cauză urmează să ia la cunoștință, astfel încât autoritățile naționale competente să poată desfășura ancheta și furniza un aviz cu privire la nivelul de autorizare care ar fi potrivit să îi fie acordat persoanei în cauză.

10. Întregul proces de verificare, împreună cu rezultatele obținute, respectă normele și regulamentele în vigoare în statele membre respective, inclusiv cele privind eventualele căi de atac.

11. Dacă autoritățile naționale competente din statele membre dau un aviz favorabil, AIFN eliberează autorizația persoanei în cauză.

12. Persoana în cauză este informată în cazul unui aviz negativ și poate cere ascultarea sa de către AIFN. În cazul în care consideră necesar, AIFN se poate adresa autorităților naționale competente pentru a solicita lămuririle suplimentare pe care acestea sunt în măsură să le ofere. În cazul în care avizul negativ se confirmă, autorizația nu poate fi acordată.

13. Orice persoană autorizată în sensul punctelor 4 și 5 primește, la data autorizării și, ulteriorl la intervale regulate, instrucțiunile necesare privind protecția informațiilor clasificate și modalitățile de a asigura această protecție. Aceasta semnează o declarație prin care confirmă că a primit aceste instrucțiuni și că se obligă să le respecte.

14. AIFN ia orice măsură necesară pentru a pune în aplicare dispozițiile prezentei secțiuni și, în special, pe cele referitoare la reglementarea accesului la lista persoanelor autorizate.

15. În mod excepțional și în funcție de necesitățile serviciului, după ce a informat în prealabil autoritățile naționale competente și în cazul în care acestea nu răspund în termen de o lună, AIFN poate să acorde o autorizație cu titlu temporar, pentru o perioadă care nu poate depăși șase luni, în așteptarea rezultatului anchetei menționate la punctul 7.

16. Autorizațiile provizorii și temporare nu permit accesul la informații de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*; acest tip de acces este rezervat funcționarilor care au fost efectiv supuși unei anchete de securitate al cărei rezultat a fost pozitiv, în conformitate cu punctul 7. În așteptarea rezultatelor anchetei de securitate, funcționarii care trebuie autorizați pentru a avea acces la nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* pot primi o autorizație temporară și provizorie pentru a avea acces la informații clasificate până la nivelul SECRET UE inclusiv.

SECȚIUNEA VII

PREGĂTIREA, DISTRIBUIREA, TRANSMITEREA, ARHIVAREA ŞI DISTRUGEREA MATERIALELOR CLASIFICATE ALE UE

Cuprins

Dispoziții generale

Prezenta secțiune explicitează măsurile pentru pregătirea, distribuirea, transmiterea, arhivarea și distrugerea documentelor clasificate ale UE, așa cum sunt acestea definite la punctul 3 litera (a) din principiile de bază și standardele minime de securitate prezentate în partea I a prezentei anexe. Aceasta va fi utilizată ca punct de referință pentru adaptarea respectivelor măsuri la alte materiale clasificate ale UE, conform tipului acestora și de la caz la caz.

Capitolul I

Pregătirea și distribuirea documentelor clasificate ale UE

PREGĂTIREA

1. Așa cum se indică în secțiunea II, clasificările și marcările UE trebuie să apară în partea superioară și în partea inferioară a fiecărei pagini, fiecare pagină trebuind numerotată. Fiecare document clasificat al UE poartă un număr de referință și o dată. În cazul documentelor de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* și SECRET UE, numărul de referință apare pe fiecare pagină. Dacă aceste documente urmează să fie distribuite în mai multe exemplare, fiecare dintre acestea va purta un număr de exemplar, care apare pe prima pagină, împreună cu numărul total al paginilor. Toate anexele și inserările sunt prezentate sub formă de listă pe prima pagină a oricărui document de nivelul CONFIDENTIEL UE *[Confidențial UE]* și mai importante.

2. Documentele de nivelul CONFIDENTIEL UE *[Confidențial UE]* și mai importante nu pot fi dactilografiate, traduse, depozitate, fotocopiate, reproduse magnetic sau pe microfilm decât de către persoane care au fost autorizate să aibă acces la informații clasificate ale UE, cel puțin până la nivelul de clasificare corespunzător documentelor în cauză, cu excepția cazurilor speciale descrise la punctul 27 din prezenta secțiune.

   Prevederile ce reglementează producerea computerizată a documentelor clasificate sunt prevăzute în secțiunea XI.

DISTRIBUIREA

3. Informațiile clasificate ale UE sunt distribuite numai persoanelor care au nevoie să le cunoască și care posedă autorizația de securitate corespunzătoare. Distribuirea inițială va fi precizată de către deținător.

4. Documentele de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* circulă prin intermediul registrelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* (a se vedea secțiunea VIII). În cazul mesajelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*, registrul competent poate autoriza șeful centrului de comunicare să realizeze numărul de exemplare precizat în lista destinatarilor.

5. Documentele de nivelul SECRET UE și mai puțin importante pot fi redistribuite de destinatarul original către alți destinatari, în funcție de necesitatea acestora de a le cunoaște. Autoritățile emitente trebuie, cu toate acesteam, să indice clar toate restricțiile pe care înțeleg să le stabilească. De fiecare dată când asemenea restricții sunt impuse, destinatarii nu pot redistribui documentele decât cu autorizația autorității emitente.

6. Fiecare document de nivelul CONFIDENTIEL UE *[Confidențial UE]* și mai importante, la sosire și la plecare, este înregistrat în registrul organismului respectiv. Datele înscrise (referințe, dată și, după caz, numărul de exemplare) sunt astfel menționate încât să ducă la identificarea documentelor și apar într-un jurnal sau pe un suport informatic special și protejat.

Capitolul II

Transmiterea/transportul documentelor clasificate ale UE

AMBALAREA

7. Documentele de nivelul CONFIDENTIEL UE *[Confidențial UE]* și mai importante sunt transmise în plicuri duble, opace și rezistente. Plicul interior trebuie să fie ștampilat și poartă marcajul nivelului de clasificare corespunzător, precum și, dacă este posibil, informații clare despre funcția și adresa destinatarului.

8. Numai controlorul registrelor sau locțiitorul acestuia au permisiunea de a deschide plicul interior și de a confirma primirea documentelor pe care le conține, cu excepția cazurilor în care plicul este adresat unei anumite persoane. În acest caz, în registru se înregistrează sosirea plicului și numai persoana căreia acesta îi este adresat are dreptul de a deschide plicul interior și de confirma primirea documentelor conținute.

9. În plicul interior se introduce un formular de confirmare de primire. Formularul, care nu este clasificat, trebuie să cuprindă numărul de referință, data și numărul de exemplar al documentului, dar niciodată informații despre conținutul acestuia.

10. Plicul interior este introdus într-un plic exterior care are înscris numărul de expediție, în scopul formalităților de primire. Nivelul de clasificare din punctul de vedere al securității nu trebuie, în nici un caz, să apară pe plicul exterior.

11. În cazul documentelor de nivelul CONFIDENTIEL UE *[Confidențial UE]* și mai importante, curierii și mesagerii primesc o confirmare de primire ce corespunde numărului de expediție.

TRANSMITEREA ÎN INTERIORUL UNEI CLĂDIRI SAU AL UNUI GRUP DE CLĂDIRI

12. În interiorul aceleiași clădiri sau al unui grup de clădiri documentele clasificate pot fi transmise într-un singur plic închis, menționând numai numele destinatarului, cu condiția ca transportul să fie efectuat de către o persoană autorizată corespunzător nivelului respectiv de clasificare.

TRANSMITEREA DOCUMENTELOR UE ÎN INTERIORUL ACELEIAȘI ȚĂRI

13. În interiorul aceleiași țări, documentele de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* trebuie transmise numai prin intermediul unui serviciu oficial de mesagerie sau cu ajutorul unor persoane autorizate să aibe acces la informații de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*.

14. Atunci când se folosește un serviciu de mesagerie pentru transmiterea unui document de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* în afara unei clădiri sau a unui grup de clădiri se respectă prevederile referitoare la ambalare și primire prevăzute de prezentul capitol. Serviciile de mesagerie trebuie să dispună de suficient personal pentru ca pachetele care conțin documente de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* să fie permanent sub directa supraveghere a unui funcționar.

15. În cazuri excepționale, documentele de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* pot fi transportate în afara clădirii sau grupului de clădiri și de alți funcționari decât mesagerii, pentru a fi utilizate local în cadrul reuniunilor sau dezbaterilor, cu condiția ca:

    (a) purtătorul să fie autorizat să aibă acces la informații de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*;

    (b) modul de transport să fie conform cu normele naționale stabilite pentru transmiterea documentelor naționale de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*;

    (c) respectivul funcționar să nu lase niciodată nesupravegheate documentele TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*;

    (d) să fie luate dispoziții pentru ca lista documentelor transportate în asemenea condiții să fie păstrată de către registrul documentelor de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* și să fie înregistrată într-un jurnal pentru a permite verificarea documentelor la înapoiere.

16. În interiorul aceleiași țări, documentele de nivelul SECRET UE sau CONFIDENTIEL UE *[Confidențial UE]* pot fi trimise fie prin poștă, dacă un astfel de sistem de transmitere este permis prin reglementările în materie de securitate în vigoare în țara respectivă și într-un mod conform respectivelor reglementări, fie printr-un serviciu de mesageri, fie prin intermediul unor persoane autorizate să aibe acces la informațiile clasificate ale UE.

17. Fiecare stat membru sau organism descentralizat al UE trebuie să elaboreze instrucțiuni, bazate pe aceste reglementări, privind transportul individual al documentelor clasificate ale UE. Purtătorului respectiv trebuie să i se ceară să citească și să semneze aceste instrucțiuni. Instrucțiunile vor prevedea îndeosebi că în niciun caz:

    (a) purtătorul nu poate să se separeu în vreun fel de documente, cu excepția cazului în care paza acestora este asigurată în conformitate cu prevederile secțiunii IV;

    (b) documentele nu pot fi lăsate nesupravegheate în mijloacele de transport în comun sau în vehiculele proprietate personală, nici în locuri publice cum ar fi restaurantele sau hotelurile; acestea nu pot fi nici depuse în seifurile hotelurilor sau încuiate fără supraveghere în camerele de hotel;

    (c) documentele nu pot fi citite în locurile publice, cum ar fi în avion sau în tren.

TRANSMITEREA DE LA UN STAT MEMBRU LA ALTUL

18. Materialele clasificate de nivelul CONFIDENTIEL UE *[Confidențial UE]* sau mai importante se transmit de la un stat membru la altul cu ajutorul unor servicii de curierat diplomatic sau militar.

19. Cu toate acestea, este permis transportul de către o persoană al materialelor clasificate de nivelul CONFIDENTIEL UE *[Confidențial UE]* sau SECRET UE, dacă dispozițiile luate pentru transport permit să se garanteze că persoanele neautorizate nu vor avea acces la documente.

20. ANS-urile pot autoriza transporturi efectuate de către persoane în cazul în care serviciile de curierat diplomatic sau militar nu pot fi utlizate sau în cazul în care utilizarea unor astfel de servicii ar avea drept rezultat întârzieri ce riscă să compromită operațiuni ale UE, iar destinatarul materialului are nevoie urgentă de acesta. Fiecare stat membru va redacta instrucțiuni privind transportul internațional, de către alte persoane decât curierii diplomatici sau militari, al materialelor clasificate până la nivelul SECRET UE inclusiv. Instrucțiunile trebuie să impună ca:

(a) purtătorul să posede autorizația de securitate corespunzătoare eliberată de statele membre;

(b) toate materialele astfel transportate să fie înregistrate de către oficiul sau registrul de securitate corespunzător;

(c) pachetele sau sacii ce conțin materiale clasificate ale UE poartă un sigiliu oficial pentru a opri sau descuraja efectuarea controlului vamal, precum și etichete de identificare cu instrucțiuni pentru cel care găsește aceste documente;

(d) purtătorul deține un certificat de curier și/sau un ordin de misiune recunoscute de toate statele UE prin care acesta este autorizat să transporte pachetul identificat în mod corespunzător;

(e) să nu fie traversate frontierele și nici teritoriile statelor nemembre UE, în cazul transportului terestru, cu excepția cazului în care aceste state au oferit garanțiile speciale statului expeditor;

(f) aranjamentele de călătorie ale purtătorului în ceea ce privește destinația, itinerariul și mijloacele de transport ce urmează a fi folosite se află în conformitate cu regulamentele UE sau, dacă regulamentele la nivel național în acest domeniu sunt mai stricte, în conformitate cu aceste regulamente;

(g) purtătorul nu trebuie să lase din posesie materialul cu excepția cazului când paza acstuia este asigurată în conformitate cu dispozițiile de securitate prevăzute în secțiunea IV;

(h) materialele nu sunt lăsate nesupravegheate în mijloacele de transport public sau privat, sau în locuri cum ar fi restaurantele sau hotelurile. De asemenea, ele nu pot fi lăsate în seiful unui hotel sau nesupravegheate în camerele de hotel;

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

Persoanele desemnate cu transportul materialelor clasificate trebuie să citească și să semneze un instructaj privind securitatea, care conține instrucțiunile enumerate mai sus și procedurile ce trebuie urmate în caz de urgență sau în cazul în care materialele respective fac obiectul controlului de către autoritățile vamale sau de securitate dintr-un aeroport.

TRANSMITEREA DOCUMENTELOR DE NIVELUL RESTREINT UE *[CIRCULAȚIE RESTRÂNSĂ UE]*

21. Nu se stabilesc norme speciale pentru transmiterea documentelor de nivelul RESTREINT UE *[Circulație restrânsă UE]*, cu excepția cazului în care trebuie să se asigure faptul că nu intră în posesia unor persoane neautorizate.

SECURITATEA CURIERILOR

22. Toți curierii și mesagerii angajați pentru transportul documentelor de nivelul SECRET UE și CONFIDENTIEL UE *[Confidențial UE]* sunt supuși verificării corespunzătoare de securitate.

Capitolul III

Transmiterea prin mijloace electrice și alte mijloace tehnice

23. Măsurile de securitate referitoare la sistemul de comunicații sunt elaborate în așa fel încât să asigure transmiterea în deplină siguranță a informațiilor clasificate ale UE. Secțiunea XI prevede în amănunt normele care trebuie respectate cu ocazia transmiterii de informații clasificate ale UE.

24. Numai centrele și rețelele de transmisiuni și/sau terminalele și sistemele omologate pot transmite informații clasificate de nivelul CONFIDENTIEL UE *[Confidențial UE]* și SECRET UE.

Capitolul IV

Exemplare suplimentare, traduceri și extrase din documentele clasificate ale UE

25. Numai deținătorul are dreptul de a autoriza copierea sau traducerea documentelor de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*.

26. În cazul în care persoane ce nu posedă autorizarea pentru informații de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* au nevoie de informații cuprinse într-un document de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* dar nu au ele însele acest nivel de clasificare, șeful registrului pentru documente TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* este autorizat să furnizeze numărul de extrase cerut din respectivul document. Acesta dispune totodată măsurile necesare pentru ca aceste documente să primească o clasificare de securitate corespunzătoare.

27. Documentele de nivelulul SECRET UE și mai puțin importante pot fi reproduse și traduse de către destinatar, în cadrul regulamentelor de securitate națională și cu condiția respectării principiului necesității de a cunoaște. Măsurile de securitate aplicabile documentului original se aplică și reproducerilor și/sau traducerilor acestora. Organismele descentralizate ale UE sunt obligate să se conformeze prezentului regulament de securitate.

Capitolul V

Inventarierea și controlul, arhivarea și distrugerea documentelor confidențiale ale UE

INVENTARIEREA ȘI CONTROLUL

28. În fiecare an, fiecare registru de documente de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*, menționat în secțiunea VIII, desfășoară o inventariere amănunțită a documentelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* în conformitate cu normele prevăzute în secțiunea VIII punctele (9)-(11). Documentele clasificate ale UE care au un nivel inferior nivelului TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* sunt supuse unor verificări interne în conformitate cu instrucțiunile stabilite la nivel național, și, în cazul SGC sau al organismelor descentralizate ale UE, conform instrucțiunilor secretarului general/Înalt reprezentant.

    Aceste operații permit îndeosebi obținerea avizului deținătorilor în ceea ce privește:

    (a) posibilitatea de a reduce nivelul de clasificare sau de a declasifica anumite documente;

    (b) documentele ce urmează a fi distruse.

ARHIVAREA INFORMAȚIILOR CLASIFICATE ALE UE

29. Pentru a minimiza problemele legate de arhivare, controlorii tuturor registrelor de documente clasificate sunt autorizați să asigure microfilmarea documentelor de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*, SECRET UE și CONFIDENTIEL UE *[Confidențial UE]* sau să le stocheze pe suport magnetic sau optic în scopul arhivării, cu condiția ca:

    (a) microfilmarea/arhivarea să fie executată de către persoane care posedă autorizarea corespunzătoare pentru a lucra cu informațiile de la un anumit nivel;

    (b) microfilmelor/înregistrărilor să li se asigure același grad de securitate ca și documentelor originale;

(c) microfilmarea/arhivarea documentelor de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* să fie semnalată deținătorului;

(d) rolele de film sau alt tip de suport să conțină numai documente cu același nivel de clasificare TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*, SECRET UE sau CONFIDENTIEL UE *[Confidențial UE]*;

(e) microfilmarea/arhivarea documentelor de nivelul SECRET UE sau TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* să fie clar indicată în registrul folosit pentru inventarul anual;

(f) documentele originale care au fost deja microfilmate sau arhivate pe un alt suport să fie distruse conform normelor stabilite la punctele (31)-(36).

30. Aceste norme se aplică de asemenea oricărui alt mijloc de arhivare autorizat de ANS, cum ar fi suporturile electromagnetice și discurile optice.

DISTRUGEREA PERIODICĂ A DOCUMENTELOR CLASIFICATE ALE UE

31. Pentru a preveni acumularea inutilă a documentelor clasificate ale UE, cele considerate de către șeful departamentului deținător drept permiate și excedentare sunt distruse în următorul mod:

(a) documentele TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* sunt distruse numai de către registrul central responsabil pentru ele. Fiecare document distrus este înscris într-un proces verbal de distrugere semnat de controlorul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* și de un martor la operațiunea de distrugere care trebuie să posede autorizarea corespunzătoare nivelului TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*. Această operațiune se va înscrie în registru;

(b) registrul este obligat să păstreze, pe termen de zece ani, procesele verbale de distrugere împreună cu fișele de distribuție. Se eliberează copii către deținătorul original sau către registrul central corespunzător numai la cererea lor expresă;

(c) documentele TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*, inclusiv toate deșeurile clasificate rezultate din pregătirea documentelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* (exemplare defectuoase, ciorne, note dactilografiate) trebuie distruse sub supravegherea unui responsabil TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*, prin incinerare, rupere, fărâmițare sau prin altă metodă care să rezulte într-o formă ce face imposibilă orice recunstituire a respectivelor informații.

32. Documentele SECRET UE trebuie distruse de către registrul de documente în sarcina căruia intră acestea, sub supravegherea unei persoane autorizate, folosind unul din procedeele descrise la punctul (31) litera (c). Documentele SECRET UE distruse sunt înscrise în procese verbale semnate, acestea urmând să fie reținute de către registru, împreună cu fișele de distribuție, pe termen de cel puțin trei ani.

33. Documentele CONFIDENTIEL UE *[Confidențial UE]* trebuie distruse de către registrul de documente în sarcina căruia intră acestea, sub supravegherea unei persoane autorizate, folosind unul din procedeele descrise la punctul (31) litera (c). Distrugerea lor este înregistrată în conformitate cu reglementările naționale și, în cazul SGC sau al organismelor descentralizate ale UE, conform instrucțiunilor secretarului general/Înalt reprezentant.

34. Documentele RESTREINT UE *[Circulație restrânsă UE]* sunt distruse de către registrul de documente în sarcina căruia intră acestea sau de către utilizator, în conformitate cu reglementările naționale și, în cazul SGC sau al agențiilor descentralizate ale UE, conform instrucțiunilor secretarului general/Înalt reprezentant.

DISTRUGEREA ÎN CAZ DE URGENȚĂ

35. SGC, statele membre și organismele descentralizate ale UE pregătesc planuri care țin seama de condițiile locale în vederea asigurării protecției materialelor clasificate ale UE în caz de criză, incluzând, dacă este necesar, planuri de distrugere și evacuare în caz de urgență; instituțiile respective promulgă, în cadrul organizațiilor lor, instrucțiuni considerate necesare pentru a evita accesul persoanelor neautorizate la informațiile clasificate ale UE.

36. Aranjamentele pentru protecția și/sau distrugerea documentelor de nivelul SECRET UE și CONFIDENTIEL UE *[Confidențial UE]* în caz de criză nu trebuie să aducă atingere sub nici o formă protecției și distrugerii materialelor de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* și, în special, materialele de cifrare, a căror tratare are prioritate față de orice alte operațiuni. Măsurile ce urmează a fi adoptate pentru protecția și distrugerea de urgență a materialelor de cifrare fac obiectul unor instrucțiuni ad-hoc.

CAPITOLUL VI

Norme speciale aplicabile documentelor destinate Consiliului

37. În cadrul SGC, un oficiu pentru informații clasificate monitorizează informațiile clasificate de nivelul SECRET UE sau CONFIDENTIEL UE *[Confidențial UE]*, atunci când acestea fac obiectul unor documentele ale Consiliului.

Sub autoritatea directorului general pentru administrație și personal, acest oficiu:

(a) gestionează operațiunile referitoare la înregistrarea, reproducerea, traducerea, transmiterea, expedierea și distrugerea informațiilor;

(b) aduce la zi registrul informațiilor clasificate;

(c) întreabă periodic emitenții privind necesitatea menținerii clasificării acestor informații;

(d) stabilește, împreună cu Oficiul de Securitate, normele metodologice pentru clasificarea și declasificarea informațiilor.

38. Oficiul pentru informații clasificate ține un registru privind următoarele date:

(a) data elaborării informației clasificate;

(b) nivelul de clasificare;

(c) data expirării clasificării respective;

(d) numele și serviciul emitent;

(e) destinatarul sau destinatarii, cu indicarea numărului de ordine;

(f) subiectul;

(g) numărul;

(h) numărul de exemplare puse în circulație;

(i) elaborarea inventarelor informațiilor clasificate prezentate Consiliului;

(j) registrul pentru reducerea nivelului de clasificare sau declasificarea informațiilor clasificate.

39. Normele generale prevăzute în capitolele I-V din prezenta secțiune se aplică oficiului pentru informații clasificate al SGC, cu excepția cazului în care acestea sunt modificate de norme speciale prevăzute în prezentul capitol.

SECȚIUNEA VIII

REGISTRELE TRÈS SECRET UE/EU TOP SECRET *[STRICT SECRET UE]*

1. Scopul existenței registrelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* este de a asigura înregistrarea, tratarea și distribuția documentelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* în conformitate cu normele de securitate. Șeful registrului TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* din fiecare stat membru, din cadrul SGC și, după caz, din cadrul organismelor descentralizate ale UE este controlorul documentelor de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*.

2. Registrele centrale constituie principala autoritate de primire și distribuție pentru statele membre, pentru SGC și pentru organismele descentralizate ale UE în care au fost constituite, precum și, dacă este cazul, pentru celelalte instituții ale UE, organizații internaționale și state terțe cu care Consiliul a încheiat acorduri privind procedurile de securitate pentru schimbul informațiilor clasificate.

3. Dacă este necesar, se întocmesc subregistre în vederea asigurării gestionării interne a documentelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*; acestea țin la zi situația fiecărui document a cărui răspundere o au.

4. Subregistrele TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* sunt înființate conform procedurii descrise în secțiunea I pentru a răspunde unei necesități permanente și sunt atașate unui registru central TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*. Dacă există numai o necesitate temporară și ocazională de consultare a documentelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*, respectivele documente pot fi comunicate fără înființarea unui subregistru TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*, cu condiția ca normele în vigoare să garanteze că acestea rămân sub controlul registrelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* și cu condiția respectării tuturor măsurilor de securitate fizică și privind personalul.

5. Subregistrele nu pot transmite documente TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* direct altor subregistre ale aceluiași registru central TRÈS SECRET UE/EU TOP SECRET fără autorizația expresă din partea acestuia din urmă.

6. Toate schimburile de documente TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* efectuate între subregistre subordonate unor registre centrale diferite trebuie să treacă prin registrele centrale.

REGISTRELE CENTRALE TRÈS SECRET UE/EU TOP SECRET *[STRICT SECRET UE]*

7. În calitate de controlor, șeful registrului central TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* este responsabil de:

   (a) asigurarea transmiterii documentelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* în conformitate cu regulamentele prevăzute în secțiunea VII;

   (b) menținerea la zi a listei cu toate subregistrele TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* împreună cu numele și semnăturile controlorilor și ale adjuncților autorizați ai acestora;

   (c) păstrarea fișelor de primire de la registre pentru toate documentele TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* distribuite de către registrul central;

   (d) ținerea unei situații privind documentele TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* deținute și distribuite;

   (e) menținerea la zi a listei tuturor registrelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* cu care ține în mod normal legătura, împreună cu numele și semnăturile controlorilor și ale adjuncților autorizați ai acestora;

   (f) asigurarea securității fizice a tuturor documentelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* deținute în respectivul registru în conformitate cu dispozițiile prevăzute în secțiunea IV.

SUBREGISTRELE TRÈS SECRET UE/EU TOP SECRET *[STRICT SECRET UE]*

8. În calitate de controlor, șeful subregistrului TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* este responsabil de:

   (a) asigurarea transmiterii documentelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* în conformitate cu dispozițiile prevăzute în secțiunea VII și punctele (5) și (6) din secțiunea VIII;

(b) menținerea la zi a listei tuturor persoanelor autorizate să aibe acces la informațiile TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* aflate sub controlul său;

(c) distribuția documentelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* în conformitate cu instrucțiunile emitentului și pe baza principiului necesității de a cunoaște, după ce s-a verificat în prealabil dacă destinatarul are autorizație de securitate de nivelul cerut;

(d) menținerea la zi a listei documentelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* deținute sau aflate în circulație sub controlul său sau care au fost transmise altor registre TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* și cu păstrarea tuturor fișelor corespunzătoare;

(e) menținerea la zi a listei registrelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* cărora este autorizat să le comunice sau de la care este autorizat să primească documente TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*, împreună cu numele și semnăturile controlorilor și ale adjuncților autorizați ai acestora;

(f) asigurarea securității fizice a tuturor documentelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* deținute în subregistru în conformitate cu dispozițiile prevăzute în secțiunea IV.

INVENTARELE

9. La fiecare 12 luni, fiecare registru TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* desfășoară un inventar amănunțit al tuturor documentelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* de care este responsabil. Se consideră că un document este inventariat de un anumit registru dacă registrul respectiv a putut să constate fizic existența acelui document sau ține fie o fișă a registrului TRÈS SECRET UE/EU TOP SECRET căruia i-a fost transmis respectivul document, fie un proces verbal de distrugere a documentului, fie un ordin de reducere a nivelului de clasificare sau de declasificare a respectivului document.

10. Subregistrele înaintează constatările făcute în cadrul inventarului anual către registrul central de care aparțin, la o dată stabilită de acesta din urmă.

11. ANS-urile, precum și instituțiile UE, organizațiile internaționale și organismele descentralizate ale UE în cadrul cărora a fost constituit un registru central TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* înaintează constatările făcute în cadrul inventarului anual desfășurat de registrele centrale TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* către secretarul general/Înalt reprezentant până la data de 1 aprilie a fiecărui an.

SECȚIUNEA IX

MĂSURI DE SECURITATE CE URMEAZĂ SĂ SE APLICE CU OCAZIA REUNIUNILOR SPECIALE ȚINUTE ÎN AFARA SEDIILOR CONSILIULUI ȘI CARE TRATEAZĂ CHESTIUNI DEOSEBIT DE SENSIBILE

GENERALITĂȚI

1. Măsurile de securitate prezentate mai jos trebuie luate în cazul în care reuniunile Consiliului European, sesiunile Consiliului, reuniunile la nivel ministerial sau alte reuniuni importante se desfășoară în afara sediilor Consiliului de la Bruxelles sau de la Luxemburg și în cazul în care aceasta se justifică din cauza necesităților de securitate speciale care decurg din nivelul înalt de sensibilitate al chestiunilor sau informațiilor în cauză. Aceste măsuri privesc numai protecția informațiilor clasificate ale UE; se pot dovedi necesare și alte măsuri de securitate.

RESPONSABILITĂȚI

Statul membru gazdă

2. Statul membru pe teritoriul căruia se desfășoară reuniunea respectivă (statul membru gazdă) este obligat să asigure, împreună cu Oficiul de Securitate al SGC, securitatea Consiliului European, a sesiunii Consiliului, a reuniunii ministeriale sau a altei reuniuni importante, precum și securitatea fizică a principalilor delegați și a colaboratorilor acestora.

În ceea ce privește protejarea securității, statul membru gazdă trebuie să asigure în special că:

(a) sunt stabilite planuri pentru a face față amenințărilor și incidentelor legate de securitate, măsurile respective având drept scop îndeosebi păstrarea în siguranță în interiorul incintelor a documentelor clasificate ale UE;

(b) sunt luate măsuri pentru a permite eventual accesul la sistemele de telecomunicații ale Consiliului pentru recepționarea și transmiterea mesajelor clasificate ale UE. Statul membru gazdă asigură de asemenea, după caz, accesul la sisteme protejate de telefonie.

Statele membre

3. Autoritățile statelor membre procedează astfel încât:

(a) autorizațiile de securitate corespunzătoare sunt furnizate, pentru delegații lor naționali, după caz prin mesaj sau fax, fie direct responsabilului pentru probleme de securitate a reuniunii, fie prin intermediul Oficiului de Securitate al SGC;

(b) se aduce la cunoștința autorităților statelor membre orice amenințare și, dacă este cazul, Oficiului de Securitate al SGC, pentru a se putea lua măsuri corespunzătoare.

Responsabilul pentru probleme de securitate a reuniunii

4. Este obligatorie desemnarea pentru reuniune a unui responsabil pentru probleme de securitate; acesta este responsabil de pregătirea generală și controlul măsurilor generale de securitate internă și de coordonarea cu celelalte autorități de securitate în cauză. Dispozițiile pe care acesta le ia privesc în general:

(a) (i) măsuri de protecție la locul reuniunii pentru a se asigura că aceasta se desfășoară fără nici un incident care ar putea compromite securitatea informațiilor clasificate ale UE utilizate în cadrul acesteia;

(ii) controlul personalului care are acces la locul reuniunii, a zonelor delegațiilor și a sălilor de conferință, precum și verificarea materialelor introduse în incinta acestora;

(iii) coordonarea permanentă cu autoritățile competente ale statului membru gazdă și cu Oficiul de Securitate al SGC;

(b) includerea unor instrucțiuni de securitate în dosarul reuniunii, ținând seama de imperativele enunțate de prezentul regulament de securitate, precum și de orice alte instrucțiuni de securitate considerate necesare.

Oficiul de Securitate al SGC

5. Oficiul de Securitate al SGC trebuie să joace rolul de consilier în materie de securitate pentru pregătirea reuniunii; acesta trebuie să fie reprezentat pentru a sprijini și consilia responsabilul pentru probleme de securitate a reuniunii și delegațiile, după caz.

6. Fiecare delegație participantă la o reuniune trebuie să desemneze un responsabil pentru probleme de securitate. Acesta este însărcinat cu problemele de securitate în cadrul delegației sale și cu menținerea legăturii cu responsabilul pentru probleme de securitate a reuniunii, precum și cu reprezentantul Oficiului de Securitate al SGC, după caz.

MĂSURI DE SECURITATE

Zone de securitate

7. Se stabilesc următoarele zone de securitate:

   (a) o zonă de securitate clasa a II-a, constând dintr-o încăpere pentru redactare, birourile și instalațiile de multiplicare ale SGC, precum și birourile delegațiilor, după caz;

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

   (c) zone administrative, constând din echipamentele destinate presei și din sectoarele rezervate administrației, alimentației și cazării, precum și zonele aflate în imediata apropiere a centrului de presă și a locului de reuniune.

Permise de trecere

8. Responsabilul pentru probleme de securitate a reuniunii eliberează ecusoane în funcție de necesitățile exprimate de delegații. După caz, se poate face distincție pentru accesul la diferite zone de securitate.

9. Instrucțiunile de securitate privind reuniunea prevăd că toate persoanele în cauză sunt obligate să poarte ecusonul în permanență și la vedere în incintele în care se desfășoară reuniunea, pentru a permite personalului de securitate să efectueze verificările necesare.

10. În afara persoanelor care dispun de ecuson, la locul reuniunii trebuie admise cât mai puține persoane. Delegațiile naționale care doresc să primească vizitatori la locul reuniunii trebuie să anunțe responsabilul pentru probleme de securitate a reuniunii. Vizitatorii primesc ecusoane speciale; se completează un permis de intrare cu numele vizitatorului și cu cel al persoanei care îl primește. Vizitatorii sunt însoțiți tot timpul de către un agent de securitate sau de persoana care îl primește. Însoțitorul poartă permisul de intrare al vizitatorului și îl înmânează personalului de securitate, împreună cu ecusonul vizitatorului, în momentul părăsirii locului respectiv de către vizitator.

Controlul echipamentelor audio și fotografice

11. Nu este permisă introducerea în zona de securitate clasa I a camerelor de luat vederi, a aparatelor fotografice sau a oricăror echipamente de înregistrare, cu excepția echipamentelor aduse de fotografii și de inginerii de sunet autorizați de către responsabilul pentru probleme de securitate a reuniunii.

Controlul servietelor, calculatoarelor portabile și pachetelor

12. Persoanele cu permise de intrare care le permit accesul într-o zonă de securitate își pot aduce, de regulă, servietele și calculatoarele portabile (numai cu sursă proprie de alimentare) fără a fi controlate. În cazul pachetelor pentru delegații, delegațiile pot prelua pachetele livrate, după controlul de către responsabilul pentru probleme de securitate al delegației sau după inspectarea prin intermediul unui echipament special sau după deschiderea de către personalul de securitate. Dacă responsabilul pentru probleme de securitate a reuniunii consideră necesar, se pot lua măsuri mai severe pentru controlul servietelor și pachetelor.

Securitatea tehnică

13. Securitatea tehnică a sălii de reuniune este garantată de o echipă tehnică de securitate, care asigură de asemenea supravegherea electronică în cursul reuniunii.

Documentele delegațiilor

14. Delegațiile sunt responsabile de transportul documentelor clasificate ale UE pe care le dețin către și de la locul reuniunii. De asemenea, acestea sunt responsabile de controlul și securitatea acestor documente în timpul utilizării acestora în cadrul incintelor care le sunt repartizate. Poate fi solicitat sprijinul statului membru gazdă în ceea ce privește transportul documentelor clasificate către și de la locul reuniunii.

Păstrarea în siguranță a documentelor

15. În cazul în care SGC, Comisia sau delegațiile nu pot pune în siguranță documentele lor clasificate în conformitate cu normele stabilite, acestea pot încredința aceste documente, în plic închis și sigilat și în schimbul unei dovezi de primire, responsabilului pentru probleme de securitate a reuniunii, în sarcina căruia va cădea să le pună în siguranță în conformitate cu normele stabilite.

Inspecția birourilor

16. Responsabilul pentru probleme de securitate a reuniunii trebuie să asigure ca birourile SGC și ale delegațiilor să fie verificate la sfârșitul fiecărei zile de lucru, pentru a se asigura că documentele clasificate ale UE sunt păstrate într-un loc sigur; în caz contrar, acesta ia măsurile necesare.

Eliminarea deșeurilor clasificate ale UE

17. Toate deșeurile trebuie considerate ca fiind deșeuri clasificate ale UE, iar SGC și delegațiilor li se vor atribui coșuri de hârtie sau saci pentru depozitarea acestora. Înaintea părăsirii incintelor care le-au fost repartizate, membrii SGC și delegațiile trebuie să ducă aceste deșeuri la responsabilul pentru probleme de securitate a reuniunii, care va dispune distrugerea acestora conform procedurilor regulamentare.

18. La încheierea reuniunii, toate documentele deținute de SGC sau de delegații și care au devenit inutile sunt considerate deșeuri. Trebuie efectuată o cercetare amănunțită a birourilor SGC și ale delegațiilor înainte ca aplicarea măsurilor de securitate luate să înceteze. Documentele pentru care s-a semnat o fișă de primire trebuie să fie distruse, în măsura posibilului, conform procedurii descrise în secțiunea VII.

SECȚIUNEA X

ÎNCĂLCAREA SECURITĂȚII ȘI COMPROMITEREA INFORMAȚIILOR CLASIFICATE UE

1. O încălcare a securității constituie o acțiune sau o omisiune contrară unei norme de securitate a Consiliului sau unei norme naționale și care ar putea compromite sau pune în pericol informații clasificate ale UE.

2. Compromiterea informațiilor clasificate ale UE se produce atunci când acestea ajung, în tot sau în parte, la persoane neautorizate, adică la persoane care nu dispun de autorizație UE corespunzătoare sau care nu au nevoie să cunoască aceste informații, ori când există o suspiciune credibilă că un asemenea fapt a avut loc.

3. Informațiile clasificate ale UE pot fi compromise prin lipsă de atenție, prin neglijență sau prin indiscreție, precum și ca urmare a activităților serviciilor care au drept țintă UE sau statele membre ale acesteia și care sunt interesate de informațiile clasificate și de activitățile UE, sau de către organizații subversive.

4. Este important ca toate persoanele cărora li se cere să lucreze cu informații clasificate ale UE să fie informate pe deplin cu privire la procedurile de securitate, la pericolele prezentate de anumite conversații indiscrete și la relațiile pe care trebuie să le aibă cu presa. Aceste persoane trebuie să fie conștiente de importanța raportării fără întârziere a oricărei încălcări a securității pe care ar putea-o observa, autorității de securitate a statului membru respectiv, a instituției sau agenției în cadrul cărora lucrează.

5. În cazul în care o autoritate de securitate constată sau este informată asupra unei încălcări a securității informațiilor clasificate ale UE sau asupra unei pierderi sau dispariții a materialelor clasificate ale UE, aceasta acționează de îndată pentru a:

   (a) stabili situația de fapt;

   (b) evalua și minimiza daunele aduse;

   (c) preveni o posibilă repetare a acelor fapte;

   (d) anunța autoritățile corespunzătoare asupra efectelor încălcării securității.

   În acest context se pun la dispoziție următoarele informații:

   (i) o descriere a informațiilor în cauză, precizând în special clasificarea acestora, referința și numărul copiei, data, deținătorul, subiectul și domeniul documentului;

   (ii) o descriere pe scurt a circumstanțelor în care s-a produs încălcarea, inclusiv data și perioada de timp în care informațiile respective au fost expuse compromiterii;

   (iii) o declarație din care să reiasă dacă autoritatea emitentă a fost sau nu informată în legătură cu acest fapt.

6. Este de datoria fiecărei autorități de securitate care a fost informată despre producerea unei încălcări de a semnala aceasta de îndată, utilizând următoarea procedură: subregistrul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* aduce incidentul al cunoștința Oficiului de Securitate al SGC prin intermediul registrului central TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*; în cazul compromiterii unor informații clasificate ale UE care a avut loc sub jurisdicția unui stat membru, incidentul se raportează Oficiului de Securitate al SGC, conform dispozițiilor punctului (5), prin intermediul ANS responsabile.

7. Cazurile ce implică informații RESTREINT UE *[Circulație restrânsă UE]* trebuie raportate numai când prezintă trăsături neobișnuite.

8. De îndată ce este informat cu privire la o încălcare, secretarul general/Înalt reprezentant:

   (a) o notifică autorității emitente care a furnizat informațiile clasificate în chestiune;

   (b) cere autorităților de securitate corespunzătoare să înceapă ancheta;

   (c) coordonează anchetele când sunt implicate mai multe autorități de securitate;

(d) obține un raport despre circumstanțele producerii încălcării respective, data și perioada în cursul căreia aceasta s-a putut produce, data și locul descoperirii sale și o descriere amănunțită a conținutului și clasificării documentelor în cauză. Prejudiciul cauzat intereselor UE sau ale unuia sau mai multor state membre și acțiunile luate pentru a preveni repetarea faptelor respective trebuie, de asemenea, arătate.

9. Autoritatea emitentă informează destinatarii și să dea instrucțiuni corespunzătoare.

10. Orice persoană care este responsabilă de compromiterea informațiilor clasificate ale UE este pasibilă de sancțiuni disciplinare conform regulamentelor în vigoare și fără a aduce atingere acțiunilor în justiție.

SECȚIUNEA XI

PROTEJAREA INFORMAȚIILOR PRELUCRATE CU AJUTORUL TEHNOLOGIEI INFORMAȚIEI ȘI AL SISTEMELOR DE COMUNICAȚIE

Cuprins

Capitolul I

Introducere

GENERALITĂȚI

1. Cerințele și politica privind securitatea, definite în prezenta secțiune, se aplică tuturor rețelelor și sistemelor informaționale și de comunicație (numite de aici înainte „SISTEME") care prelucrează informații clasificate de nivelul CONFIDENTIEL UE *[Confidențial UE]* sau mai înalt.

2. SISTEMELE care prelucrează informații de nivelul RESTREINT UE *[Circulație restrânsă UE]* necesită, de asemenea, măsuri de securitate pentru protecția confidențialității informațiilor respective. Toate SISTEMELE necesită aplicarea unor măsuri de securitate pentru protejarea integrității și disponibilității acestora și a informațiilor conținute. Măsurile de securitate ce urmează a fi aplicate acestor sisteme sunt stabilite de către Autoritatea de Acreditare în domeniul Securității (AAS) competentă; acestea sunt proporționale cu gradul riscurilor estimate și conforme cu politica stabilită prin prezentul regulament de securitate.

3. Protejarea sistemelor de detecție ce conțin sisteme TI este stabilită și specificată în contextul general al sistemelor de care aparțin folosind, pe cât posibil, prevederile aplicabile ale acestei secțiuni.

VULNERABILITATEA SISTEMELOR ȘI EVENTUALELE AMENINȚĂRI

4. În termeni generali, o amenințare poate fi definită ca fiind o potențială compromitere în mod accidental sau deliberat a securității. În cazul SISTEMELOR, o astfel de compromitere implică pierderea uneia sau mai multor calități, care sunt confidențialitatea, integritatea și disponibilitatea. Caracterul vulnerabil poate fi definit ca fiind o slăbiciune sau o lipsă de control care facilitează sau permite apariția unei amenințări la adresa unui anumit bun sau obiectiv. Caracterul vulnerabil poate rezulta și dintr-o omisiune sau să fie legat de un control prea deficitar, incomplet sau inegal.. Ea se poate situa în planul tehnic, în cel procedural sau în cel al exploatării.

5. Informațiile clasificate sau neclasificate ale UE, prelucrate în cadrul SISTEMELOR sub o formă concentrată pentru a putea fi identificate, comunicate și utilizate rapid sunt expuse multor riscuri. Aceste riscuri includ accesul la ele al unor utilizatori neautorizați sau, dimpotrivă, imposibilitatea accesării lor de către utilizatori autorizați. Există și riscurile de divulgare, alterare, modificare sau eliminare neautorizată a informațiilor. Uneori echipamentele respective sunt fragile și complexe, sunt costisitoare și adeseori greu de reparat sau de înlocuit rapid. Prin urmare, aceste sisteme constituie ținte atractive pentru operațiuni de strângere de informații și pentru acte de sabotaj, în special dacă măsurile de securitate apar ca fiind ineficiente.

MĂSURI DE SECURITATE

6. Scopul principal al măsurilor de securitate enunțate în prezenta secțiune este de a asigura protecție împotriva divulgării neautorizate a informațiilor (pierderea confidențialității) și împotriva pierderii integrității și disponibilității informațiilor. Pentru a asigura o protecție corespunzătoare a SISTEMELOR de prelucrare a informațiilor clasificate ale UE, este necesar să se prevadă norme corespunzătoare de protecție clasică, precum și procedurile și tehnicile adecvate de securitate concepute special pentru fiecare SISTEM.

7. Se elaborează și se pune în aplicare un set echilibrat de măsuri de securitate pentru a crea un mediu sigur în care să opereze aceste SISTEME. Domeniile de aplicare a acestor măsuri implică elemente fizice, personalul, procedurile non-tehnice și procedurile de exploatare privind calculatoarele și comunicațiile.

8. Măsurile de securitate a calculatoarelor (dispozitive de securitate a hardware-ului și a programelor) trebuie să permită aplicarea principiului necesității de a cunoaște și evitarea sau detectarea divulării neautorizate a informațiilor. Încrederea ce poate fi acordată măsurilor de securitate aplicabile calculatoarelor se stabilește în cursul procesului de definire a exeigențelor de securitate. Procesul de omologare permite să se stabilească existența unui nivel de asigurări suficient pentru a justifica încrederea în aceste măsuri.

DECLARAȚIA PRIVIND CERINȚELE DE SECURITATE PRIVIND UN ANUMIT SISTEM (SSRS)

9. Pentru toate SISTEMELE ce prelucrează informații clasificate de nivelul CONFIDENTIEL UE *[Confidențial UE]* sau mai înalt este necesară stabilirea unei declarații privind cerințele de securitate privind un anumit sistem (SSRS) de către Autoritatea de exploatare a sistemului TI (ITSOA), după caz cu contribuția și sprijinul responsabililor de proiect și ale Autorității INFOSEC și aprobată de AAS. O SSRS se stabilește și în cazul în care AAS consideră esențială disponibilitatea și integritatea informațiilor de nivelul UE RESTREINT sau a informațiilor neclasificate.

10. SSRS va fi formulată în faza incipientă a unui proiect și dezvoltată sau lărgită pe măsură ce proiectul progresează, îndeplinind diferite roluri în diferite stagii ale ciclului de viață al proiectului și SISTEMULUI respective.

11. SSRS are rolul de acord de legătură între Autoritatea Operațională a Sistemelor TI și AAS pe baza cărora este acreditat SISTEMUL.

12. SSRS este o declarație completă și explicită despre principiile de securitate ce urmează a fi aplicate și despre cerințele de securitate ce trebuie îndeplinite. Această declarație se bazează pe politica de securitate a Consiliului și pe evaluarea riscurilor sau este impusă de parametrii mediului operațional, de autorizația de securitate pentru personal de nivelul cel mai jos, de cea mai înaltă clasificare a informațiilor prelucrate, de modul de operare a securității și de cerințele utilizatorilor. SSRS este o parte integrantă din documentația proiectului înaintată autorităților corespunzătoare în scopul aprobării tehnice, bugetare și de securitate. În formă finală SSRS constituie o declarație completă despre ceea ce înseamnă securitatea SISTEMELOR.

MODURI DE OPERARE ALE SECURITĂȚII

13. Toate SISTEMELE de prelucrare a informațiilor clasificate de nivelul CONFIDENTIEL UE *[Confidențial UE]* și mai importante trebuie să opereze într-un mod anumit de operare sau, acolo unde există garanții asigurate de diferite cerințe în timpul unor perioade de timp specificate, în mai multe moduri de operare, sau în echivalentele lor naționale:

(a) specializate;

(b) sisteme înalte;

(c) sisteme pe mai multe nivele.

Capitolul II

Definiții

MARCAJE SUPLIMENTARE

14. Marcajele suplimentare, cum ar fi CRYPTO sau alți indicatori de operare recunoscuți de UE, se aplică unde este necesară o distribuție limitată și o prelucrare specială suplimentară față de cele stabilite prin clasificarea gradelor de securitate.

15. MODUL DE OPERARE „SPECIALIZAT" se referă la: un mod de operare în care TOȚI indivizii cu acces la SISTEM sunt verificați până la cel mai înalt nivel de clasificare a informațiilor prelucrate prin SISTEMUL respectiv; aceste persoane au nevoie să cunoască respectivele informații prelucrate în cadrul SISTEMULUI.

Note:

(1) Principiul nevoii de cunoaștere a informațiilor respective indică faptul că nu există o cerință obligatorie pentru ca funcțiile de securitate ale calculatorului să separe informațiile în interiorul SISTEMULUI.

(2) Celelalte funcții de securitate (de exemplu fizică, procedurală sau a personalului) se conformează cerințelor celui mai înalt nivel de clasificare și tuturor indicatorilor de categorie pentru informațiile prelucrate în cadrul SISTEMULUI.

16. MODUL DE OPERARE AL „SISTEMELOR ÎNALTE" se referă la: un mod de operare în care TOȚI indivizii cu acces la SISTEM sunt verificați până la cel mai înalt nivel de clasificare a informațiilor prelucrate prin SISTEMUL respectiv, dar nu TOȚI indivizii cu acces la SISTEM au nevoie expresă de a cunoaște informațiile operate în cadrul SISTEMULUI.

Note:

(1) Lipsa nevoii de cunoaștere a informațiilor respective indică faptul că există o cerință obligatorie pentru ca funcțiile de securitate ale calculatorului să furnizeze acces selectiv și separarea informațiilor în cadrul SISTEMULUI.

(2) Celelalte funcții de securitate (de exemplu fizică, procedurală sau a personalului) se conformează cerințelor celui mai înalt nivel de clasificare și tuturor indicatorilor de categorie pentru informațiile prelucrate în cadrul SISTEMULUI.

(3) Toate informațiile prelucrate sau făcute disponibile SISTEMULUI prin acest mod de operare sunt protejate în funcție de indicatorul de categorie a informațiilor și de cel mai înalt nivel de clasificare, cu excepția cazului în care există un nivel acceptabil de încredere care poate fi atribuit oricărei funcționalități a procesului de etichetare.

17. SISTEMUL DE OPERARE „PE MAI MULTE NIVELE” se referă la: un mod de operare în care NU TOȚI indivizii autorizați pentru a avea acces la SISTEM sunt verificați la cel mai înalt nivel de clasificare a informațiilor prelucrate în cadrul SISTEMULUI, și NU TOATE persoanele cu acces la sistem au nevoie expresă de a cunoaște informațiile operate în SISTEMUL respectiv.

Note:

(1) Acest mod de operare permite prelucrarea informațiilor de diferite niveluri și cu diferiți indicatori de categorie.

(2) Faptul că nu toate persoanele sunt verificate la cel mai înalt nivel de clasificare, împreună cu lipsa nevoii de cunoaștere, indică faptul că există o cerință a funcțiilor de securitate ale calculatorului de a furniza accesul și separarea informațiilor în interiorul SISTEMULUI.

18. INFOSEC se referă la: aplicarea măsurilor de securitate pentru a proteja informațiile procesate, stocate sau transmise în cadrul sistemelor informaționale și de comunicație, sau de alt tip electronic, împotriva pierderii, în mod accidental sau intenționat, a confidențialității, a integrității sau a disponibilității și să prevină pierderea caracterului integru și disponibil al sistemelor înseși. Măsurile INFOSEC includ pe cele referitoare la securitatea calculatoarelor, transmisiilor, emisiilor și celor cu caracter criptografic, și detectarea, documentarea și opunerea amenințărilor aduse la adresa informațiilor și SISTEMELOR.

19. Securitatea calculatoarelor (COMPUSEC) se referă la: aplicarea funcțiilor de securitate a hardware-ului, firmware-ului și softului la sistemul de calculatoare pentru a preveni sau a le proteja împotriva divulgării, manipulării, modificării sau eliminării informațiilor sau împotriva neacordării accesului la sisteme.

20. PRODUSUL DE SECURITATE A CALCULATOARELOR se referă la: un articol cu caracter generic din cadrul funcției de securitate a calculatorului care are drept scop încorporarea unui sistem TI pentru a-l utiliza la lărgirea informațiilor sau care asigură confidențialitatea, integritatea și disponibilitatea respectivelor informații.

21. SECURITATEA DE COMUNICARE (COMSEC) se referă la: aplicarea unor măsuri de securitate în sistemul de telecomunicații pentru a nu permite persoanelor neautorizate accesul la informații a căror valoare poate proveni din posesia sau studiul unor astfel de sisteme de telecomunicație sau pentru a asigura autenticitatea unor asemenea sisteme de telecomunicații.

Notă:

Aceste măsuri includ securitate criptografică, de transmisie sau emisie; includ, de asemenea, securitatea fizică și procedurală a calculatoarelor, a documentelor, a personalului.

22. EVALUAREA se referă la: o examinare tehnică detaliată, întreprinsă de către o autoritate corespunzătoare, a aspectelor legate de securitatea SISTEMELOR sau a unui produs de securitate a calculatoarelor sau cu caracter criptografic.

Note:

(1) Evaluarea investighează prezența funcțiilor de securitate cerute și absența efectelor secundare compromițătoare rezultate din aceste funcții și evaluează caracterul incoruptibil al acestor funcții.

(2) Evaluarea determină măsura în care cerințele de securitate ale SISTEMULUI sau performanțele de securitate ale unui produs de securitate a calculatoarelor sunt satisfăcute și stabilește nivelul de siguranță al SISTEMULUI ASA al funcțiilor de securitate, cu caracter criptografic, ale calculatorului.

23. CERTIFICAREA se referă la: eliberarea unei declarații formale însoțită de o revizuire independentă a rezultatelor evaluării, din care să reiasă măsura în care SISTEMUL corespunde cerințelor de securitate sau în care produsul de securitate al unui calculator prezintă performanțele de securitate prestabilite.

24. ACREDITAREA se referă la: autorizarea sau acordul dat unui sistem de a procesa informații clasificate ale UE în mediul său operațional.

Notă:

Această acreditare se face după ce toate procedurile de securitate corespunzătoare au fost puse în aplicare și a fost atins un nivel satisfăcător de protecție a sistemului. Acreditarea trebuie, în mod normal, făcută pe baza SSRS-urilor și trebuie să cuprindă următoarele:

(a) o declarație despre obiectivele acreditării sistemului; în special, se vor furnzia informații despre nivelul de clasificare a informațiilor cu care urmează să se lucreze și despre modurile de operare ale sistemelor și rețelelor de securitate propuse;

(b) prezentarea unei evaluării a administrării riscurilor pentru a identifica prezența unor amenințări sau a unui caracter vulnerabil și pentru a lua măsuri de prevenire a acestora;

(c) procedurile operaționale de securitate, împreună cu o descriere a operațiunilor propuse (de exemplu modalități, servicii ce urmează a fi furnizate), incluzând o descriere a funcțiilor de securitate ale SISTEMULUI care formează baza de acreditare;

(d) un plan pentru implementarea și menținerea funcțiilor de securitate;

(e) un plan pentru testarea inițială și viitoare a sistemelor și rețelelor de securitate, împreună cu evaluarea și certificarea acestui test și

(f) certificarea, unde este cazul, împreună cu celelalte elemente al acreditării.

25. SISTEMELE TI se referă la: un ansamblu de echipamente, metode și proceduri și, unde este necesar, de personal, organizat pentru a îndeplini funcții de procesare a informațiilor.

Note:

(1) Acest lucru se referă la un ansamblu de incinte, configurat pentru a procesa informațiile în interiorul sistemului.

(2) Aceste sisteme pot veni în sprijinul aplicațiilor de consultanță, de comandă, control, comunicații cu caracter științific sau administrativ, inclusiv procesării cuvintelor.

(3) Limitele unui sistem sunt, în general, stabilite ca fiind elemente aflate sub controlul unei singure ITSOA.

(4) Un sistem TI poate conține subsisteme care, la rândul lor, sunt considerate sisteme TI.

26. Funcțiile de securitate ale sistemelor TI cuprind toate funcțiile, caracteristicile și trăsăturile hardware/firmware/software, proceduri operaționale, proceduri de contabilizare și de control al accesului, zona TI, zona terminală izolată și obligațiile administrative, structura și dispozitivele fizice, controalele personalului și a comunicațiilor necesare pentru a asigura un nivel de protecție a informațiilor clasificate ce urmează a fi procesate în cadrul unui sistem TI.

27. REȚELELE TI se referă la: o organizare, dispusă geografic, a sistemelor TI interconectate pentru a face schimb de date; această organizare cuprinde sistemele TI interconectate și interfața acestora cu datele ajutătoare și rețelele de comunicație.

Note:

(1) O rețea TI poate utiliza serviciile uneia sau mai multor rețele de comunicație interconectate pentru a face schimb de date; câteva rețele TI pot folosi serviciile unei rețele obișnuite de comunicație.

(2) Se numește „locală" o rețea care leagă mai multe calculatoare în același loc.

28. FUNCȚIILE DE SECURITATE ALE REȚELELOR TI includ funcțiile de securitate ale sistemelor TI individuale, ce cuprind rețeaua împreună cu acele componente și funcții suplimentare asociate cu rețeaua respectivă (de exemplu comunicații de rețea, mecanisme și proceduri de identificare a securității și de etichetare, controale ale accesului, piste de audit și programe) necesare pentru a asigura informațiilor clasificate un nivel acceptabil de protecție.

29. ZONA TI se referă la: o zonă care cuprinde unul sau mai multe calculatoare, unitățile lor periferice sau de stocare locale, unitățile de control și echipamente specializate pentru rețele și comunicații.

Notă:

Acestea nu includ o zonă separată în care dispozitivele periferice și terminalele și stațiile sunt plasate, chiar dacă aceste dispozitive sunt conectate la echipamente din zone TI.

30. ZONA RETRASĂ PENTRU TERMINALE ȘI STAȚII se referă la: o zonă în care se află anumite echipamente de calculatoare, dispozitive periferice locale și stații/terminale și orice alt echipament de comunicații, separate de zona TI.

31. Măsuri de protecție împotriva DESCĂRCĂRILOR ELECTRICE: măsuri de securitate menite să protejeze echipamentele și infrastructurile de comunicație împotriva compromiterii informațiilor clasificate prin emisii electromagnetice accidentale.

Capitolul III

Răspunderi privind securitatea

GENERALITĂȚI

32. Responsabilitățile Comitetului de securitate, definite în secțiunea I, alineatul (4), includ chestiuni legate de INFOSEC. Comitetul de securitate își organizează activitățile în așa fel încât să ofere consultanță în problemele menționate mai sus.

33. În cazul unor probleme legate de securitate (incidente, încălcări ale acesteia etc.), Oficiul de Securitate al SGC și/sau Autoritatea Națională iau măsuri imediat. Toate probleme sunt aduse la cunoștința Oficiul de Securitatel al SGC.

34. Secretarul general/Înalt reprezentant sau, după caz, șeful unui organism descentralizat al UE creează Oficiul INFOSEC pentru a oferi orientare autorității de securitate în ceea ce privește implementarea și controlul funcțiilor speciale de securitate prevăzute ca parte integrantă a sistemelor.

AUTORITATEA DE ACREDITARE ÎN MATERIE DE SECURITATE (AAS)

35. AAS este una dintre următoarele:

— o ANS;

— Autoritatea desemnată de către secretarul general/Înalt reprezentant;

— autoritatea de securitate a unui organism descentralizat al UE sau

— reprezentanții delegați/numiți ai acesteia, ce depind de sistemul ce urmează a fi acreditat.

36. AAS este responsabilă cu asigurarea corespondenței SISTEMELOR cu politica Consiliului în ceea ce privește securitatea. Una dintre sarcinile ei este de a-și da acordul ca un anumit SISTEM să opereze informații clasificate UE la un nivel de clasificare stabilit în mediul său operațional. În ceea ce privește SGC și organismele descentralizate ale UE, AAS își exercită responsabilitatea de a asigura securitatea în numele secretarului general/Înalt reprezentant sau al șefilor organismelor descentralizate.

Jurisdicția AAS a SGC acoperă toate SISTEMELE care se află în operare în interiorul sediilor SGC. Sistemele și componentele SISTEMELOR în operare în cadrul statelor membre rămân în jurisdicția statului membru respectiv. Când diferite componente ale unui SISTEM ajung în jurisdicția AAS a SGC și a altor AAS, toate părțile numesc un consiliu de acreditare unit aflat sub coordonarea AAS a SGC.

AUTORITATEA INFOSEC (IA)

37. Autoritatea INFOSEC este responsabilă de activitățile Oficiului INFOSEC. În ceea ce privește SGC și, după caz, organismele descentralizate ale UE, autoritatea INFOSEC este responsabilă cu:

— furnizarea către AAS de asistență și consultanță tehnice;

— asistența în procesul de dezvoltare a SSRS-urilor;

— revizuirea SSRS-urilor pentru a asigura conformitatea cu regulamentele securității, cu politica INFOSEC și cu documentele de structură;

— participarea la reuniuni de acreditare, la cerere, și cu furnizarea unor recomandări din partea INFOSEC pentru acreditarea AAS;

— asigurarea de sprijin în activitățile educaționale și de instruire ale INFOSEC;

— furnizarea de consultanță tehnică în investigarea incidentelor legate de INFOSEC;

— stabilirea unei orientări a politicii tehnice pentru a se asigura faptul că se utilizează numai programe autorizate.

AUTORITATEA OPERAȚIONALĂ A SISTEMELOR TI (ITSOA)

38. Autoritatea INFOSEC transferă către ITSOA responsabilitatea pentru implementarea și operarea controalelor și a funcțiilor de securitate ale SISTEMELOR. Această responsabilitate se extinde pe tot parcursul ciclului de viață a sistemelor respective începând cu conceperea acestora până la stadiul final.

39. ITSOA este responsabilă cu toate măsurile de securitate concepute ca parte integrantă a sistemelor. Această responsabilitate implică și pregătirea procedurilor de operare a securității. ITSOA specifică standardele și practicile de securitate ce trebuie avute în vedere de către furnizorul SISTEMELOR.

40. ITSOA poate transfera o parte din responsabilitățile sale, după caz, către responsabilii INFOSEC însărcinați cu sistemul și, respectiv, cu amplasamentul. Diferitele funcții ale INFOSEC pot fi îndeplinite de o singură persoană.

UTILIZATORII

41. Toți utilizatorii sunt responsabili cu asigurarea faptului că acțiunile lor nu afectează securitatea SISTEMELOR folosite.

INSTRUIREA INFOSEC

42. Educarea și instruirea INFOSEC sunt disponibile la orice nivel pentru personal diferit, în cadrul SGC, al organismelor descentralizate ale UE și în cadrul departamentelor guvernamentale ale statelor membre.

Capitolul IV

Măsuri de securitate care nu au caracter tehnic

PERSONALUL DE SECURITATE

43. Utilizatorii sistemelor sunt verificați și trebuie să aibă nevoie de informațiile respective, în funcție de nivelul de clasificare și de conținutul informațiilor procesate în cadrul sistemelor acestora. Accesul la anumite echipamente sau informații importante pentru securitatea sistemului cer existența unei autorizații speciale eliberată conform procedurilor Consiliului.

44. AAS desemnează toate pozițiile importante și specifică nivelul de verificare și supraveghere cerut de personalul care ocupă aceste poziții.

45. SISTEMELE sunt specificate și proiectate în așa fel încât să faciliteze distribuirea îndatoririlor și responsabilităților către personal într-o manieră în care să evite ca o singură persoană să cunoască în totalitate sau să controleze punctele cheie de securitate ale sistemului. Scopul acestei practici este crearea unei necesități pentru existența unei înțelegeri secrete între două sau mai multe persoane în ceea ce privește modificarea sau degradarea intenționată a sistemelor sau a rețelelor.

SECURITATEA FIZICĂ

46. Zonele TI sau terminale/stațiile de lucru [definite în alineatele (29) și (30)], în care sunt procesate informațiile clasificate de nivelul CONFIDENTIEL UE *[Confidențial UE]* sau mai importante, sau unde este posibil accesul la aceste informații, sunt stabilite ca fiind zone de securitate clasa I și clasa a II-a sau echivalentele naționale ale acestor tipuri.

47. Zonele TI sau terminalele/stațiile de lucru retrase, unde securitatea sistemului poate fi modificată, sunt ocupate de mai mult de o singură persoană autorizată/alt funcționar.

CONTROLUL ACCESULUI LA UN SISTEM

48. Toate informațiile și materialele care permit controlul accesului la un sistem sunt protejate prin procedee proporționale cu cea mai înaltă clasificare și cu indicatorul de categorie al informațiilor la care se poate avea acces.

49. Când nu se mai utilizează în acest scop, informațiile și materialele de control al accesului sunt distruse în concordanță cu procedeele descrise în alineatele (61)-(63).

Capitolul V

Măsuri tehnice de securitate

SECURITATEA INFORMAȚIILOR

50. Deținătorul informațiilor este obligat să identifice și să clasifice toate documentele care conțin informații fie sub formă de copii externe, fie stocate în calculator. Fiecare pagină a copiilor externe este marcată, în susul și în josul paginii, având specificată clasificarea respectivă. Copia, fie sub formă de copie externă sau pe mediu de calculator, are aceeași clasificare ca și cea mai importantă clasificare a informațiilor folosite la producerea ei. Modul în care este operat un sistem poate avea un impact asupra clasificării copiilor din cadrul acelui sistem.

51. Organizațiile sau deținătorii de informații sunt obligați să ia în considerare problemele legate de elementele individuale ale informațiilor și interferențele ce pot rezulta din elemente înrudite, și să hotărască dacă o anumită clasificare este potrivită pentru totalitatea informațiilor.

52. Faptul că informația reprezintă un cod temporar, un cod de transmisie sau o formă de reprezentare binară nu asigură securității nici un fel de protecție și, astfel, nu influențează clasificarea informațiilor.

53. Când se transferă informații de la un sistem la altul, aceste informații sunt protejate în timpul transferului și în interiorul sistemului primitor într-un grad echivalent cu gradul de protecție al clasificării și categoriei originale ale respectivelor informații.

54. Toate mediile de calculator pentru stocarea informațiilor sunt operate într-un grad proporțional cu cea mai importantă clasificare a informațiilor stocate sau cu eticheta media, și sunt protejate tot timpul.

55. Mediile refolosibile de calculator pentru stocarea informațiilor, utilizate la înregistrarea informațiilor clasificate ale UE, au cea mai importantă clasificare la care au fost vreodată folosite până în momentul în care acestea au fost declasate sau declasificate iar mediile respective au fost reclasate în mod corespunzător sau au fost distruse sau declasificate de către un SGC sau printr-o procedură la nivel național [a se vedea alineatele (61)-(63)].

CONTROLUL ȘI RĂSPUNDEREA AVUTĂ FAȚĂ DE INFORMAȚII

56. Se țin jurnale manuale sau automate (piste de audit) ca fiind registre cu accesul la informațiile clasificate de nivelul SECRET UE și mai importante. Aceste registre sunt păstrate în conformitate cu aceste regulamente de securitate.

57. Copiile informațiilor clasificate ale UE, deținute în cadrul zonelor TI, pot fi operate ca fiind un singur articol secret și nu au nevoie de înregistrare, cu condiția ca materialele respective să fie identificate, marcate cu clasificarea potrivită și controlate într-o manieră corespunzătoare.

58. În momentul în care apar copii din sistemele ce operează cu informații clasificate ale UE, și aceste copii sunt transmise unei zone terminale/stații de lucru retrase, din cadrul unei zone TI, se elaborează un set de proceduri pentru controlarea acelei zone retrase. În ceea ce privește informațiile SECRET UE și mai importante, aceste proceduri includ instrucțiuni specifice pentru răspunderea avută față de acestea.

OPERAREA ȘI CONTROLUL MEDIILOR DETAȘABILE DE CALCULATOR PENTRU STOCAREA INFORMAȚIILOR

59. Toate mediile detașabile de calculator pentru stocarea informațiilor de nivelul CONFIDENTIEL UE *[Confidențial UE]* și mai importante sunt considerate materiale și li se aplică norme generale. Marcajele de identificare și clasificare trebuie să fie adaptate la aspectul fizic al mediului respectiv pentru ca acesta să fie ușor recunoscut.

60. Utilizatorii își iau responsabilitatea de a asigura faptul că informațiile sunt stocate pe medii cu marcaje corespunzătoare și protecție adecvată. Se elaborează proceduri pentru a asigura faptul că, la toate nivelele informațiilor UE, stocarea informațiilor pe medii de calculator se face conform prezentelor regulamente de securitate.

DECLASIFICAREA ȘI DISTRUGEREA MEDIILOR DE CALCULATOR PENTRU STOCARE

61. Mediile de calculator pentru stocarea informațiilor clasificate ale UE pot fi declasate sau declasificate dacă pentru aceasta se aplică proceduri aprobate la nivel național sau de SGC.

62. Mediile de calculator pentru stocarea informațiilor de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* sau de o categorie specială nu sunt declasificate sau refolosite.

63. Dacă mediul de calculator respectiv nu poate fi declasificat sau refolosit, acesta este distrus prin proceduri aprobate la nivel național sau de SGC.

SECURITATEA COMUNICAȚIILOR

64. Când informațiile clasificate ale UE sunt transmise prin mijloace electromagnetice, se iau măsuri speciale pentru protejarea confidențialității, integrității și disponibilității respectivei transmisii. AAS hotărăște cerințele necesare pentru protejarea transmisiei împotriva detectării sau interceptării. Informațiile transmise prin sistemele de comunicație sunt protejate conform cerințelor de confidențialitate, integritate și disponibilitate.

65. Când se cer metode criptografice pentru asigurarea protecției confidențialității, integrității și disponibilității, aceste metode sau altele asemănătoare trebuie adoptate pentru acest scop de către AAS.

66. În timpul transmisiei, confidențialitatea informațiilor clasificate de nivelul SECRET UE și mai importante este protejată cu ajutorul metodelor criptografice aprobate de către Consiliu la recomandarea Comitetului de securitate a Consiliului. În timpul transmisiei, informațiile de nivelul CONFIDENTIEL UE *[Confidențial UE]* sau RESTREINT UE *[Circulație restrânsă UE]* sunt protejate cu ajutorul metodelor criptografice aprobate fie de secretarul general/Înalt reprezentant la recomandarea Comitetului de securitate a Consiliului, fie de către un stat membru.

67. Se elaborează norme metodologice aplicabile transmiterii informațiilor clasificate ale UE; aceste norme formează niște instrucțiuni de securitate aprobate de Consiliu la recomandarea Comitetului de securitate a Consiliului.

68. În circumstanțe speciale informațiile clasificate de nivelul RESTREINT UE *[Circulație restrânsă UE]*, CONFIDENTIEL UE *[Confidențial UE]* și SECRET UE pot fi transmise sub formă de text, cu condiția ca fiecare transmisie să fie autorizată. Aceste ocazii excepționale pot fi:

(a) înaintea sau în timpul unor crize, conflicte sau situații de război;

(b) când rapiditatea livrării este foarte importantă și nu sunt disponibile mijloace de codificare și se presupune că informațiile transmise nu pot fi exploatate cu scopul de a afecta operațiunile respective.

69. Un SISTEM are capacitatea de a nu acorda acces la informații clasificate ale UE în cadrul oricăror stații de lucru/terminal retrase, când acest lucru este cerut de o deconectare fizică sau de anumite funcții speciale ale software-ului, aprobate de AAS.

SECURITATEA INSTALAȚIILOR ȘI RADIAȚIILOR

70. Instalarea inițială a sistemelor și schimbările aduse acestora se fac în așa fel încât această operațiune să se desfășoare cu ajutorul unor instalatori verificați și autorizați aflați sub supravegherea constantă a personalului calificat tehnic, care, la rândul său, are acces la informațiile clasificate ale UE la un nivel echivalent cu cea mai înaltă clasificare pe care sistemul se presupune că o poate stoca și procesa.

71. Toate echipamentele sunt instalate în conformitate cu politica prezentă a Consiliului în ceea ce privește securitatea.

72. SISTEMELE ce procesează informații clasificate de nivelul CONFIDENTIEL UE *[Confidențial UE]* și mai importante sunt protejate în așa fel încât să nu poată fi amenințate prin emisii compromițătoare, studiul și controlul cărora sunt tratate în alineatul (31).

73. Măsurile de protecție împotriva descărcărilor electromagnetice pentru instalațiile din cadrul SGC și al organismelor descentralizate ale UE sunt revizuite și aprobate de o autoritate în acest sens desemnată de autoritatea securității SGC. În ceea ce privește instalațiile la nivel național, care procesează informații clasificate ale UE, autoritatea aprobatoare este autoritatea națională aprobatoare în problema descărcărilor electromagnetice.

Capitolul VI

Securitatea în timpul procesării informațiilor

PROCEDURI DE OPERARE A SECURITĂȚII

74. SecOP-urile definesc principiile ce urmează a fi adoptate cu privire la chestiunea securității, procedurile operaționale ce urmează a fi aplicate, și responsabilitățile personalului. ITSOA are responsabilitatea pregătirii SecOP-urilor.

PROTEJAREA SOFTWARE/ADMINISTRAREA CONFIGURAȚIILOR

75. Protecția securității programelor de aplicații este determinată pe baza unei evaluări a clasificării securității programului în sine și nu pe baza clasificării informațiilor ce urmează a fi protejate. Versiunile software aflate în uz trebuie verificate regulat pentru a li se asigura integritatea și funcționarea corectă.

76. Versiunile noi sau modificate ale softului nu trebuie puse în folosință pentru procesarea informațiilor clasificate ale UE fără a fi verificate în prealabil de către ITSOA.

VERIFICAREA ÎN VEDEREA DETECTĂRII VIRUȘILOR DE SOFT SAU CALCULATOR

77. Verificarea în vederea detectării virușilor de soft sau calculator are loc periodic conform cerințelor AAS.

78. Toate mediile de calculator pentru stocare ce ajung la SGC sau la organismele descentralizate ale UE sau în statele membre, trebuie verificate în vederea detectării virușilor de soft sau calculator, înaintea introducerii acestora în sisteme.

ÎNTREȚINEREA

79. Contractele sau procedurile pentru întreținerea programată sau la cerere a sistemelor pentru care a fost concepută o SSRS specifică cerințe și aranjamente pentru personalul de întreținere și pentru echipamentele acestora, care intră în zona TI.

80. Aceste cerințe sunt clar specificate în SSRS și procedurile respective sunt clar descrise în SecOP-uri. Procedurile de întreținere prin diagnosticare sunt permise numai în cazuri excepționale, sub control atent, și numai cu aprobarea AAS.

Capitolul VII

Achiziționarea

81. Orice produs de securitate ce urmează a fi folosit la SISTEMUL achiziționat trebuie să fie ori evaluat sau notificat, sau să se afle sub evaluarea sau notificarea unui Organ de evaluare sau notificare pe baza unor criterii recunoscute internațional (cum ar fi Criteriile comune pentru Evaluarea securității tehnologiei informaționale, a se vedea ISO 15 408).

82. În momentul luării deciziei asupra cumpărării sau achiziționării în leasing a echipamentelor trebuie avut în vedere faptul că aceste echipamente, odată folosite pentru procesarea informațiilor clasificate ale UE, nu pot fi plasate în afara unui mediu sigur fără a fi mai întâi declasificate, cu aprobarea AAS, iar obținerea acestei aprobări nu este întotdeauna posibilă.

ACREDITAREA

83. Toate sistemele pentru care s-a elaborat o SSRS, înainte de procesarea informațiilor clasificate ale UE, vor fi acreditate pe baza informațiilor furnizate de AAS, de SSRS, SecOP-uri și alte documentații relevante. Subsistemele și terminalele/stațiile de lucru retrase sunt acreditate ca fiind parte integrantă din sistemele la care sunt conectate. În cazul în care un sistem suportă și Consiliul și alte organizații, SGC și autoritățile de securitate corespunzătoare cad de acord asupra acreditării.

84. Procesul de acreditare se poate desfășura în conformitate cu strategia de acreditare corespunzătoare sistemului și definită de către AAS.

EVALUAREA ȘI NOTIFICAREA

85. În anumite cazuri, înaintea acreditării, funcțiile de securitate hardware, firmware și software ale unui sistem sunt evaluate și notificate ca având capacitatea de a proteja informațiile la nivelul de clasificare corespunzător.

86. Cerințele pentru evaluare și notificare sunt incluse în planificarea sistemelor și sunt clar descrise în SSRS.

87. Procesele de evaluare și notificare se desfășoară în conformitate cu liniile directoare și cu ajutorul unui personal verificat, autorizat și calificat tehnic acționând din partea ITSOA.

88. Echipele respective pot proveni de la o autoritate de notificare și evaluare din statele membre sau de la reprezentanții acestora, de exemplu din partea unui contractant competent și autorizat.

89. Gradul proceselor de evaluare și notificare implicate poate fi mai scăzut (de exemplu operațiunea se poate limita la aspectele de integrare) în cazul în care sistemele respective se bazează pe existența unor produse pentru securitatea calculatoarelor evaluate și notificate la nivel național.

VERIFICAREA DE RUTINĂ A FUNCȚIILOR DE SECURITATE PENTRU ACREDITARE CONTINUĂ

90. ITSOA stabilește proceduri de control de rutină care au menirea de a asigura faptul că toate funcțiile sistemului sunt încă valide.

91. Tipurile de schimbări care ar necesita o nouă acreditare sau aprobarea în prealabil a AAS sunt clar identificate și descrise în SSRS. După fiecare modificare, reparație sau lipsă de funcționare care ar fi putut afecta funcțiile de securitate ale sistemului, ITSOA asigură faptul că se face o verificare pentru a corecta operarea funcțiilor de securitate. Continuarea acreditării depinde de desfășurarea satisfăcătoare a verificărilor.

92. Toate sistemele la care au fost puse în aplicare funcții de securitate sunt inspectate și revizuite periodic de către AAS. În ceea ce privește sistemele ce prelucrează informații clasificate de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* sau cu marcaje suplimentare inspecțiile se desfășoară în fiecare an.

Capitolul VIII

Utilizarea temporară sau ocazională

SECURITATEA MICROCALCULATOARELOR/A CALCULATOARELOR PERSONALE

93. Microcalculatoarele/calculatoarele personale cu discuri fixe (sau alte medii de stocare fixe) care operează fie singure, fie în rețea, și dispozitive de calculator portabile (calculatoare portabile sau „caiete" electronice) cu hard disc fix sunt considerate medii de stocare a informațiilor în aceeași măsură ca și dischetele sau alte medii de stocare detașabile.

94. Acestui tip de echipament i se asigură protecție în ceea ce privește accesul, procesarea, stocarea și transmiterea, la un nivel corespunzător celei mai înalte clasificări a informațiilor procesate sau stocate vreodată (până în momentul declasării sau declasificării executate conform procedurilor aprobate).

UTILIZAREA ECHIPAMENTELOR TI PERSONALE LA MUNCA DE BIROU DIN CADRUL CONSILIULUI

95. În ceea ce privește procesarea informațiilor clasificate ale UE, este interzisă utilizarea de echipamente de tehnologie a informațiilor personale (de exemplu calculatoare și dispozitive electronice protabile) cu capacități de stocare.

96. Hardware, software sau alte medii personale nu pot fi aduse în incinta zonelor din clasa I și clasa II, unde informațiile clasificate ale UE se procesează fără aprobarea șefului Oficiului de Securitate al SGC sau al serviciului unui stat membru ori al organismului descentralizat ale UE în cauză.

UTILIZAREA PENTRU LUCRĂRILE DE SERVICIU DIN CADRUL CONSILIULUI A ECHIPAMENTELOR TI FURNIZATE LA NIVEL NAȚIONAL SAU AFLATE ÎN PROPRIETATEA UNOR CONTRACTANȚI

97. Utilizarea software-ului și echipamentelor TI aflate în proprietatea unor contractanți în cadrul diferitelor organizații pentru a sprijini munca Consiliului este permisă de către șeful Oficiul de Securitatel al SGC, de către un departament a vreunui stat membru sau de către organismul descentralizat al UE. Este permisă și folosirea echipamentelor TI furnizate la nivel național; aceste echipamente sunt utilizate de către angajații SGC sau ai agențiilor descentralizate UE; în acest caz, echipamentele respective sunt puse sub controlul inventarului SGC corespunzător. În oricare dintre cazuri, dacă echipamentele TI respective urmează a fi folosite pentru procesarea informațiilor clasificate ale UE, trebuie consultată AAS corespunzătoare pentru ca elementele INFOSEC care se aplică utilizării respectivelor echipamente să fie luate în considerare și puse în aplicare.

SECȚIUNEA XII

ELIBERAREA INFORMAȚIILOR CLASIFICATE UE CĂTRE STATELE TERȚE ȘI ORGANIZAȚIILE INTERNAȚIONALE

PRINCIPII CARE REGLEMENTEAZĂ ELIBERAREA INFORMAȚIILOR CLASIFICATE UE

1. Eliberarea informațiilor clasificate ale UE către statele terțe și organizațiile internaționale se face:

   — pe baza naturii și conținutului acestor informații;

   — în funcție de nevoia de cunoaștere a destinatarilor;

   — pe măsura avantajelor UE.

   Se cere aprobarea statului membru deținător al acestor informații pentru eliberarea acestora.

2. Aceste decizii se iau pentru fiecare caz în parte, luând în considerare:

   — gradul de cooperare cu statele terțe și organizațiile internaționale interesate;

   — încrederea acordată acestora, care rezultă din nivelul de securitate ce urmează a fi aplicat acestor informații cedate statelor și organizațiilor respective și din corespondența existentă între normele de securitate aplicabile în cadrul acestora și cele aplicabile în interiorul UE; Comitetul de securitate a Consiliului va da Consiliului avizul său în legătură cu aceste chestiuni.

3. Acceptarea informațiilor clasificate ale UE de către statele terțe sau organizațiile internaționale implică asigurarea faptului că respectivele informații sunt folosite numai în scopul ce motivează eliberarea sau schimbul lor și că li se acordă protecția cerută de Consiliu.

NIVELURI

4. Odată ce Consiliul a decis faptul că anumite informații clasificate pot fi eliberate sau schimbate cu un anume stat membru sau organizație internațională, se va decide și asupra nivelului de cooperare posibil. Acest lucru depinde în special de politica și regulamentele de securitate aplicate de acel stat sau organizație.

5. Există 3 niveluri de cooperare:

   Nivelul 1

   Cooperarea cu statele terțe sau cu organizațiile internaționale ale căror regulamente și politică a securității se apropie foarte mult de cele ale UE.

   Nivelul 2

   Cooperarea cu statele terțe sau cu organizațiile internaționale ale căror regulamente și politică a securității sunt diferite de cele ale UE.

   Nivelul 3

   Cooperarea ocazională cu statele terțe sau cu organizațiile internaționale ale căror regulamente și politică a securității nu pot fi evaluate.

6. Fiecare nivel de cooperare stabilește regulamentele de securitate elaborate pentru fiecare caz în parte în lumina avizului tehnic al Comitetului de securitate a Consiliului, și anume în aceea că beneficiarilor li se cere protejarea informațiilor clasificate ce le sunt eliberate. Aceste proceduri și regulamente de securitate sunt descrise în detaliu în anexele 4, 5 și 6.

ACORDURILE

7. Odată ce Consiliul decide faptul că există o necesitate permanentă sau de lungă durată a schimbului de informații clasificate între UE și statele terțe sau organizațiile internaționale, acesta întocmește acorduri asupra procedurilor de securitate în ceea ce privește schimbul de informații clasificate, definind scopul cooperării și normele reciproce pentru protecția informațiilor schimbate.

8. În cazul nivelului 3 de cooperare ocazională, care prin definiție este limitat ca scop și timp, un simplu memorandum de acord, care să definească natura informațiilor ce urmează a fi schimbate și obligațiile reciproce referitoare la respectivele informații, poate lua locul acordului asupra procedurilor în ceea ce privește schimbul de informații clasificate cu condiția ca respectivele informații să aibă clasificarea RESTREINT UE *[Circulație restrânsă UE]* sau mai puțin importantă.

9. Comitetul de securitate aprobă primele versiuni ale acordului și memorandumului înainte ca acestea să fie prezentate Consiliului pentru aprobarea finală.

10. ANS-urile oferă secretarului general/Înalt reprezentant asistență pentru a asigura faptul că informațiile eliberate sunt utilizate și protejate în conformitate cu prevederile acordurilor asupra procedurilor de securitate și memorandumurilor de acord.

Anexa 1

Lista autorităților naționale de securitate

BELGIA

Ministère des Affaires Étrangères, du Commerce Extérieur et de la Coopération au Développement
Direction de la sécurité – A 01
Rue des Petits Carmes, 15
B-1000 Bruxelles
Telefon: 32-2-501 85 14
Fax: 32-2-501 80 58
Telex: 21376
Adresă telegraf: Direction de la sécurité A01 – MINAFET

DANEMARCA

Politiets Efterretningstjeneste
Borups Alle 266
DK-2400 Copenhagen NV
Telefon: 45-33 14 88 88
Fax: 45-38 19 07 05

Forsvarsministeriet
Forsvarets Efterretningstjeneste
Kastellet 30
DK-2100 Copenhagen Ø
Telefon: 45-33 32 55 66
Fax: 45-33 93 13 20

GERMANIA

Bundesministerium des Innern
Referat IS 4
Alt-Moabit 101D
D-10559 Berlin
Telefon: 49-30-39 81 15 28
Fax: 49-30-39 81 16 10

GRECIA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Υπηρεσία Στρατιωτικών Πληροφοριών (ΥΣΠ – Β' Κλάδος)
Γραφείο Ασφάλειας
ΣΤΓ 1020– Χολαργός (Αθήνα)
Ελλαδα
Τηλέφωνα: 30–1– 655 22 03 (ώρες γραφείου)
30–1– 655 22 05 (εικοσιτετράωρο)
Φαξ: 30–1– 642 69 40

Hellenic National Defence
General Staff (HNDGS)
Intelligence Branch/Security
(INT.BR./SEC)
STG 1020, Holargos – Atena
Grecia
Telefon: 30-1-655 22 03 (program birou)
30-1-655 22 05 (non-stop)
Fax: 30-1-642 69 40

SPANIA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera Nacional Radial VI, km 8 500
E-28023 Madrid
Telefon: 34-91-372 57 07
Fax: 34-91-372 58 08
E-mail: nsa-sp@areatec.com

FRANȚA

Secrétariat général de la Défense Nationale
Service de Sécurité de Défense (SGDN/SSD)
51 Boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Telefon: 33-0-144 18 81 80
Fax: 33-0-144 18 82 00
Telex: SEGEDEFNAT 200019
Adresă telegraf: SEGEDEFNAT PARIS

IRLANDA

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
Dublin 2
Telefon: 353-1-478 08 22
Fax: 353-1-478 14 84

ITALIA

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Ufficio Centrale per la Sicurezza
Via della Pineta Sacchetti, 216
I-00168 Roma
Telefon: 39-06-627 47 75
Fax: 39-06-614 33 97
Telex: 623876 AQUILA 1
Adresă telegraf: ess: PCM-ANS-UCSI-ROMA

LUXEMBURG

Autorité Nationale de Sécurité
Ministère d'État
Boîte Postale 2379
L-1023 Luxemburg
Telefon: 352-478 22 10 central
352-478 22 35 direct
Fax: 352-478 22 43
352-478 22 71
Telex: 3481 SERET LU
Adresă telegraf: MIN D'ETAT – ANS

ȚĂRILE DE JOS

Ministerie van Binnenlandse Zaken
Postbus 20010
NL-2500 EA Den Haag
Telefon: 31-70-320 44 00
Fax: 31-70-320 07 33
Telex: 32166 SYTH NL

Minsterie van Defensie
Militaire Inlichtingendiest (MID)
Postbus 20701
NL-2500 ES Den Haag
Telefon: 31-70-318 70 60
Fax: 31-70-318 79 51

AUSTRIA

Bundesministerium für auswärtige Angelegenheiten
Abteilung I.9
Ballhausplatz 2
A-1014 Wien
Telefon: 43-1-531 15 34 64
Fax: 43-1-531 8 52 19

PORTUGALIA

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1449-004 Lisboa
Telefon: 351-21-301 55 10
351-21-301 00 01, interior 20 45 37
Fax: 351-21-302 03 50

FINLANDA

Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Ulkoasiainministeriö/Utrikesministeriet
Laivastokatu/Maringatan 22
PL/PB 176
FIN-00161 Helsinki/Helsingfors
Telefon: 358-9-13 41 53 38
Fax: 358-9-13 41 53 03

SUEDIA

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Telefon: 46-8-405 54 44
Fax:. 46-8-723 11 76

REGATUL UNIT

The Secretary (for DIR/5)
PO Box 5656
London EC1A 1AH
Telefon: 44-20-72 70 87 51
Fax: 44-20-76 30 14 28
Adresă telegraf: UK Delegation to Security Policy Dept FCO, marked (in Box 5656 for DIR/5)

Anexa 2

Comparație a clasificărilor la nivel național

Clasificare UE	Très secret UE/EU Top Secret	Secret UE	Confidentiel UE	Restreint UE
Clasificare NATO (1)				
Clasificare UEO	Focal Top Secret	WEU Secret	WEU Confidential	WEU Restricted
Belgia	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Danemarca	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Germania	Streng Geheim	Geheim	VS (2) - Vertraulich	VS - Nur für den Dienstgebrauch
Grecia	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Spania	Secreto	Reservado	Confidencial	Difusion Limitada
Franța	Très Secret Défense (3)	Secret Défense	Confidentiel Défense	Diffusion restreinte
Irlanda	Top Secret	Secret	Confidential	Restricted
Italia	Segretissimo	Segreto	Riservatissimo	Riservato
Luxemburg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Țările de Jos	STG Zeer Geheim	STG Geheim	STG Confidentieel	
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Portugalia	Muito Secreto	Secreto	Confidencial	Reservado
Finlanda	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Suedia	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Regatul Unit	Top Secret	Secret	Confidential	Restricted

(1) NATO: corespondența cu nivelele de clasificare NATO se stabilește odată cu negocierea Acordului de Securitate dintre UE și NATO.

(2) Germania: VS – Verschlussache.

(3) Franța: clasificarea „Très Secret Défense”, care acoperă chestiuni de prioritate ale guvernului, poate fi schimbată numai cu permisiunea primului-ministru.

Anexa 3

Ghid practic de clasificare

Acest ghid are rol orientativ și nu poate schimba dispozițiile prevăzute în secțiunile II și III.

Clasificare	Când	Cine	Marcaje	Reducerea nivelului de clasificare/Declasificarea/Distrugerea	
				Cine	Când
TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*: Această clasificare se aplică numai informațiilor și materialelor a căror divulgare poate aduce prejudicii grave intereselor principale ale Uniunii Europene sau unuia sau mai multor state membre din cadrul acesteia [SII(1)].	Compromiterea bunurilor marcate TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* poate: — amenința în mod direct stabilitatea internă a UE sau a unuia din statele membre ale acesteia, precum și a unor țări prietene — aduce daune excepțional de grave relațiilor dintre guverne — conduce direct la pierderi de vieți — aduce daune excepțional de grave eficienței sau securității operaționale ale statelor membre sau ale altor forțe de contribuție, sau continuării funcționării eficace a serviciilor de securitate — aduce daune pe termen lung economiilor UE sau a statelor membre.	Statele membre: Persoane autorizate (deținători) [SIII(4)]; SGC: Persoane autorizate (deținători) [SIII(4)] SG/ÎR și DSG. Deținătorii specifică o dată la care documentele respective pot fi declasificate sau declasate. În caz contrar, ei păstrează documentele și le revizuiesc o dată la 5 ani pentru a se asigura că este necesară clasificarea originală [SIII(10)].	Clasificarea TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* se aplică documentelor TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* și, unde este aplicabil, se introduce marcajul de apărare ESDP *[PESA]*, prin mijloace manuale sau mecanice [SII(8)]. Clasificarea UE apare în susul și în josul fiecărei pagini, pe centru, iar fiecare pagină este numerotată. Fiecare document are un număr de referință și o dată; acest număr de referință apare pe fiecare pagină. Dacă urmează a se distribui în copii, fiecare dintre acestea va purta un număr, înscris pe fiecare pagină, împreună cu numărul total de pagini. Toate anexele și inserările sunt specificate pe prima pagină [SVII(1)].	Numai deținătorul poate declasa sau declasifica documente, sau GS/ÎR sau DSG, care va informa despre aceste schimbări pe destinatarii cărora le sunt trimise sau copiate documente [SVIII(9)]. Documentele TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* sunt distruse de Registrul Central sau de subregistrul responsabil pentru ele. Fiecare document distrus este specificat într-un certificat de distrugere, semnat de controlorul corespunzător nivelului TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* și de către agentul martor la distrugere, care este autorizat TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*. Această procedură se înscrie în logbook. Registrul păstrează certificatele de distrugere, împreună cu fișa de distribuție, pentru o perioadă de 10 ani [SVII(31)].	Copiile în plus sau documentele inutile trebuie distruse [SVII(31)]. Documentele TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*, inclusiv deșeurile rezultate de pe urma procesării acestor documente, cum ar fi copii stricate, ciorne, note bătute la mașină se vor distruge, sub supravegherea unui responsabil care posedă verificarea corespunzătoare nivelului TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* prin proceduri de ardere, fărâmițare sau altele, reducându-le la o formă imposibil de recunoscut sau reconstituit [SVII(31)].

Clasificare	Când	Cine	Marcaje	Reducerea nivelului de clasificare/Declasificarea/Distrugerea	
				Cine	Când
SECRET UE: Această clasificare se aplică acelor informații și materiale a căror divulgare neautorizată poate aduce daune serioase intereselor principale ale Uniunii Europene sau unuia sau mai multor state membre din cadrul acesteia [SII(2)].	Compromiterea bunurilor marcate SECRET UE poate: — crea tensiuni la nivel internațional — aduce daune serioase relațiilor dintre guverne — constitui o amenințare pentru viață sau prejudicia serios ordinea publică sau securitatea și libertatea individuală — aduce daune serioase eficienței sau securității operaționale ale statelor membre sau ale altor forțe de contribuție, sau continuării funcționării eficace a serviciilor de securitate — aduce daune materiale substanțiale intereselor financiare, economice, comerciale sau monetare ale statelor membre sau ale UE.	Statele membre: Persoane autorizate (deținători) [SIII(2)]; Organismele descentralizate ale UE sau SGC: Persoane autorizate (deținători) [SIII(2)], directori generali, SG/ÎR sau DSG. Deținătorii specifică o dată la care documentele respective pot fi declasificate sau declasate. În caz contrar, ei păstrează documentele și le revizuiesc o dată la 5 ani pentru a se asigura că este necesară clasificarea originală [SVII(1)].	Clasificarea SECRET UE se aplică documentelor SECRET UE și, unde este aplicabil, se introduce marcajul de apărare ESDP *[PESA]*, prin mijloace manuale sau mecanice [SIII(8)]. Clasificarea UE apare în susul și în josul fiecărei pagini, pe centru, iar fiecare pagină este numerotată. Fiecare document are un număr de referință și o dată; acest număr de referință apare pe fiecare pagină. Dacă urmează a se distribui în mai multe exemplare, fiecare dintre acestea va purta un număr, înscris pe fiecare pagină, împreună cu numărul total de pagini. Toate anexele sunt specificate pe prima pagină [SVII(1)].	Numai autoritatea care l-a emis, SG/ÎR sau SGA au dreptul de a reduce nivelul de clasificare sau de a declasifica documente; aceștia informează destinatarii cărora le-a fost transmis originalul sau o copie a documentului cu privire la schimbările survenite [SIII(9)]. Documentele SECRET UE sunt distruse de către registrul responsabil cu acestea, sub supravegherea unei persoane autorizate. Documentele SECRET UE distruse sunt înscrise în certificate de distrugere semnate; acestea urmează a fi păstrate de către Registru, împreună cu formularele de distrugere, pentru o perioadă de cel puțin 3 ani [SVII(32).	Exemplarele excedentare sau documentele inutile trebuie distruse [SVII(31)]. Documentele SECRET UE, inclusiv deșeurile rezultate în urma procesării acestor documente, cum ar fi copii stricate, ciorne, note bătute la mașină sunt distruse prin proceduri de ardere, fărâmițare sau altele, reducându-le la o formă imposibil de recunoscut sau reconstituit [SVII(31), (32)].

Clasificare	Când	Cine	Marcaje	Reducerea nivelului de clasificare/Declasificarea/Distrugerea	
				Cine	Când
CONFIDENTIEL UE *[Confidențial UE]*: Această clasificare se aplică acelor informații și materiale a căror divulgare neautorizată poate dăuna intereselor principale ale UE și unuia sau mai multor state membre [SII(3)].	Compromiterea bunurilor marcate CONFIDENTIEL UE *[Confidențial UE]* poate: — aduce daune materiale relațiilor diplomatice, și anume proteste formale sau alte sancțiuni — prejudicia securitatea și libertatea personală — aduce daune eficienței operaționale și securității statelor membre sau altor forțe de contribuție, sau eficacității serviciilor de securitate — submina în mod substanțial viabilitatea organizațiilor principale — împiedica desfășurarea unor investigații sau facilita comiterea unor crime serioase — acționa în prejudiciul intereselor financiare, monetare, economice și comerciale ale statelor membre sau UE — împiedica dezvoltarea și desfășurarea politicilor UE — opri sau întrerupe activitățile importante ale UE.	Statele membre: Persoane autorizate (deținători) [SIII(2)]; SGC sau organismele descentralizate ale UE: Persoane autorizate (deținători) [SIII(2)], directori generali, SG/ÎR și DSG. Deținătorii specifică o dată sau perioadă când informațiile pot fi declasate sau declasificate. În caz contrar aceștia păstrează documentele pentru a le revizui o dată la 5 ani cu scopul de a asigura că clasificarea originală este încă necesară [SIII(10)].	Clasificarea CONFIDENTIEL UE *[Confidențial UE]* se aplică documentelor CONFIDENTIEL UE *[Confidențial UE]* și, unde este aplicabil, se introduce și un marcaj ESDP *[PESA]* prin mijloace mecanice sau manuale, prin gravare sau ștampilare [SII(8)]. Clasificarea UE apare în partea centrală de sus și jos a paginii, iar fiecare pagină este numerotată. Fiecare document poartă un număr de referință și o dată. Toate anexele și inserările sunt specificate pe prima pagină [SVII(1)].	Numai deținătorul, SG/ÎR sau DSG au dreptul de a declasifica sau declasa documente; aceștia informează destinatarii cărora le sunt trimise copii ale documentului cu privire la schimbările survenite [SVII(31)]. Documentele CONFIDENTIEL UE *[Confidențial UE]* sunt distruse de registrul responsabil pentru acestea, sub supravegherea unei persoane autorizate. Distrugerea este înregistrată conform regulamentelor naționale și, în cazul SGC sau al organismelor descentralizate ale UE, conform instrucțiunilor SG/ÎR sau DSG [SVII(33)].	Copiile în plus sau documentele inutile trebuie distruse [SVII(31)]. Documentele CONFIDENTIEL UE *[Confidențial UE]*, inclusiv deșeurile rezultate din pregătirea acestora, cum ar fi copii stricate, ciorne, note bătute la mașină, sunt distruse prin ardere sau fărâmițare, reducându-le la o formă imposibil de recunoscut sau reconstituit [SVII(31), (33)].

Clasificare	Când	Cine	Marcaje	Reducerea nivelului de clasificare/Declasificarea/Distrugerea	
				Cine	Când
RESTREINT UE *[Circulație restrânsă UE]*: Această clasificare se aplică acelor informații și materiale a căror divulgare neautorizată poate fi în dezavantajul intereselor principale ale UE și unuia sau mai multor state membre [SII(4)].	Compromiterea unor bunuri marcate RESTREINT UE *[Circulație restrânsă UE]* poate: — afecta relațiile diplomatice — cauza stress indivizilor — îngreuna menținerea eficacității sau securității statelor membre sau a altor forțe de cotribuție — cauza pierderi financiare sau facilita câștiguri sau avantaje necuvenite pentru indivizi sau companii — încălca prevederile menite să mențină încrederea în informațiile furnizate de state terțe — încălca restricțiile cu privire la divulgarea informațiilor — prejudicia desfășurarea unor investigații sau facilita comiterea unor crime — crea un dezavantaj UE sau statelor membre în negocierile politice sau comerciale cu alte state — împiedica dezvoltarea și desfășurarea politicilor UE — submina administrarea corectă a UE și a operațiunilor acesteia.	Statele membre: Persoane autorizate (deținători) [SIII(2)] SGC sau organismele descentralizate ale UE: Persoane autorizate (deținători) [SIII(2)], directori generali, SG/ÎR și DSG. Deținătorii specifică o dată sau perioadă când informațiile pot fi declasate sau declasificate. În caz contrar aceștia păstrează documentele pentru a le revizui o dată la 5 ani cu scopul de a asigura că clasificarea originală este încă necesară [SIII(10)].	Clasificarea RESTREINT UE *[Circulație restrânsă UE]* se aplică documentelor RESTREINT UE *[Circulație restrânsă UE]* și, unde este aplicabil, se introduce și un marcaj ESDP *[PESA]* prin mijloace mecanice sau manuale, prin gravare sau ștampilare [SII(8)]. Clasificarea UE apare în partea centrală de sus și jos a paginii, iar fiecare pagină este numerotată. Fiecare document poartă un număr de referință și o dată [SVII(1)].	Numai deținătorul, SG/ÎR sau DSG au dreptul de a declasifica sau declasa documente; aceștia informează destinatarii cărora le sunt trimise copii ale documentului cu privire la schimbările survenite [SIII(9)]. Documentele RESTREINT UE *[Circulație restrânsă UE]* sunt distruse de registrul responsabil pentru acestea, în conformitate cu regulamentele naționale și, în cazul SGC sau al organismelor descentralizate ale UE, conform instrucțiunilor SG/ÎR sau DSG [SVII(34)].	Copiile în plus și documentele inutile trebuie distruse [SVII(31)].

Anexa 4

Linii directoare pentru eliberarea informațiilor clasificate ale UE către state terțe și organizații internaționale

Nivelul 1 de cooperare

PROCEDURI

1. Consiliul are autoritatea de a elibera informații clasificate ale UE către țările nesemnatare a Tratatului asupra Uniunii Europene sau către alte organizații internaționale a căror politică în privința securității este asemănătoare cu cea a UE.

2. Consiliul poate delega decizia de a elibera informații clasificate. Respectiva delegație specifică natura informațiilor ce urmează să fie eliberate și nivelul de clasificare al acestora, care, în mod normal, nu este mai important decât CONFIDENTIEL UE *[Confidențial UE]*.

3. Făcând subiectul unui acord de securitate, cererile privind eliberarea de informații clasificate ale UE sunt adresate secretarului general/Înalt reprezentant de către organele statelor sau organizațiilor internaționale interesate, care vor preciza scopul pentru care sunt necesare aceste informații și natura informațiilor ce urmează a fi eliberate.

   Cererile pot fi întocmite și de un stat membru sau de un organism descentralizat al UE. Acestea vor cuprinde precizări despre scopul și beneficiul avut de UE din eliberarea acestor informații, specificând natura și clasificarea informațiilor ce urmează a fi eliberate.

4. Cererea este luată în considerare de SGC, care:

   — necesită avizele statelor membre sau, după caz, ale organismelor descentralizate ale UE care dețin informațiile ce urmează a fi eliberate;

   — stabilește contactele necesare cu organele de securitate ale țărilor sau organizațiilor internaționale beneficiare pentru a verifica dacă regulamentele acestora privind politica de securitate garantează protejarea informațiilor eliberate conform prezentelor regulamente de securitate;

   — necesită avizele tehnice ale Autorităților naționale de securitate ale statelor membre în ceea ce privește gradul de încredere acordat statelor sau organizațiilor internaționale beneficiare.

5. SGC înaintează Consiliului cererea și recomandarea Oficiului de Securitatel; Consiliul urmează să ia decizia finală.

REGULAMENTELE DE SECURITATE CE URMEAZĂ A FI APLICATE DE CĂTRE BENEFICIARI

6. Secretarul general/Înalt reprezentant anunță statele și organizațiile internaționale beneficiare în legătură cu decizia Consiliului de a autoriza eliberarea informațiilor clasificate ale UE, prezentând toate copiile necesare ale acestor regulamente de securitate. Dacă cererea a fost înaintată de un stat membru, acest stat anunță beneficiarul în legătură cu autorizarea eliberării.

   Decizia de a elibera informații intră în vigoare numai după ce beneficiarii prezintă în scris o asigurare asupra faptului că:

   — vor folosi informațiile respective numai în scopurile specificate;

   — vor proteja informațiile în conformitate cu prezentele regulamente de securitate și, în special, cu dispozițiile prevăzute mai jos.

7. *Personalul*

   (a) Numărul funcționarilor cu acces la informațiile clasificate ale UE este strict limitat, fiind stabilit pe baza principiului „ce trebuie cunoscut” și este acordat numai persoanelor ale căror sarcini de serviciu necesită accesul respectiv.

(b) Toți funcționarii sau cetățenii ce urmează a avea acces la informații de nivelul CONFIDENTIEL UE *[Confidențial UE]* și mai importante au fie un certificat de securitate pentru nivelul corespunzător, fie autorizația de securitate necesară, fiecare dintre acestea fiind eliberate de către guvernul propriului stat.

8. *Transmiterea documentelor*

(a) Procedurile folosite pentru transmiterea documentelor sunt decise prin acord pe baza prevederilor secțiunii VII din Regulamentele de securitate ale Consiliului. Acestea specifică registrele către care sunt înaintate informațiile clasificate ale UE.

(b) Dacă informațiile clasificate a căror eliberare este autorizată de către Consiliu include informații de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]*, statul sau organizația internațională beneficiară elaborează un Registru central și, dacă este necesar, subregistre UE. Aceste registre funcționează după prevederile secțiunii VIII din prezentele regulamente de securitate.

9. *Înregistrarea*

După ce un registru primește documente clasificate de nivelul CONFIDENTIEL UE *[Confidențial UE]* sau mai importante, acesta plasează documentul într-un registru special ținut de către organizație, prevăzut cu coloane pentru datele primite, pentru datele particulare ale documentului (dată, număr de referință și numărul copiei), clasificarea acestuia, titlul, numele și poziția primitorului, data de înapoiere și data la care documentul este returnat deținătorului UE sau distrus.

10. *Distrugerea*

(a) Documentele clasificate ale UE sunt distruse în conformitate cu instrucțiunile prevăzute în secțiunea VI a prezentelor regulamente de securitate. Copiile certificatelor de distrugere pentru documentele de nivelul SECRET UE și TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* sunt trimise registrului UE care a înaintat documentele respective.

(b) Documentele clasificate ale UE sunt incluse în planurile de distrugere în caz de urgență pentru propriile documente clasificate ale organelor beneficiare.

11. *Protejarea documentelor*

Se iau măsuri pentru a preveni accesul persoanelor neautorizate la informațiile clasificate ale UE.

12. *Copii, extrase și traduceri*

Nu se pot scoate extrase, face traduceri sau copii dintr-un document secret de nivelul CONFIDENTIEL UE *[Confidențial UE]* sau SECRET UE fără autorizația șefului securității organizației interesate; acesta înregistrează și verifică copiile, traducerile și extrasele respective și le ștampilează, dacă este necesar.

Reproducerea sau traducerea unui document de nivelul TRÈS SECRET UE/EU TOP SECRET *[Strict secret UE]* poate avea autorizarea numai a deținătorului, care specifică numărul de copii autorizat; dacă deținătorul nu își dă acordul, cererea este îndreptată către Oficiul de Securitatel al SGC.

13. *Încălcarea securității*

Dacă se suspectează sau a avut loc încălcarea securității, se iau următoarele acțiuni, acestea fiind menite să ducă la încheierea unui acord de securitate:

(a) se desfășoară o investigație pentru a stabili circumstanțele încălcării securității;

(b) este anunțat Oficiul de Securitatel al SGC, Autoritatea securității naționale și autoritatea deținătoare sau se specifică faptul că aceasta din urmă nu a fost anunțată, în cazul în care acest lucru nu a avut loc;

(c) se ia acțiune pentru a minimaliza efectele încălcării securității;

(d) se reconsideră și se pun în aplicare măsuri pentru a preveni repetarea acestei încălcări;

(e) se pun în aplicare măsurile recomandate de Oficiul de Securitatel al SGC pentru a preveni repetarea acestei încălcări.

14. *Inspecțiile*

Oficiul de Securitatel al SGC are permisiunea, prin acord cu statele și organizațiile interesate, de a desfășura o evaluare a eficacității măsurilor pentru protejarea informațiilor clasificate eliberate.

15. *Raportarea*

Făcând subiectul încheierii unui acord de securitate, statul sau organizațiile, pe parcursul întregii perioade de deținere a informațiilor clasificate, trebuie să înainteze un raport anual, până la o dată stabilită pentru acordarea autorizației de eliberare a informațiilor, care să confirme faptul că sunt urmate prezentele regulamente de securitate.

Anexa 5

Linii directoare pentru eliberarea informațiilor clasificate UE către state terțe sau organizații internaționale

Cooperare de nivelul 2

PROCEDURI

1. Autoritatea de a elibera informații clasificate ale UE către statele terțe sau organizațiile internaționale a căror politică de securitate și regulamente sunt marcate diferit de cele ale UE cade în răspunderea Consiliului. În principiu, este restrânsă la informațiile clasificate până la și incluzând SECRET UE; exclude informațiile naționale rezervate specific statelor membre și categoriilor de informații clasificate protejate de însemnări speciale.

2. Consiliul poate delega decizia: pentru delegare, în cadrul constrângerilor stabilite în primul paragraf, va exprima natura informațiilor care pot fi eliberate și nivelul lor de clasificare, care va fi nu mai mare de RESTREINT UE *[Circulație restrânsă UE]*.

3. Sub rezerva concluziilor unui acord de siguranță, cererile pentru eliberarea de informații clasificate UE vor fi făcute către secretarul general/Înalt reprezentant de către serviciile de securitate ale statelor sau organizațiilor internaționale implicate, care vor exprima scopurile pentru care această eliberare este intenționată și natura și clasificarea informațiilor care vor fi eliberate.

   Pot fi făcute de asemenea cereri de către un stat membru sau un organism descentralizat al UE care privesc eliberarea de informații clasificate UE așa cum se dorește; ei vor exprima obiectele și beneficiul UE a unei asemenea eliberări, specificând natura și clasificarea informațiilor care vor fi eliberate.

4. Cererea este prelucrată de către SGC, care:

   — solicită avizul statelor membre sau, după caz, al organismului descentralizat al UE de la care provin informațiile care trebuie comunicate;

   — stabilește contactele preliminare cu serviciile de securitate ale statelor beneficiare sau ale organizațiilor pentru a se informa cu privire la politica și reglementările lor în materie de securitate și, în special, pentru a întocmi un tabel de echivalență între nivelele de clasificare în vigoare în UE și în statul sau în cadrul organizației în cauză;

   — organizează o reuniune a Comitetului de Securitate al Consiliului sau solicită, după caz conform procedurii acordului tacit, punctul de vedere al autorităților naționale de securitate ale statelor membre în vederea obținerii avizului tehnic al Comitetului de securitate.

5. Avizul Comitetului de Securitate al Consiliului constă în:

   — încrederea plasată în statele beneficiare sau organizațiile internaționale cu privire la aprecierea riscurilor securității create de UE sau statele sale membre;

   — aprecierea abilității beneficiarilor de a proteja informațiile clasificate eliberate de UE;

   — propuneri pentru procedurile practice de manevrare a informațiilor clasificate UE (de exemplu prevederea versiunilor epurate ale unui text) și documentelor transmise (reținerea sau ștergerea titlurilor de clasificare UE, marcări speciale etc.);

   — reducerea sau declasificarea de către autoritatea de origine înainte ca informațiile să fie eliberate țărilor beneficiare sau organizațiilor internaționale ([1]).

([1]) Aceasta face necesară cererea autorității de origine a procedurii definite la paragraful 9, secțiunea III, în cazul tuturor copiilor în circulație pe teritoriul UE.

6. Secretarul general/Înalt reprezentant înaintează Consiliului, în scopul luării unei decizii, cererea și avizul tehnic al Comitetului de Securitate al Consiliului obținut de Oficiul de Securitate al SGC.

REGLEMENTĂRI DE SECURITATE CARE VOR FI APLICATE DE BENEFICIARI

7. Decizia Consiliului pentru a autoriza eliberarea de informații clasificate UE va fi adusă în atenția țărilor beneficiare sau organizațiilor internaționale de către secretarul general/Înalt reprezentant, împreună cu un tabel comparând clasificările aplicabile în UE și statele sau organizațiile implicate. Dacă cererea a fost făcută de către un stat membru, acest stat va notifica beneficiarul de eliberarea autorizată.

Decizia care va fi eliberată va intra în vigoare doar atunci când beneficiarii dau o asigurare scrisă că vor:

— folosi informațiile numai în scopurile stabilite;

— proteja informațiile în conformitate cu regulamentele stabilite de Consiliu.

8. Următoarele norme de protecție vor fi stabilite doar dacă Consiliul, obținând avizul tehnic al Comisiei Consiliului de Securitate, nu decide asupra unei proceduri de manevrare a documentelor clasificate ale UE (ștergând menționarea clasificării UE, marcării specifice etc.).

Normele vor fi adaptate în acest caz.

9. *Personalul*

(a) Numărul autorităților care au acces la informațiile clasificate trebuie să fie strict limitat, bazat pe principiul necesității de a ști, la acele persoane ale căror îndatoriri necesită acest acces.

(b) Toate autoritățile sau cetățenii autorizați să aibă acces la informațiile clasificate eliberate de UE au o autorizare de securitate națională de acces, în cazul informațiilor naționale clasificate, la un nivel asemănător celui al UE, definit în tabelul comparativ.

(c) Aceste clarificări de securitate națională sau autorizări vor fi înaintate secretarului general/Înalt reprezentant pentru informare.

10. *Transmiterea documentelor*

(a) Procedurile practice pentru transmiterea documentelor sunt stabilite de comun acord între Oficiul de Securitate al SGC și serviciile de securitate ale statelor primitoare sau ale organizațiilor internaționale destinatare, pe baza normelor prevăzute de secțiunea VII a prezentului regulament. Ele vor menționa în special adresa exactă la care documentele trebuie expediate, precum și serviciile de curierat sau poștale folosite pentru transmiterea informațiilor clasificate UE.

(b) Documentele clasificate CONFIDENTIEL UE *[Confidențial UE]* și mai sus vor fi emise sub dublă acoperire. Plicul din interior va fi însemnat „UE" împreună cu clasificarea de securitate. Un formular de primire va fi inclus pentru fiecare document clasificat. Acest formular de primire, care nu va fi el însuși clasificat, va cita doar detaliile documentului (referința sa, data, numărul copiei) și limba sa, nu titlul.

(c) Plicul interior va fi apoi plasat în plicul exterior, care va purta un număr de înscriere pentru scopuri de primire. Plicul exterior nu va purta o clasificare de securitate.

(d) O chitanță arătând numărul de înscriere va fi întotdeauna dată curierilor.

11. *Înregistrarea la sosire*

ANS-ul statului adresant sau echivalentul său în stat care primește în numele guvernului său informațiile clasificate înaintate de UE sau biroul de securitate al organizației internaționale primitoare va deschide un registru special pentru a înregistra informațiile clasificate la primirea lor. Registrul va conține coloane indicând data primirii, detaliile documentului (data, referința și numărul copiei), clasificarea sa, titlul, numele sau titlul adresantului, data returnării primirii și data returnării documentului în UE sau distrugerea sa.

12. *Returnarea documentelor*

Când primitorul returnează un document clasificat Consiliului sau statului membru care l-a eliberat va proceda după cum este indicat în paragraful 10.

13. *Protecția*

(a) Când documentele nu sunt în uz, ele sunt păstrate într-un container de securitate care este aprobat pentru păstrarea materialelor național clasificate de aceeași clasificare. Containerul nu va purta nici o indicație în legătură cu conținutul său, care va fi accesibil doar persoanelor autorizate să manevreze informații clasificate UE. Când se folosesc încuietori cu cifru, combinația va fi cunoscută doar de acele autorități din stat sau organizații care au acces autorizat la informațiile clasificate ale UE ținute în container și vor fi schimbate la fiecare șase luni, sau mai devreme la transferul unei autorități, la retragerea autorizării de securitate a uneia dintre autoritățile care cunoaște combinația sau dacă există risc de compromis.

(b) Documentele clasificate ale UE vor fi retrase din containerul de securitate doar de către acele autorități autorizate pentru accesul la documentele clasificate UE și care au necesitatea de a le cunoaște. Ei rămân responsabili pentru custodia sigură a acelor documente atât timp cât sunt în posesia lor și, în special, pentru a asigura că nici o persoană neautorizată nu are acces la documente. Ei vor asigura de asemenea că documentele sunt păstrate într-un container de securitate când au terminat consultarea lor și în afara orelor de serviciu.

(c) Nici o fotocopie a unui document clasificat CONFIDENTIEL UE *[Confidențial UE]* sau mai important nu poate fi făcută, nici un extras luat, fără autorizarea Oficiului de Securitate al SGC.

(d) Procedura pentru distrugerea rapidă și totală a documentelor în caz de urgență trebuie definită și confirmată de Oficiul de Securitate al SGC.

14. *Securitatea fizică*

(a) Atunci când nu sunt în uz, containerele de securitate folosite pentru păstrarea documentelor clasificate UE sunt ținute întotdeauna încuiate.

(b) Atunci când este necesară intrarea sau activitatea personalului de întreținere sau de curățenie într-o incintă care găzduiește containere de securitate, acesta va fi însoțit în permanență de un membru al serviciului de securitate al statului sau al organizației sau de către agentul anume răspunzător de supravegherea securității incintei.

(c) În afara orelor obișnuite de lucru (noaptea, la sfârșit de săptămână și în timpul perioadelor de concedii), containerele de securitate care conțin documente clasificate ale UE sunt protejate fie de un agent de pază, fie de un sistem automat de alarmă.

15. *Încălcări ale securității*

Atunci când o încălcare a securității implicând un document clasificat al UE a avut loc sau este suspectată, trebuie luate imediat următoarele măsuri:

(a) înaintarea imediată a unui raport către Oficiul de Securitate al SGC sau către ANS a statului membru care a luat inițiativa de a comunica documentele (cu transmiterea unei copii către Oficiul de Securitate al SGC);

(b) efectuarea unei anchete, la finele căreia un raport complet se înaintează serviciului de securitate [a se vedea litera (a) de mai sus]. Trebuie apoi adoptate măsurile necesare pentru remedierea situației.

16. *Inspecțiile*

Oficiul de Securitate al SGC este autorizat să efectueze, de comun acord cu statele sau organizațiile internaționale în cauză, verificări ale eficienței măsurilor de protecție a imformațiilor clasificate ale UE comunicate.

17. *Raportarea*

Atât timp cât statul sau organizația deține informații clasificate ale UE, acesta sau aceasta prezintă, la o dată specificată atunci când este autorizat(ă) să primească aceste informații. când autorizarea de eliberare a informațiilor este dată, un raport anual care confirmă că prezentul regulament de securitate este respectat.

Anexa 6

Linii directoare privind comunicarea informațiilor clasificate ale UE către state terțe sau către organizații internaționale

Nivelul 3 de cooperare

PROCEDURI

1. Consiliul poate hotărî să coopereze, în anumite circumstanțe speciale, cu state sau cu organizații care nu pot da asigurările cerute de prezentul regulament de securitate, însă o asemenea cooperare poate totuși necesita comunicarea de informații clasificate ale UE. Într-un asemenea caz, informațiile naționale anume rezervate statelor membre nu pot fi comunicate.

2. În asemenea circumstanțe speciale, solicitările de cooperare cu UE, indiferent că emană de la state terțe sau de la organizații internaționale sau că sunt propuse de către statele membre sau de către organisme descentralizate ale UE, sunt examinate în prealabil, pe fond, de către Consiliu, care trebuie, după caz, să obțină avizul statului membru sau al organismului descentralizat de la care emană informațiile. Consiliul apreciază oportunitatea comunicării informațiilor clasificate, apreciază necesitatea de a cunoaște a beneficiarilor și stabilește natura informațiilor clasificate care pot fi comunicate.

3. În cazul în care Consiliul adoptă un aviz favorabil, îi revine secretarului general/Înalt reprezentant să convoace Comitetul de securitate al Consiliului sau să consulte, eventual prin procedura acordului tacit, autoritățile naționale de securitate ale statelor membre pentru a obține avizul tehnic al Comitetului de securitate.

4. Avizul tehnic al Comitetului de securitate al Consiliului privește următoarele elemente:

   (a) evaluarea riscurilor de securitate pentru UE sau statele sale membre;

   (b) gradul de clasificare a informațiilor care poate fi comunicate, după caz în funcție de natura acestora;

   (c) reducerea nivelului de clasificare sau declasificarea prealabilă de către autoritatea de origine a informațiilor înainte de a fi comunicată țărilor sau organizațiilor internaționale în cauză ([1]);

   (d) procedurile de prelucrare a documentelor care vor fi comunicate (a se vedea punctul 5 de mai jos);

   (e) metodele posibile de transmitere (folosirea serviciilor poștale publice, a rețelelor publice sau protejate de telecomunicații, valiză diplomatic, curieri speciali etc.).

5. Documentele comunicate statelor sau organizațiilor vizate de prezenta anexă sunt pregătite, în principiu, fără a indica referința de origine sau nivelul de clasificare UE. Comitetul de securitate al Consiliului poate recomanda:

   — folosirea unui simbol sau cod special;

   — folosirea unui sistem special de clasificare, prin care se face legătura între diferitele nivele de sensibilitate a informațiilor comunicate și măsurile de control cerute din partea beneficiarilor și metodele de transmitere a documentelor (a se vedea exemplele de la punctul 14).

6. Oficiul de Securitate al SGC înaintează Consiliului avizul tehnic al Comitetului de securitate, anexând, după caz, propunerile de delegare de atribuții necesare pentru îndeplinirea misiunii, îndeosebi în cazurile urgente.

7. Odată ce Consiliul a aprobat comunicarea de informații clasificate ale UE și procedurile practice de executare, Oficiul de Securitate al SGC stabilește contactele necesare cu serviciul de securitate al statului sau al organizației în cauză pentru a facilita aplicarea măsurilor de securitate propuse.

([1]) Aceasta face necesară aplicarea de către autoritatea de origine a procedurii definite la punctul 9 din secțiunea III în cazul tuturor copiilor în circulație în interiorul UE.

8. Ca referință, Oficiul de Securitate al SGC pune în circulație un tabel către toate statele membre și, după caz, către organismele descentralizate ale UE, tabel care rezumă natura, nivelul de clasificare al informației și enumeră organizațiile și țările cărora acestea le pot fi comunicate, în conformitate cu deciziile Consiliului.

9. ANS a statului membru care face eliberarea sau Oficiul de Securitate al SGC ia toate măsurile necesare pentru a facilita eventualele ulterioare evaluări ale prejudiciilor și revizuiri ale procedurilor.

10. Consiliul este sesizat de fiecare dată când condițiile cooperării se modifică.

REGULAMENTE DE SECURITATE CARE TREBUIE APLICATE DE BENEFICIARI

11. Decizia Consiliului de a elibera informații clasificate ale UE va fi adusă în atenția statelor beneficiare sau organizațiilor internaționale de către secretarul general/Înalt reprezentant, împreună cu modalitățile de protecție propuse de Comitetul de securitate al Consiliului și aprobată de Consiliu. Dacă cererea a fost făcută de un stat membru, acest stat va înștiința beneficiarul de eliberarea autorizată.

Decizia va intra în vigoare doar atunci când beneficiarii dau o asigurare în scris că:

— nu vor folosi informațiile în nici un alt scop decât cooperarea decisă de Consiliu;

— vor oferi informațiilor protecția cerută de Consiliu.

12. *Transmiterea documentelor*

(a) Procedurile practice pentru transmiterea documentelor va fi stabilită între Oficiul de Securitate al SGC și serviciile de securitate ale statelor primitoare sau organizațiile internaționale. Ele vor specifica în special adresele specifice la care documentele trebuie trimise.

(b) Documentele clasificate CONFIDENTIEL UE *[Confidențial UE]* și mai sus vor fi transmise sub o dublă acoperire. Plicul din interior va fi însemnat „UE" împreună cu clasificarea de securitate. Un formular de primire va fi inclus pentru fiecare document clasificat. Acest formular de primire, care nu va fi el însuși clasificat, va cita doar detaliile documentului (referința sa, data, numărul copiei) și limba sa, nu titlul.

(c) Plicul interior va fi apoi plasat în plicul exterior, care va purta un număr de pachet/înscriere pentru scopuri de primire. Plicul exterior nu va purta clasificare de securitate.

(d) O chitanță arătând numărul de înscriere va fi întotdeauna dată curierilor.

13. *Înregistrarea la sosire*

ANS-ul statului adresant sau echivalentul său în stat care primește în numele guvernului său informațiile clasificate înaintate de UE sau biroul de securitate al organizației internaționale primitoare va deschide un registru special pentru a înregistra informațiile clasificate la primirea lor. Registrul va conține coloane indicând data primirii, detaliile documentului (data, referința și numărul copiei), clasificarea sa, titlul, numele sau titlul adresantului, data returnării primirii și data returnării documentului în UE sau data distrugerii sale.

14. *Folosirea și protecția informațiilor clasificate schimbate*

(a) Informațiile de nivel SECRET UE vor fi manevrate de autorități special desemnate autorizate să aibă acces la informațiile cu această clasificare. Vor fi păstrate în cabinete de înaltă securitate care pot fi deschise doar de persoanele autorizate să aibă acces la informațiile pe care le conțin. Zonele în care acele cabinete sunt amplasate vor fi în permanență păzite și va fi stabilit un sistem de verificare pentru a se asigura că doar persoanele autorizate corespunzător sunt lăsate să intre. Informațiile de nivel SECRET UE vor fi înaintate prin genți diplomatice, servicii poștale și telecomunicații sigure. Un document SECRET UE poate fi copiat doar cu acordul scris al autorității de origine. Toate copiile vor fi înregistrate și monitorizate. Vor fi emise chitanțe pentru toate operațiile în legătură cu documentele SECRET UE.

(b) Informațiile de nivel CONFIDENTIEL UE *[Confidențial UE]* vor fi manevrate de autoritățile autorizate să fie informate asupra subiectului. Documentele vor fi păstrate în cabinete de securitate încuiate în zone controlate.

Informațiile de nivel CONFIDENTIEL UE *[Confidențial UE]* vor fi înaintate prin genți diplomatice, servicii poștale și telecomunicații sigure. Pot fi făcute copii de către corpul de destinație, numărul și distribuirea lor fiind înregistrate în registre speciale.

(c) Informațiile de nivel RESTREINT UE *[Circulație restrânsă UE]* vor fi manevrate în premisa că nu sunt accesibile persoanelor neautorizate și sunt ținute în containere încuiate. Documentele pot fi înaintate prin servicii poștale publice precum corespondență înregistrată într-un plic dublu și, în situații de urgență în timpul operațiunilor, prin sistemul de telecomunicații public, neprotejat. Adresanții pot face copii.

(d) Informațiile neclasificate nu necesită măsuri de protecție speciale și pot fi transmise prin poștă și prin sistemul de telecomunicații publice. Destinatarii își pot face copii.

15. *Distrugerea*

Documentele care nu mai sunt de folos trebuie distruse. În cazul documentelor de nivel RESTREINT UE *[Circulație restrânsă UE]* sau CONFIDENTIEL UE *[Confidențial UE]* va fi înscrisă o notă corespunzătoare în registrele speciale. În cazul documentelor de nivel SECRET UE, certificatele de distrugere vor fi emise și semnate de două persoane martore la distrugerea lor.

16. *Nerespectarea securității*

În cazul în care se constată că o informație de nivel CONFIDENTIEL UE *[Confidențial UE]* sau SECRET UE este compromisă sau există o suspiciune de compromitere, ANS a statului sau responsabilul cu securitatea din organizație face o anchetă cu privire la circumstanțele compromiterii. Dacă ancheta are rezultate pozitive, autoritatea de origine va fi înștiințată. Vor fi urmați pașii necesari pentru remedierea procedurilor neadecvate sau metodelor de păstrare dacă au dat naștere la compromise. Secretarul general/Înalt reprezentant al ANS sau al statului membru care a eliberat informațiile compromise pot cere beneficiarilor detalii asupra anchetei.