II

(Acte fără caracter legislativ)

DECIZII

DECIZIA CONSILIULUI

din 31 martie 2011

privind normele de securitate pentru protecția informațiilor UE clasificate

(2011/292/UE)

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 240 alineatul (3),

având în vedere Decizia 2009/937/UE a Consiliului din 1 decembrie 2009 de adoptare a regulamentului său de procedură [1], în special articolul 24,

întrucât:

(1) În vederea dezvoltării activităților Consiliului în toate domeniile care necesită gestionarea informațiilor clasificate se impune instituirea unui sistem de securitate cuprinzător pentru protecția informațiilor clasificate, care să includă Consiliul, Secretariatul General al Consiliului și statele membre.

(2) Prezenta decizie ar trebui să se aplice în cazurile în care Consiliul, grupurile de pregătire ale acestuia și Secretariatul General al Consiliului (SGC) gestionează informații UE clasificate (IUEC).

(3) Statele membre ar trebui, în conformitate cu actele cu putere de lege și dispozițiile administrative naționale și în măsura necesară pentru funcționarea Consiliului, să respecte prezenta decizie în cazurile în care autoritățile competente, personalul sau contractanții acestora gestionează IUEC, astfel încât fiecare dintre ele să aibă garanția acordării unui nivel echivalent de protecție a IUEC.

(4) Consiliul și Comisia își asumă angajamentul de a aplica standarde echivalente de securitate pentru protecția IUEC.

(5) Consiliul subliniază importanța asocierii, dacă este cazul, a Parlamentului European și a altor instituții, agenții, organisme sau oficii ale UE, la principiile, standardele și normele pentru protecția informațiilor clasificate necesare pentru protejarea intereselor Uniunii și ale statelor sale membre.

(6) Agențiile și organismele UE instituite în temeiul titlului V capitolul 2 din Tratatul privind Uniunea Europeană, Europol și Eurojust aplică, în cadrul organizării lor interne, principiile de bază și standardele minime stabilite în prezenta decizie pentru protecția IUEC, în conformitate cu prevederile din actele lor de instituire respective.

(7) Operațiile de gestionare a crizelor instituite în temeiul titlului V capitolul 2 din TUE și personalul operațiilor în cauză aplică normele de securitate pentru protecția IUEC adoptate de Consiliu.

(8) Reprezentanții Speciali ai UE și membrii echipelor acestora aplică normele de securitate adoptate de Consiliu pentru protecția IUEC.

(9) Prezenta decizie se adoptă fără a aduce atingere articolelor 15 și 16 din Tratatul privind funcționarea Uniunii Europene (TFUE) și instrumentelor de punere în aplicare a acestora.

(10) Prezenta decizie se adoptă fără a aduce atingere practicilor existente în interiorul statelor membre cu privire la informarea parlamentelor lor naționale despre activitățile Uniunii,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Obiectiv, domeniu de aplicare și definiții

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

[1] JO L 325, 11.12.2009, p. 35.

(2) Aceste principii de bază și standarde minime de securitate se aplică Consiliului și SGC și sunt respectate de statele membre, în conformitate cu actele cu putere de lege și dispozițiile administrative naționale ale acestora, astfel încât fiecare dintre ele să aibă garanția utilizării unui nivel echivalent de protecție a IUEC.

(3) În sensul prezentei decizii, se aplică definițiile stabilite în apendicele A.

Articolul 2

Definiția IUEC, a clasificărilor și a marcajelor de securitate

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

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

(a) TRÈS SECRET UE/EU TOP SECRET: 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 sau mai multor state membre.

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

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

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

(3) IUEC au un marcaj de clasificare de securitate, în conformitate cu alineatul (2). Acestea pot avea marcaje suplimentare care indică domeniul de activitate la care se referă, identifică emitentul, limitează distribuirea, restrâng utilizarea sau precizează dacă pot fi comunicate.

Articolul 3

Gestionarea clasificărilor

(1) Autoritățile competente se asigură că IUEC sunt clasificate corespunzător, identificate în mod clar ca informații clasificate și că nivelul de clasificare al acestora este menținut doar atât timp cât este necesar.

(2) IUEC nu sunt clasificate la un nivel de securitate inferior sau declasificate și niciun marcaj menționat la articolul 2 alineatul (3) nu este modificat sau eliminat fără acordul prealabil scris al emitentului.

(3) Consiliul aprobă o politică de securitate privind crearea IUEC care include un ghid practic al clasificărilor.

Articolul 4

Protecția informațiilor clasificate

(1) IUEC sunt protejate în conformitate cu prezenta decizie.

(2) Deținătorul oricărei informații UE clasificate este responsabil de protecția acesteia, în conformitate cu prezenta decizie.

(3) În cazul în care statele membre introduc informații clasificate care conțin un marcaj național de clasificare de securitate în structurile sau rețelele Uniunii Europene, Consiliul și SGC protejează informațiile respective în conformitate cu cerințele aplicabile IUEC de nivel echivalent, astfel cum se precizează în tabelul de echivalență a clasificărilor de securitate din apendicele B.

(4) Cumularea sau compilarea IUEC poate justifica protecția la un nivel corespunzător unei clasificări superioare.

Articolul 5

Managementul riscului de securitate

(1) Riscul la adresa IUEC este gestionat ca proces. Acest proces urmărește determinarea riscurilor de securitate cunoscute, definirea măsurilor de securitate destinate reducerii acestor riscuri la un nivel acceptabil în conformitate cu principiile de bază și standardele minime de securitate stabilite în prezenta decizie și aplicarea acestor măsuri în conformitate cu conceptul apărării în profunzime așa cum este definit în apendicele A. Eficacitatea acestor măsuri este evaluată permanent.

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

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

(4) Măsurile de prevenire și de recuperare destinate minimizării impactului erorilor sau incidentelor majore survenite în timpul gestionării și păstrării IUEC sunt incluse în Planurile de continuare a activității.

Articolul 6

Punerea în aplicare a prezentei decizii

(1) Dacă este necesar, Consiliul, la recomandarea Comitetului de securitate, aprobă politici de securitate care stabilesc măsurile pentru punerea în aplicare a prezentei decizii.

(2) Comitetul de securitate poate conveni, la nivelul său, asupra unor linii directoare de securitate menite să completeze sau să sprijine prezenta decizie sau orice politici de securitate aprobate de Consiliu.

Articolul 7

Securitatea personalului

(1) Securitatea personalului înseamnă aplicarea unor măsuri care să garanteze că accesul la IUEC este acordat numai persoanelor care:

— prezintă necesitatea de a cunoaște;

— au primit certificatul de securitate pentru nivelul corespunzător, dacă este cazul; și

— au fost informate cu privire la responsabilitățile care le revin.

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

(3) Întregul personal al SGC, ale cărui atribuții pot necesita accesul la IUEC de nivel CONFIDENTIEL UE/EU CONFIDENTIAL sau superior, este autorizat pentru nivelul corespunzător înainte de acordarea accesului la respectivele IUEC. Procedura de autorizare a personalului pentru funcționarii SGC și alți agenți este prevăzută în anexa I.

(4) Personalul statelor membre menționat la articolul 14 alineatul (3), ale cărui atribuții pot necesita accesul la IUEC de nivel CONFIDENTIEL UE/EU CONFIDENTIAL sau superior, este autorizat pentru nivelul corespunzător sau este autorizat în alt mod prin natura funcțiilor deținute, în conformitate cu actele cu putere de lege și actele administrative naționale, înainte de acordarea accesului la respectivele IUEC.

(5) Înainte de acordarea accesului la IUEC și ulterior la intervale periodice, întregul personal este informat și ia cunoștință de responsabilitățile care îi revin cu privire la protejarea IUEC, în conformitate cu prezenta decizie.

(6) Anexa I cuprinde dispozițiile pentru punerea în aplicare a prezentului articol.

Articolul 8

Securitatea fizică

(1) Securitatea fizică reprezintă aplicarea măsurilor de protecție fizică și tehnică în vederea împiedicării accesului neautorizat la IUEC.

(2) Măsurile de securitate fizică sunt concepute astfel încât să împiedice accesul disimulat sau forțat al vreunui intrus, să descurajeze, să împiedice și să detecteze acțiunile neautorizate și să permită separarea personalului în ceea ce privește accesul acestuia la IUEC, pe baza principiului necesității de a cunoaște. Aceste măsuri sunt stabilite pe baza unui proces de management al riscului.

(3) Măsurile de securitate fizică sunt instituite pentru toate incintele, imobilele, birourile, încăperile și alte zone în care sunt gestionate sau păstrate IUEC, inclusiv zonele care adăpostesc sisteme informatice și de comunicații astfel cum sunt definite la articolul 10 alineatul (2).

(4) Zonele în care sunt păstrate IUEC clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior sunt stabilite ca zone securizate în conformitate cu anexa II și aprobate de autoritatea de securitate competentă.

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

(6) Anexa II cuprinde dispozițiile pentru punerea în aplicare a prezentului articol.

Articolul 9

Managementul informațiilor clasificate

(1) Managementul informațiilor clasificate reprezintă aplicarea unor măsuri administrative pentru a controla IUEC pe durata ciclului lor de viață, în vederea completării măsurilor prevăzute la articolele 7, 8 și 10, contribuind astfel la descurajarea, detectarea și remedierea compromiterii sau pierderii deliberate sau accidentale a informațiilor. Aceste măsuri se referă, în special, la crearea, înregistrarea, copierea, traducerea, transportul și distrugerea IUEC.

(2) Din motive de securitate, informațiile clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior sunt înregistrate, la primirea acestora, înainte de a fi distribuite. În acest scop, autoritățile competente din SGC și din statele membre înființează sisteme de registre. Informațiile clasificate TRÈS SECRET UE/EU TOP SECRET sunt înregistrate în registre speciale.

(3) Serviciile și incintele unde sunt gestionate sau păstrate IUEC sunt supuse unor inspecții periodice ale autorităților de securitate competente.

(4) IUEC sunt transmise între servicii și incinte situate în afara zonelor protejate fizic după cum urmează:

(a) ca regulă generală, IUEC sunt transmise prin mijloace electronice protejate prin intermediul unor produse criptografice aprobate în conformitate cu articolul 10 alineatul (6);

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

(i) pe suport electronic (de ex. chei USB, CD-uri, hard diskuri) protejat prin intermediul unor produse criptografice aprobate în conformitate cu articolul 10 alineatul (6); sau

(ii) în toate celelalte cazuri, conform indicațiilor primite de la autoritatea de securitate competentă, în conformitate cu măsurile de protecție prevăzute la anexa III.

(5) Anexa III cuprinde dispozițiile pentru punerea în aplicare a prezentului articol.

Articolul 10

Protecția IUEC gestionate în sisteme informatice și de comunicații

(1) Asigurarea informațiilor (AI) în domeniul sistemelor informatice și de comunicații reprezintă încrederea în faptul că aceste sisteme vor proteja informațiile pe care le gestionează și vor funcționa corespunzător, atunci când este necesar, sub controlul utilizatorilor legitimi. O AI eficientă asigură grade adecvate de confidențialitate, integritate, disponibilitate, nerepudiere și autenticitate. AI se bazează pe un proces de management al riscului.

(2) „Sistemul informatic și de comunicații" reprezintă un sistem care permite gestionarea informațiilor clasificate în format electronic. Un sistem informatic și de comunicații cuprinde toate activele necesare pentru a funcționa, inclusiv infrastructura, organizarea, personalul și resursele informaționale. Prezenta decizie se aplică sistemelor informatice și de comunicații care gestionează IUEC (SIC).

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

(4) Toate SIC sunt supuse unui proces de acreditare. Acreditarea urmărește să garanteze faptul că au fost puse în aplicare toate măsurile de securitate corespunzătoare și că s-a obținut un nivel suficient de protecție a IUEC și a SIC, în conformitate cu prezenta decizie. Declarația de acreditare stabilește nivelul maxim de clasificare a informațiilor care poate fi gestionat de SIC, precum și termenii și condițiile acreditării respective.

(5) Sistemele de comunicații și informații care gestionează informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL și de nivel superior sunt protejate astfel încât informațiile să nu poată fi compromise prin emisii electromagnetice accidentale („măsuri de securitate TEMPEST").

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

(a) confidențialitatea informațiilor clasificate la nivelul SECRET UE/EU SECRET și la un nivel superior este protejată prin produse criptografice aprobate de Consiliu în calitate de autoritate de aprobare criptografică (AAC) la recomandarea Comitetului de securitate;

(b) confidențialitatea informațiilor clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau RESTREINT UE/EU RESTRICTED este protejată prin produse criptografice aprobate de Secretarul General al Consiliului (denumit în continuare „Secretarul General") în calitate de AAC, la recomandarea Comitetului de securitate.

Fără a aduce atingere literei (b), în cadrul sistemelor naționale ale statelor membre, confidențialitatea IUEC clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau RESTREINT UE/EU RESTRICTED poate fi protejată prin produse criptografice aprobate de AAC a unui stat membru.

(7) În cursul transmiterii IUEC prin mijloace electronice, se folosesc produse criptografice aprobate. Fără a aduce atingere acestei cerințe, pot fi aplicate proceduri specifice în situații de urgență sau în cadrul unor configurații tehnice specifice, astfel cum se specifică în anexa IV.

(8) Autoritățile competente ale SGC și ale statelor membre instituie următoarele funcții aferente AI:

(a) o autoritate AI (AAI);

(b) o autoritate TEMPEST (AT);

(c) o autoritate de aprobare criptografică (AAC);

(d) o autoritate de distribuire a materialului criptografic (ADMC)

(9) Pentru fiecare sistem, autoritățile competente ale SGC, respectiv ale statelor membre, instituie:

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

(b) o autoritate operațională AI.

(10) Anexa IV cuprinde dispozițiile pentru punerea în aplicare a prezentului articol.

Articolul 11

Securitatea industrială

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

(2) SGC poate încredința prin contract sarcini care implică sau determină accesul la IUEC sau gestionarea sau păstrarea acestora de entități industriale sau de altă natură înregistrate într-un stat membru sau într-un stat terț care a încheiat un acord sau un acord administrativ în conformitate cu articolul 12 alineatul (2) litera (a) sau (b).

(3) Atunci când atribuie contracte clasificate entităților industriale sau de altă natură, SGC, în calitate de autoritate contractantă, asigură respectarea standardelor minime privind securitatea industrială stabilite în prezenta decizie și menționate în contract.

(4) Autoritatea națională de securitate (ANS), autoritatea desemnată de securitate (ADS) și oricare altă autoritate competentă din statele membre se asigură, în măsura permisă de actele cu putere de lege și dispozițiile administrative naționale, că atât contractanții cât și subcontractanții iau toate măsurile necesare pentru protecția IUEC în cursul negocierilor premergătoare contractului precum și pe parcursul executării contractelor clasificate.

(5) ANS, ADS sau oricare altă autoritate de securitate competentă din fiecare stat membru se asigură, în conformitate cu actele cu putere de lege și dispozițiile administrative naționale, că atât contractanții cât și subcontractanții înregistrați în statele membre respective care participă la contracte sau subcontracte necesitând accesul, în obiectivele lor, la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET, fie în cursul executării contractelor respective, fie în etapa precontractuală, trebuie să dețină un certificat de securitate industrială (CSI), la nivelul de clasificare necesar.

(6) Personalului contractantului sau al subcontractantului ale cărui atribuții pot necesita accesul la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET în scopul executării unui contract clasificat i se acordă un certificat de securitate a personalului (CSP) de către ANS/ADS corespunzătoare sau de către orice altă autoritate de securitate competentă, în conformitate cu actele cu putere de lege și dispozițiile administrative naționale și cu standardele minime prevăzute în anexa I.

(7) Anexa V cuprinde dispozițiile pentru punerea în aplicare a prezentului articol.

Articolul 12

Schimbul de informații clasificate cu state terțe și organizații internaționale

(1) În cazul în care Consiliul stabilește necesitatea schimbului de IUEC cu un stat terț sau o organizație internațională, se instituie un cadru corespunzător în acest sens.

(2) Pentru a stabili un astfel de cadru și pentru a defini reguli reciproce pentru protejarea informațiilor clasificate care fac obiectul schimbului,

(a) Consiliul încheie acorduri privind procedurile de securitate pentru schimbul de informații clasificate și protecția acestora (denumite în continuare „acorduri privind securitatea informațiilor"); sau

(b) Secretarul General poate încheia acorduri administrative, în condițiile prevăzute în anexa VI la punctul 17 în cazul în care nivelul de clasificare a IUEC care urmează a fi comunicate nu depășește, ca regulă generală, nivelul RESTREINT UE/EU RESTRICTED.

(3) Acordurile privind securitatea informațiilor sau acordurile administrative menționate la alineatul (2) conțin dispoziții care garantează că, atunci când statele terțe sau organizațiile internaționale primesc IUEC, acestea beneficiază de protecția corespunzătoare nivelului lor de clasificare, pe baza unor standarde cel puțin la fel de stricte precum cele instituite prin prezenta decizie.

(4) Decizia de a comunica IUEC provenite de la Consiliu către un stat terț sau o organizație internațională se ia de către Consiliu, de la caz la caz, în funcție de natura și conținutul informațiilor respective, necesitatea de a cunoaște a destinatarului lor și măsura avantajului pentru UE. Dacă emitentul informațiilor clasificate a căror comunicare este solicitată nu este Consiliul, SGC trebuie să solicite, mai întâi, consimțământul scris al emitentului. În cazul în care emitentul nu poate fi identificat, Consiliul își asumă răspunderea.

(5) Se organizează vizite de evaluare pentru a se stabili eficiența măsurilor de securitate aplicate într-un stat terț sau de către o organizație internațională pentru protecția IUEC furnizate sau schimbate.

(6) Anexa VI cuprinde dispozițiile pentru punerea în aplicare a prezentului articol.

Articolul 13

Încălcări ale securității și compromiterea IUEC

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

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

(3) Orice încălcare sau suspiciune de încălcare a securității este raportată imediat autorităților competente de securitate.

(4) În cazul în care se cunoaște sau există motive întemeiate să se presupună că IUEC au fost compromise sau pierdute, autoritatea competentă de securitate ia toate măsurile corespunzătoare în conformitate cu actele cu putere de lege și dispozițiile administrative relevante pentru:

(a) a informa emitentul;

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

(c) a evalua potențialele prejudicii aduse intereselor UE sau ale statelor membre;

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

(e) a notifica autorităților competente acțiunea întreprinsă.

(5) Orice persoană responsabilă de încălcarea normelor de securitate prevăzute în prezenta decizie poate fi pasibilă de acțiuni disciplinare, în conformitate cu legile, normele și dispozițiile administrative aplicabile. Orice persoană responsabilă pentru compromiterea sau pierderea IUEC este pasibilă de acțiuni disciplinare și/sau în justiție, în conformitate cu legile, normele și dispozițiile administrative aplicabile.

Articolul 14

Responsabilitatea pentru punerea în aplicare

(1) Consiliul ia toate măsurile necesare pentru a asigura coerența globală în aplicarea prezentei decizii.

(2) Secretarul General ia toate măsurile necesare pentru a asigura, în cazul gestionării sau păstrării IUEC sau a oricăror altor informații clasificate, aplicarea prezentei decizii în incintele utilizate de Consiliu și în cadrul SGC, inclusiv în cadrul birourilor de legătură ale acestuia, situate în state terțe, de către funcționari și alți agenți ai SGC, de către personalul detașat la SGC și de către contractanții SGC.

(3) Statele membre iau măsurile corespunzătoare, în conformitate cu actele cu putere de lege și dispozițiile administrative proprii, pentru a se asigura că, în momentul gestionării sau păstrării IUEC, prezenta decizie este respectată de către:

(a) personalul reprezentanțelor permanente ale statelor membre pe lângă Uniunea Europeană și membrii delegațiilor naționale care participă la reuniunile Consiliului sau ale organismelor pregătitoare ale acestuia, sau care participă la alte activități ale Consiliului;

(b) alți membri ai administrațiilor naționale ale statelor membre, inclusiv personalul detașat pe lângă acele administrații, indiferent dacă își desfășoară activitatea pe teritoriul statelor membre sau în străinătate;

(c) alte persoane din statele membre, care, datorită funcțiilor ocupate, sunt autorizate să aibă acces la IUEC; și

(d) contractanții statelor membre, aflați pe teritoriul acestora sau în străinătate.

Articolul 15

Organizarea securității la nivelul Consiliului

(1) Ca parte a rolului său de asigurare a coerenței globale în aplicarea prezentei decizii, Consiliul aprobă:

(a) acordurile menționate la articolul 12 alineatul (2) litera (a);

(b) deciziile care autorizează comunicarea de IUEC către state terțe și organizații internaționale;

(c) un program de inspecții anuale propus de Secretarul General și recomandat de Comitetul de securitate pentru inspecții ale serviciilor și incintelor statelor membre și ale agențiilor și organismelor UE instituite în temeiul titlului V capitolul 2 din TUE, precum și ale Europol și Eurojust, și vizite de evaluare în state terțe și la organizații internaționale, în scopul stabilirii eficienței măsurilor puse în aplicare pentru protecția IUEC; și

(d) politici de securitate, astfel cum sunt prevăzute la articolul 6 alineatul (1).

(2) Secretarul General este autoritatea de securitate a SGC. În această calitate, Secretarul General:

(a) pune în aplicare politica de securitate a Consiliului și o supune reexaminării;

(b) colaborează cu ANS ale statelor membre cu privire la toate chestiunile de securitate privind protecția informațiilor clasificate relevante pentru activitățile Consiliului;

(c) acordă CSP UE funcționarilor și altor agenți ai SGC, în conformitate cu articolul 7 alineatul (3), înainte ca acestora să le fie acordat accesul la informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior;

(d) după caz, dispune efectuarea de investigații cu privire la orice compromitere sau pierdere, reală sau bănuită, de informații clasificate deținute sau elaborate de Consiliu și solicită autorităților de securitate competente să contribuie la astfel de investigații;

(e) efectuează inspecții periodice ale măsurilor de securitate pentru protecția informațiilor clasificate în incinta SGC;

(f) efectuează inspecții periodice ale măsurilor de securitate destinate protecției IUEC din agențiile și organismele UE instituite în temeiul titlului V capitolul 2 din TUE, din Europol și Eurojust, precum și din operațiile de gestionare a crizelor instituite în temeiul titlului V capitolul 2 din TUE, precum și ale Reprezentanților Speciali ai UE (RSUE) și ale membrilor echipelor acestora;

(g) efectuează, împreună și de comun acord cu ANS interesate, inspecții periodice ale măsurilor de securitate pentru protecția IUEC din serviciile și incintele aparținând statelor membre;

(h) coordonează măsurile de securitate, împreună cu autoritățile competente ale statelor membre care sunt responsabile cu protecția informațiilor clasificate și, după caz, ale statelor terțe sau ale organizațiilor internaționale, inclusiv în ceea ce privește natura amenințărilor la adresa securității IUEC și mijloacele de protecție împotriva acestora;

(i) încheie acordurile administrative menționate la articolul 12 alineatul (2) litera (b); și

(j) efectuează vizite inițiale și periodice de evaluare în state terțe sau la organizații internaționale, în scopul stabilirii eficienței măsurilor puse în aplicare pentru protecția IUEC puse la dispoziția acestora sau schimbate cu acestea.

Oficiul de Securitate al SGC este la dispoziția Secretarului General pentru a-l asista în îndeplinirea acestor responsabilități.

(3) În sensul punerii în aplicare a articolului 14 alineatul (3), statele membre ar trebui:

(a) să desemneze o ANS responsabilă cu măsurile de securitate pentru protecția IUEC, astfel încât:

(i) IUEC deținute în cadrul tuturor departamentelor, organismelor sau agențiilor naționale, publice sau private, pe teritoriul național sau în străinătate, să fie protejate în conformitate cu prezenta decizie;

(ii) măsurile de securitate pentru protecția IUEC să fie inspectate periodic;

(iii) întregul personal angajat în cadrul unei administrații naționale sau de către un contractant și căruia îi poate fi acordat accesul la informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior să beneficieze de un certificat de securitate adecvat sau de un alt tip de autorizație în temeiul funcțiilor deținute, în conformitate cu actele cu putere de lege și dispozițiile administrative naționale;

(iv) să fie instituite programe de securitate în funcție de necesități pentru a reduce la minim riscul de pierdere sau de compromitere a IUEC;

(v) chestiunile de securitate legate de protecția IUEC să fie abordate în colaborare cu alte autorități naționale competente, inclusiv cu cele menționate în prezenta decizie; și

(vi) să se răspundă cererilor corespunzătoare de certificate de securitate din partea agențiilor și organismelor UE instituite în temeiul titlului V capitolul 2 din TUE, a Europol și Eurojust, precum și a operațiilor de gestionare a crizelor instituite în temeiul titlului V capitolul 2 din TUE sau a RSUE și a echipelor acestora.

ANS sunt enumerate în apendicele C;

(b) să se asigure că autoritățile competente ale acestora oferă informații și consultanță guvernelor respective și, prin intermediul acestora, Consiliului cu privire la natura amenințărilor la adresa securității IUEC și la mijloacele de protecție împotriva acestora.

Articolul 16

Comitetul de securitate

(1) Se instituie un Comitet de securitate. Acesta examinează și evaluează orice aspect al securității care intră sub incidența prezentei decizii și adresează Consiliului recomandările corespunzătoare.

(2) Comitetul de securitate este compus din reprezentanți ai ANS ale statelor membre, iar un reprezentant al Comisiei și un reprezentant al Serviciului European de Acțiune Externă participă la lucrările sale. Comitetul este prezidat de Secretarul General sau de către delegatul desemnat al acestuia. Comitetul se reunește la indicația Consiliului sau la cererea Secretarului General sau a unei ANS.

La reuniunile acestuia pot fi invitați să asiste și reprezentanți ai agențiilor și organismelor UE instituite în temeiul titlului V capitolul 2 din TUE, precum și ai Europol și Eurojust, atunci când chestiunile dezbătute le privesc.

(3) Comitetul de securitate își organizează activitățile în așa fel încât să ofere recomandări cu privire la domenii de securitate specifice. Comitetul instituie un subdomeniu de experți pentru chestiunile AI și alte subdomenii de experți, după caz. Comitetul stabilește termeni de referință pentru aceste subdomenii de experți și primește rapoarte de la aceștia cu privire la activitățile lor, inclusiv, dacă este cazul, orice recomandări pentru Consiliu.

Articolul 17

Înlocuirea deciziei anterioare

(1) Prezenta decizie abrogă și înlocuiește Decizia 2001/264/CE a Consiliului din 19 martie 2001 de adoptare a regulamentului de securitate al Consiliului [1].

(2) Toate IUEC clasificate în conformitate cu Decizia 2001/264/CE continuă să fie protejate în conformitate cu dispozițiile corespunzătoare ale prezentei decizii.

Articolul 18

Intrarea în vigoare

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

Adoptată la Bruxelles, 31 martie 2011.

Pentru Consiliu

Președintele

VÖLNER P.

[1] JO L 101, 11.4.2001, p. 1.

ANEXE

ANEXA I

Securitatea personalului

ANEXA II

Securitatea fizică

ANEXA III

Managementul informațiilor clasificate

ANEXA IV

Protecția IUEC gestionate în SIC

ANEXA V

Securitatea industrială

ANEXA VI

Schimbul de informații clasificate cu state terțe și organizații internaționale

ANEXA I

SECURITATEA PERSONALULUI

I. INTRODUCERE

1. Prezenta anexă stabilește dispozițiile pentru punerea în aplicare a articolului 7. Aceasta stabilește, în special, criteriile pentru a determina dacă o persoană poate avea acces la IUEC, ținându-se seama de loialitatea și onestitatea acesteia și de încrederea pe care o inspiră, precum și procedurile administrative și de investigare care trebuie urmate în acest sens.

2. Pe tot cuprinsul prezentei anexe, cu excepția cazului în care există o distincție clară, termenul certificat de securitate a personalului se referă la certificatul național de securitate a personalului pentru acces la informații UE clasificate (CSP național) și/sau la certificatul UE de securitate a personalului (CSP UE), conform definițiilor din apendicele A.

II. AUTORIZAREA ACCESULUI LA IUEC

3. Unei persoane i se permite accesul la informații clasificate la nivel CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior numai după parcurgerea următoarelor etape:

(a) a fost stabilită necesitatea de a cunoaște a acesteia;

(b) i s-a acordat un CSP de nivel corespunzător sau beneficiază de un alt tip de autorizație în temeiul funcțiilor deținute, în conformitate cu actele cu putere de lege și dispozițiile administrative naționale; și

(c) a fost instruită cu privire la normele și procedurile de securitate pentru protecția IUEC și și-a asumat responsabilitățile cu privire la protecția informațiilor respective.

4. Fiecare stat membru și SGC identifică pozițiile din structurile lor care necesită accesul la informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior și care, prin urmare, necesită un CSP de nivel corespunzător.

III. CERINȚE PRIVIND CERTIFICATUL DE SECURITATE A PERSONALULUI

5. După ce a primit o cerere autorizată corespunzător, ANS sau alte autorități naționale competente sunt responsabile pentru a asigura că cetățenii lor, cărora trebuie să li se acorde accesul la informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior, sunt supuși investigațiilor de securitate. Standardele de investigație respectă actele cu putere de lege și dispozițiile administrative naționale.

6. În cazul în care persoana respectivă are reședința pe teritoriul unui alt stat membru sau al unui stat terț, autoritățile naționale competente solicită asistența autorității competente din statul de reședință, în conformitate cu actele cu putere de lege și dispozițiile administrative naționale. Statele membre se sprijină reciproc în efectuarea investigațiilor de securitate, în conformitate cu actele cu putere de lege și dispozițiile administrative naționale.

7. În cazul în care actele cu putere de lege și dispozițiile administrative naționale o permit, ANS sau alte autorități naționale competente pot efectua investigații de securitate pentru neresortisanți cărora trebuie să li se acorde accesul la informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior. Standardele de investigație respectă actele cu putere de lege și dispozițiile administrative naționale.

Criteriile investigațiilor de securitate

8. Loialitatea, onestitatea și încrederea inspirată de o persoană în scopul acordării unui CSP pentru accesul la informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior sunt stabilite prin intermediul unei investigații de securitate. Autoritatea națională competentă efectuează o evaluare generală pe baza rezultatelor unei astfel de investigații de securitate. Nicio informație adversă unică nu constituie, neapărat, un motiv de refuz al unui CSP. Principalele criterii utilizate în acest scop ar trebui să includă, în măsura permisă de actele cu putere de lege și de dispozițiile administrative naționale, observația dacă persoana respectivă:

(a) a comis sau a încercat să comită, a conspirat la, a acordat ajutor sau a incitat o altă persoană să comită orice act de spionaj, terorism, sabotaj, trădare sau instigare la rebeliune;

(b) este sau a fost asociată cu spioni, teroriști, sabotori sau persoane suspectate, pe baza unor motive întemeiate, de a fi fost asociate reprezentanților unor organizații ale altor state, inclusiv ai serviciilor secrete, care pot amenința securitatea UE și/sau a statelor membre, cu excepția cazurilor în care astfel de asocieri au fost autorizate pentru îndeplinirea unor atribuții oficiale;

(c) este sau a fost membră a unei organizații care încearcă, prin mijloace violente, subversive, sau alte mijloace ilegale, inter alia, să înlăture guvernul unui stat membru, să schimbe ordinea constituțională a unui stat membru sau să schimbe forma sau politicile de guvernare ale unui stat membru;

(d) este sau a fost susținătoare a unei organizații descrise la litera (c) sau este sau a fost asociată îndeaproape cu membrii unor astfel de organizații;

(e) a ascuns, denaturat sau falsificat în mod intenționat informații semnificative, în special referitoare la securitate, sau a mințit cu bună-știință în cursul completării chestionarului privind securitatea personalului sau în timpul interviului de securitate;

(f) a fost condamnată în urma uneia sau mai multor infracțiuni;

(g) are un istoric de dependență de alcool, de folosire a unor substanțe stupefiante ilegale și/sau de folosire abuzivă a unor substanțe legale;

(h) a manifestat sau manifestă comportamente care ar putea antrena riscul de vulnerabilitate la șantaj sau presiuni;

(i) prin fapte sau limbaj, a demonstrat lipsă de onestitate și loialitate, incapacitate de a inspira încredere;

(j) a încălcat în mod grav sau repetat regulamentele de securitate; sau a încercat sau a reușit să desfășoare o activitate neautorizată legată de sistemele informatice și de comunicații;

(k) poate fi expus la presiuni (de exemplu în virtutea deținerii uneia sau mai multor cetățenii ale unor state non-membre UE sau prin intermediul unor rude sau asociați apropiați care ar putea fi vulnerabili față de servicii secrete străine, grupări teroriste sau alte organizații sau persoane subversive, ale căror scopuri pot amenința interesele de securitate ale UE și/sau ale statelor membre.

9. După caz și în conformitate cu actele cu putere de lege și dispozițiile administrative naționale, situația financiară și medicală a unei persoane poate fi, de asemenea, considerată relevantă în cadrul investigației de securitate.

10. După caz și în conformitate cu actele cu putere de lege și dispozițiile administrative naționale, caracterul, comportamentul și situația soțului/soției, partenerului/partenerei sau ale unui membru apropiat al familiei, pot fi, de asemenea, considerate relevante în cadrul investigației de securitate.

Cerințe de investigare pentru acordarea accesului la IUEC

Acordarea inițială a CSP

11. Acordarea inițială a CSP pentru acces la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET se bazează pe o investigație de securitate care acoperă cel puțin ultimii cinci ani, sau perioada cuprinsă între împlinirea vârstei de 18 ani și până în prezent, în funcție de care dintre aceste perioade este mai scurtă și cuprinde:

(a) completarea unui chestionar național de securitate a personalului pentru nivelul IUEC la care persoanei trebuie să i se acorde accesul; odată completat, acest chestionar este înaintat autorității de securitate competente;

(b) verificarea identității/cetățeniei/naționalității – se verifică data și locul nașterii persoanei, precum și identitatea acesteia. Se stabilesc cetățenia și/sau naționalitatea trecute și prezente ale persoanei; aceasta include evaluarea oricărei forme de vulnerabilitate la presiuni din surse străine, de exemplu, datorită reședinței anterioare sau unor asocieri din trecut; și

(c) verificarea evidențelor naționale și locale – se realizează o verificare a evidențelor de securitate naționale și a cazierului judiciar central, dacă există, precum și/sau ale altor evidențe guvernamentale sau polițienești comparabile. Se verifică evidențele agențiilor de aplicare a legii având competență juridică în locul în care persoana a locuit sau a lucrat.

12. CSP inițial acordat pentru accesul la informații clasificate TRÈS SECRET UE/EU TOP SECRET se bazează pe o investigație de securitate care acoperă cel puțin ultimii zece ani, sau perioada cuprinsă între împlinirea vârstei de 18 ani și prezent, în funcție de care dintre aceste perioade este mai scurtă. Dacă interviurile descrise la litera (e) au loc, investigațiile acoperă cel puțin ultimii șapte ani sau perioada cuprinsă între împlinirea vârstei de 18 ani și prezent, în funcție de care dintre aceste perioade este mai scurtă. În plus față de criteriile indicate la punctul 8 de mai sus, sunt investigate următoarele elemente, în măsura permisă de actele cu putere de lege și dispozițiile administrative naționale, înaintea acordării unui CSP TRÈS SECRET UE/EU TOP SECRET; acestea pot fi investigate și înaintea acordării unui CSP CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET, dacă acest lucru este cerut de actele cu putere de lege și dispozițiile administrative naționale:

(a) situația financiară – se caută informații privind finanțele persoanei, pentru a evalua orice vulnerabilitate la presiuni străine sau naționale cauzate de dificultăți financiare grave, sau pentru a descoperi orice formă de prosperitate neexplicată;

(b) educația – se caută informații pentru a verifica parcursul educațional al persoanei, la școlile, universitățile și la alte instituții de învățământ frecventate de la împlinirea vârstei de 18 ani sau pentru o perioadă considerată oportună de către autoritatea care realizează investigația;

(c) situația profesională – se caută informații privind situația profesională prezentă și trecută, consultându-se surse cum ar fi evidențe privind angajarea în muncă, rapoarte de performanță și eficiență, precum și angajatori și autorități de supraveghere;

(d) serviciul militar – după caz, se verifică serviciul persoanei respective în slujba forțelor armate și statutul cu care a fost eliberat din serviciul militar; și

(e) interviuri – în cazurile prevăzute și admise de legislația națională, au loc unul sau mai multe interviuri cu persoana în cauză. De asemenea, au loc interviuri cu alte persoane care pot oferi o evaluare nepărtinitoare a mediului, activităților, loialității, onestității și gradului de încredere inspirată de persoana în cauză. Atunci când practica națională prevede că subiectul investigației trebuie să furnizeze referințe, persoanele citate ca referințe trebuie intervievate, cu excepția cazului în care există motive întemeiate pentru a nu face acest lucru.

13. În cazul în care este necesar și în conformitate cu actele cu putere de lege și dispozițiile administrative naționale, pot avea loc investigații suplimentare pentru a colecta toate informațiile relevante disponibile cu privire la persoana în cauză și pentru a dovedi sau infirma informațiile adverse.

Revalidarea CSP

14. După acordarea inițială a unui CSP și dacă persoana a lucrat neîntrerupt în cadrul unei administrații naționale sau în cadrul SGC și necesită accesul permanent la IUEC, CSP este reexaminat în vederea revalidării la intervale de maximum cinci ani pentru certificatul TRÈS SECRET UE/EU TOP SECRET, respectiv zece ani pentru certificatele SECRET UE/EU SECRET și CONFIDENTIEL UE/EU CONFIDENTIAL, cu începere de la data comunicării rezultatului ultimei investigații de securitate pe care s-au bazat. Toate investigațiile de securitate destinate revalidării CSP acoperă perioada scursă de la investigația anterioară.

15. Pentru revalidarea CSP se investighează elementele menționate la punctele 11 și 12.

16. Cererile de revalidare se depun în timp util, ținându-se seama de perioada necesară pentru investigațiile de securitate. Cu toate acestea, în cazul în care ANS competentă sau o altă autoritate națională competentă a primit solicitarea relevantă privind revalidarea și chestionarul aferent privind securitatea personalului înainte de expirarea CSP, iar investigația de securitate necesară nu a fost finalizată, autoritatea națională competentă poate, dacă acest lucru este permis de actele cu putere de lege și de dispozițiile administrative naționale, prelungi validitatea CSP existent cu maximum 12 luni. Dacă la sfârșitul acestei perioade de 12 luni, investigația de securitate nu a fost încă finalizată, persoanei îi sunt încredințate atribuții care nu necesită un CSP.

Procedurile referitoare la CSP în cadrul SGC

17. În cazul funcționarilor și al altor agenți ai SGC, autoritatea de securitate a SGC înaintează chestionarul privind securitatea personalului completat către ANS a statului membru a cărui naționalitate o deține persoana în cauză, solicitând efectuarea unei investigații de securitate pentru nivelul IUEC la care va trebui să i se acorde accesul respectivei persoane.

18. În cazul în care SGC intră în posesia unor informații relevante pentru o investigație de securitate referitoare la o persoană care a solicitat un CSP UE, SGC, acționând în conformitate cu actele cu putere de lege și dispozițiile administrative relevante, notifică ANS competentă.

19. După finalizarea investigației de securitate, ANS competentă notifică autorității de securitate a SGC rezultatul respectivei investigații, în forma standard pentru corespondență stabilită de Comitetul de securitate.

(a) În cazul în care investigația de securitate stabilește cu certitudine că nu se cunosc fapte adverse care să pună la îndoială loialitatea, onestitatea și încrederea inspirate de respectiva persoană, autoritatea responsabilă cu numirile din cadrul SGC poate acorda un CSP UE persoanei în cauză și autoriza accesul acesteia la IUEC până la nivelul relevant și până la o dată precisă.

(b) În cazul în care investigația de securitate nu are drept rezultat o astfel de garanție, autoritatea responsabilă cu numirile din cadrul SGC anunță persoana vizată, care poate solicita să fie audiată de către autoritatea responsabilă cu numirile. Aceasta din urmă îi poate solicita ANS competente orice clarificare suplimentară posibilă, în conformitate cu actele cu putere de lege și dispozițiile administrative naționale ale acesteia. Dacă rezultatul este confirmat, CSP UE nu este acordat.

20. Investigația de securitate și rezultatele obținute sunt supuse actelor cu putere de lege și dispozițiilor administrative relevante în vigoare în statul membru în cauză, inclusiv celor privind căile de atac. Deciziile autorității responsabile cu numirile din cadrul SGC pot face obiectul unor căi de atac, în conformitate cu Statutul funcționarilor Uniunii Europene și Regimul aplicabil celorlalți agenți ai Uniunii Europene, stabilit în Regulamentul (CEE, Euratom, CECO) nr. 259/68 ([1]) (denumit în continuare „Statutul și Regimul aplicabil").

21. Garanțiile pe care se bazează un CSP UE, cu condiția ca acestea să rămână valabile, acoperă orice funcție deținută de persoana în cauză în cadrul SGC sau al Comisiei.

22. Dacă o persoană nu își începe activitatea în termen de 12 luni de la notificarea rezultatului investigației de securitate autorității responsabile cu numirile din cadrul SGC, sau dacă intervine o pauză de 12 luni în exercitarea atribuțiilor sale, timp în care persoana în cauză nu a fost angajată în cadrul SGC sau într-o poziție în cadrul administrației naționale a unui stat membru, rezultatul respectiv este prezentat ANS competente, pentru a se confirma menținerea valabilității și oportunității acestuia.

23. În cazul în care SGC intră în posesia unor informații privind un risc de securitate reprezentat de o persoană care deține un CSP UE valabil, SGC, acționând în conformitate cu actele cu putere de lege și dispozițiile administrative relevante, notifică ANS competentă. În cazul în care o ANS notifică SGC privind retragerea unei garanții acordate în conformitate cu punctul 19 litera (a) pentru o persoană care deține un CSP UE valabil, autoritatea responsabilă cu numirile din cadrul SGC poate solicita ANS orice clarificare pe care aceasta o poate furniza, în conformitate cu actele cu putere de lege și dispozițiile administrative naționale ale acesteia. În cazul în care informațiile adverse sunt confirmate, persoanei i se retrage CSP UE și i se refuză accesul la IUEC și la pozițiile care permit accesul la acestea sau din care ar putea compromite securitatea.

24. Orice decizie de retragere a CSP UE al unui funcționar sau al altui agent al SGC și, după caz, motivele care stau la baza acesteia sunt comunicate persoanei în cauză, care poate solicita să fie audiată de către autoritatea responsabilă cu numirile. Informațiile furnizate de o ANS sunt supuse actelor cu putere de lege și dispozițiilor administrative relevante în vigoare în statul membru în cauză, inclusiv celor privind căile de atac. Deciziile autorității responsabile cu numirile din cadrul SGC pot face obiectul unor căi de atac, în conformitate cu Statutul și Regimul aplicabil.

25. Experții naționali detașați în cadrul SGC într-o poziție care necesită un CSP UE prezintă autorității de securitate a SGC, înainte de a-și prelua funcția, un CSP național valabil pentru accesul la IUEC.

Evidența CSP

26. Fiecare stat membru și SGC țin o evidență a CSP naționale și, respectiv, a CSP UE acordate în vederea accesului la IUEC. Evidențele respective conțin cel puțin detalii cu privire la nivelul IUEC la care este permis accesul persoanei (CONFIDENTIEL UE/EU CONFIDENTIAL sau superior), data acordării CSP și perioada de valabilitate a acestuia.

27. Autoritatea de securitate competentă poate elibera o confirmare privind deținerea certificatului de securitate a personalului (CCSP) care indică nivelul IUEC la care este permis accesul persoanei respective (CONFIDENTIEL UE/EU CONFIDENTIAL sau superior), perioada de valabilitate a CSP național pentru acces la IUEC sau a CSP UE relevant și data expirării certificatului în cauză.

Scutiri de la obligația de a deține un CSP

28. Accesul la IUEC al unor persoane din statele membre, autorizate în temeiul funcțiilor deținute, este stabilit în conformitate cu actele cu putere de lege și dispozițiile administrative naționale; astfel de persoane sunt informate cu privire la obligațiile de securitate privind protecția IUEC.

IV. EDUCAȚIA ȘI CONȘTIENTIZAREA ÎN MATERIE DE SECURITATE

29. Toate persoanele cărora li s-a acordat un CSP confirmă în scris faptul că își înțeleg obligațiile cu privire la protecția IUEC, precum și consecințele compromiterii IUEC. Statele membre și SGC, după caz, țin evidența acestor confirmări scrise.

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

31. Toate persoanele care încetează să aibă atribuții care necesită acces la IUEC sunt informate asupra obligațiilor care le revin pentru protecția continuă a IUEC și, dacă este cazul, le confirmă în scris.

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

V. ÎMPREJURĂRI EXCEPȚIONALE

32. În cazul în care actele cu putere de lege și dispozițiile administrative naționale o permit, un certificat de securitate a personalului acordat de o autoritate națională competentă a unui stat membru pentru accesul la informații clasificate naționale poate, pentru o perioadă temporară, până la acordarea unui CSP național pentru accesul la IUEC, permite accesul funcționarilor naționali la IUEC până la nivelul echivalent celui stabilit în tabelul de echivalențe din apendicele B, în cazul în care un astfel de acces temporar este necesar în interesul UE. ANS informează Comitetul de securitate cu privire la cazurile în care actele cu putere de lege și dispozițiile administrative naționale nu permit un astfel de acces temporar la IUEC.

33. Din motive de urgență, în cazuri de interes de serviciu justificate corespunzător și în așteptarea finalizării unei investigații de securitate complete, autoritatea responsabilă cu numirile din cadrul SGC poate acorda o autorizație temporară funcționarilor și altor agenți ai SGC pentru accesul la IUEC pentru o funcție specifică, după consultarea ANS a statului membru a cărui cetățenie este deținută de persoana respectivă și cu condiția ca rezultatul verificărilor preliminare să ateste că nu se cunosc informații adverse. Astfel de autorizații temporare sunt valabile maximum șase luni și nu permit accesul la informații clasificate TRÈS SECRET UE/EU TOP SECRET. Toate persoanele cărora li s-a acordat o autorizație temporară confirmă în scris faptul că își înțeleg obligațiile cu privire la protecția IUEC, precum și consecințele compromiterii IUEC. SGC ține evidența acestei confirmări scrise.

34. În cazul în care o persoană urmează să fie numită într-o poziție care necesită un CSP la nivelul superior celui deținut în prezent de persoana în cauză, numirea se poate face provizoriu, cu condiția ca:

(a) nevoia vitală de acces la IUEC de nivel superior să fie justificată, în scris, de către superiorul persoanei în cauză;

(b) accesul să fie limitat la anumite informații UE clasificate, în sprijinul numirii;

(c) persoana să dețină un CSP național sau un CSP UE valabil;

(d) să fie inițiate demersurile pentru obținerea accesului la nivelul necesar pentru poziția în cauză;

(e) autoritatea competentă să fi efectuat verificări satisfăcătoare, care să confirme că persoana nu a încălcat în mod grav sau repetat normele de securitate;

(f) numirea persoanei să fie aprobată de autoritatea competentă; și

(g) excepția să se consemneze la registrul sau la registrul subordonat responsabil, împreună cu descrierea informațiilor la care a fost aprobat accesul.

35. Procedura de mai sus este utilizată pentru accesul unic la IUEC la nivelul superior următor celui pentru care persoana deține certificatul de securitate. Nu se recurge in mod repetat la această procedură.

36. În împrejurări absolut excepționale, precum misiunile în medii ostile sau în perioade de tensiune internațională crescândă, când măsurile de urgență o impun, în special în scopul salvării de vieți, statele membre și Secretarul General pot acorda, dacă este posibil în scris, accesul la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET unor persoane care nu posedă CSP necesar, cu condiția ca permisiunea în acest sens să fie absolut necesară și să nu existe suspiciuni întemeiate cu privire la loialitatea, onestitatea și încrederea inspirată de persoana respectivă. Permisiunea se consemnează, cu descrierea informațiilor la care s-a aprobat accesul.

37. În cazul informațiilor clasificate TRÈS SECRET UE/EU TOP SECRET, accesul de urgență este limitat la cetățeni ai statelor UE care beneficiază de acces autorizat fie la nivelul național echivalent al TRÈS SECRET UE/EU TOP SECRET, fie la informații clasificate SECRET UE/EU SECRET.

38. Comitetul de securitate este informat cu privire la cazurile în care se recurge la procedura stabilită la punctele 36 și 37.

39. În cazul în care actele cu putere de lege și dispozițiile administrative naționale ale unui stat membru cuprind norme mai stricte cu privire la autorizațiile temporare, numirile provizorii, accesul unic sau la accesul de urgență al persoanelor la informații clasificate, procedurile prevăzute în prezenta secțiune se aplică numai în cadrul limitelor stabilite de actele cu putere de lege și dispozițiile administrative naționale relevante.

40. Comitetul de securitate primește un raport anual cu privire la utilizarea procedurilor prevăzute în această secțiune.

VI. PARTICIPAREA LA REUNIUNILE CONSILIULUI

41. Sub rezerva punctului 28, persoanele desemnate să participe la reuniunile Consiliului sau ale grupurilor sale de lucru, în cadrul cărora se discută informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior, pot participa numai după ce se confirmă că dețin un CSP. În cazul delegaților, CCSP sau o altă dovadă a CSP este trimisă de autoritățile competente Oficiului de Securitate al SGC, sau, în cazuri excepționale, este prezentată de către delegatul în cauză. După caz, se poate folosi o listă centralizată de nume, cuprinzând dovada relevantă a CSP.

42. În cazul în care, din motive de securitate, un CSP național pentru acces la IUEC îi este retras unei persoane ale cărei atribuții necesită participarea la reuniuni ale Consiliului sau ale organismelor pregătitoare ale acestuia, autoritatea competentă informează SGC.

VII. POSIBILITATEA ACCESULUI LA IUEC

43. În cazul în care persoane trebuie angajate în funcții care le pot permite accesul la informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior, acestea sunt verificate în prealabil din punct de vedere al securității sau sunt escortate în permanență.

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

ANEXA II

SECURITATEA FIZICĂ

I. INTRODUCERE

1. Prezenta anexă stabilește dispozițiile pentru punerea în aplicare a articolului 8. Anexa stabilește cerințele minime pentru protecția fizică a incintelor, clădirilor, birourilor, încăperilor și a altor zone în care se gestionează și se păstrează IUEC, inclusiv a zonelor care adăpostesc SIC.

2. Măsurile de securitate fizică sunt menite să împiedice accesul neautorizat la IUEC și sunt concepute astfel încât:

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

(b) să permită separarea personalului din punctul de vedere al accesului la IUEC, pe baza principiului necesității de a cunoaște și, după caz, a certificatului de securitate;

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

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

II. CERINȚE ȘI MĂSURI DE SECURITATE FIZICĂ

3. Măsurile de securitate fizică sunt selectate pe baza unei evaluări a amenințărilor efectuate de autoritățile competente. SGC și statele membre folosesc, fiecare, un proces de management al riscului pentru protecția IUEC în incintele lor, pentru a asigura aplicarea unui nivel de protecție fizică proporțional cu riscul evaluat. Procesul de management al riscului ține seama de toți factorii relevanți, în special de:

(a) nivelul de clasificare al IUEC;

(b) forma și volumul IUEC, ținând seama de faptul că, pentru cumularea sau compilarea de IUEC, poate fi necesară aplicarea unor măsuri de protecție mai severe;

(c) mediul înconjurător și structura clădirilor sau a zonelor care adăpostesc IUEC; și

(d) evaluarea amenințării reprezentate de către serviciile secrete care au drept țintă UE sau statele sale membre și de sabotaje, acte teroriste, subversive sau alte activități criminale.

4. Autoritatea de securitate competentă, prin aplicarea conceptului apărării în profunzime, stabilește combinația corespunzătoare de măsuri de securitate fizică care trebuie implementate. Acestea pot include una sau mai multe dintre următoarele:

(a) o barieră de incintă: o barieră fizică care protejează limitele unei zone care necesită protecție;

(b) sisteme de detectare a intruziunilor (SDI): un SDI poate fi utilizat pentru a spori nivelul de securitate oferit de o barieră de incintă sau folosit în încăperi sau clădiri, în locul personalului de securitate sau în sprijinul acestuia;

(c) controlul accesului: controlul accesului se poate aplica la nivelul unui obiectiv, al uneia sau mai multor clădiri aparținând obiectivului respectiv sau la nivelul unor zone sau încăperi dintr-o clădire. Controlul poate fi efectuat prin mijloace electronice, electromecanice, de către personalul de securitate și/sau persoana de la recepție sau prin alte mijloace fizice;

(d) personalul de securitate: poate fi angajat personal de securitate format, supravegheat și, dacă este necesar, posesor al unui certificat de securitate corespunzător pentru, *inter alia*, a descuraja anumite persoane să plănuiască intrarea clandestină;

(e) televiziunea cu circuit închis (TVCI): TVCI poate fi utilizată de către personalul de securitate pentru a verifica incidentele și alarmele declanșate de SDI în spații vaste sau în perimetre;

(f) iluminatul de securitate: iluminatul de securitate poate fi utilizat pentru a descuraja un intrus potențial, precum și pentru a asigura lumina necesară pentru supravegherea directă de către personalul de securitate, sau indirectă, printr-un sistem TVCI; și

(g) orice alte măsuri de securitate fizică menite să descurajeze sau să detecteze accesul neautorizat sau să împiedice pierderea sau deteriorarea IUEC.

5. Autoritatea competentă poate fi autorizată să efectueze controale la intrare și la ieșire, pentru a descuraja introducerea neautorizată de materiale sau sustragerea IUEC din incinte sau clădiri.

6. Atunci când există riscul vizualizării, chiar accidentale, a IUEC, se iau măsuri adecvate pentru contracararea acestui risc.

7. În ceea ce privește obiectivele noi, cerințele de securitate fizică și specificațiile funcționale ale acestora se definesc ca parte a planificării și concepției obiectivelor. Pentru obiectivele existente, cerințele de securitate fizică sunt puse în aplicare în cea mai mare măsură posibilă.

III. ECHIPAMENTE DESTINATE PROTECȚIEI FIZICE A IUEC

8. La achiziționarea echipamentului destinat protecției fizice a IUEC (cum ar fi containere de securitate, mașini de tocat în fâșii, încuietori pentru uși, sisteme electronice de control al accesului, SDI, sisteme de alarmă), autoritatea de securitate competentă se asigură că echipamentul respectă standardele tehnice aprobate și cerințele minime.

9. Specificațiile tehnice ale echipamentelor destinate protecției fizice a IUEC sunt prevăzute în liniile directoare de securitate care urmează să fie aprobate de Comitetul de securitate.

10. Sistemele de securitate sunt inspectate la intervale regulate și echipamentele sunt întreținute periodic. Lucrările de întreținere țin seama de rezultatul inspecțiilor pentru a se asigura funcționarea echipamentelor la cote optime.

11. Eficacitatea măsurilor individuale de securitate și a sistemului de securitate în ansamblul său sunt reevaluate cu ocazia fiecărei inspecții.

IV. ZONE PROTEJATE FIZIC

12. Pentru protecția fizică a IUEC, se instituie două tipuri de zone protejate fizic sau echivalentele acestora la nivel național:

(a) zone administrative; și

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

În cadrul prezentei decizii, toate trimiterile la zonele administrative și la zonele securizate, inclusiv la zonele securizate din punct de vedere tehnic, trebuie înțelese, de asemenea, ca trimiteri la echivalentele naționale ale acestora.

13. Autoritatea de securitate competentă stabilește o zonă care îndeplinește cerințele pentru a fi desemnată drept zonă administrativă, zonă securizată sau zonă securizată din punct de vedere tehnic.

14. Pentru zonele administrative:

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

(b) accesul neînsoțit este permis numai persoanelor autorizate în mod corespunzător de autoritatea competentă; și

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

15. Pentru zonele securizate:

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

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

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

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

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

(b) toți vizitatorii au nevoie de o autorizație specifică pentru a intra în zona respectivă, sunt escortați în permanență și sunt verificați din punct de vedere al securității în mod corespunzător, cu excepția cazului în care sunt instituite măsuri care fac imposibil orice acces la IUEC.

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

(a) aceste zone sunt echipate cu SDI, sunt încuiate atunci când nu sunt ocupate și păzite atunci când sunt ocupate. Toate cheile sunt controlate în conformitate cu secțiunea VI;

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

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

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

18. Fără a aduce atingere punctului 17 litera (d), înainte de a fi utilizate în zonele în care se desfășoară reuniuni sau se lucrează cu informații cu nivel de clasificare SECRET UE/EU SECRET sau superior acestuia și în cazul în care amenințarea la adresa IUEC este evaluată ca fiind semnificativă, toate dispozitivele de comunicare și echipamentele electrice și electronice de orice tip sunt examinate, mai întâi, de autoritatea de securitate competentă pentru a se asigura faptul că nicio informație inteligibilă nu poate fi transmisă în mod accidental sau ilicit prin intermediul unor asemenea echipamente în afara perimetrului zonei securizate.

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

20. Zonele securizate și zonele securizate din punct de vedere tehnic pot fi stabilite, în mod temporar, într-o zonă administrativă, în scopul unei reuniuni clasificate sau în alt scop similar.

21. Pentru fiecare zonă securizată se elaborează proceduri operaționale de securitate, care prevăd:

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

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

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

(d) acolo unde este cazul, procedurile pentru escortări sau pentru protecția IUEC în cazul autorizării accesului oricăror altor persoane la zona respectivă;

(e) orice alte măsuri și proceduri relevante.

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

V. MĂSURI DE PROTECȚIE FIZICĂ PENTRU GESTIONAREA ȘI PĂSTRAREA IUEC

23. IUEC clasificate RESTREINT UE/EU RESTRICTED pot fi gestionate:

(a) într-o zonă securizată;

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

(c) în afara unei zone securizate sau a unei zone administrative, cu condiția ca deținătorul să transporte IUEC în condițiile prevăzute la anexa III, punctele 28-40 și să se angajeze să respecte măsurile compensatorii stabilite în instrucțiunile de securitate emise de autoritatea de securitate competentă pentru a se asigura că IUEC sunt protejate împotriva accesului persoanelor neautorizate.

24. IUEC clasificate RESTREINT UE/EU RESTRICTED sunt păstrate în mobilier de birou încuiat în mod corespunzător, într-o zonă administrativă sau o zonă securizată. Aceste informații pot fi păstrate, în mod temporar, în afara unei zone securizate sau a unei zone administrative, cu condiția ca deținătorul să se angajeze să respecte măsurile compensatorii stabilite în instrucțiunile de securitate emise de autoritatea de securitate competentă.

25. IUEC clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET pot fi gestionate:

(a) într-o zonă securizată;

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

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

(i) să transporte IUEC în condițiile prevăzute la anexa III, punctele 28-40;

(ii) s-a angajat să respecte măsurile compensatorii stabilite în instrucțiunile de securitate emise de autoritatea de securitate competentă pentru a se asigura că IUEC sunt protejate împotriva accesului persoanelor neautorizate;

(iii) menține IUEC în permanență sub controlul său personal; și

(iv) în cazul documentelor în format tipărit, a notificat registrul competent în această privință.

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

27. IUEC clasificate TRÈS SECRET UE/EU TOP SECRET sunt gestionate într-o zonă securizată.

28. IUEC clasificate TRÈS SECRET UE/EU TOP SECRET sunt păstrate într-o zonă securizată, în una dintre următoarele condiții:

(a) într-un container de securitate conform dispozițiilor punctului 8, și să beneficieze de unul sau mai multe din următoarele controale suplimentare:

(i) protecție continuă sau controale efectuate de personalul de securitate sau de serviciu posesor al unui certificat de securitate;

(ii) un SDI aprobat și personal de securitate de intervenție;

sau

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

29. Anexa III conține norme care reglementează transportul IUEC în afara zonelor protejate fizic.

VI. CONTROLUL CHEILOR ȘI AL COMBINAȚIILOR DE CIFRURI UTILIZATE PENTRU PROTECȚIA IUEC

30. Autoritatea de securitate competentă întocmește proceduri pentru gestionarea cheilor și a combinațiilor de cifruri pentru birouri, încăperi, camere tezaur și containere de securitate. Astfel de proceduri au rolul de a asigura protecția împotriva accesului neautorizat.

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

(a) cu ocazia oricărei schimbări de personal care cunoaște cifrul;

(b) de fiecare dată când intervine sau este suspectată compromiterea acestora;

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

(d) cel puțin la fiecare 12 luni.

ANEXA III

MANAGEMENTUL INFORMAȚIILOR CLASIFICATE

I. INTRODUCERE

1. Prezenta anexă stabilește dispozițiile pentru punerea în aplicare a articolului 9. Anexa stabilește măsurile administrative pentru controlul IUEC pe durata ciclului lor de viață, în scopul de a contribui la împiedicarea, detectarea și remedierea compromiterii deliberate sau accidentale a informațiilor de acest tip.

II. GESTIONAREA CLASIFICĂRILOR

Clasificări și marcaje

2. Informațiile se clasifică atunci când este necesară protecția confidențialității acestora.

3. Emitentul IUEC are responsabilitatea de a stabili nivelul de clasificare de securitate, în conformitate cu liniile directoare de clasificare relevante și de a efectua diseminarea inițială a informațiilor.

4. Nivelul de clasificare IUEC se stabilește în conformitate cu articolul 2 alineatul (2) și pe baza politicii de securitate care urmează să fie aprobată în conformitate cu articolul 3 alineatul (3).

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

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

7. Nivelul de clasificare general al unui document sau al unui dosar este cel puțin echivalent cu cel al componentei sale având cel mai ridicat nivel de clasificare. La compilarea unor informații din surse diferite, produsul final este reexaminat pentru a i se stabili nivelul general de clasificare de securitate, deoarece poate necesita o clasificare superioară celei atribuite părților sale componente.

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

9. Nivelul de clasificare al adreselor sau notelor care însoțesc documente clasificate trebuie să fie același cu cel mai ridicat nivel al documentelor atașate. Emitentul indică clar nivelul de clasificare pe care adresele sau notele îl vor avea după ce sunt separate de documentele atașate, de exemplu:

CONFIDENTIEL UE/EU CONFIDENTIAL

Fără anexă/anexe RESTREINT UE/EU RESTRICTED

Marcaje

10. În afară de marcajele clasificărilor de securitate stabilite la articolul 2 alineatul (2), IUEC pot purta marcajele suplimentare, precum:

(a) un element de identificare care desemnează emitentul;

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

(c) marcaje de comunicare;

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

Marcaje de clasificare abreviate

11. Pentru a indica nivelul de clasificare al anumitor alineate din text, pot fi utilizate marcaje de clasificare abreviate standardizate. Abrevierile nu înlocuiesc marcajele de clasificare complete.

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

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

Crearea IUEC

13. La crearea unui document UE clasificat:

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

(b) fiecare pagină este numerotată;

(c) documentul conține un număr de referință și un subiect care, în sine, nu reprezintă o informație clasificată, cu excepția cazului în care acestea sunt marcate ca atare;

(d) documentul este datat;

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

14. În cazul în care există IUEC cărora nu li se poate aplica punctul 13, se iau alte măsuri corespunzătoare în conformitate cu liniile directoare de securitate convenite în temeiul articolului 6 alineatul (2).

Scăderea nivelului de clasificare și declasificarea IUEC

15. În momentul elaborării documentului, emitentul indică, atunci când este posibil și în special pentru informații clasificate RESTREINT UE/EU RESTRICTED, dacă informațiilor UE clasificate le poate fi scăzut nivelul de clasificare sau dacă pot fi declasificate la o anumită dată sau în urma unui anumit eveniment.

16. SGC reexaminează IUEC pe care le deține în mod periodic, pentru a evalua necesitatea menținerii nivelului de clasificare. SGC stabilește un sistem de revizuire, cel puțin o dată la cinci ani, a nivelului de clasificare al IUEC înregistrate pe care le-a emis. O astfel de reexaminare nu este necesară în cazul în care emitentul a indicat de la început că informațiilor trebuie să li se scadă nivelul de clasificare sau că trebuie declasificată automat, iar informațiile au fost marcate în consecință.

III. ÎNREGISTRAREA IUEC DIN MOTIVE DE SECURITATE

17. Pentru fiecare entitate organizațională din cadrul SGC și din cadrul administrațiilor naționale ale statelor membre în care sunt gestionate IUEC este identificat un registru responsabil pentru a garanta gestionarea IUEC în conformitate cu prezenta decizie. Registrele sunt stabilite ca zone securizate în conformitate cu anexa II.

18. În sensul prezentei decizii, înregistrarea din motive de securitate (denumită în continuare „înregistrarea") înseamnă aplicarea unor proceduri care înregistrează ciclul de viață al materialului, inclusiv diseminarea și distrugerea acestuia.

19. Toate materialele clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL și la un nivel superior sunt înregistrate în registre desemnate ori de câte ori parvin unei entități organizaționale sau părăsesc entitatea respectivă.

20. Registrul central din cadrul SGC ține evidența tuturor informațiilor clasificate comunicate statelor terțe și organizațiilor internaționale de către Consiliu și SGC, precum și a tuturor informațiilor clasificate primite de la acestea.

21. În cazul unui SIC, procedurile de înregistrare pot fi efectuate prin procese din cadrul respectivului SIC.

22. Consiliul aprobă o politică de securitate privind înregistrarea IUEC din motive de securitate.

Registre TRÈS SECRET UE/EU TOP SECRET

23. În statele membre și în cadrul SGC se desemnează un registru care acționează ca principală autoritate de primire și diseminare a informațiilor clasificate TRÈS SECRET UE/EU TOP SECRET. Dacă este necesar, pot fi desemnate registre subordonate care să gestioneze astfel de informații în scopul înregistrării.

24. Aceste registre subordonate nu pot transmite direct documente TRÈS SECRET UE/EU TOP SECRET altor registre subordonate ale aceluiași registru central TRÈS SECRET UE/EU TOP SECRET sau unor destinatari externi în absența aprobării explicite a acestuia din urmă.

IV. COPIEREA ȘI TRADUCEREA DOCUMENTELOR CLASIFICATE UE

25. Documentele TRÈS SECRET UE/EU TOP SECRET nu pot fi copiate sau traduse decât cu consimțământul scris prealabil al emitentului.

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

27. Măsurile de securitate aplicabile documentului original se aplică copiilor și traducerilor acestuia.

V. TRANSPORTUL IUEC

28. Transportul IUEC respectă măsurile de protecție prevăzute la punctele 30-40. În cazul în care IUEC sunt transportate pe suporturi electronice și fără a aduce atingere articolului 9 alineatul (4), măsurile de protecție prevăzute mai jos pot fi suplimentate prin contramăsuri tehnice adecvate conform dispozițiilor autorității de securitate competente, astfel încât riscul pierderii sau compromiterii lor să fie redus la minim.

29. Autoritățile de securitate competente din cadrul SGC sau din statele membre emit instrucțiuni privind transportul IUEC în conformitate cu prezenta decizie.

În interiorul unei clădiri sau al unui grup autonom de clădiri

30. IUEC transportate în interiorul unei clădiri sau al unui grup autonom de clădiri sunt acoperite, astfel încât observarea conținutului acestora să fie împiedicată.

31. În interiorul unei clădiri sau al unui grup autonom de clădiri, informațiile clasificate TRÈS SECRET UE/EU TOP SECRET sunt transportate într-un plic securizat, menționând numai numele destinatarului.

În UE

32. IUEC transportate între clădiri sau incinte aflate în UE sunt ambalate astfel încât să fie protejate împotriva divulgării neautorizate.

33. Transportul informațiilor clasificate până la nivelul SECRET UE/EU SECRET pe teritoriul UE se efectuează prin următoarele mijloace:

(a) curier militar, guvernamental sau diplomatic, după caz;

(b) transport personal, în următoarele condiții:

(i) IUEC să nu iasă din posesia purtătorului, cu excepția cazului când acestea sunt păstrate în conformitate cu cerințele stabilite în anexa II;

(ii) IUEC să nu fie deschise pe drum sau citite în locuri publice;

(iii) persoanele să fie informate cu privire la responsabilitățile care le revin în materie de securitate;

(iv) să se acorde persoanelor un certificat de curier, dacă este necesar;

(c) servicii poștale sau servicii de curierat comercial, în următoarele condiții:

(i) să fie aprobate de ANS relevante în conformitate cu actele cu putere de lege și dispozițiile administrative naționale;

(ii) să ia alte măsuri de protecție corespunzătoare în conformitate cu cerințele minime care vor fi prevăzute în liniile directoare de securitate convenite în temeiul articolului 6 alineatul (2).

În cazul transportului dintr-un stat membru în alt stat membru, dispozițiile de la litera (c) se aplică numai informațiilor clasificate până la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL.

34. Materialele clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET (de exemplu, echipamente sau mașini) care nu pot fi transportate prin mijloacele prevăzute la punctul 33 sunt transportate ca marfă de societățile comerciale de curierat, în conformitate cu Anexa V.

35. Transportul informațiilor clasificate TRÈS SECRET UE/EU TOP SECRET între clădiri sau incinte din UE se efectuează prin curier militar, guvernamental sau diplomatic, după caz.

Din UE către teritoriul unui stat terț

36. IUEC transportate din UE către teritoriul unui stat terț sunt ambalate, astfel încât să fie protejate împotriva divulgării neautorizate.

37. Transportul informațiilor clasificate CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET din UE către teritoriul unui stat terț se efectuează prin următoarele mijloace:

(a) curier militar sau diplomatic;

(b) transport personal, în următoarele condiții:

(i) pachetul să poarte un sigiliu oficial sau să fie ambalat astfel încât să indice că este un transport oficial și nu trebuie supus controlului vamal sau verificărilor de securitate;

(ii) persoanele să dețină un certificat de curier care identifică pachetul și le autorizează să transporte pachetul;

(iii) IUEC să nu iasă din posesia purtătorului, cu excepția cazului când acestea sunt păstrate în conformitate cu cerințele stabilite în anexa II;

(iv) IUEC să nu fie deschise pe drum sau citite în locuri publice; și

(v) persoanele să fie informate cu privire la responsabilitățile care le revin în materie de securitate.

38. Transportul informațiilor clasificate CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET comunicate de UE unui stat terț sau unei organizații internaționale respectă dispozițiile relevante prevăzute de un acord privind securitatea informațiilor sau de un acord administrativ încheiat în conformitate cu articolul 12 alineatul (2) literele (a) și (b).

39. Informațiile clasificate RESTREINT UE/EU RESTRICTED pot fi, de asemenea, transportate prin intermediul serviciilor poștale sau al serviciilor de curierat comercial.

40. Transportul al informațiilor clasificate TRÈS SECRET UE/EU TOP SECRET din UE către teritoriul unui stat terț se efectuează prin curier militar sau diplomatic.

VI. DISTRUGEREA IUEC

41. Documentele UE clasificate care nu mai sunt necesare pot fi distruse, fără a se aduce atingere normelor și reglementărilor relevante privind arhivarea.

42. Documentele care trebuie înregistrate în conformitate cu articolul 9 alineatul (2) se distrug de către registrul responsabil la instrucțiunile deținătorului sau ale unei autorități competente. Registrele de evidență și alte informații de înregistrare sunt actualizate corespunzător.

43. În ceea ce privește documentele clasificate SECRET UE/EU SECRET sau TRÈS SECRET UE/EU TOP SECRET, distrugerea are loc în prezența unui martor, care deține un certificat de securitate de nivel cel puțin echivalent nivelului documentului distrus.

44. Gestionarul și martorul, în cazul în care este necesară prezența acestuia, semnează un proces-verbal de distrugere, care este păstrat la registru. Registrul păstrează procesele-verbale de distrugere a documentelor TRÈS SECRET UE/EU TOP SECRET o perioadă de cel puțin zece ani și a documentelor clasificate CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET o perioadă de cel puțin cinci ani.

45. Documentele clasificate, inclusiv cele clasificate RESTREINT UE/EU RESTRICTED, sunt distruse prin metode care îndeplinesc standardele relevante UE sau echivalente sau care au fost aprobate de statele membre în conformitate cu standardele tehnice naționale astfel încât să se împiedice reconstituirea lor totală sau parțială.

46. Distrugerea suporturilor informatice de stocare utilizate pentru IUEC se realizează în condițiile prevăzute în anexa IV punctul 36.

VII. INSPECȚII ȘI VIZITE DE EVALUARE

47. Termenul „inspecție" este folosit în continuare pentru a desemna orice:

(a) inspecție în conformitate cu articolul 9 alineatul (3) și cu articolul 15 alineatul (2) literele (e), (f) și (g); sau

(b) vizită de evaluare în conformitate cu articolul 12 alineatul (5),

având rolul de a evalua eficiența măsurilor aplicate pentru protecția IUEC.

48. Inspecțiile urmăresc, *inter alia*:

(a) asigurarea faptului că standardele minime necesare stabilite în prezenta decizie pentru protecția IUEC sunt respectate;

(b) sublinierea importanței securității și a unui management al riscului de securitate eficient în interiorul entităților inspectate;

(c) recomandarea unor contramăsuri pentru a atenua impactul specific al pierderii confidențialității, integrității sau disponibilității informațiilor clasificate; și

(d) consolidarea programelor de educație continuă și de conștientizare privind securitatea destinate autorităților de securitate.

49. Înainte de sfârșitul fiecărui an calendaristic, Consiliul adoptă programul de inspecții prevăzut la articolul 15 alineatul (1) litera (c) pentru anul următor. Datele efective ale fiecărei inspecții se stabilesc de comun acord cu agenția sau organismul UE, statul membru, statul terț sau organizația internațională interesată.

Desfășurarea inspecțiilor

50. Inspecțiile sunt efectuate pentru a verifica normele, regulamentele și procedurile relevante ale entității inspectate și a se asigura că practicile entității respectă principiile de bază și standardele minime stabilite în prezenta decizie și în dispozițiile care reglementează schimbul de informații clasificate cu entitatea respectivă.

51. Inspecțiile se desfășoară în două faze. Înaintea inspecției propriu-zise se organizează o reuniune pregătitoare, dacă este necesar, cu entitatea interesată. După această reuniune pregătitoare, echipa de inspecție stabilește, împreună cu entitatea menționată, un program de inspecție detaliat care acoperă toate domeniile de securitate. Echipa de inspecție are acces la toate locațiile în care se gestionează IUEC, în special la registre și la SIC.

52. Inspecțiile în cadrul administrațiilor naționale ale statelor membre se desfășoară sub responsabilitatea unei echipe mixte de inspecție a SGC/Comisiei, printr-o deplină cooperare cu funcționarii entității inspectate.

53. Inspecțiile în statele terțe și în organizațiile internaționale se desfășoară sub responsabilitatea unei echipe mixte de inspecție a SGC/Comisiei, printr-o deplină cooperare cu funcționarii statului terț sau ai organizației internaționale inspectate.

54. Inspecțiile în cadrul agențiilor și organismelor UE instituite în temeiul titlului V capitolul 2 din TUE, precum și în cadrul Europol și Eurojust, sunt desfășurate de Oficiul de Securitate al SGC, cu asistența experților ANS pe teritoriul căreia este situată agenția sau organismul. Direcția Securitate a Comisiei Europene (DSCE) poate fi asociată în cazul în care aceasta efectuează schimburi regulate de IUEC cu agenția sau organul în cauză.

55. În cazul inspecțiilor în cadrul agențiilor și organismelor UE instituite în temeiul titlului V capitolul 2 din TUE, precum și în cadrul Europol și Eurojust și în cazul inspecțiilor în state terțe și organizații internaționale, vor fi solicitate asistența și contribuțiile experților ANS, în conformitate cu măsurile detaliate care vor fi convenite de Comitetul de securitate.

Rapoarte de inspecție

56. La sfârșitul inspecției, entității inspectate i se prezintă principalele concluzii și recomandări. Ulterior se redactează un raport privind inspecția sub responsabilitatea autorității de securitate a SGC (Oficiul de Securitate). În cazurile în care s-au propus măsuri de remediere și recomandări, raportul cuprinde suficiente detalii pentru a sprijini concluziile obținute. Raportul este înaintat autorității competente din cadrul entității inspectate.

57. Pentru inspecțiile derulate în cadrul administrațiilor naționale ale statelor membre:

(a) proiectul raportului de inspecție este înaintat ANS interesate, pentru a i se verifica corectitudinea factuală și faptul că nu conține informații cu un nivel de clasificare superior față de RESTREINT UE/EU RESTRICTED;

(b) cu excepția cazului în care ANS a statului membru în cauză solicită împiedicarea distribuției generale, rapoartele de inspecție sunt trimise membrilor Comitetului de securitate și DSCE; raportul este clasificat la nivelul RESTREINT UE/EU RESTRICTED;

Sub responsabilitatea autorității de securitate a SGC (Oficiul de Securitate) se elaborează un raport periodic care ilustrează principalele concluzii desprinse în urma inspecțiilor desfășurate în statele membre într-o perioadă specificată și care este analizat de Comitetul de securitate.

58. În cazul vizitelor de evaluare în statele terțe și în cadrul organizațiilor internaționale, raportul este distribuit Comitetului de securitate și DSCE. Raportul este clasificat cel puțin la nivelul RESTREINT UE/EU RESTRICTED. Orice măsură de remediere este verificată în cursul unei vizite de monitorizare și raportată Comitetului de securitate.

59. În cazul inspecțiilor în cadrul agențiilor și organizațiilor UE instituite în temeiul titlului V capitolul 2 din TUE, precum și în cadrul Europol și Eurojust, rapoartele de inspecție sunt distribuite membrilor Comitetului de securitate și DSCE. Proiectul raportului de inspecție este înaintat agenției sau organului interesate, pentru a i se verifica corectitudinea factuală și faptul că nu conține informații cu un nivel de clasificare superior față de RESTREINT UE/EU RESTRICTED. Orice măsură de remediere este verificată în cursul unei vizite de monitorizare și raportată Comitetului de securitate.

60. Autoritatea de securitate a SGC desfășoară inspecții periodice ale entităților organizaționale ale SGC în scopurile enunțate la punctul 48.

Lista de control pentru inspecție

61. Autoritatea de securitate a SGC (Oficiul de securitate) elaborează și actualizează o listă de control pentru inspecții de securitate, cuprinzând aspectele care urmează să fie verificate în cursul unei inspecții. Lista de control respectivă este înaintată Comitetului de securitate.

62. Informațiile necesare pentru completarea listei de control sunt obținute în special în timpul inspecției de la personalul de conducere responsabil cu securitatea al entității inspectate. Odată completată cu răspunsurile detaliate, lista de control este clasificată în acord cu entitatea inspectată. Aceasta nu face parte din raportul de inspecție.

ANEXA IV

PROTECȚIA IUEC GESTIONATE ÎN SIC

I. INTRODUCERE

1. Prezenta anexă stabilește dispozițiile pentru punerea în aplicare a articolului 10.

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

Autenticitate:	garanția faptului că informațiile sunt originale și provin de la surse de bună credință;
Disponibilitate:	calitatea de a fi accesibile și utilizabile la cerere de către o entitate autorizată;
Confidențialitate:	proprietatea de a nu divulga informații persoanelor, entităților sau proceselor neautorizate;
Integritate:	proprietatea de a proteja acuratețea și caracterul complet al informațiilor și al activelor;
Nerepudiere:	capacitatea de a dovedi că o acțiune sau eveniment a avut loc, astfel încât să nu poată fi negate ulterior.

II. PRINCIPII DE ASIGURARE A INFORMAȚIILOR

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

Managementul riscului de securitate

4. Managementul riscului de securitate reprezintă o componentă esențială a definirii, dezvoltării, utilizării și întreținerii SIC. Managementul riscului (evaluarea, tratarea, acceptarea și comunicarea) se desfășoară sub forma unui proces iterativ, reunind reprezentanți ai proprietarilor de sisteme, autorităților de proiect, autorităților operaționale și autorităților de aprobare în materie de securitate, utilizând un proces de evaluare a riscului confirmat, transparent și ușor de înțeles. Domeniul SIC și al activelor sale este definit clar în momentul inițierii procesului de management al riscului.

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

6. Rolul tratării riscului de securitate este de a aplica un set de măsuri de securitate, care duc la un echilibru satisfăcător între cerințele utilizatorului, cost și riscul rezidual de securitate.

7. Cerințele specifice, scara și gradul de detaliere stabilite de AAS competentă pentru acreditarea unui SIC este proporțională cu riscul evaluat, luând seama de toți factorii relevanți, inclusiv nivelul de clasificare a IUEC gestionate în cadrul SIC. Acreditarea implică o declarație formală privind riscul rezidual și acceptarea riscului rezidual de către o autoritate responsabilă.

Securitatea pe parcursul ciclului de viață al SIC

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

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

10. Orice SIC, inclusiv măsurile sale de securitate tehnice și netehnice, face obiectul unor teste de securitate în cursul procesului de acreditare, pentru a se asigura obținerea unui nivel de asigurare corespunzător și a se verifica dacă măsurile respective sunt corect puse în aplicare, integrate și configurate.

11. Evaluările, inspecțiile și reexaminările de securitate sunt efectuate periodic, în cursul operării și al întreținerii unui SIC, precum și în împrejurări excepționale.

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

Cele mai bune practici

13. SGC și statele membre cooperează pentru a elabora cele mai bune practici pentru protejarea IUEC gestionate în SIC. Liniile directoare de bune practici descriu măsuri de securitate de ordin tehnic, fizic, organizatoric și procedural, pentru SIC, a căror eficacitate în contracararea unor amenințări și vulnerabilități a fost dovedită.

14. Protecția IUEC gestionate în SIC se bazează pe lecțiile învățate de entitățile implicate în AI, atât din interiorul, cât și din exteriorul UE.

15. Diseminarea și punerea în aplicare ulterioară a celor mai bune practici contribuie la atingerea unui nivel de asigurare echivalent pentru diversele SIC care gestionează IUEC și sunt operate de SGC și de statele membre.

Apărarea în profunzime

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

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

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

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

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

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

Gradul de strictețe a acestor măsuri de securitate este determinat în urma unei evaluări a riscului.

17. Autoritățile competente se asigură că au capacitatea de a reacționa la incidente care pot depăși limitele organizațiilor și ale statelor, în scopul coordonării reacțiilor și al partajării informațiilor cu terțe părți cu privire la astfel de incidente și riscuri conexe (capacități informatizate de reacție în situații de urgență).

Principiul minimului necesar și al privilegiului minim

18. În vederea evitării riscurilor care nu sunt necesare, sunt puse în aplicare numai funcțiile, dispozitivele și serviciile esențiale pentru îndeplinirea cerințelor operaționale.

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

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

Conștientizarea privind asigurarea informațiilor

21. Conștientizarea riscurilor și măsurile de securitate disponibile constituie prima linie de apărare pentru securitatea SIC. În special, toți membrii personalului implicați în ciclul de viață al SIC, inclusiv utilizatorii, înțeleg:

(a) că breșele de securitate pot afecta semnificativ SIC;

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

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

22. Pentru a garanta înțelegerea responsabilităților de securitate, educația cu privire la AI și formarea cu rol de conștientizare sunt obligatorii pentru tot personalul implicat, inclusiv personalul de conducere și utilizatorii SIC.

Evaluarea și aprobarea produselor de securitate IT

23. Gradul necesar de încredere în măsurile de securitate, definit ca nivel de asigurare, este determinat în urma rezultatului procesului de management al riscurilor și în conformitate cu politicile și liniile directoare de securitate relevante.

24. Gradul de încredere se verifică prin utilizarea unor procese și metodologii utilizate la nivel internațional sau aprobate la nivel național. Acestea includ în principal evaluare, controale și audit.

25. Produsele criptografice destinate protecției IUEC sunt evaluate și aprobate de o AAC națională a unui stat membru.

26. Înainte de a fi recomandate pentru aprobare de către Consiliu sau de către Secretarul General, în conformitate cu articolul 10 alineatul (6), aceste produse criptografice sunt supuse unei evaluări de către o a doua parte, efectuată de o autoritate calificată adecvat (ACA) a unui stat membru neimplicat în concepția sau fabricarea echipamentului. Gradul de detaliere necesar în cursul evaluării a celei de a doua părți depinde de nivelul maxim de clasificare al IUEC care urmează să fie protejate prin aceste produse. Consiliul aprobă o politică de securitate privind evaluarea și aprobarea produselor criptografice.

27. Dacă acest lucru este justificat de motive operaționale specifice, Consiliul sau Secretarul General pot, după caz, la recomandarea Comitetului de securitate, să acorde derogări de la cerința prevăzută la punctul 25 sau 26 și să acorde o aprobare provizorie pentru o anumită perioadă în conformitate cu procedura prevăzută la articolul 10 alineatul (6).

28. ACA este o AAC (autoritate de aprobare criptografică) a unui stat membru, acreditată pe baza unor criterii stabilite de Consiliu pentru a efectua cea de a doua evaluare a produselor criptografice pentru protejarea IUEC.

29. Consiliul aprobă o politică de securitate privind calificarea și aprobarea produselor de securitate IT necriptografice.

Transmiterea în cadrul zonelor securizate

30. Fără a aduce atingere dispozițiilor prezentei decizii, în cazul în care transmiterea IUEC este limitată la zone securizate, distribuția necriptată sau criptarea la nivel inferior pot fi folosite, pe baza rezultatului unui proces de gestionare a riscurilor și cu condiția aprobării AAS.

Interconectări securizate ale SIC

31. În sensul prezentei decizii, o interconectare reprezintă conectarea directă a două sau mai multe sisteme IT în scopul partajării datelor și a altor resurse informaționale (de exemplu, de comunicații) în mod unidirecțional sau multidirecțional.

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

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

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

(b) interconectarea este supusă unui proces de management al riscului și de acreditare și necesită aprobarea AAS competente; și

(c) sunt puse în aplicare servicii de protecție a perimetrului (Boundary Protection Services – BPS) în perimetrul tuturor SIC.

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

Dacă rețeaua neprotejată sau publică este utilizată numai ca transportator și informațiile sunt criptate prin intermediul unui produs criptografic aprobat în conformitate cu articolul 10, o astfel de conexiune nu este considerată ca fiind o interconectare.

35. Este interzisă interconectarea directă sau în cascadă a unui SIC acreditat să gestioneze informații TRÈS SECRET UE/EU TOP SECRET la rețele neprotejate sau publice.

Suporturile informatice de stocare

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

37. Suporturilor informatice de stocare le poate fi scăzut nivelul de clasificare sau acestea pot fi declasificate în conformitate cu o politică de securitate instituită în conformitate cu articolul 6 alineatul (1).

Situații de urgență

38. Fără a aduce atingere dispozițiilor prezentei decizii, procedurile specifice descrise în continuare pot fi aplicate într-o situație de urgență, cum ar fi înaintea sau în timpul unor crize, conflicte sau situații de război sau în cazul unor împrejurări operaționale excepționale.

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

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

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

40. Informațiile clasificate transmise în împrejurările enunțate la punctul 38 nu poartă niciun marcaj sau indicație care să le distingă de orice informații neclasificate sau care pot fi protejate cu ajutorul unui produs de criptare disponibil. Destinatarilor le este notificat fără întârziere nivelul de clasificare, prin alte mijloace.

41. Dacă se acționează în temeiul dispozițiilor de la punctul 38, se înaintează un raport ulterior autorității competente și Comitetului de securitate.

III. FUNCȚII ȘI AUTORITĂȚI DE ASIGURARE A INFORMAȚIILOR

42. În statele membre și la SGC se stabilesc următoarele funcții aferente AI. Aceste funcții nu necesită entități organizaționale unice. Ele au mandate separate. Cu toate acestea, aceste funcții și responsabilitățile care le corespund pot fi grupate sau integrate în aceeași entitate organizațională sau distribuite în entități organizaționale diferite, cu condiția să fie evitate conflictele interne de interese sau de sarcini.

Autoritatea de asigurare a informațiilor

43. AAI este responsabilă cu:

(a) elaborarea de politici de securitate și linii directoare de securitate privind AI și monitorizarea eficienței și pertinenței acestora;

(b) protejarea și gestionarea informațiilor tehnice privind produsele criptografice;

(c) asigurarea compatibilității dintre măsurile AI selectate pentru protejarea IUEC și politicile relevante care reglementează eligibilitatea și selecția acestora;

(d) asigurarea selectării produselor criptografice în conformitate cu politicile care reglementează eligibilitatea și selecția acestora;

(e) coordonarea formării și conștientizării cu privire la AI;

(f) consultarea furnizorului de sistem, a actorilor din domeniul securității și a reprezentanților utilizatorilor cu privire la politicile de securitate și la liniile directoare de securitate privind AI; și

(g) asigurarea disponibilității expertizei adecvate în cadrul subdomeniului de experți al Comitetului de securitate pentru chestiunile AI.

Autoritatea TEMPEST

44. Autoritatea TEMPEST (AT) este responsabilă cu asigurarea conformității SIC cu politicile și liniile directoare TEMPEST. Aceasta aprobă contramăsurile TEMPEST pentru instalațiile și produsele de protecție a IUEC la un anumit nivel de clasificare, în mediul său operațional.

Autoritatea de aprobare criptografică

45. Autoritatea de aprobare criptografică (AAC) este responsabilă pentru asigurarea conformității produselor criptografice cu politica națională sau a Consiliului în domeniul criptografiei. Aceasta acordă aprobarea unui produs criptografic pentru protejarea IUEC la un anumit nivel de clasificare, în mediul său operațional. În ceea ce privește statele membre, AAC este, în plus, responsabilă cu evaluarea produselor criptografice.

Autoritatea de distribuire a materialului criptografic

46. Autoritatea de distribuire a materialului criptografic (ADMC) este responsabilă cu:

(a) gestionarea și evidența materialului criptografic al UE;

(b) garantarea impunerii unor proceduri și a stabilirii unor canale pentru evidența, gestionarea securizată, păstrarea și distribuirea întregului material criptografic al UE; și

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

Autoritatea de acreditare în materie de securitate

47. AAS este responsabilă, pentru fiecare sistem, cu:

(a) asigurarea respectării de către SIC a politicilor de securitate și a liniilor directoare de securitate relevante, stabilirea unei declarații de aprobare a SIC în vederea gestionării IUEC la un anumit nivel de clasificare, în mediul său operațional, stabilirea termenilor și a condițiilor acreditării, precum și a criteriilor pentru determinarea obligativității reaprobării;

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

(c) definirea unei strategii de acreditare de securitate, stabilind un grad de detaliere a procesului de acreditare proporțional cu nivelul de asigurare cerut;

(d) examinarea și aprobarea documentației de securitate, inclusiv a declarațiilor privind managementul riscului și riscul rezidual, a declarațiilor privind cerințele de securitate specifice sistemului (denumite în continuare CSSS), a documentației de verificare a aplicării securității și procedurilor operaționale de securitate (denumite în continuare SecOP) și asigurarea conformității acestora cu normele și politicile de securitate ale Consiliului;

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

(f) definirea cerințelor de securitate (precum nivelul autorizațiilor pentru personal) pentru pozițiile sensibile în relație cu SIC;

(g) aprobarea selecției produselor criptografice și TEMPEST utilizate pentru asigurarea securității unui SIC;

(h) aprobarea sau, după caz, participarea la aprobarea comună a interconectării unui SIC cu alte SIC; și

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

48. AAS din cadrul SGC este responsabilă cu acreditarea tuturor SIC care funcționează în subordinea SGC.

49. AAS relevantă a unui stat membru este responsabilă pentru acreditarea SIC și a componentelor din cadrul acestuia care funcționează în subordinea unui stat membru.

50. Un consiliu mixt de acreditare în materie de securitate (CAS) este responsabil cu acreditarea SIC din domeniul de competență atât a AAS a SGC, cât și a AAS ale statelor membre. Acesta este compus dintr-un reprezentant al AAS din fiecare stat membru, iar la lucrările sale participă un reprezentant AAS al Comisiei Europene. Alte entități, care dispun de puncte de conectare la un SIC, sunt invitate să participe, atunci când discuțiile privesc respectivul sistem.

CAS este prezidat de un reprezentant al AAS a SGC. Acesta hotărăște prin consensul reprezentanților AAS ale instituțiilor, statelor membre și altor entități care au puncte de conectare la SIC. CAS înaintează Comitetului de securitate rapoarte periodice cu privire la activitățile sale și notifică în acestea toate declarațiile de acreditare.

Autoritatea operațională de asigurare a informațiilor

51. Autoritatea operațională AI este responsabilă, pentru fiecare sistem, cu:

(a) elaborarea unei documentații de securitate, în conformitate cu politicile de securitate și liniile directoare de securitate, în special a CSSS, inclusiv a declarației privind riscul rezidual, a SecOP și a planului criptografic în cadrul procesului de acreditare a SIC;

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

(c) participarea la selectarea măsurilor de securitate și a dispozitivelor TEMPEST, dacă sunt necesare în cadrul CSSS, și garantarea instalării și întreținerii lor securizate în cooperare cu AT;

(d) monitorizarea punerii în aplicare și a aplicării SecOP având posibilitatea, după caz, de a delega responsabilitățile în materie de securitate operațională proprietarului sistemului;

(e) gestionarea și tratarea produselor criptografice, asigurând custodia elementelor criptografice și a elementelor controlate și, după caz, asigurarea generării de variabile criptografice;

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

(g) furnizarea de formare AI specifică SIC;

(h) punerea în aplicare și utilizarea unor măsuri de securitate specifice SIC.

ANEXA V

SECURITATEA INDUSTRIALĂ

I. INTRODUCERE

1. Prezenta anexă stabilește dispozițiile pentru punerea în aplicare a articolului 11. Aceasta cuprinde dispoziții generale în materie de securitate aplicabile entităților industriale sau de altă natură în cursul negocierilor anterioare încheierii contractelor și pe toată durata contractelor clasificate încheiate de SGC.

2. Consiliul aprobă o politică privind securitatea industrială descriind în special cerințe detaliate referitoare la CSI, anexa de securitate (AS), vizite, transmiterea și transportul IUEC.

II. ELEMENTE DE SECURITATE ÎNTR-UN CONTRACT CLASIFICAT

Ghidul clasificărilor de securitate (GCS)

3. Înainte de a iniția o procedură de ofertare sau de a încheia un contract clasificat, SGC, în calitate de autoritate contractantă, stabilește clasificarea de securitate a oricăror informații care urmează a fi furnizate ofertanților și contractanților, precum și clasificarea de securitate a oricăror informații care urmează să fie create de contractant. În acest scop, SGC elaborează un GCS care urmează să fie folosit pentru executarea contractului.

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

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

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

(c) atunci când este cazul, SGC ia legătura cu ANS/ADS ale statelor membre sau cu orice altă autoritate de securitate competentă implicată, în cazul unor schimbări în ceea ce privește clasificarea informațiilor create de contractanți sau furnizate acestora în cursul executării contractului sau în cazul oricăror modificări ulterioare ale GCS.

Anexa de securitate (AS)

5. Cerințele de securitate specifice contractului sunt descrise în AS. AS cuprinde, atunci când este cazul, GCS și constituie o parte integrantă a contractului sau a subcontractului clasificat.

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

Instrucțiuni de securitate pentru program/proiect (ISP)

7. În funcție de domeniul de aplicare al programelor sau proiectelor care implică accesul, gestionarea sau păstrarea IUEC, pot fi elaborate instrucțiuni de securitate pentru program/proiect (ISP) de către autoritatea contractantă desemnată să gestioneze respectivul program sau proiect. ISP necesită aprobarea de către ANS/ADS sau de către oricare alte autorități de securitate competente ale statelor membre care participă la program/proiect și pot conține cerințe de securitate suplimentare.

III. CERTIFICATUL DE SECURITATE INDUSTRIALĂ (CSI)

8. CSI se acordă de către ANS/ADS sau de către orice altă autoritate de securitate competentă a unui stat membru pentru a atesta că, în conformitate cu actele cu putere de lege și dispozițiile administrative naționale, o entitate industrială sau de altă natură poate proteja IUEC la nivelul de clasificare adecvat (CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET) în interiorul obiectivelor sale. CSI trebuie prezentat SGC, în calitate de autoritate contractantă, înainte ca unui contractant sau subcontractant, sau unui potențial contractant sau subcontractant, să îi poată fi furnizat sau acordat accesul la IUEC.

9. La eliberarea unui CSI, ANS sau ADS relevantă asigură cel puțin:

(a) evaluarea integrității entității industriale sau de altă natură;

(b) evaluarea regimului de proprietate, a controlului sau a potențialului de exersare a unei influențe necuvenite care ar putea fi considerată un risc de securitate;

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

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

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

10. După caz, SGC, în calitate de autoritate contractantă, înștiințează ANS/ADS adecvată sau orice altă autoritate de securitate competentă că este necesar un CSI, fie în etapa precontractuală, fie pentru executarea contractului. Este necesar un CSI sau la CSP în etapa precontractuală în cazul în care trebuie furnizate IUEC clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET pe parcursul procesului de licitare.

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

12. ANS/ADS sau orice altă autoritate de securitate competentă care a eliberat un CSI notifică SGC, în calitate de autoritate contractantă, în legătură cu orice modificări care afectează CSI. În cazul subcontractelor, ANS/ADS sau orice altă autoritate de securitate competentă este informată în mod corespunzător.

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

IV. CONTRACTE ȘI SUBCONTRACTE CLASIFICATE

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

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

16. În cazul în care un astfel de contract încetează, SGC, în calitate de autoritate contractantă (și/sau ANS/ADS sau orice altă autoritate de securitate competentă, după caz, în cazul subcontractelor) notifică de îndată ANS/ADS sau orice altă autoritate de securitate competentă a statului membru în care este înregistrat contractantul sau subcontractantul.

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

18. Dispoziții specifice privind înlăturarea IUEC în timpul executării contractului sau la încheierea acestuia sunt prevăzute în AS.

19. În cazul în care contractantul sau subcontractantul este autorizat să rețină IUEC după încheierea unui contract, standardele minime cuprinse în prezenta decizie sunt respectate în continuare și confidențialitatea IUEC este protejată de către contractant sau subcontractant.

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

21. Un contractant obține permisiunea SGC, în calitate de autoritate contractantă, înainte de a subcontracta părți ale unui contract clasificat. Nu se atribuie subcontracte entităților industriale sau de altă natură înregistrate într-un stat care nu este membru al UE care nu a încheiat un acord privind securitatea informațiilor cu UE.

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

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

V. VIZITE PRIVIND CONTRACTELE CLASIFICATE

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

25. Accesul vizitatorilor la IUEC legate de contractul SGC se acordă pe baza deținerii unui CSP corespunzător și a respectării principiului necesității de a cunoaște.

26. Vizitatorilor li se acordă accesul numai la IUEC legate de scopul vizitei.

VI. TRANSMITEREA ȘI TRANSPORTUL IUEC

27. În ceea ce privește transmiterea IUEC prin mijloace electronice, se aplică dispozițiile relevante de la articolul 10 și din anexa IV.

28. În ceea ce privește transportul IUEC, se aplică dispozițiile relevante din anexa III, în conformitate cu actele cu putere de lege și dispozițiile administrative naționale.

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

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

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

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

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

(e) călătoriile sunt directe ori de câte ori este posibil și sunt finalizate cât mai repede, în funcție de împrejurări;

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

VII. TRANSFERUL IUEC CĂTRE CONRACTANȚII AFLAȚI ÎN STATE TERȚE

30. IUEC sunt transferate contractanților și subcontractanților aflați în state terțe în conformitate cu măsurile de securitate convenite între SGC, în calitate de autoritate contractantă, și ANS/ADS a statului terț implicat în care este înregistrat contractantul.

VIII. GESTIONAREA ȘI PĂSTRAREA IUEC CLASIFICATE RESTREINT UE/EU RESTRICTED

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

32. În măsura în care este necesar în temeiul actelor cu putere de lege și dispozițiilor administrative naționale, ASN/ADS sau orice altă autoritate de securitate competentă este înștiințată de SGC, în calitatea sa de autoritate contractantă, cu privire la contractele sau subcontractele care conțin informații clasificate RESTREINT UE/EU RESTRICTED.

33. Pentru contractele încheiate de SGC care conțin informații clasificate RESTREINT UE/EU RESTRICTED nu se solicită CSI sau CSP contractanților sau subcontractanților și personalului acestora.

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

35. Condițiile pe care trebuie să le îndeplinească contractantul pentru a putea subcontracta trebuie să fie conforme cu punctul 21.

36. Atunci când contractul necesită gestionarea informațiilor clasificate RESTREINT UE/EU RESTRICTED într-un SIC gestionat de un contractant, SGC, în calitatea sa de autoritate contractantă, se asigură că în contract sau în eventuale subcontracte, se specifică cerințele tehnice și administrative necesare în ceea ce privește acreditarea SIC, proporționale cu riscul evaluat, luându-se în considerare toți factorii relevanți. Domeniul de acreditare al unui astfel de SIC este convenit de autoritatea contractantă cu ANS/ADS competentă.

ANEXA VI

SCHIMBUL DE INFORMAȚII CLASIFICATE CU STATE TERȚE ȘI ORGANIZAȚII INTERNAȚIONALE

I. INTRODUCERE

1. Prezenta anexă stabilește dispozițiile pentru punerea în aplicare a articolului 12.

II. CADRE CARE REGLEMENTEAZĂ SCHIMBUL DE INFORMAȚII CLASIFICATE

2. În cazul în care Consiliul stabilește că există o necesitate pe termen lung de schimb de informații clasificate:

— se încheie un acord privind securitatea informațiilor; sau

— se încheie un acord administrativ,

în conformitate cu articolul 12 alineatul (2) și cu secțiunile III și IV și pe baza unei recomandări a Comitetului de securitate.

3. În cazul în care IUEC generate pentru o operație PSAC urmează să fie puse la dispoziția unor state terțe sau organizații internaționale care participă la respectiva operație și nu există niciun cadru dintre cele prevăzute la punctul (2), schimbul de IUEC cu statul terț sau organizația internațională participantă este reglementat, în conformitate cu secțiunea V, de:

— un acord-cadru de participare;

— un acord de participare ad hoc; sau

— în absența oricăruia dintre acordurile de mai sus, un acord administrativ ad hoc.

4. În lipsa unuia dintre cadrele menționate la punctele 2 și 3 și în cazul în care se adoptă o decizie privind comunicarea IUEC unui stat terț sau unei organizații internaționale pe bază excepțională ad hoc, în conformitate cu secțiunea VI, statului terț sau organizației internaționale respective i se solicită garanții scrise pentru a se asigura că protejează orice IUEC care i-au fost comunicate, în conformitate cu principiile de bază și standardele minime stabilite în prezenta decizie.

III. ACORDURILE PRIVIND SECURITATEA INFORMAȚIILOR

5. Acordurile privind securitatea informațiilor stabilesc principiile de bază și standardele minime care reglementează schimbul de informații clasificate între UE și un stat terț sau o organizație internațională.

6. Acordurile privind securitatea informațiilor prevăd măsuri tehnice de punere în aplicare care urmează a fi convenite între Oficiul de Securitate al SGC, DSCE și autoritatea de securitate competentă a statului terț sau a organizației internaționale în cauză. Aceste măsuri țin seama în mod corespunzător de nivelul de protecție prevăzut de regulamentele de securitate, structurile și procedurile existente în statul terț sau organizația internațională în cauză. Aceste măsuri se aprobă de către Comitetul de securitate.

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

8. Acordurile privind securitatea informațiilor prevăd că anterior schimbului de informații clasificate în temeiul acordului, Oficiul de Securitate al SGC și DSCE convin că destinatarul este capabil să protejeze și să apere în mod corespunzător informațiile care îi sunt puse la dispoziție.

9. Atunci când Consiliul încheie un acord de securitate a informațiilor, se desemnează un registru pentru fiecare parte, ca principal punct de intrare și ieșire pentru schimbul de informații clasificate.

10. Pentru a evalua eficiența regulamentelor, a structurilor și a procedurilor de securitate din statul terț sau din organizația internațională interesată, sunt organizate vizite de evaluare de către Oficiul de Securitate al SGC împreună cu DSCE, de comun acord cu statul terț sau cu organizația internațională în cauză. Aceste vizite de evaluare se desfășoară în conformitate cu dispozițiile relevante din anexa III și evaluează:

(a) cadrul de reglementare aplicabil pentru protecția informațiilor clasificate;

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

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

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

11. Echipa care desfășoară o vizită de evaluare în numele UE evaluează dacă regulamentele și procedurile de securitate ale statului terț sau ale organizației internaționale în cauză sunt adecvate pentru protecția IUEC la un anumit nivel.

12. Rezultatele unor astfel de vizite sunt prezentate într-un raport pe baza căruia Comitetul de securitate stabilește nivelul maxim al IUEC care pot fi comunicate în format tipărit și, după caz, în format electronic părții terțe interesate, precum și condițiile care reglementează schimbul cu această parte.

13. Se întreprind toate demersurile necesare desfășurării unei vizite complete de evaluare a securității în statul terț sau organizația internațională în cauză înainte de aprobarea de către Comitetul de securitate a măsurilor de punere în aplicare pentru stabilirea tipului și eficienței sistemului de securitate existent. Cu toate acestea, dacă acest lucru nu este posibil, Comitetul de securitate primește un raport cât mai complet din partea Oficiului de Securitate al SGC, bazat pe informațiile de care acesta dispune, prin care se informează Comitetul de securitate asupra regulamentelor de securitate aplicabile și asupra modului în care este organizată securitatea în statele terțe sau organizațiile internaționale în cauză.

14. Comitetul de securitate poate decide ca, până la formularea concluziilor unei vizite de evaluare, IUEC nu pot fi comunicate, sau pot fi comunicate numai până la un anumit nivel, sau poate stabili alte condiții specifice care reglementează comunicarea IUEC către statul terț sau organizația internațională în cauză. Acest lucru trebuie comunicat de către Oficiul de Securitate al SGC statului terț sau organizației internaționale în cauză.

15. De comun acord cu statul terț sau cu organizația internațională în cauză, Oficiul de Securitate al SGC desfășoară, la intervale periodice, vizite de evaluare cu rol de monitorizare pentru a verifica dacă măsurile existente respectă în continuare standardele minime convenite.

16. Odată ce acordul privind securitatea informațiilor intră în vigoare, iar informațiile clasificate sunt schimbate cu statul terț sau organizația internațională în cauză, Comitetul de securitate poate decide să modifice nivelul maxim al IUEC care pot fi schimbate în format tipărit sau electronic, în special din perspectiva oricărei vizite ulterioare de evaluare.

IV. ACORDURI ADMINISTRATIVE

17. În cazul în care există o necesitate pe termen lung de schimb de informații clasificate, ca regulă generală, cel mult la nivelul RESTREINT UE/EU RESTRICTED, cu un stat terț sau o organizație internațională, dar Comitetul de securitate a stabilit că partea în cauză nu deține un sistem de securitate suficient de dezvoltat pentru a permite încheierea unui acord privind securitatea informațiilor, Secretarul General poate, sub rezerva aprobării de către Consiliu, să încheie un acord administrativ cu autoritățile competente ale statului terț sau ale organizației internaționale în cauză.

18. În cazul în care, din motive operaționale urgente, este necesară instituirea rapidă a unui cadru pentru schimbul de informații clasificate, Consiliul poate decide, în mod excepțional, încheierea unui acord administrativ pentru schimbul de informații având un nivel de clasificare mai ridicat.

19. Ca regulă generală, acordurile administrative iau forma unui schimb de scrisori.

20. Înaintea comunicării efective a IUEC către statul terț sau organizația internațională în cauză are loc o vizită de evaluare, menționată la punctul 10, iar raportul este înaintat Comitetului de securitate și aprobat de acesta. Cu toate acestea, în cazul în care intervin motive excepționale pentru schimbul urgent de informații clasificate, aduse în atenția Consiliului, pot fi comunicate IUEC, cu condiția să se ia toate măsurile necesare pentru organizarea vizitei de evaluare cât mai curând.

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

V. SCHIMBUL DE INFORMAȚII CLASIFICATE ÎN CONTEXTUL OPERAȚIILOR PSAC

22. Acordurile-cadru de participare reglementează participarea statelor terțe sau a organizațiilor internaționale la operațiile PSAC. Aceste acorduri includ dispoziții privind comunicarea IUEC generate pentru operațiile PSAC către statele terțe sau organizațiile internaționale contribuitoare. Nivelul maxim de clasificare al IUEC care pot fi schimbate este RESTREINT UE/EU RESTRICTED pentru operații civile PSAC și CONFIDENTIEL UE/EU CONFIDENTIAL pentru operații militare PSAC, cu excepția situațiilor în care se prevede altfel în decizia de instituire a fiecărei operații PSAC.

23. Acordurile de participare ad hoc încheiate pentru o anumită operație PSAC includ dispoziții privind comunicarea IUEC generate pentru această operație statului terț sau organizației internaționale contribuitoare. Nivelul maxim de clasificare al IUEC care pot fi schimbate este RESTREINT UE/EU RESTRICTED pentru operații civile PSAC și CONFIDENTIEL UE/EU CONFIDENTIAL pentru operații militare PSAC, cu excepția situațiilor în care se prevede altfel în decizia de instituire a fiecărei operații PSAC

24. Acordurile administrative ad hoc privind participarea unui stat terț sau a unei organizații internaționale la o anumită operație PSAC pot reglementa, *inter alia*, comunicarea către statul terț sau organizația internațională în cauză a IUEC generate în scopul operației. Astfel de acorduri administrative ad hoc se încheie în conformitate cu procedurile stabilite la punctele 17 și 18 de la secțiunea IV de mai sus. Nivelul maxim de clasificare al IUEC care pot fi schimbate este RESTREINT UE/EU RESTRICTED pentru operații civile PSAC și CONFIDENTIEL UE/EU CONFIDENTIAL pentru operații militare PSAC, cu excepția situațiilor în care se prevede altfel în decizia de instituire a fiecărei operații PSAC.

25. Nu sunt necesare măsuri de punere în aplicare sau vizite de evaluare înaintea punerii în aplicare a dispozițiilor privind comunicarea IUEC în contextul punctelor 22, 23 și 24.

26. În cazul în care statul-gazdă pe teritoriul căruia se desfășoară o operație PSAC nu a încheiat niciun acord privind securitatea informațiilor sau acord administrativ cu UE în vederea schimbului de informații clasificate, în cazul unei nevoi operaționale specifice și imediate poate fi instituit un acord administrativ ad hoc. Această posibilitate este prevăzută în decizia de instituire a operației PSAC. IUEC comunicate în astfel de împrejurări se limitează la cele generate în scopurile operației PSAC și sunt clasificate cel mult la nivelul RESTREINT UE/EU RESTRICTED. În temeiul unui astfel de acord administrativ ad hoc, statul-gazdă se angajează să protejeze IUEC în conformitate cu standarde cel puțin la fel de stricte precum cele stabilite prin prezenta decizie.

27. Dispozițiile privind informațiile clasificate care urmează să fie incluse în acordurile-cadru de participare, acordurile de participare ad hoc și acordurile administrative ad hoc menționate la punctele 22-24 prevăd că statul terț sau organizația internațională în cauză se asigură că personalul său, detașat în cadrul oricărei operații, va proteja IUEC în conformitate cu normele de securitate ale Consiliului și cu îndrumările suplimentare elaborate de autoritățile competente, inclusiv de lanțul de comandă al operației.

28. Dacă un stat terț sau organizație internațională contribuitoare încheie ulterior cu UE un acord privind securitatea informațiilor, acesta prevalează asupra oricărui acord-cadru de participare, acord de participare ad hoc sau acord administrativ ad hoc, din punctul de vedere al schimbului și al gestionării IUEC.

29. Schimbul de IUEC prin mijloace electronice este permis în cadrul unui acord-cadru de participare, al unui acord de participare ad hoc sau al unui acord administrativ ad hoc cu un stat terț sau o organizație internațională numai dacă acest lucru este prevăzut explicit în acordul în cauză.

30. IUEC generate pentru o operație PSAC pot fi divulgate personalului detașat în cadrul respectivei operații de către statele terțe sau organizațiile internaționale în condițiile prevăzute la punctele 22-29. În cadrul autorizării accesului personalului menționat la IUEC în incintele sau în SIC ale unei operații PSAC, sunt luate măsuri (inclusiv înregistrarea IUEC divulgate) pentru a se reduce riscul pierderii sau al compromiterii. Măsurile de acest fel sunt definite în documentele relevante de planificare sau în documentele de misiune.

VI. COMUNICAREA AD HOC EXCEPȚIONALĂ A IUEC

31. În cazul în care nu există niciun cadru în conformitate cu secțiunile III-V, iar Consiliul sau unul dintre organismele sale pregătitoare stabilește necesitatea excepțională a comunicării IUEC către un stat terț sau organizație internațională, SGC:

(a) în măsura posibilului, verifică împreună cu autoritățile de securitate ale statului terț sau ale organizației internaționale în cauză dacă regulamentele, structurile și procedurile de securitate ale acestora garantează faptul că IUEC comunicate vor fi protejate la standarde la fel de stricte precum cele stabilite de prezenta decizie;

(b) invită Comitetul de securitate, pe baza informațiilor disponibile, să emită o recomandare privind încrederea care poate fi acordată regulamentelor, structurilor și procedurilor de securitate din statul terț sau organizația internațională care urmează să fie destinatarul IUEC.

32. În cazul în care Comitetul de securitate emite o recomandare favorabilă comunicării IUEC, chestiunea este prezentată Comitetului reprezentanților permanenți (COREPER), care adoptă o decizie privind comunicarea acestora.

33. În cazul în care recomandarea Comitetului de securitate nu este în favoarea comunicării IUEC:

(a) pentru chestiuni legate de PESC/PSAC, Comitetul politic și de securitate discută chestiunea și formulează o recomandare pentru decizia care urmează a fi luată de COREPER;

(b) pentru toate celelalte chestiuni, COREPER discută chestiunea și ia o decizie.

34. Atunci când acest lucru este considerat oportun și sub rezerva consimțământului scris prealabil al emitentului, COREPER poate decide ca informațiile clasificate să fie comunicate numai parțial, sau numai după ce au fost declasificate sau li s-a scăzut nivelul de clasificare, sau ca informațiile care urmează să fie comunicate să fie pregătite fără a face trimitere la sursă sau la nivelul UE inițial de clasificare.

35. Pe baza deciziei de comunicare a IUEC, SGC înaintează documentul în cauză, care poartă un marcaj de comunicare care indică statul terț sau organizația internațională destinatară. Înaintea sau în timpul comunicării efective, partea terță în cauză se angajează în scris să protejeze IUEC primite în conformitate cu principiile de bază și standardele minime stabilite în prezenta decizie.

VII. COMPETENȚA DE A COMUNICA IUEC CĂTRE STATE TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

36. În cazul în care există un cadru, în conformitate cu punctul (2), pentru schimbul de informații clasificate cu un stat terț sau o organizație internațională, Consiliul adoptă o decizie de autorizare a Secretarului General să comunice IUEC, în conformitate cu principiul consimțământului emitentului, către statul terț sau organizația internațională în cauză.

37. În cazul în care există un cadru, în conformitate cu punctul 3, pentru schimbul de informații clasificate cu un stat terț sau o organizație internațională, Secretarul General este autorizat să comunice IUEC, în conformitate cu decizia de instituire a operației PSAC și cu principiul consimțământului emitentului.

38. Secretarul General poate delega această autorizare funcționarilor superior ai SGC sau altor persoane din subordinea sa.

Apendice

Apendicele A

Definiții

Apendicele B

Echivalența clasificărilor de securitate

Apendicele C

Lista autorităților naționale de securitate (ANS)

Apendicele D

Lista de abrevieri

Apendicele A

DEFINIȚII

În sensul prezentei decizii, se aplică următoarele definiții:

„Acreditarea” reprezintă procesul care duce la o declarație formală a autorității de acreditare în materie de securitate (AAS), potrivit căreia un sistem deține aprobarea de a funcționa cu un nivel de clasificare definit, într-un anumit mod de securitate, în mediul său operațional și la un nivel de risc acceptabil, pe baza premisei că a fost pus în aplicare un set aprobat de măsuri de securitate de ordin tehnic, fizic, organizațional și procedural.

„Activ” înseamnă orice reprezintă o valoare pentru o organizație, pentru operațiunile de funcționare a acesteia și continuitatea acestora, inclusiv resursele informaționale care sprijină misiunea organizației.

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

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

„Apărarea în profunzime” înseamnă aplicarea unor măsuri de securitate organizate pe niveluri de apărare multiple.

„Asigurarea informațiilor” – a se vedea articolul 10 alineatul (1).

„Autoritate desemnată de securitate” (ADS) înseamnă o autoritate care răspunde în fața autorității naționale de securitate (ANS) a unui stat membru, însărcinată să comunice entităților industriale sau de altă natură politica națională în materie de securitate industrială și să ofere indicații și asistență pentru punerea în aplicare a acesteia. Atribuțiile ADS pot fi îndeplinite de ANS sau de orice altă autoritate competentă.

„Certificat de securitate a personalului” (CSP) înseamnă unul dintre lucrurile următoare sau ambele:

— „Certificatul UE de securitate a personalului UE” (CSP UE) pentru accesul la IUEC înseamnă o autorizare acordată de autoritatea responsabilă cu numirile din cadrul SGC, adoptată în conformitate cu prezenta decizie după încheierea unei investigații de securitate efectuate de autoritățile competente ale unui stat membru și care garantează faptul că unei persoane îi poate fi acordat accesul la IUEC până la un nivel precizat (CONFIDENTIEL UE/EU CONFIDENTIAL sau superior) până la o anumită dată, odată ce a fost stabilită necesitatea de a cunoaște în cazul său; se consideră că persoana astfel descrisă deține „certificatul de securitate”;

— „Certificatul național de securitate a personalului” (CSP național) pentru accesul la IUEC înseamnă o declarație a unei autorități competente a unui stat membru, dată după încheierea unei investigații de securitate efectuate de autoritățile competente ale unui stat membru și care garantează faptul că unei persoane îi poate fi acordat accesul la IUEC până la un nivel precizat (CONFIDENTIEL UE/EU CONFIDENTIAL sau superior) până la o anumită dată, odată ce a fost stabilită necesitatea de a cunoaște în cazul său; se consideră că persoana astfel descrisă deține „certificatul de securitate”.

„Certificat de securitate industrială” (CSI) înseamnă o decizie administrativă a ANS sau ADS conform căreia, în ceea ce privește securitatea, un obiectiv poate oferi un nivel de protecție adecvat IUEC clasificate cu un anumit nivel de clasificare a securității, iar personalul său căruia trebuie să i se acorde acces la IUEC beneficiază de certificatul de securitate în acest sens și a fost informat cu privire la cerințele relevante de securitate necesare pentru a avea acces la IUEC și a le proteja.

„Ciclul de viață al SIC” înseamnă întreaga durată a existenței unui SIC, care include inițierea, conceperea, planificarea, analiza cerințelor, proiectarea, dezvoltarea, testarea, implementarea, utilizarea, mentenanța și dezafectarea.

„Confirmarea privind deținerea certificatului de securitate a personalului” (CCSP) înseamnă un certificat eliberat de o autoritate competentă care stabilește că o persoană deține certificatul de securitate și deține un CSP național sau un CSP UE valabil și care indică nivelul IUEC la care este permis accesul persoanei respective (CONFIDENTIEL UE/EU CONFIDENTIAL sau superior), perioada de valabilitate a CSP respectiv și data expirării confirmării în cauză.

„Contract clasificat” înseamnă un contract încheiat de SGC cu un contractant pentru livrarea de bunuri, executarea de lucrări sau prestarea de servicii, a cărui executare necesită sau implică accesul la IUEC sau crearea acestora.

„Contractant” înseamnă o persoană fizică sau juridică având capacitatea juridică de a încheia contracte.

„Declasificare” înseamnă eliminarea clasificării de securitate.

„Deținător” înseamnă o persoană autorizată corespunzător cu privire la care s-a stabilit necesitatea de a cunoaște, care se află în posesia unei informații UE clasificate și, în consecință, răspunde de protecția acesteia.

„Document” reprezintă orice informație înregistrată, indiferent de forma sau caracteristicile sale fizice.

„Emitent” înseamnă instituția, agenția sau organismul UE, statul membru, statul terț sau organizația internațională sub a cărei autoritate s-au creat și/sau introdus în structurile UE informațiile clasificate.

„Entitate industrială sau de altă natură” înseamnă o entitate care livrează bunuri, execută lucrări sau furnizează servicii; aceasta poate fi o entitate industrială, comercială, de prestări de servicii, din domeniul științific, de cercetare, educațională sau de dezvoltare ori o persoană fizică autorizată.

„Gestionarea” IUEC înseamnă toate acțiunile posibile al căror obiect îl pot face IUEC de-a lungul ciclului lor de viață. Aceasta cuprinde crearea, prelucrarea, transportul, scăderea nivelului de clasificare, declasificarea și distrugerea. În relație cu SIC, aceasta cuprinde, de asemenea, colectarea, afișarea și păstrarea.

„Ghidul clasificărilor de securitate” (GCS) înseamnă un document care descrie elementele unui program sau ale unui contract clasificat, precizând nivelurile aplicabile de protecție a informațiilor. GCS poate fi extins pe toată durata programului sau a contractului respectiv, iar informațiile pot fi reclasificate sau le poate fi scăzut nivelul de clasificare; în cazul în care există un GCS, acesta face parte din AS.

„Informații UE clasificate” (IUEC) – a se vedea articolul 2 alineatul (1).

„Instrucțiuni de securitate pentru program/proiect” (ISP) înseamnă o listă de proceduri de securitate care sunt aplicate unui program/proiect specific în scopul standardizării procedurilor de securitate. Acestea pot fi revizuite pe parcursul programului/proiectului.

„Interconectare” – a se vedea anexa IV, punctul 31.

„Investigație de securitate” înseamnă procedurile de investigare derulate de autoritatea națională competentă a unui stat membru, în conformitate cu actele cu putere de lege și dispozițiile administrative naționale din statul membru în cauză, pentru a garanta că nu se cunosc fapte adverse, care să împiedice o persoană să beneficieze de un CSP național sau UE în vederea accesului la IUEC până la un nivel precizat (CONFIDENTIEL UE/EU CONFIDENTIAL sau superior).

„Înregistrare” – a se vedea anexa III, punctul 18.

„Managementul informațiilor clasificate” – a se vedea articolul 9 alineatul (1).

„Material criptografic (criptat)” înseamnă algoritmi criptografici, module criptografice hardware și software și produse care includ detalii privind punerea în aplicare și materialele asociate de documentare și cele legate de chei.

„Materiale” reprezintă orice document sau obiect de tip mașină sau echipament, fabricat sau în proces de fabricație.

„Mod de operare de securitate” înseamnă definirea condițiilor în care funcționează un SIC pe baza clasificării informațiilor gestionate și a nivelului certificatelor, a aprobărilor de acces formale și a necesității de a cunoaște a utilizatorilor acestuia. Există patru moduri de operare pentru gestionarea sau transmiterea informațiilor clasificate: modul dedicat, modul de nivel înalt, modul compartimentat și modul multinivel:

— „mod dedicat” înseamnă un mod de operare în care toate persoanele care au acces la SIC sunt autorizate la cel mai înalt nivel de clasificare a informațiilor gestionate în cadrul SIC și au o necesitate comună de a cunoaște toate informațiile gestionate în cadrul SIC;

— „mod de nivel înalt” înseamnă un mod de operare în care toate persoanele care au acces la SIC dețin un certificat pentru cel mai înalt nivel de clasificare a informațiilor gestionate în cadrul SIC, dar nu toate persoanele care au acces la SIC au o necesitate comună de a cunoaște informațiile gestionate în cadrul SIC; aprobarea pentru accesul la informații poate fi acordată de o persoană;

— „mod compartimentat” înseamnă un mod de operare în care toate persoanele care au acces la SIC dețin un certificat pentru cel mai înalt nivel de clasificare a informațiilor gestionate în cadrul SIC, dar nu toate persoanele care au acces la SIC au o autorizație formală pentru acces la toate informațiile gestionate în cadrul SIC; autorizația formală se bazează pe gestionarea formală la nivel central a controlului accesului și nu pe voința unei persoane de a acorda accesul;

— „mod multinivel" înseamnă un mod de operare în care nu toate persoanele care au acces la SIC dețin un certificat pentru cel mai înalt nivel de clasificare a informațiilor gestionate în SIC respectiv și nu toate persoanele care au acces la SIC au o necesitate comună de a cunoaște informațiile gestionate în cadrul SIC.

„Operație PSAC" înseamnă o operație militară sau civilă de gestionare a crizelor în temeiul titlului V capitolul 2 din TUE.

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

„Risc" reprezintă posibilitatea ca o anumită amenințare să exploateze vulnerabilitățile interne și externe ale unei organizații sau a oricăruia dintre sistemele pe care aceasta le utilizează și, în consecință, să cauzeze un prejudiciu organizației sau activelor sale corporale sau necorporale. Riscul se măsoară sub forma combinației dintre probabilitatea materializării amenințărilor și impactul acestora:

— „acceptarea riscului" este decizia, după tratarea riscului, de a accepta existența în continuare a unui risc rezidual;

— „evaluarea riscului" reprezintă identificarea amenințărilor și a vulnerabilităților și efectuarea analizei riscurilor conexe, respectiv analiza de probabilitate și de impact;

— „comunicarea riscului" reprezintă realizarea conștientizării riscurilor în rândurile comunităților de utilizatori ai SIC, informarea autorităților de aprobare cu privire la aceste riscuri și raportarea lor către autoritățile operaționale;

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

„Riscul rezidual" reprezintă riscul care persistă după punerea în aplicare a măsurilor de securitate, ținând seama de faptul că nu toate amenințările sunt contracarate și nu toate vulnerabilitățile pot fi eliminate.

„Scăderea nivelului de securitate" înseamnă atribuirea unui nivel de clasificare inferior.

„Securitate industrială" – a se vedea articolul 11 alineatul (1).

„Securitatea fizică" – a se vedea articolul 8 alineatul (1).

„Securitatea personalului" – a se vedea articolul 7 alineatul (1).

„Sistem informatic și de comunicații" (SIC) – a se vedea articolul 10 alineatul (2).

„Subcontract clasificat" înseamnă un contract încheiat de un contractant al SGC cu un alt contractant (respectiv, subcontractantul) pentru livrarea de bunuri, executarea de lucrări sau prestarea de servicii, a cărui executare necesită sau implică accesul la IUEC sau crearea acestora.

„TEMPEST" înseamnă investigarea, studiul și controlul emisiilor electromagnetice compromițătoare și măsurile de eliminare a acestora.

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

Apendicele B

ECHIVALENȚA CLASIFICĂRILOR DE SECURITATE

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Belgia	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	*nota ([1]) de mai jos*
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Republica Cehă	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danemarca	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Germania	STRENG GEHEIM	GEHEIM	VS ([2])— VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irlanda	Top Secret	Secret	Confidential	Restricted
Grecia	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spania	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Franța	Très Secret Défense	Secret Défense	Confidentiel Défense	*nota ([3]) de mai jos*
Italia	Segretissimo	Segreto	Riservatissimo	Riservato
Cipru	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Letonia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lituania	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Ungaria	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Țările de Jos	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polonia	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalia	Muito Secreto	Secreto	Confidencial	Reservado
România	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Slovenia	Strogo tajno	Tajno	Zaupno	Interno
Slovacia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finlanda	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Suedia (4)	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Regatul Unit	Top Secret	Secret	Confidential	Restricted

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

(2) Germania: VS = Verschlusssache.

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

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

Apendicele C

LISTA AUTORITĂȚILOR NAȚIONALE DE SECURITATE (ANS)

BELGIA
Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
B-1000 Bruxelles

Telefon secretariat: + 32/2/501 45 42
Fax: + 32/2/501 45 96
E-mail: nvo-ans@diplobel.fed.be

DANEMARCA
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
DK-2860 Søborg

Telefon: + 45/33/14 88 88
Fax: + 45/33/43 01 90

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
DK-2100 Copenhagen Ø

Telefon: + 45/33/32 55 66
Fax: + 45/33/93 13 20

BULGARIA
State Commission on Information Security
90 Cherkovna Str.
BG-1505 Sofia

Telefon: + 359/2/921 5911
Fax: + 359/2/987 3750
E-mail: dksi@government.bg
Website: www.dksi.bg

GERMANIA
Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin

Telefon: + 49/30/18 681 0
Fax: + 49/30/18 681 1441
E-mail: oesIII3@bmi.bund.de

REPUBLICA CEHĂ
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
CZ-150 06 Praha 56

Telefon: + 420/257 28 33 35
Fax: + 420/257 28 31 10
E-mail: czech.nsa@nbu.cz
Website: www.nbu.cz

ESTONIA
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
EE-15094 Tallinn

Telefon: +372/7170 113, +372/7170 117
Fax: +372/7170 213
E-mail: nsa@kmin.ee

IRLANDA
National Security Authority
Department of Foreign Affairs
76 - 78 Harcourt Street
Dublin 2 Ireland

Telefon: + 353/1/ 478 08 22
Fax: + 353/1/ 408 29 59

SPANIA
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
E-28023 Madrid

Telefon: + 34/91/372 50 00
Fax: + 34/91/372 58 08
E-mail: nsa-sp@areatec.com

GRECIA
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα

Τηλέφωνα: + 30/210/657 20 45 (ώρες γραφείου)
+ 30/210/657 20 09 (ώρες γραφείου)
Φαξ: + 30/210/653 62 79
+ 30/210/657 76 12

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos – Athens

Telefon: + 30/210/657 20 45
+ 30/210/657 20 09
Fax: + 30/210/653 62 79
+ 30/210/657 76 12

FRANȚA
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
F-75700 Paris 07 SP

Telefon: + 33/1/71 75 81 77
Fax: + 33/1/71 75 82 00

ITALIA
Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
D.I.S. - U.C.Se.
Via di Santa Susanna, 15
I-00187 Roma

Telefon: + 39/06/611 742 66
Fax: + 39/06/488 52 73

CIPRU
ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος

Τηλέφωνα: + 357/22/80 75 69, + 357/22/80 76 43,
+ 357/22/80 77 64
Τηλεομοιότυπο: + 357/22/30 23 51

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
CY-1432 Nicosia

Telefon: + 357/22/80 75 69, + 357/22/80 76 43,
+357 /22/80 77 64
Fax: + 357/22/30 23 51
E-mail: cynsa@mod.gov.cy

LUXEMBURG
Autorité nationale de Sécurité
Boîte postale 2379
L-1023 Luxembourg

Telefon: + 352/2478 22 10 (centrală)
+ 352/2478 22 53 (număr direct)
Fax: + 352/2478 22 43

UNGARIA
Nemzeti Biztonsági Felügyelet
(National Security Authority)
P.O. Box 2
HU-1357 Budapest

Telefon: + 361/346 96 52
Fax: + 361/346 96 58
E-mail: nbf@nbf.hu
Website: www.nbf.hu

MALTA
Ministry of Justice and Home Affairs
P.O. Box 146
MT-Valletta

Telefon: + 356/21 24 98 44
Fax: + 356/25 69 53 21

LETONIA
National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV-1001 Riga

Telefon: + 371/6702 54 18
Fax: + 371/6702 54 54
Email: ndi@sab.gov.lv

LITUANIA
Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania
National Security Authority)
Gedimino 40/1
LT-01110 Vilnius

Telefon: + 370/5/266 32 01,
+ 370/5/266 32 02
Fax: + 370/5/266 32 00
E-mail: nsa@vsd.lt

ȚĂRILE DE JOS
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
NL-2500 EA Den Haag

Telefon: + 31/70/320 44 00
Fax: + 31/70/320 07 33

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
NL-2500 ES Den Haag

Telefon: + 31/70/318 70 60
Fax: + 31/70/318 75 22

AUSTRIA
Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
A-1014 Wien

Telefon: + 43/1/531 15 25 94
Fax: + 43/1/531 15 26 15
E-mail: ISK@bka.gv.at

POLONIA
Agencja Bezpieczeństwa Wewnętrznego – ABW
(Internal Security Agency)
2A Rakowiecka St.
PL-00-993 Warszawa

Telefon: + 48/22/585 73 60
Fax: + 48/22/585 85 09
E-mail: nsa@abw.gov.pl
Website: www.abw.gov.pl

Służba Kontrwywiadu Wojskowego
(Military Counter-Intelligence Service)
Classified Information Protection Bureau
Oczki 1
PL-02-007 Warszawa

Telefon: + 48/22/684 12 47
Fax: + 48/22/684 10 76
E-mail: skw@skw.gov.pl

ROMÂNIA
Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA – ORNISS
National Registry Office for Classified Information)
str. Mureș, nr. 4,
sector 1 RO-012275 București

Telefon: + 40 21 2245830
Fax: + 40 21 2240714
E-mail: nsa.romania@nsa.ro
Website: www.orniss.ro

PORTUGALIA
Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
P-1300-342 Lisboa

Telefon: +351/ 213 031 710
Fax: +351/ 213 031 711

SLOVENIA
Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
SVN-1000 Ljubljana

Telefon: + 386/1/478 13 90
Fax: + 386/1/478 13 99

SLOVACIA
Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
SVK-850 07 Bratislava

Telefon: + 421/2/68 69 23 14
Fax: + 421/2/63 82 40 05
Website: www.nbusr.sk

SUEDIA
Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
S-103 39 Stockholm

Telefon: + 46/8/405 10 00
Fax: + 46/8/723 11 76
E-mail: ud-nsa@foreign.ministry.se

FINLANDA
National Security
Authority Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government

Telefon 1: + 358/9/160 56487
Telefon 2: +358/9/160 56484
Fax: + 358/9/160 55140
E-mail: NSA@formin.fi

REGATUL UNIT
UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS

Telefon 1: + 44/20/7276 5649
Telefon 2: + 44/20/7276 5497
Fax: + 44/20/7276 5651
Email: UK-NSA@cabinet-office.x.gsi.gov.uk

Appendicele D

LISTA ABREVIERILOR

Acronim	Sens
AAC	autoritate de aprobare criptografică
AAI	autoritate pentru asigurarea informațiilor
AAS	autoritate de acreditare în materie de securitate
ACA	autoritate calificată adecvat
ADC	autoritate de distribuție criptografică
ADS	autoritatea desemnată de securitate
AI	asigurarea informațiilor
ANS	autoritatea națională de securitate
AS	anexa de securitate
AT	autoritate TEMPEST
CAS	consiliu mixt de acreditare în materie de securitate
CCSP	confirmare privind deținerea certificatului de securitate a personalului
CCTV	televiziune cu circuit închis
COREPER	Comitetul reprezentanților permanenți
CSI	certificat de securitate industrială
CSP	certificat de securitate a personalului
DCSS	declarații privind cerințele de securitate specifice unui sistem
DSCE	Direcția Securitate a Comisiei Europene
GCS	Ghidul clasificărilor de securitate
IDS	sisteme de detectare a intruziunilor
ISP	instrucțiuni de securitate pentru program/proiect
IT	tehnologia informației
IUEC	informații UE clasificate
PESC	Politica externă și de securitate comună
PSAC	Politica de securitate și apărare comună
RSUE	Reprezentant Special al UE
SecOP	proceduri operaționale de securitate
SGC	Secretariatul General al Consiliului
SIC	sisteme informatice și de comunicații care gestionează IUEC
SPL	servicii de protecție a limitelor