Jurnalul Oficial C 126

al Uniunii Europene

Anul 61

Ediția în limba română **Comunicări și informări** 10 aprilie 2018

Cuprins

RO

IV

(Informări)

INFORMĂRI PROVENIND DE LA INSTITUȚIILE, ORGANELE ȘI ORGANISMELE UNIUNII EUROPENE

SERVICIUL EUROPEAN DE ACȚIUNE EXTERNĂ

Decizia Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate din 19 septembrie 2017 privind normele de securitate pentru Serviciul European de Acțiune Externă

ADMIN(2017) 10

(2018/C 126/01)

ÎNALTUL REPREZENTANT AL UNIUNII PENTRU AFACERI EXTERNE ȘI POLITICA DE SECURITATE,

având în vedere Decizia 2010/427/UE a Consiliului din 26 iulie 2010 privind organizarea și funcționarea Serviciului European de Acțiune Externă ([1]) („SEAE”),

având în vedere avizul comitetului menționat la articolul 9 alineatul (6) din Decizia Înaltului Reprezentant din 15 iunie 2011 privind normele de securitate pentru Serviciul European de Acțiune Externă ([2]),

întrucât:

(1) SEAE, în calitate de organism al Uniunii Europene (UE) care își desfășoară activitatea în mod autonom, ar trebui să dispună de norme de securitate, astfel cum se prevede la articolul 10 alineatul (1) din Decizia 2010/427/UE.

(2) Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate (denumit în continuare „Înaltul Reprezentant” sau „ÎR”) ar trebui să decidă cu privire la norme de securitate pentru SEAE care să acopere toate aspectele de securitate legate de funcționarea SEAE, astfel încât SEAE să poată gestiona în mod eficace riscurile la adresa personalului aflat sub responsabilitatea sa, a activelor sale corporale, a informațiilor și a vizitatorilor și să își poată îndeplini responsabilitățile în privința obligației de diligență.

(3) În special, ar trebui garantat un nivel de protecție pentru personalul aflat sub responsabilitatea SEAE, pentru activele corporale ale SEAE, inclusiv pentru sistemele informatice și de comunicații, pentru informații și pentru vizitatori, care să corespundă celor mai bune practici din cadrul Consiliului, al Comisiei, al statelor membre și, după caz, din cadrul organizațiilor internaționale.

(4) Normele de securitate pentru SEAE ar trebui să contribuie la realizarea unui cadru general mai coerent și cuprinzător în interiorul UE pentru protejarea informațiilor UE clasificate (denumite în continuare „IUEC”), pe baza normelor de securitate ale Consiliului Uniunii Europene (denumit în continuare „Consiliul”) și a dispozițiilor în materie de securitate ale Comisiei Europene și menținând o coerență cât mai mare cu acestea.

(5) SEAE, Consiliul și Comisia se angajează să aplice standarde de securitate echivalente pentru protecția IUEC.

(6) 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.

([1]) JO L 201, 3.8.2010, p. 30.
([2]) JO C 304, 15.10.2011, p. 7.

(7) Este necesar să se stabilească modalitățile de organizare a securității în cadrul SEAE și de repartizare a sarcinilor de securitate în cadrul structurilor SEAE.

(8) Înaltul Reprezentant ar trebui să se bazeze pe expertiza relevantă a statelor membre, a Secretariatului General al Consiliului și a Comisiei, în funcție de necesități.

(9) Înaltul Reprezentant ar trebui să ia toate măsurile corespunzătoare necesare pentru punerea în aplicare a acestor norme, cu sprijinul statelor membre, al Secretariatului General al Consiliului și al Comisiei.

(10) Secretarul general al SEAE este autoritatea de securitate a SEAE, iar la articolul 1 din Decizia ADMIN (2015) 34 din 14 septembrie 2015 a Secretarului general al Serviciului European de Acțiune Externă se prevede că atribuțiile în materie de securitate ale autorității de securitate, astfel cum sunt prevăzute în normele de Securitate ale SEAE, se exercită de către Directorul general pentru buget și administrație,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Obiectiv și domeniu de aplicare

Prezenta decizie stabilește normele de securitate pentru Serviciul European de Acțiune Externă (denumite în continuare „normele de securitate pentru SEAE").

În temeiul articolului 10 alineatul (1) din Decizia 2010/427/UE a Consiliului din 26 iulie 2010 privind organizarea și funcționarea Serviciului European de Acțiune Externă, prezenta decizie se aplică tuturor membrilor personalului SEAE și tuturor membrilor personalului din delegațiile Uniunii, indiferent de funcția lor administrativă sau de originea lor, și stabilește cadrul de reglementare general pentru gestionarea eficace a riscurilor la adresa personalului aflat sub responsabilitatea SEAE, astfel cum este definit la articolul 2, la adresa incintelor, a activelor corporale, a informațiilor și a vizitatorilor SEAE.

Articolul 2

Definiții

În sensul prezentei decizii, se aplică următoarele definiții:

(a) „personalul SEAE" înseamnă funcționarii și alți agenți ai SEAE, inclusiv membrii personalului din cadrul serviciilor diplomatice ale statelor membre numiți în funcție în calitate de agenți temporari, și experții naționali detașați, astfel cum sunt definiți la articolul 6 din Decizia 2010/427/UE a Consiliului din 26 iulie 2010 privind organizarea și funcționarea Serviciului European de Acțiune Externă;

(b) „personalul aflat sub responsabilitatea SEAE" înseamnă personalul SEAE care își desfășoară activitatea la sediu și în delegațiile Uniunii și toți ceilalți membri ai personalului din delegațiile Uniunii, indiferent de funcția lor administrativă sau de originea lor, precum și, în contextul prezentei decizii, Înaltul Reprezentant și, după caz, alte categorii de personal aflat în incintele sediului SEAE;

(c) „persoane aflate în întreținere" înseamnă membrii de familie ai membrului personalului aflat sub responsabilitatea SEAE în delegațiile Uniunii care fac parte din gospodăria respectivă, astfel cum au fost notificați Ministerului Afacerilor Externe al statului gazdă;

(d) „incintele SEAE" înseamnă toate unitățile SEAE, inclusiv clădiri, birouri, săli și alte spații, precum și spațiile în care sunt amplasate sistemele informatice și de comunicații (inclusiv cele care manipulează IUEC), în care SEAE desfășoară activități permanente sau temporare;

(e) „interesele în materie de securitate ale SEAE" înseamnă personalul aflat sub responsabilitatea SEAE, incintele, persoanele aflate în întreținere, activele corporale, inclusiv sistemele informatice și de comunicații, informațiile și vizitatorii SEAE;

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

(g) „delegație a Uniunii” înseamnă delegațiile din țările terțe și din cadrul organizațiilor internaționale, astfel cum sunt menționate la articolul 1 alineatul (4) din Decizia 2010/427/UE a Consiliului din 26 iulie 2010 privind organizarea și funcționarea Serviciului European de Acțiune Externă.

Alte definiții sunt enumerate în anexele relevante și în apendicele A.

Articolul 3

Obligația de diligență

(1) Normele de securitate pentru SEAE au ca scop îndeplinirea responsabilităților SEAE în privința obligației de diligență.

(2) Obligația de diligență a SEAE cuprinde diligența necesară pentru adoptarea tuturor măsurilor rezonabile destinate punerii în aplicare a măsurilor de securitate pentru prevenirea prejudiciilor previzibile în mod rezonabil la adresa intereselor în materie de securitate ale SEAE.

Aceasta cuprinde atât elemente de securitate, cât și de siguranță, inclusiv elemente care rezultă din situații de urgență sau de criză, indiferent de natura lor.

(3) Având în vedere responsabilitatea în privința obligației de diligență a statelor membre, a instituțiilor sau organelor UE și a altor părți care au personal în delegațiile Uniunii și/sau în incintele delegațiilor Uniunii sau o astfel de responsabilitate care revine SEAE atunci când delegațiile Uniunii sunt găzduite în incinte aparținând altor părți menționate mai sus, SEAE încheie acorduri administrative cu fiecare dintre entitățile menționate mai sus, prin care sunt stabilite rolurile și responsabilitățile, sarcinile și mecanismele de cooperare ale fiecăreia.

Articolul 4

Securitatea fizică și a infrastructurii

(1) SEAE instituie toate măsurile adecvate de securitate fizică (permanente sau temporare), inclusiv modalități de control al accesului, în toate incintele SEAE, pentru protejarea intereselor în materie de securitate ale SEAE. Astfel de măsuri sunt adoptate luând în considerare conceperea și planificarea incintelor noi sau înainte de închirierea unor incinte existente.

(2) Din considerente de securitate, se pot impune obligații sau restricții speciale personalului aflat sub responsabilitatea SEAE și persoanelor aflate în întreținere, pentru o anumită perioadă de timp și în anumite spații.

(3) Măsurile menționate la alineatele (1) și (2) sunt proporționale cu riscurile evaluate.

Articolul 5

Stările de alertă și gestionarea situațiilor de criză

(1) Autoritatea de securitate a SEAE, astfel cum este definită la articolul 13 alineatul (1) secțiunea I, este responsabilă de instituirea măsurilor adecvate privind stările de alertă pentru a anticipa sau pentru a răspunde la amenințările și incidentele care afectează securitatea în cadrul SEAE și de instituirea măsurilor necesare pentru gestionarea situațiilor de criză.

(2) Măsurile privind stările de alertă menționate la alineatul (1) trebuie să fie proporționale cu nivelul de amenințare la adresa securității. Nivelurile stării de alertă trebuie definite în strânsă cooperare cu serviciile competente ale celorlalte instituții, agenții și organe ale Uniunii și ale statului membru ori ale statelor membre pe teritoriul cărora se află incinte ale SEAE.

(3) Autoritatea de securitate a SEAE este punctul de contact pentru stările de alertă și gestionarea situațiilor de criză.

Articolul 6

Protecția informațiilor clasificate

(1) Protecția IUEC este reglementată de cerințele prevăzute în prezenta decizie și în special în anexa A. Deținătorul oricărei IUEC este responsabil de protejarea în consecință a acesteia.

(2) SEAE se asigură că accesul la informațiile clasificate este acordat numai persoanelor care îndeplinesc condițiile prevăzute la articolul 5 din anexa A.

(3) Condițiile în care agenții locali pot avea acces la IUEC sunt, de asemenea, stabilite de Înaltul Reprezentant, în conformitate cu normele pentru protecția IUEC prevăzute în anexa A la prezenta decizie.

(4) Direcția SEAE responsabilă de securitate gestionează o bază de date privind certificatele de securitate ale tuturor membrilor personalului aflat sub responsabilitatea SEAE și ale contractanților SEAE.

(5) În cazul în care statele membre introduc în structurile sau în rețelele SEAE informații clasificate care poartă un marcaj național de clasificare a securității, SEAE protejează aceste informații în conformitate cu cerințele aplicabile IUEC de nivel echivalent, astfel cum se prevede în tabelul de echivalență a clasificărilor de securitate din apendicele B la prezenta decizie.

(6) Spațiile din cadrul SEAE în care sunt păstrate informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior sau informațiile clasificate la un nivel echivalent sunt stabilite ca zone securizate în conformitate cu normele aplicabile în temeiul anexei A II la prezenta decizie și sunt aprobate de către autoritatea de securitate a SEAE.

(7) Procedurile pentru exercitarea responsabilităților Înaltului Reprezentant în cadrul acordurilor sau al acordurilor administrative pentru schimbul de IUEC cu state terțe sau cu organizații internaționale sunt descrise în anexele A și A VI la prezenta decizie.

(8) Secretarul general stabilește condițiile în care SEAE poate transmite altor instituții, agenții și organe ale Uniunii IUEC pe care le deține. Va fi instituit în acest sens un cadru adecvat, inclusiv prin încheierea de acorduri interinstituționale sau de alte tipuri de acorduri, după caz.

(9) Orice astfel de cadru trebuie să asigure faptul că se acordă IUEC o protecție care este adecvată în raport cu nivelul de clasificare al acestor informații și care este conformă cu principii de bază și standarde minime echivalente celor prevăzute în prezenta decizie.

Articolul 7

Incidente de securitate și situații de urgență

(1) În vederea asigurării unei reacții prompte și eficace la incidentele de securitate, SEAE stabilește un proces de raportare a acestor incidente și situații de urgență care să fie operațional douăzeci și patru de ore pe zi, șapte zile pe săptămână și care să acopere orice tip de incidente de securitate sau de amenințări la adresa intereselor în materie de securitate ale SEAE (de exemplu, accidente, conflicte, acțiuni răuvoitoare, acte criminale, situații de răpire sau de luare de ostatici, urgențe medicale, incidente legate de sistemele informatice și de comunicații, atacuri cibernetice etc.).

(2) Se stabilesc canale de legătură de urgență între sediul SEAE, delegațiile Uniunii, Consiliu, Comisie, reprezentanții speciali ai UE și statele membre, pentru a îi sprijini în gestionarea incidentelor de securitate în care este implicat personalul și a consecințelor acestora, inclusiv în planificarea pentru situații de urgență.

(3) Această gestionare a incidentelor în materie de securitate cuprinde, printre altele:

— procedurile pentru sprijinirea efectivă a procesului decizional în ceea ce privește un incident de securitate în care este implicat personalul, inclusiv a deciziilor referitoare la retragerea personalului sau suspendarea unei misiuni; și

— o politică și proceduri pentru recuperarea personalului – de exemplu, în cazul dispariției unui membru al personalului sau în situații de răpire și luare de ostatici – luând în considerare responsabilitățile specifice ale statelor membre, ale instituțiilor UE și ale SEAE în această privință. Necesitatea de a avea la dispoziție capacități specifice, în cadrul gestionării unor astfel de operațiuni în această privință, este avută în vedere ținând cont de resursele care ar putea fi furnizate de statele membre.

(4) SEAE instituie măsuri administrative adecvate pentru raportarea incidentelor de securitate din delegațiile Uniunii. După caz, trebuie informate statele membre, Comisia, orice alte autorități relevante, precum și comitetele relevante în materie de securitate.

(5) Procesele de gestionare a incidentelor ar trebui testate și revizuite periodic.

Articolul 8

Securitatea sistemelor informatice și de comunicații

(1) SEAE protejează informațiile manipulate în sistemele informatice și de comunicații („SIC") împotriva amenințărilor la adresa confidențialității, integrității, disponibilității, autenticității și nerepudierii.

(2) Autoritatea de securitate a SEAE aprobă norme și orientări de securitate, precum și un program de securitate pentru protejarea tuturor SIC deținute sau operate de SEAE.

(3) Normele, politica și programul sunt conforme cu cele ale Consiliului și ale Comisiei și, după caz, cu politicile de securitate aplicate de statele membre și sunt puse în aplicare în strânsă coordonare cu acestea.

(4) Toate SIC care manipulează informații clasificate fac obiectul unui proces de acreditare. SEAE aplică un sistem pentru gestionarea acreditării de securitate în consultare cu Secretariatul General al Consiliului și cu Comisia.

(5) În cazul în care protecția IUEC manipulate de SEAE este asigurată prin produse criptografice, acestea sunt aprobate de către autoritatea de aprobare criptografică a SEAE, la recomandarea Comitetului de securitate al Consiliului.

(6) Autoritatea de securitate a SEAE, în măsura în care este necesar, instituie următoarele funcții de asigurare a informațiilor:

(a) o autoritate de asigurare a informațiilor;

(b) o autoritate TEMPEST;

(c) o autoritate de aprobare criptografică;

(d) o autoritate de distribuție criptografică.

(7) Pentru fiecare sistem, autoritatea de securitate a SEAE instituie următoarele funcții:

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

(b) o autoritate operațională de asigurare a informațiilor.

(8) Dispozițiile pentru punerea în aplicare a prezentului articol în ceea ce privește protecția IUEC sunt prevăzute în anexele A și A IV.

Articolul 9

Încălcări ale securității și compromiterea informațiilor clasificate

(1) O încălcare a securității apare ca urmare a unei acțiuni sau omisiuni care contravine normelor de securitate prevăzute în prezenta decizie și/sau politicilor sau orientărilor în materie de securitate care definesc măsurile necesare pentru punerea în aplicare a acesteia, astfel cum au fost aprobate în conformitate cu articolul 21 alineatul (1).

(2) O compromitere a informațiilor clasificate apare atunci când acestea au fost divulgate, integral sau parțial, unor persoane sau entități neautorizate.

(3) Orice încălcare sau suspiciune de încălcare a securității și orice compromitere sau suspiciune de compromitere a informațiilor clasificate sunt raportate imediat Direcției SEAE responsabile de securitate, care ia măsurile adecvate prevăzute în anexa A articolul 11.

(4) Orice persoană care este răspunzătoare de o încălcare a normelor de securitate prevăzute în prezenta decizie sau de compromiterea informațiilor clasificate poate fi pasibilă de acțiuni disciplinare și/sau în justiție, în conformitate cu actele cu putere de lege, normele și reglementările aplicabile, astfel cum se prevede la articolul 11 alineatul (3) din anexa A.

Articolul 10

Investigarea incidentelor, încălcărilor și/sau compromiterilor în materie de securitate și acțiuni corective

(1) Fără a aduce atingere articolului 86 (măsuri disciplinare) și anexei IX la Statutul funcționarilor ([1]), anchetele privind securitatea pot fi efectuate de către Direcția SEAE responsabilă de securitate:

(a) în cazul unor eventuale scurgeri de informații UE clasificate, de informații clasificate ale Euratom ori de informații sensibile neclasificate ori în cazul utilizării necorespunzătoare sau al compromiterii acestor informații;

(b) pentru a combate atacurile serviciilor de informații ostile la adresa SEAE și a membrilor personalului său;

(c) pentru a combate atacurile teroriste la adresa SEAE și a membrilor personalului său;

(d) în caz de incidente cibernetice;

(e) în cazul altor incidente care afectează sau care pot afecta securitatea generală în cardul SEAE, inclusiv în cazurile în care se suspectează comiterea unor infracțiuni.

(2) Direcția SEAE responsabilă de securitate, asistată de experți din statele membre și/sau din alte instituții ale UE, după caz, după ce a fost autorizată de către autoritatea de securitate a SEAE, dacă este necesar, pune în aplicare acțiunile corective care se impun în urma anchetelor, atunci când este cazul și în modul adecvat.

Numai membrii personalului care sunt autorizați printr-un mandat nominal, conferit, ținând seama de atribuțiile lor curente, de către autoritatea de securitate a SEAE pot fi împuterniciți să efectueze și să coordoneze anchete de securitate în cadrul SEAE.

(3) Investigatorii au acces la toate informațiile necesare pentru desfășurarea unor astfel de investigații și beneficiază de sprijinul deplin al tuturor serviciilor și membrilor personalului SEAE în această privință.

Investigatorii pot adopta măsuri adecvate pentru a proteja ansamblul elementelor de probă, întrun mod proporțional cu gravitatea chestiunii care face obiectul investigației.

(4) În cazul în care accesul la informații se referă la date cu caracter personal, inclusiv la cele din sistemele informatice și de comunicații, acest acces este acordat în conformitate cu Regulamentul (CE) nr. 45/2001 ([2]).

(5) În cazul în care este necesară crearea unei baze de date pentru investigații care să conțină date cu caracter personal, acest lucru este notificat Autorității Europene pentru Protecția Datelor (AEPD) în conformitate cu regulamentul menționat anterior.

Articolul 11

Gestionarea riscurilor de securitate

(1) Pentru a-și stabili nevoile în materie de protecție a securității, SEAE elaborează, în strânsă colaborare cu Direcția Securitate a Comisiei și, după caz, cu Oficiul de securitate al Secretariatului General al Consiliului, o metodologie globală de evaluare a riscurilor de securitate.

(2) Riscurile la adresa intereselor în materie de securitate ale SEAE sunt gestionate ca proces. Acest proces vizează stabilirea riscurilor de securitate cunoscute, definirea măsurilor de securitate pentru reducerea acestor riscuri la un nivel acceptabil și punerea în aplicare de măsuri în conformitate cu conceptul de apărare în profunzime. Eficacitatea unor astfel de măsuri, precum și nivelul riscurilor sunt evaluate în permanență.

([1]) Statutul funcționarilor Uniunii Europene și Regimul aplicabil celorlalți agenți ai Uniunii Europene, stabilit în Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului (JO L 56, 4.3.1968, p. 1), denumit în continuare „Statutul funcționarilor”.

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

(3) Rolurile, responsabilitățile și sarcinile prevăzute în prezenta decizie nu aduc atingere responsabilității fiecărui membru al personalului aflat sub responsabilitatea SEAE; în special, personalul UE aflat în misiune în țări terțe trebuie să facă uz de bun simț și de discernământ în ceea ce privește propria siguranță și securitate și trebuie să respecte toate normele, reglementările, procedurile și instrucțiunile de securitate aplicabile.

(4) Pentru a preveni și a controla riscurile la adresa securității, membrii personalului autorizat pot efectua verificări ale antecedentelor persoanelor care intră în sfera de aplicare a prezentei decizii, pentru a stabili dacă acordarea accesului acestor persoane în incintele sau la informațiile SEAE prezintă o amenințare la adresa securității. În acest sens și în conformitate cu Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului, membrii personalului autorizat: (a) pot utiliza orice sursă de informații de care dispune SEAE, ținând seama de fiabilitatea sursei de informații; (b) pot avea acces la dosarul de personal sau la datele referitoare la personal de care dispune SEAE cu privire la persoanele care lucrează în cadrul SEAE sau pe care intenționează să le angajeze ori la membrii personalului contractanților, atunci când acest lucru se justifică în mod corespunzător.

(5) SEAE ia toate măsurile rezonabile pentru a asigura protecția intereselor sale în materie de securitate și a preveni daunele previzibile în mod rezonabil.

(6) Măsurile de securitate din cadrul SEAE pentru protejarea IUEC pe durata ciclului lor de viață trebuie să fie proporționale în special cu nivelul clasificării lor de securitate, cu forma și volumul informațiilor sau al materialelor, cu amplasarea și construirea localurilor în care sunt amplasate IUEC și cu amenințarea, inclusiv amenințarea evaluată local, pe care o reprezintă activitățile răuvoitoare și/sau infracționale, inclusiv spionajul, sabotajul și terorismul.

Articolul 12

Sensibilizare și formare în materie de securitate

(1) Autoritatea de securitate a SEAE se asigură că sunt elaborate și puse în aplicare programe adecvate de sensibilizare și formare în materie de securitate și că personalul aflat sub responsabilitatea SEAE și, după caz, persoanele aflate în întreținerea acestora, primesc informările și formările de sensibilizare necesare, proporționale cu riscurile existente la locul lor de muncă sau de reședință.

(2) Înainte de a i se acorda accesul la IUEC și, ulterior, la intervale de timp periodice, personalul este informat și ia cunoștință de responsabilitățile care îi revin cu privire la protejarea IUEC, în conformitate cu normele prevăzute la articolul 6.

Articolul 13

Organizarea securității în cadrul SEAE

Secțiunea 1

Dispoziții generale

(1) Secretarul general este autoritatea de securitate a SEAE. În această calitate, secretarul general se asigură că:

(a) măsurile de securitate sunt coordonate, în funcție de necesități, cu autoritățile competente ale statelor membre, cu Secretariatul General al Consiliului și cu Comisia Europeană și, după caz, cu state terțe sau organizații internaționale în ceea ce privește toate aspectele de securitate relevante pentru activitățile SEAE, inclusiv cu privire la natura riscurilor la adresa intereselor în materie de securitate ale SEAE și la mijloacele de protecție împotriva acestora;

(b) aspectele de securitate sunt luate pe deplin în considerare de la bun început în ceea ce privește toate activitățile SEAE;

(c) accesul la informații clasificate este acordat numai persoanelor care îndeplinesc condițiile prevăzute la articolul 5 din anexa A;

(d) se instituie un sistem de registre care asigură faptul că informațiile clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior sunt manipulate în conformitate cu prezenta decizie în cadrul SEAE și atunci când acestea sunt transmise statelor membre ale UE, instituțiilor, organelor sau agențiilor UE sau altor destinatari autorizați. Se păstrează un registru separat al tuturor IUEC transmise de SEAE statelor terțe sau organizațiilor internaționale și al tuturor informațiilor clasificate primite de la state terțe sau organizații internaționale;

(e) sunt efectuate inspecțiile de securitate prevăzute la articolul 16;

(f) se efectuează investigații în cazul oricărei încălcări reale sau presupuse a securității, inclusiv în cazul oricărei compromiteri sau pierderi reale sau presupuse de informații clasificate, deținute de către SEAE sau provenind de la SEAE, și că autoritățile de securitate competente sunt invitate să asiste la astfel de investigații;

(g) se instituie planuri și mecanisme adecvate de gestionare a incidentelor și a consecințelor acestora în vederea asigurării unei reacții prompte și eficace la incidentele de securitate;

(h) se iau măsurile adecvate în cazul în care anumite persoane nu respectă dispozițiile prezentei decizii;

(i) sunt instituite măsurile fizice și organizatorice adecvate pentru protejarea intereselor în materie de securitate ale SEAE.

În acest sens, autoritatea de securitate a SEAE:

— stabilește categoria de securitate a delegațiilor Uniunii, cu consultarea Comisiei;

— decide, după consultarea ÎR, după caz, momentul în care personalul delegațiilor Uniunii ar trebui evacuat dacă situația de securitate impune acest lucru;

— decide cu privire la măsurile care trebuie aplicate pentru protejarea persoanelor aflate în întreținere, atunci când este cazul, ținând seama de acordurile cu instituțiile UE menționate la articolul 3 alineatul (3);

— aprobă politica de comunicare criptografică, în special programul de instalare a produselor și a mecanismului criptografice.

(2) Autoritatea de securitate a SEAE este asistată în această sarcină de către Directorul general pentru buget și administrație (DGBA), de către directorul Direcției SEAE responsabile de securitate și, după caz, de către secretarul general adjunct pentru PSAC și răspuns la crize.

(3) În calitate de autoritate de securitate a SEAE, secretarul general poate delega sarcini în această privință, după caz.

(4) Fiecare șef de departament/serviciu este responsabil pentru punerea în aplicare a normelor privind protecția IUEC în departamentul/serviciul său.

Deși deține în continuare responsabilitatea, după cum s-a menționat mai sus, fiecare șef de departament/serviciu poate desemna un membru al personalului pentru îndeplinirea unei funcții de coordonator de securitate pe departament, ale cărui resurse sunt proporționale cu volumul de IUEC manipulate de departamentul/serviciul în cauză.

Coordonatorii de securitate pe departament îl asistă și îl sprijină, atunci când este cazul, pe șeful de departament/serviciu în executarea sarcinilor legate de securitate, cum ar fi:

(a) elaborarea oricăror cerințe de securitate suplimentare care corespund nevoilor specifice ale departamentului/serviciului;

(b) organizarea periodică a unor informări privind securitatea adresate membrilor departamentului/serviciului lor;

(c) garantarea faptului că principiul necesității de a cunoaște este respectat în departamentul/serviciul lor;

(d) gestionarea unei liste actualizate a codurilor și a cheilor de siguranță;

(e) menținerea procedurilor și a măsurilor de securitate;

(f) raportarea oricăror încălcări ale securității și/sau compromiteri ale IUEC atât către directorul lor, cât și către Direcția responsabilă de securitate;

(g) organizarea de sesiuni de informare pentru personalul care își încetează activitatea în cadrul SEAE;

(h) furnizarea periodică de rapoarte, prin intermediul ierarhiei, privind chestiunile de securitate ale departamentului/serviciului;

(i) asigurarea legăturii cu Direcția SEAE responsabilă de securitate cu privire la chestiunile de securitate.

Orice activitate sau chestiune care ar putea avea un impact asupra securității este notificată în timp util Direcției SEAE responsabilă de securitate.

(5) Fiecare șef de delegație răspunde de punerea în aplicare a tuturor măsurilor legate de securitatea delegației Uniunii.

Secțiunea 2

Direcția SEAE responsabilă de securitate

(1) SEAE are o direcție responsabilă de securitate. Aceasta:

(a) gestionează, coordonează, monitorizează și/sau pune în aplicare toate măsurile de securitate în toate incintele aflate sub responsabilitatea SEAE, la sediu, în interiorul UE și în statele terțe;

(b) asigură coerența și consecvența cu prezenta decizie și cu dispozițiile de punere în aplicare a oricărei activități care ar putea avea un impact asupra protecției intereselor în materie de securitate ale SEAE;

(c) este principalul consilierul al ÎR, al autorității de securitate a SEAE și a secretarului general adjunct cu privire la toate aspectele legate de securitate;

(d) este asistată de serviciile competente ale statelor membre, în conformitate cu articolul 10 alineatul (3) din Decizia 2010/427/UE a Consiliului privind organizarea și funcționarea SEAE;

(e) sprijină activitățile Autorității de acreditare în materie de securitate a SEAE prin efectuarea de evaluări ale securității fizice a mediului de securitate generală (GSE)/a mediului de securitate locală (LSE) ale sistemelor informatice și de comunicații care manipulează IUEC, precum și ale incintelor care urmează a fi autorizate pentru manipularea și păstrarea IUEC.

(2) Directorul SEAE responsabil de securitate răspunde de:

(a) asigurarea protecției globale a intereselor în materie de securitate ale SEAE;

(b) elaborarea, revizuirea și actualizarea normelor de securitate, precum și de coordonarea măsurilor de securitate cu autoritățile competente ale statelor membre și, dacă este cazul, cu autoritățile competente din statele terțe și cu organizațiile internaționale cu care UE a încheiat acorduri și/sau înțelegeri în materie de securitate;

(c) sprijinirea activităților Comitetului de securitate al SEAE, instituit prin articolul 15 alineatul (1) din prezenta decizie;

(d) asigurarea legăturii cu toți partenerii sau autoritățile, altele decât cele prevăzute la litera (b) de mai sus, privind aspecte legate de securitate, după caz;

(e) stabilirea priorităților și elaborarea de propuneri privind gestiunea bugetului pentru securitate la sediu și în delegațiile Uniunii.

(3) Șeful Direcției SEAE responsabile de securitate:

(a) se asigură că încălcările securității și cazurile de compromitere a securității sunt înregistrate și că sunt inițiate și efectuate investigații acolo unde și atunci când este necesar;

(b) se întâlnește periodic și ori de câte ori este necesar pentru a purta discuții cu privire la domeniile de interes comun cu directorul responsabil de securitate din cadrul Secretariatului General al Consiliului și cu directorul Direcției Securitate a Comisiei.

(4) Direcția SEAE responsabilă de securitate stabilește contactul și menține o cooperare strânsă:

— cu departamentele responsabile de securitate din cadrul ministerelor afacerilor externe din statele membre;

— cu autoritățile naționale de securitate (ANS) și/sau alte autorități de securitate competente ale statelor membre pentru a obține asistența acestora în ceea ce privește informațiile de care are nevoie pentru a evalua pericolele și amenințările la adresa SEAE, a personalului său, a activităților, activelor și resurselor sale, precum și a informațiilor sale clasificate la locul obișnuit de desfășurare a activității;

— cu autoritățile de securitate competente ale statelor membre sau ale statelor gazdă pe teritoriul cărora SEAE își poate exercita activitatea, cu privire la orice chestiune privind protecția personalului său, a activității sale, a activelor și resurselor sale și a informațiilor sale clasificate, pentru perioada în care se află pe teritoriul acestor state;

— cu Oficiul de Securitate al Secretariatului General al Consiliului și cu Direcția Securitate din cadrul Direcției Generale Resurse Umane și Securitate a Comisiei și, atunci când este necesar, cu serviciile de securitate ale celorlalte instituții, organe și agenții ale UE;

— cu serviciile de securitate ale statelor terțe sau ale organizațiilor internaționale, în vederea oricărei coordonări utile; și

— cu autoritățile naționale de securitate ale statelor membre, cu privire la orice chestiune referitoare la protecția IUEC.

Secțiunea 3

Delegațiile Uniunii

(1) Fiecare șef de delegație răspunde de punerea în aplicare și gestionarea la nivel local a tuturor măsurilor referitoare la protejarea intereselor în materie de securitate ale SEAE în cadrul incintelor și a domeniilor de competență ale delegațiilor Uniunii.

În consultare cu autoritățile competente ale statului gazdă, atunci când este necesar, șeful de delegație va lua toate măsurile care pot fi întreprinse în mod rezonabil pentru a se asigura că există măsuri fizice și organizatorice adecvate pentru a atinge acest obiectiv.

Șeful de delegație elaborează proceduri de securitate pentru protecția persoanelor aflate în întreținere, astfel cum sunt definite la articolul 2 litera (c), după caz, luând în considerare orice acord administrativ menționat la articolul 3 alineatul (3). Șeful de delegație prezintă șefului Direcției SEAE responsabilă de securitate rapoarte cu privire la toate aspectele legate de securitate care intră în sfera competențelor sale.

Șeful de delegație este asistat în îndeplinirea sarcinilor menționate mai sus de Direcția SEAE responsabilă de securitate, de echipa de gestionare a securității din cadrul delegației Uniunii, care este alcătuită din membrii personalului care îndeplinesc atribuții și funcții de securitate, precum și de personalul de securitate detașat, după caz.

Delegația Uniunii stabilește contacte și menține o cooperare strânsă în materie de securitate cu misiunile diplomatice ale statelor membre.

(2) În plus, șeful de delegație:

— instituie planuri detaliate de securitate și de urgență pentru delegația Uniunii, pe baza procedurilor operaționale standard generale;

— operează un sistem operațional 24 de ore din 24, 7 zile pe săptămână pentru gestionarea incidentelor de securitate și a situațiilor de urgență în cadrul sferei de activitate a delegației Uniunii;

— se asigură că tot personalul afectat în delegația Uniunii este asigurat, în conformitate cu condițiile din domeniu;

— se asigură că securitatea face parte din formarea inițială oferită tuturor membrilor personalului numit în funcție în cadrul delegației Uniunii, la sosirea în delegația Uniunii; și

— se asigură că toate recomandările făcute în urma evaluărilor privind securitatea sunt puse în aplicare și întocmește periodic rapoarte scrise cu privire la punerea în aplicare a recomandărilor și la alte aspecte legate de securitate, adresate autorității de securitate a SEAE.

(3) Deși rămâne responsabil și poate fi tras la răspundere pentru garantarea gestionării securității, precum și pentru asigurarea rezilienței corporative, șeful de delegație poate delega executarea sarcinilor sale de securitate coordonatorului de securitate al delegației, care este șeful adjunct al delegației sau, atunci când în această funcție nu este numită nicio persoană, altei persoane adecvate.

În special, coordonatorului de securitate al delegației i se pot încredința următoarele responsabilități:

— coordonarea atribuțiilor de securitate din cadrul delegației Uniunii;

— asigurarea legăturii cu privire la chestiuni de securitate cu autoritățile competente ale statului gazdă și cu omologii lor din ambasadele și misiunile diplomatice ale statelor membre;

— punerea în aplicare a unor proceduri adecvate de gestionare a securității în ceea ce privește interesele în materie de securitate ale SEAE, inclusiv protecția IUEC;

— asigurarea respectării normelor și instrucțiunilor în materie de securitate;

— informarea personalului cu privire la normele de securitate care le sunt aplicabile și cu privire la riscurile specifice din statul gazdă;

— prezentarea de cereri către direcția SEAE responsabilă de certificarea de securitate în ceea ce privește funcțiile pentru care este necesar un certificat de securitate a personalului (CSP); și

— informarea constantă a șefului de delegație, a responsabilului regional cu securitatea (RSO) și a Direcției SEAE responsabilă de securitate cu privire la incidentele sau evoluțiile din zonă care au un impact asupra protecției intereselor în materie de securitate ale SEAE.

(4) Șeful de delegație poate delega sarcini de securitate cu caracter administrativ sau tehnic șefului administrației și altor membri ai personalului delegației Uniunii.

(5) Delegația Uniunii este asistată de un RSO. În delegațiile Uniunii, RSO îndeplinesc rolurile definite mai jos, în fiecare zonă geografică de care răspund.

În anumite circumstanțe, când situația de securitate din momentul respectiv impune acest lucru, un RSO special poate fi desemnat să își desfășoare activitatea cu normă întreagă într-o anumită delegație a Uniunii.

Un RSO poate fi transferat într-o zonă din afara zonei de care răspunde în prezent, inclusiv la sediu, sau poate chiar prelua un post rezidențial, în funcție de situația unei țări în materie de securitate și astfel cum dispune Direcția SEAE responsabilă de securitate.

(6) RSO se află sub controlul operațional direct al serviciului SEAE de la sediu responsabil de securitatea pe teren, însă sub controlul administrativ comun al șefului delegației în care își desfășoară activitatea și al serviciului de la sediu responsabil de securitatea pe teren. RSO oferă consiliere și asistă șeful de delegație și personalul delegației Uniunii în organizarea și punerea în aplicare a tuturor măsurilor fizice, organizaționale și procedurale legate de securitatea delegației Uniunii.

(7) RSO furnizează consultanță și sprijin șefului de delegație și personalului delegației Uniunii. După caz, în special atunci când un RSO își desfășoară activitatea cu normă întreagă într-o delegație a Uniunii, acesta ar trebui să asiste delegația Uniunii în gestionarea și aplicarea securității, inclusiv în pregătirea contractele de servicii de securitate, în gestionarea acreditărilor și a certificatelor de securitate.

Articolul 14

Operațiuni PSAC și reprezentanți speciali ai UE

Direcția SEAE responsabilă de securitate oferă consiliere directorului Direcției de planificare și de gestionare a crizelor (CMDP), directorului general al Statului Major al Uniunii Europene (EUMS), comandantului operațiunilor civile aflat la conducerea Capacității civile de planificare și conducere (CPCC), comandanților operațiunilor militare ale UE privind aspectele de securitate ale operațiunilor PSAC și reprezentanților speciali ai UE privind aspectele de securitate ale mandatului lor, în mod complementar dispozițiilor specifice existente în această privință în politicile relevante adoptate de Consiliu.

Articolul 15

Comitetul de securitate al SEAE

(1) Se instituie un Comitet de securitate al SEAE.

Acesta este prezidat de autoritatea de securitate a SEAE sau de către delegatul desemnat al acesteia și se reunește la solicitarea președintelui sau la cererea oricăruia dintre membrii săi. Direcția SEAE responsabilă de securitate sprijină președintele în această funcție și oferă asistență administrativă, după caz, pentru activitățile comitetului.

(2) Comitetul de securitate al SEAE este alcătuit din reprezentanți ai:

— fiecărui stat membru;

— Oficiului de Securitate al Secretariatului General al Consiliului;

— Direcției Securitate din cadrul Direcției Generale Resurse Umane și Securitate a Comisiei.

Delegația unui stat membru în cadrul Comitetului de securitate al SEAE poate fi constituită din membri ai:

— autorității naționale de securitate și/sau ai autorității de securitate desemnate;

— departamentelor responsabile cu securitatea din cadrul ministerelor afacerilor externe.

(3) Reprezentanții comitetului pot fi însoțiți și pot primi consultanță din partea unor experți, după cum consideră că este necesar. Pot fi invitați să asiste la reuniunile comitetului reprezentanți ai altor instituții, agenții sau organe ale UE atunci când se discută aspecte relevante pentru securitatea acestora.

(4) Fără a aduce atingere alineatului (5) de mai jos, Comitetul de securitate al SEAE sprijină SEAE, prin consultări, cu privire la toate chestiunile de securitate relevante pentru activitățile SEAE, pentru sediu și pentru delegațiile Uniunii.

În special, fără a aduce atingere alineatului (5) de mai jos, Comitetul de securitate al SEAE:

(a) este consultat cu privire la:

— politicile, orientările, conceptele de securitate sau alte documente metodologice legate de securitate, în special în ceea ce privește protecția informațiilor clasificate și măsurile care trebuie adoptate în cazul în care personalul SEAE nu respectă normele de securitate;

— aspecte tehnice de securitate care pot influența decizia ÎR de a transmite Consiliului o recomandare privind deschiderea negocierilor pentru acordurile privind securitatea informațiilor menționate la articolul 10 alineatul (1) litera (a) din anexa A;

— orice modificare a prezentei decizii;

(b) poate fi consultat sau informat, după caz, cu privire la chestiuni legate de securitatea personalului și a activelor de la sediul SEAE și din delegațiile Uniunii, fără a aduce atingere articolului 3 alineatul (3);

(c) este informat cu privire la toate cazurile de compromiteri sau de pierderi ale IUEC care s-au produs în cadrul SEAE.

(5) Orice modificare a normelor referitoare la protecția IUEC conținute în prezenta decizie și în anexa A la aceasta necesită un aviz favorabil unanim din partea statelor membre, astfel cum sunt reprezentate în Comitetul de securitate al SEAE. Un astfel de aviz favorabil unanim este, de asemenea, necesar înainte de a:

— intra în negocieri privind acordurile administrative menționate la articolul 10 alineatul (1) litera (b) din anexa A;

— comunica informații clasificate în circumstanțele excepționale menționate la punctele 9, 11 și 12 din anexa A VI;

— se asuma responsabilitatea de emitent al informațiilor în cazurile menționate la articolul 10 alineatul (6) ultima teză din anexa A.

Atunci când este necesar un aviz favorabil unanim, acesta este obținut dacă, în cursul procedurilor comitetului, delegațiile statelor membre nu prezintă obiecții.

(6) Comitetul de securitate al SEAE ține seama pe deplin de politicile și orientările de securitate în vigoare din cadrul Consiliului și al Comisiei.

(7) Comitetul de securitate al SEAE primește lista inspecțiilor anuale ale SEAE și rapoartele de inspecție, de îndată ce au fost finalizate.

(8) Organizarea reuniunilor:

— Comitetul de securitate al SEAE se întrunește cel puțin de două ori pe an. Reuniuni suplimentare, fie în configurația completă, fie în format de securitate ANS/ASD sau MFA, pot fi convocate de președinte sau organizate la solicitarea membrilor comitetului;

— Comitetul de securitate al SEAE își organizează activitățile în așa fel încât să poată să formuleze recomandări cu privire la domenii de securitate specifice. Acesta poate crea alte subdomenii specializate, după caz. Comitetul stabilește mandatul acestor subdomenii specializate și primește rapoartele de activitate cu privire la acestea;

— Direcția SEAE responsabilă de securitate este responsabilă de pregătirea elementelor care urmează a fi discutate. Președintele stabilește ordinea de zi provizorie a fiecărei reuniuni. Membrii comitetului pot propune chestiuni suplimentare spre a fi discutate.

Articolul 16

Inspecții de securitate

(1) Autoritatea de securitate a SEAE se asigură că sunt întreprinse în mod regulat inspecții de securitate la sediul SEAE și în cadrul delegațiilor Uniunii, pentru a evalua caracterul adecvat al măsurilor de securitate și conformitatea acestora cu prezenta decizie. Direcția SEAE responsabilă de securitate poate, după caz, desemna experți care să furnizeze contribuții la inspecțiile de securitate în agențiile și organele UE instituite în temeiul titlului V capitolul 2 din TUE.

(2) Inspecțiile de securitate ale SEAE sunt efectuate sub autoritatea Direcției SEAE responsabilă de securitate și, după caz, cu sprijinul experților în securitate care reprezintă alte instituții ale UE sau statele membre, în special în contextul acordurilor menționate la articolul 3 alineatul (3).

(3) SEAE se poate baza, în funcție de necesități, pe expertiza statelor membre, a Secretariatului General al Consiliului și a Comisiei Europene.

După caz, la inspecția de securitate din delegația Uniunii pot fi invitați să participe experți relevanți în domeniul securității din misiunile statului membru în state terțe și/sau reprezentanți ai departamentelor de securitate diplomatice ale statelor membre.

(4) Dispozițiile privind punerea în aplicare a prezentului articol în ceea ce privește protecția IUEC sunt prevăzute în anexa A III.

Articolul 17

Vizite de evaluare

Se organizează vizite de evaluare pentru a se stabili eficacitatea măsurilor de securitate aplicate întrun stat terț sau într-o organizație internațională pentru protecția IUEC schimbate în cadrul unui acord administrativ, astfel cum este menționat la articolul 10 alineatul (1) litera (b) din anexa A.

Direcția SEAE responsabilă de securitate poate desemna experți care să furnizeze contribuții la vizitele de evaluare din statele terțe sau din organizațiile internaționale cu care UE a încheiat un acord privind securitatea informațiilor, astfel cum este menționat la articolul 10 alineatul (1) litera (a) din anexa A.

Articolul 18

Planificarea continuității activității

Direcția SEAE responsabilă de securitate asistă autoritatea de securitate a SEAE în gestionarea aspectelor de securitate legate de procesele de asigurare a continuității activității SEAE ca parte a planificării generale a continuității activității SEAE.

Articolul 19

Recomandări de călătorie pentru misiunile în afara UE

Direcția SEAE responsabilă de securitate se asigură că sunt disponibile recomandări de călătorie în ceea ce privește misiunile în afara UE ale personalului aflat sub responsabilitatea SEAE, pe baza resurselor din toate serviciile relevante ale SEAE – în special SITROOM, INTCEN, departamentele geografice și delegațiile Uniunii.

Direcția SEAE responsabilă de securitate oferă, la cerere și pe baza resurselor menționate anterior, recomandări de călătorie specifice în ceea ce privește misiunile efectuate de personalul aflat sub responsabilitatea SEAE în statele terțe care prezintă un risc ridicat sau crescut.

Articolul 20

Sănătate și siguranță

Normele de securitate ale SEAE completează normele SEAE privind protecția sănătății și a siguranței, astfel cum au fost adoptate de către Înaltul Reprezentant.

Articolul 21

Punere în aplicare și reexaminare

(1) După caz, autoritatea de securitate a SEAE, în urma consultării cu Comitetul de securitate al SEAE, aprobă orientările de securitate prin care se stabilesc măsurile necesare pentru punerea în aplicare a acestor norme în cadrul SEAE și creează capacitatea necesară care să cuprindă toate aspectele legate de securitate, în strânsă cooperare cu autoritățile de securitate competente ale statelor membre și cu sprijinul serviciilor relevante ale instituțiilor UE.

(2) În conformitate cu articolul 4 alineatul (5) din Decizia 2010/427/UE a Consiliului din 26 iulie 2010 privind organizarea și funcționarea Serviciului European de Acțiune Externă, pot fi utilizate, după caz, dispoziții tranzitorii, prin înțelegeri la nivel de serviciu cu serviciile relevante ale Secretariatului General al Consiliului și ale Comisiei.

(3) ÎR asigură coerența globală în aplicarea prezentei decizii și examinează în mod periodic aceste norme de securitate.

(4) Normele de securitate ale SEAE trebuie puse în aplicare în strânsă cooperare cu autoritățile de securitate competente ale statelor membre.

(5) SEAE se asigură că toate aspectele procesului de securitate sunt luate în considerare în cadrul sistemului SEAE de răspuns la situații de criză.

(6) Secretarul general, în calitate de autoritate de securitate, și șeful Direcției SEAE responsabilă de securitate asigură punerea în aplicare a prezentei decizii.

Articolul 22

Înlocuirea deciziilor anterioare

Prezenta decizie abrogă și înlocuiește Decizia Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate din 19 aprilie 2013 privind normele de securitate pentru Serviciul European de Acțiune Externă ([1]).

Articolul 23

Dispoziții finale

Prezenta decizie intră în vigoare la data semnării.

Se publică în *Jurnalul Oficial al Uniunii Europene*.

Autoritățile competente din cadrul SEAE îi informează în mod corespunzător și în timp util pe toți membrii personalului care intră sub incidența prezentei decizii și a anexelor la aceasta cu privire la conținutul, intrarea în vigoare și orice modificări ulterioare aduse acestora.

Adoptată la Bruxelles, 19 septembrie 2017.

Federica MOGHERINI

Înalt Reprezentant al Uniunii pentru afaceri externe și politica de securitate

([1]) JO C 190, 29.6.2013, p. 1.

ANEXA A

PRINCIPII ȘI STANDARDE PENTRU PROTECȚIA IUEC

Articolul 1

Obiectiv, domeniu de aplicare și definiții

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

(2) Aceste principii de bază și standarde minime se aplică SEAE și personalului aflat sub responsabilitatea SEAE, astfel cum sunt menționate și definite la articolele 1 și 2 din prezenta decizie.

Articolul 2

Definiția IUEC, a clasificărilor și marcajelor de securitate

(1) „Informații 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 unuia sau mai multor state membre.

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

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

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

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

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

(3) IUEC au un marcaj de clasificare de securitate care respectă alineatul (2). Acestea pot avea marcaje suplimentare pentru a indica domeniul de activitate la care se referă, a identifica emitentul, a limita distribuirea, a restrânge utilizarea sau a preciza dacă pot fi comunicate.

Articolul 3

Gestionarea clasificărilor

(1) SEAE se asigură că IUEC sunt clasificate corespunzător, că sunt 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) Autoritatea de securitate a SEAE aprobă, după consultarea Comitetului de securitate al SEAE în temeiul articolului 15 alineatul (5) din prezenta decizie, orientările de securitate privind crearea IUEC, care includ un ghid practic de clasificare.

Articolul 4

Protecția informațiilor clasificate

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

(2) Deținătorul oricărui element de IUEC este responsabil de protecția acestuia, 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 în rețelele SEAE, SEAE 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.

SEAE instituie proceduri adecvate pentru a ține o evidență exactă a emitentului

— informațiilor clasificate pe care le primește SEAE; și

— materialului-sursă inclus în informațiile clasificate emise de SEAE.

Comitetul de securitate al SEAE este informat cu privire la aceste proceduri.

(4) Cantități mari de IUEC sau o compilație de astfel de informații poate justifica un nivel de protecție care corespunde unei clasificări al cărei nivel este mai ridicat decât cel al informațiilor componente.

Articolul 5

Securitatea personalului în ceea ce privește manipularea informațiilor UE clasificate

(1) „Securitatea personalului” înseamnă aplicarea unor măsuri prin care se garantează că accesul la IUEC este acordat numai persoanelor:

— în cazul cărora există necesitatea de a cunoaște;

— care, pentru accesul la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior, au primit certificatul de securitate pentru nivelul corespunzător sau sunt autorizate în alt mod corespunzător în temeiul funcțiilor deținute în conformitate cu actele cu putere de lege și dispozițiile administrative naționale; și

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

(2) Procedurile de acordare a certificatului de securitate a personalului stabilesc dacă o persoană poate fi autorizată să aibă acces la IUEC, ținându-se seama de loialitatea, onestitatea și seriozitatea acesteia.

(3) Înainte de a primi acces la IUEC și, ulterior, la intervale regulate, întregul personal este informat și confirmă în scris ca a luat cunoștință de responsabilitățile care îi revin cu privire la protejarea IUEC, în conformitate cu prezenta decizie.

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

Articolul 6

Securitatea fizică a informațiilor UE clasificate

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

(2) Măsurile de securitate fizică sunt concepute astfel încât să prevină accesul clandestin sau forțat al vreunui intrus, să descurajeze, să împiedice și să detecteze acțiunile neautorizate și să permită stabilirea unei distincții între membrii personalului în privința accesului la IUEC, pe baza principiului necesității de a cunoaște. Aceste măsuri sunt stabilite pe baza unui proces de gestionare a riscurilor.

(3) Măsurile de securitate fizică sunt instituite pentru toate incintele, clădirile, birourile, sălile și alte spații în care sunt manipulate sau păstrate IUEC, inclusiv spațiile în care sunt amplasate sistemele informatice și de comunicații, astfel cum sunt definite la articolul 8 alineatul (2) din anexa A.

(4) Spațiile în care sunt păstrate IUEC clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior sunt stabilite a fi zone securizate în conformitate cu anexa A II și aprobate de autoritatea de securitate a SEAE.

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

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

Articolul 7

Gestionarea informațiilor clasificate

(1) Gestionarea informațiilor clasificate reprezintă aplicarea unor măsuri administrative pentru a controla IUEC pe durata ciclului lor de viață, în vederea completării măsurilor prevăzute la articolele 5, 6 și 8, 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, manipularea, păstrarea și distrugerea IUEC.

(2) Informațiile clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior sunt înregistrate din motive de securitate înainte de a fi distribuite și la primirea acestora. În acest scop, autoritățile competente din SEAE înființează o registratură. Informațiile clasificate TRES SECRET UE/EU TOP SECRET sunt înregistrate în registre speciale.

(3) Serviciile și incintele unde sunt manipulate sau păstrate IUEC sunt supuse unor inspecții periodice de către autoritatea de securitate a SEAE.

(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 7 alineatul (5) din prezenta decizie și în conformitate cu proceduri operaționale de securitate clar definite;

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

(i) fie pe suport electronic (de exemplu, stick-uri memorie USB, CD-uri, hard diskuri) protejat prin intermediul unor produse criptografice aprobate în conformitate cu articolul 8 alineatul (5) din prezenta decizie, fie

(ii) în toate celelalte cazuri, conform indicațiilor primite de la autoritatea de securitate a SEAE, în conformitate cu măsurile de protecție relevante prevăzute în anexa A III secțiunea V.

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

Articolul 8

Protecția IUEC manipulate în sistemele informatice și de comunicații

(1) Asigurarea informațiilor (AI) în domeniul sistemelor informatice și de comunicații reprezintă certitudinea că aceste sisteme vor proteja informațiile pe care le manipulează și vor funcționa corespunzător, atunci când este necesar, sub controlul utilizatorilor legitimi. O AI eficace asigură niveluri adecvate de confidențialitate, integritate, disponibilitate, nerepudiere și autenticitate. AI se bazează pe un proces de gestionare a riscurilor.

(2) „Sistemul informatic și de comunicații" (SIC) reprezintă un sistem care permite manipularea informațiilor în format electronic. Un sistem informatic și de comunicații cuprinde toate activele necesare pentru a funcționa, inclusiv infrastructura, organizarea, personalul și resursele informaționale. Prezenta anexă se aplică tuturor SIC ale SEAE care manipulează IUEC.

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

(4) Toate SIC care manipulează IUEC 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 pot fi manipulate de SIC, precum și termenii și condițiile acreditării respective.

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

(6) În cazul în care protecția IUEC este asigurată prin intermediul unor produse criptografice, acestea trebuie să fie aprobate în conformitate cu articolul 8 alineatul (5) din prezenta decizie.

(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 precizează în anexa A IV.

(8) În temeiul articolului 8 alineatul (6) din prezenta decizie, vor fi create următoarele funcții aferente AI, în măsura în care este necesar:

(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) În temeiul articolului 8 alineatul (7) din prezenta decizie, pentru fiecare sistem se instituie:

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

(b) o autoritate operațională AI.

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

Articolul 9

Securitatea industrială

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

(2) SEAE poate încredința prin contract sarcini care implică sau determină accesul la IUEC sau manipularea sau păstrarea acestora de entități industriale sau de altă natură înregistrate într-un stat membru sau într-un stat terț cu care a fost încheiat un acord privind securitatea informațiilor sau un acord administrativ menționat la articolul 10 alineatul (1) din anexa A.

(3) Atunci când atribuie contracte clasificate entităților industriale sau de altă natură, SEAE, în calitate de autoritate contractantă, asigură respectarea standardelor minime privind securitatea industrială stabilite în prezenta decizie și menționate în contract. SEAE asigură respectarea acestor standarde minime prin intermediul ANS/ASD competente.

(4) Contractanții sau subcontractanții înregistrați într-un stat membru care participă la contracte sau subcontracte clasificate care trebuie să manipuleze și să păstreze în cadrul incintelor proprii 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, acordat de ANS, ASD sau oricare altă autoritate de securitate competentă din statul membru respectiv.

(5) Personalul 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 deține un certificat de securitate a personalului (CSP) acordat de către autoritatea națională de securitate (ANS), autoritatea de securitate desemnată (ASD) 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 A I.

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

Articolul 10

Schimbul de informații clasificate cu state terțe și organizații internaționale

(1) SEAE poate schimba IUEC cu un stat terț sau cu o organizație internațională numai în cazul în care:

(a) este în vigoare un acord privind securitatea informațiilor între UE și statul terț sau organizația internațională respectivă, încheiat în conformitate cu articolul 37 din TUE și cu articolul 218 din TFUE; sau

(b) a intrat în vigoare un acord administrativ între ÎR și autoritățile de securitate competente din statul terț sau organizația internațională respectivă pentru schimbul de informații clasificate, în principiu, la un nivel nu mai ridicat decât RESTREINT UE/EU RESTRICTED, încheiat în conformitate cu procedura prevăzută la articolul 15 alineatul (5) din prezenta decizie; sau

(c) este aplicabil un acord-cadru sau un acord de participare ad hoc între UE și statul terț respectiv în contextul unei operațiuni PSAC de gestionare a crizelor, încheiat în conformitate cu articolul 37 din TUE și articolul 218 din TFUE,

iar condițiile prevăzute în instrumentul respectiv au fost îndeplinite.

Anexa A VI secțiunea V cuprinde excepții de la regula generală de mai sus.

(2) Acordurile administrative menționate la alineatul (1) litera (b) conțin dispoziții care garantează că, atunci când statele terțe sau organizațiile internaționale primesc IUEC, aceste informații beneficiază de protecția corespunzătoare nivelului lor de clasificare, pe baza unor standarde minime cel puțin la fel de stricte precum cele instituite prin prezenta decizie.

Informațiile schimbate pe baza acordurilor menționate la alineatul (1) litera (c) se limitează la informațiile privind operațiunile PSAC la care participă statul terț în cauză pe baza acestor acorduri și în conformitate cu dispozițiile acestora.

(3) Dacă se încheie ulterior un acord privind securitatea informațiilor între Uniune și un stat terț sau o organizație internațională participantă, acordul privind securitatea informațiilor prevalează asupra dispoziției privind schimbul de informații clasificate prevăzute în acordurile-cadru de participare, acordurile de participare ad hoc sau acordurile administrative ad hoc în ceea ce privește schimbul de IUEC și manipularea IUEC.

(4) IUEC generate în scopul unei operațiuni PSAC pot fi divulgate personalului detașat în vederea operațiunii respective de către state terțe sau organizații internaționale în conformitate cu alineatele (1)-(3) și cu anexa A VI. Atunci când se autorizează accesul personalului menționat anterior la IUEC în incintele sau în SIC ale unei operații PSAC, se aplică măsuri (inclusiv înregistrarea IUEC divulgate) de reducere a riscului de pierdere sau compromitere. Aceste măsuri sunt definite în documentele de planificare sau de misiune relevante.

(5) Sunt organizate vizite de evaluare în statele terțe sau în cadrul organizațiilor internaționale, astfel cum sunt menționate la articolul 17 din prezenta decizie, pentru a se stabili eficacitatea măsurilor de securitate instituite pentru protecția tuturor IUEC schimbate.

(6) Decizia de a comunica IUEC deținute de SEAE către un stat terț sau o organizație internațională se ia de la caz la caz, în funcție de natura și conținutul informațiilor respective, de necesitatea de a cunoaște a destinatarului lor și de măsura în care acest lucru prezintă un avantaj pentru UE.

SEAE solicită consimțământul scris al oricărei entități care a furnizat informații clasificate ca material-sursă pentru IUEC care au fost emise de SEAE, pentru a se stabili că nu există obiecții cu privire la comunicarea acestora.

Dacă emitentul informațiilor clasificate a căror comunicare este avută în vedere nu este SEAE, SEAE trebuie să solicite, mai întâi, consimțământul scris al emitentului privind comunicarea acestora.

Dacă, cu toate acestea, SEAE nu poate stabili cine este emitentul, autoritatea de securitate a SEAE își asumă responsabilitatea emitentului după obținerea avizului favorabil unanim al statelor membre, astfel cum sunt reprezentate în Comitetul de securitate al SEAE.

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

Articolul 11

Încălcări ale securității și compromiterea informațiilor clasificate

(1) Orice încălcare sau suspiciune de încălcare a securității și orice compromitere sau suspiciune de compromitere a informațiilor clasificate sunt raportate imediat Direcției SEAE responsabilă de securitate, care informează, după caz, statul membru (statele membre) în cauză sau orice altă entitate interesată.

(2) În cazul în care se cunoaște sau există motive rezonabile pentru a se suspecta că au fost compromise sau pierdute informații clasificate, Direcția SEAE responsabilă de securitate informează ANS a statului membru (statelor membre) în cauză și ia toate măsurile corespunzătoare în conformitate cu actele cu putere de lege și dispozițiile administrative relevante pentru:

(a) a proteja elementele de probă;

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

(c) a informa imediat emitentul sau orice altă entitate vizată;

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

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

(f) a notifica autorităților competente efectele compromiterii efective sau suspectate și acțiunile întreprinse.

(3) Orice membru al personalului aflat sub responsabilitatea SEAE care este responsabil de o încălcare a normelor de securitate stabilite în prezenta decizie poate fi pasibil de acțiune disciplinară în conformitate cu normele și reglementările aplicabile.

Orice persoană responsabilă de compromiterea sau pierderea unor informații clasificate este pasibilă de acțiuni disciplinare și/sau în justiție în conformitate cu actele cu putere de lege, normele și reglementările aplicabile.

(4) Pe durata desfășurării investigației privind încălcarea și/sau compromiterea, șeful Direcției SEAE responsabilă de securitate poate suspenda accesul persoanei respective la IUEC și la incintele SEAE. Direcția Securitate din cadrul Direcției Generale Resurse Umane și Securitate a Comisiei, Oficiul de Securitate al Secretariatului General al Consiliului, ANS a statului membru (statelor membre) în cauză sau orice altă entitate interesată este imediat informată cu privire la această decizie.

ANEXA A I

SECURITATEA PERSONALULUI

I. INTRODUCERE

1. Prezenta anexă conține dispoziții pentru punerea în aplicare a articolului 5 din anexa A. Aceasta stabilește, în special, criteriile aplicate de SEAE pentru a determina dacă o persoană poate fi autorizată să aibă acces la IUEC, ținându-se seama de loialitatea, onestitatea și seriozitatea acesteia, precum și de procedurile administrative și de investigare care trebuie urmate în acest sens.

2. „Certificatul de securitate a personalului" (CSP) pentru accesul la IUEC este o declarație a unei autorități competente a unui stat membru făcută după încheierea unei investigații de securitate efectuate de autoritățile competente ale unui stat membru, care certifică faptul că unei persoane îi poate fi acordat accesul la IUEC până la un nivel precizat (CONFIDENTIEL UE/EU CONFIDENTIAL sau superior), 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".

3. „Certificarea autorizării de securitate a personalului" (CASP) este un certificat eliberat de autoritatea de securitate a SEAE care atestă faptul că o persoană a făcut obiectul verificărilor de securitate și deține un CSP valabil, care indică nivelul IUEC la care acesteia i se poate acorda acces, data de valabilitate a CSP relevant și data de expirare a certificării.

4. „Autorizația de acces la IUEC" este o autorizație din partea autorității de securitate a SEAE care este luată în conformitate cu prezenta decizie în urma eliberării unui CSP de către autoritățile competente ale unui stat membru și care certifică 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 autorizația de acces".

II. AUTORIZAREA ACCESULUI LA IUEC

5. Accesul la informații clasificate RESTREINT UE/EU RESTRICTED nu necesită deținerea unui certificat de securitate și este acordat după ce:

   (a) a fost stabilită legătura statutară sau contractuală a persoanei respective cu SEAE;

   (b) a fost determinată necesitatea de a cunoaște a persoanei în cauză;

   (c) persoana în cauză a fost instruită cu privire la normele și procedurile de securitate pentru protecția IUEC și a confirmat în scris că a luat cunoștință de responsabilitățile care îi revin de a proteja IUEC în conformitate cu prezenta decizie.

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

   (a) a fost stabilită legătura statutară sau contractuală a persoanei respective cu SEAE;

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

   (c) 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

   (d) persoana a fost instruită cu privire la normele și procedurile de securitate pentru protecția IUEC și a confirmat în scris că a luat cunoștință de responsabilitățile care îi revin în ceea ce privește protejarea acestor informații.

7. SEAE identifică funcțiile din structurile sale care necesită accesul la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior și care, prin urmare, necesită deținerea unui CSP de nivel corespunzător, astfel cum este menționat la punctul 4 de mai sus.

8. Personalul SEAE declară dacă deține cetățenia mai multor țări.

Procedurile de solicitare a CSP în cadrul SEAE

9. Pentru personalul SEAE, autoritatea de securitate a SEAE înaintează chestionarul privind securitatea personalului completat către ANS a statului membru a cărui cetățenie o deține persoana în cauză, solicitând efectuarea unei investigații de securitate pentru nivelul IUEC la care va trebui să i se acorde accesul persoanei respective.

10. În cazul în care o persoană deține cetățenia mai multor țări, cererea de verificare va fi adresată ANS a țării a cărei cetățenie a fost declarată de persoana respectivă în momentul în care a fost recrutată.

11. În cazul în care SEAE intră în posesia unor informații relevante pentru o investigație de securitate referitoare la o persoană care a solicitat un CSP, SEAE, acționând în conformitate cu actele cu putere de lege și dispozițiile administrative relevante, notifică acest lucru ANS competente.

12. După încheierea investigației de securitate, ANS competentă notifică Direcției SEAE responsabilă de securitate rezultatul acestei investigații.

    (a) În cazul în care investigația de securitate stabilește cu certitudine că nu se cunosc fapte nefavorabile care să pună la îndoială loialitatea, onestitatea și seriozitatea persoanei respective, autoritatea de securitate a SEAE poate acorda persoanei în cauză o autorizație de acces la IUEC până la nivelul relevant, până la o dată specificată.

    (b) SEAE ia toate măsurile adecvate pentru a asigura punerea în aplicare corespunzătoare a condițiilor sau a restricțiilor impuse de ANS. ANS va fi informată cu privire la rezultate.

    (c) În cazul în care investigația de securitate nu are drept rezultat o astfel de certitudine, autoritatea de securitate a SEAE anunță persoana în cauză, care poate solicita să fie audiată de către autoritatea de securitate a SEAE. Autoritatea de securitate a SEAE îi poate solicita ANS competente orice clarificare suplimentară pe care o poate furniza în conformitate cu actele cu putere de lege și dispozițiile administrative naționale ale acesteia. Dacă rezultatul este confirmat, autorizația de acces la IUEC nu este acordată. În acest caz, SEAE ia toate măsurile adecvate pentru a se asigura că solicitantului i se va refuza orice acces la IUEC.

13. Investigația de securitate, împreună cu rezultatele obținute, pe care SEAE își întemeiază decizia de a acorda sau nu o autorizație de acces la IUEC, face obiectul actelor cu putere de lege și dispozițiilor administrative relevante în vigoare în statul membru în cauză, inclusiv celor privind căile de atac. Deciziile autorității de securitate a SEAE pot face obiectul unor căi de atac, în conformitate cu Statutul funcționarilor

14. Garanțiile pe care se bazează un CSP, cu condiția ca acestea să rămână valabile, acoperă orice funcție deținută de persoana în cauză în cadrul SEAE, al Secretariatului General al Consiliului sau al Comisiei.

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

16. Dacă o persoană nu își începe activitatea în termen de 12 luni de la notificarea rezultatului investigației de securitate autorității de securitate a SEAE sau dacă intervine o pauză de 12 luni sau mai mare în exercitarea atribuțiilor persoanei respective, timp în care aceasta nu a fost angajată în cadrul SEAE, în alte instituții, agenții sau organe ale UE sau într-o funcție în cadrul administrației naționale a unui stat membru care necesită accesul la informații clasificate, rezultatul respectiv al investigației este prezentat ANS competente, pentru a se confirma că este în continuare valabil și pertinent.

17. În cazul în care SEAE intră în posesia unor informații privind un risc de securitate reprezentat de o persoană care deține un CSP valabil, SEAE, acționând în conformitate cu actele cu putere de lege și dispozițiile administrative relevante, notifică acest lucru ANS competente și poate suspenda accesul la IUEC sau poate retrage autorizația de acces la IUEC. În cazul în care o ANS notifică SEAE retragerea unei garanții acordate în conformitate cu punctul 12 litera (a) unei persoane care deține o autorizație valabilă de acces la IUEC, autoritatea de securitate a SEAE 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 nefavorabile sunt confirmate, persoanei respective i se retrage autorizația menționată mai sus și i se interzice accesul la IUEC și la funcțiile care permit accesul la acestea sau din care ar putea compromite securitatea.

18. Orice decizie de a retrage unui membru al personalului SEAE autorizația de acces la IUEC și, după caz, motivele care stau la baza acestui lucru sunt comunicate persoanei în cauză, care poate solicita să fie audiată de către autoritatea de securitate a SEAE. Informațiile furnizate de o ANS fac obiectul actelor cu putere de lege și dispozițiilor administrative relevante în vigoare în statul membru în cauză, inclusiv a celor privind căile de atac. Deciziile autorității de securitate a SEAE pot face obiectul unor căi de atac, în conformitate cu Statutul funcționarilor.

19. Experții naționali detașați în cadrul SEAE pentru a exercita o funcție care necesită accesul la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior trebuie să prezinte autorității de securitate a SEAE, înainte de a-și prelua funcția, un CSP valabil pentru accesul la IUEC la nivelul relevant. Procesul de mai sus este gestionat de statul membru care detașează experții respectivi.

Registrele cu CSP

20. SEAE păstrează o bază de date privind certificatele de securitate ale tuturor membrilor personalului aflat sub responsabilitatea SEAE și ale personalului contractanților SEAE. Aceste registre conțin nivelul IUEC la care se poate acorda acces persoanei în cauză (CONFIDENTIEL UE/EU CONFIDENTIAL sau un nivel superior), data acordării CSP și perioada de valabilitate a acestuia.

21. Împreună cu statele membre și cu alte instituții, agenții și organe ale UE, se instituie proceduri de coordonare adecvate pentru a se asigura că SEAE deține registre exacte și complete ale certificatelor de securitate ale tuturor membrilor personalului aflat sub responsabilitatea SEAE și ale personalului contractanților SEAE.

22. Autoritatea de securitate a SEAE poate elibera o certificare a autorizării de securitate a personalului (CASP) care să indice nivelul IUEC la care se poate acorda acces persoanei în cauză (CONFIDENTIEL UE/EU CONFIDENTIAL sau un nivel superior), data de valabilitate a CSP relevant sau a autorizației relevante și data de expirare a certificării.

Scutiri de la obligația de a deține un CSP

23. Persoanele autorizate în mod corespunzător să aibă acces la IUEC în temeiul funcțiilor lor în conformitate cu actele cu putere de lege și reglementările naționale sunt informate, după caz, de către Direcția SEAE responsabilă de securitate cu privire la obligațiile de securitate care le revin în ceea ce privește protecția IUEC.

III. FORMAREA ȘI SENSIBILIZAREA ÎN DOMENIUL SECURITĂȚII

24. Înainte de a fi autorizate să aibă acces la IUEC, toate persoanele confirmă în scris faptul că își înțeleg obligațiile cu privire la protecția IUEC, precum și consecințele compromiterii IUEC. SEAE păstrează un registru cu aceste confirmări scrise.

25. Toate persoanele autorizate să aibă acces la IUEC sau care trebuie să manipuleze IUEC primesc, inițial, informații cu privire la amenințările la adresa securității, 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.

26. Toate persoanele cărora li s-a acordat acces la IUEC trebuie să facă obiectul unor măsuri de securitate a personalului continue (și anume, sunt monitorizate) pentru perioada în care manipulează IUEC. Securitatea permanentă a personalului se află în responsabilitatea:

(a) persoanelor cărora li s-a acordat acces la IUEC: persoanele în cauză sunt responsabile personal de propriul comportament în materie de securitate și trebuie să raporteze imediat autorităților de securitate competente orice abordare sau activitate pe care o consideră suspectă sau neobișnuită și orice modificări ale situației lor personale care pot avea un impact asupra propriului CSP sau a autorizației de acces la IUEC;

(b) superiorilor ierarhici direcți: aceștia au responsabilitatea de a se asigura că personalul aflat în subordinea lor cunoaște măsurile de securitate și responsabilitățile pentru protecția IUEC, de a monitoriza comportamentul în materie de securitate al personalului din subordinea lor, precum și fie de a aborda ei înșiși orice probleme de securitate, fie de a raporta autorităților de securitate competente orice informații nefavorabile care pot avea un impact asupra CSP sau a autorizației de acces la IUEC a personalului din subordinea lor;

(c) actorilor din domeniul securității din organizarea securității SEAE menționați la articolul 12 din prezenta decizie: aceștia au responsabilitatea de a furniza informări de sensibilizare în domeniul securității pentru a asigura faptul că personalul din sectorul lor este informat periodic, de a promova o cultură solidă a securității în sfera lor de responsabilitate, de a institui măsuri pentru monitorizarea comportamentului în materie de securitate al personalului și de a raporta autorităților de securitate competente orice informații nefavorabile care pot avea un impact asupra CSP al oricărei persoane;

(d) SEAE și a statelor membre: acestea instituie canalele necesare pentru a comunica informații care pot avea un impact asupra CSP sau a autorizației de acces la IUEC ale oricărei persoane.

27. 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, confirmă acest lucru în scris.

IV. ÎMPREJURĂRI EXCEPȚIONALE

28. În cazuri de urgență, când interesul SEAE o justifică corespunzător și în așteptarea finalizării unei investigații de securitate complete, autoritatea de securitate a SEAE poate acorda o autorizație temporară funcționarilor și altor agenți ai SEAE 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 nefavorabile. Investigația de securitate completă ar trebui finalizată cât mai curând posibil. Astfel de autorizații temporare vor fi valabile pentru maximum șase luni și nu permit accesul la informații clasificate TRES 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. SEAE păstrează registre ale acestor confirmări scrise.

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

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

(b) accesul să fie limitat la anumite IUEC și să fie necesar exercitării funcției respective;

(c) persoana în cauză să dețină un CSP valabil;

(d) să fie inițiate demersurile pentru obținerea accesului la nivelul necesar pentru funcția 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 SEAE competentă;

(g) să fi fost consultată ANS/ASD competentă care a eliberat CSP-ul persoanei respective și să nu se fi primit nicio obiecție; și

(h) o dovadă a accesului excepțional, inclusiv o descriere a informațiilor la care a fost aprobat accesul, să fie păstrată de registratura sau de registratura subordonată responsabilă.

30. Procedura de mai sus este utilizată pentru a se acorda acces o singură dată la IUEC de nivel superior următor celui pentru care persoana deține certificatul de securitate. Nu se recurge în mod repetat la această procedură.

31. În împrejurări absolut excepționale, precum misiunile în medii ostile sau în perioade de creștere a tensiunii internaționale, atunci când măsurile de urgență o impun, în special în scopul salvării de vieți, ÎR, autoritatea de securitate a SEAE sau DGBA poate acorda, dacă este posibil în scris, accesul la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET unor persoane care nu dețin CSP-ul necesar, cu condiția ca permisiunea în acest sens să fie absolut necesară. Se păstrează o dovadă a acestor permisiuni, cu descrierea informațiilor la care s-a aprobat accesul.

32. În cazul informațiilor clasificate TRES SECRET UE/EU TOP SECRET, acest acces de urgență este limitat la cetățeni ai UE cărora li s-a autorizat accesul fie la nivelul național echivalent al TRES SECRET UE/EU TOP SECRET, fie la informații clasificate SECRET UE/EU SECRET.

33. Comitetul de securitate al SEAE este informat cu privire la cazurile în care se utilizează procedura prevăzută la punctele 31 și 32.

34. Comitetul de securitate al SEAE primește un raport anual cu privire la utilizarea procedurilor prevăzute în prezenta secțiune.

V. PARTICIPAREA LA REUNIUNI LA SEDIUL SEAE ȘI ÎN DELEGAȚIILE UNIUNII

35. Persoanele desemnate să participe la reuniuni la sediul SEAE și în delegațiile Uniunii în cadrul cărora se discută informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior pot participa numai după ce se confirmă că dețin un CSP. Pentru reprezentanții statelor membre, pentru funcționarii Secretariatului General al Consiliului și ai Comisiei, o CASP sau o altă dovadă a CSP este transmisă de autoritățile competente Direcției SEAE responsabilă de securitate, coordonatorului de securitate al delegației Uniunii sau, în mod excepțional, este prezentată de către persoana în cauză. După caz, se poate folosi o listă consolidată a numelor, care să cuprindă dovada relevantă a CSP.

36. În cazul în care un CSP care permite accesul la IUEC i se retrage unei persoane ale cărei atribuții impun participarea la reuniuni la sediul SEAE sau într-o delegație a Uniunii la care se discută informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la nivel superior, SEAE este informat în acest sens de către autoritatea competentă.

VI. ACCES POTENȚIAL LA IUEC

37. În cazul în care o persoană urmează a fi angajată într-o funcție în care este posibil să aibă acces la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior, aceasta deține un certificat de securitate adecvat sau este escortată în permanență.

38. 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 periodic cu privire la procedurile de securitate pentru protecția IUEC și la obligațiile care le revin pentru protecția acestor informații care le sunt încredințate sau la care pot avea acces în mod accidental.

ANEXA A II

SECURITATEA FIZICĂ A INFORMAȚIILOR UE CLASIFICATE

I. INTRODUCERE

1. Prezenta anexă conține dispoziții pentru punerea în aplicare a articolului 6 din anexa A. Anexa stabilește cerințele minime pentru protecția fizică a incintelor, clădirilor, birourilor, sălilor și a altor spații în care se manipulează și se păstrează IUEC, inclusiv a spațiilor în care sunt amplasate SIC.

2. Măsurile de securitate fizică sunt concepute pentru a împiedica accesul neautorizat la IUEC prin faptul că:

   (a) garantează că IUEC sunt manipulate și păstrate într-un mod adecvat;

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

   (c) descurajează, împiedică și detectează acțiunile neautorizate; și

   (d) împiedică sau întârzie accesul clandestin sau forțat al intrușilor.

II. CERINȚE ȘI MĂSURI DE SECURITATE FIZICĂ

3. SEAE folosește un proces de gestionare a riscurilor pentru protejarea IUEC în incintele sale, pentru a asigura aplicarea unui nivel de protecție fizică proporțional cu riscurile evaluate. Procesul de gestionare a riscurilor 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 o cantitate mare de IUEC sau pentru compilații de astfel de informații, poate fi necesară aplicarea unor măsuri de protecție mai severe;

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

   (d) evaluarea amenințării reprezentate de țara terță, elaborată de INTCEN în special pe baza rapoartelor delegației Uniunii; și

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

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

   (a) o barieră de securizare a unui perimetru: o barieră fizică care protejează limitele unei zone care trebuie protejată;

   (b) sisteme de detectare a intruziunilor (SDI): un SDI poate fi utilizat pentru a spori nivelul de securitate oferit de o barieră de securizare a unui perimetru sau poate fi folosit în săli sau imobile, în locul personalului de securitate sau în sprijinul acestuia;

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

   (d) personalul de securitate: poate fi angajat personal de securitate care a urmat cursuri de formare, supravegheat și, dacă este necesar, posesor al unui certificat de securitate corespunzător pentru, *inter alia*, a descuraja persoanele care intenționează să intre clandestin;

   (e) televiziune 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 anumite 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 eficace 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. Direcția SEAE responsabilă de securitate poate efectua controale la intrare și la ieșire, pentru a descuraja introducerea neautorizată de materiale sau sustragerea neautorizată de 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 incintele noi, cerințele de securitate fizică și specificațiile funcționale ale acestora se definesc ca parte a planificării și concepției incintelor. Pentru incintele 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 echipamentelor destinate protecției fizice a IUEC (cum ar fi containere de securitate, mașini de distrus documente, încuietori pentru uși, sisteme electronice de control al accesului, SDI, sisteme de alarmă), autoritatea de securitate a SEAE se asigură că echipamentele în cauză respectă standardele tehnice și cerințele minime aprobate.

9. Specificațiile tehnice ale echipamentelor destinate protecției fizice a IUEC sunt prevăzute în orientările de securitate care trebuie aprobate de Comitetul de securitate al SEAE.

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 este reevaluată 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).

13. Autoritatea de securitate a SEAE decide că o zonă 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 Direcția SEAE responsabilă de securitate; și

(c) toate celelalte 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 dețin certificatul de securitate la nivelul corespunzător și autorizația specifică de a intra în zona respectivă, acordate pe baza necesității de a cunoaște a acestora;

(c) toate celelalte persoane sunt escortate în permanență sau sunt supuse unor controale echivalente.

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

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

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

(c) dispozitivele electronice sunt lăsate în afara zonei respective.

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 din prezenta anexă;

(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 a SEAE. De asemenea, astfel de inspecții sunt efectuate în urma oricărui acces neautorizat sau a suspiciunii de acces neautorizat; și

(d) aceste zone nu sunt prevăzute cu linii de comunicații, telefoane sau alte dispozitive de comunicare și echipamente electrice 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 clasificate SECRET UE/EU SECRET și la un nivel superior și în cazul în care amenințarea la adresa IUEC este evaluată ca fiind semnificativă, toate dispozitivele de comunicare și echipamentele electrice sau electronice sunt examinate, mai întâi, de autoritatea de securitate a SEAE pentru a se asigura faptul că nicio informație inteligibilă nu poate fi transmisă în mod accidental sau ilicit prin intermediul unor astfel de echipamente în afara perimetrului zonei securizate.

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

20. Pot fi instituite temporar zone securizate și zone securizate din punct de vedere tehnic întro zonă administrativă, în scopul unei reuniuni clasificate sau în orice alt scop similar.

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

(a) nivelul IUEC care pot fi manipulate și păstrate în zona respectivă;

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

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

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

(e) orice alte măsuri și proceduri relevante.

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

V. MĂSURI DE PROTECȚIE FIZICĂ PENTRU MANIPULAREA ȘI PĂSTRAREA IUEC

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

(a) într-o zonă securizată;

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

(c) în afara unei zone securizate sau a unei zone administrative, cu condiția ca deținătorul să transporte IUEC în conformitate cu punctele 30-42 din Anexa A III și să se fi angajat să respecte măsurile compensatorii stabilite în instrucțiunile de securitate emise de autoritatea de securitate a SEAE pentru a se asigura faptul 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 temporar în afara unei zone securizate sau a unei zone administrative, cu condiția ca deținătorul să se fi angajat să respecte măsurile compensatorii stabilite în instrucțiunile de securitate emise de autoritatea de securitate a SEAE.

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

(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 conformitate cu punctele 30-42 din Anexa A III;

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

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

(iv) în cazul documentelor pe suport hârtie, să fi notificat registraturii competente acest fapt.

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

27. IUEC clasificate TRES SECRET UE/EU TOP SECRET sunt manipulate într-o zonă securizată.

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

(a) într-un container de securitate care respectă dispozițiile punctului 8, fiind supus unuia sau mai multora dintre 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 A 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 a SEAE definește proceduri pentru gestionarea cheilor și a combinațiilor de cifruri pentru birouri, săli, 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 tezaur în care sunt păstrate IUEC sunt schimbate:

(a) la primirea unui nou container;

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

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

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

(e) cel puțin la fiecare 12 luni.

ANEXA A III

GESTIONAREA INFORMAȚIILOR CLASIFICATE

I. INTRODUCERE

1. Prezenta anexă conține dispoziții pentru punerea în aplicare a articolului 7 din anexa A. Anexa stabilește măsurile administrative pentru controlul IUEC pe durata ciclului lor de viață, în scopul de a contribui la descurajarea, detectarea și remedierea compromiterii sau pierderii 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 orientările de clasificare relevante, și de a efectua diseminarea informațiilor.

4. Nivelul de clasificare al IUEC se stabilește în conformitate cu articolul 2 alineatul (2) din anexa A și pe baza orientărilor de securitate care trebuie aprobate în conformitate cu articolul 3 alineatul (3) din anexa A.

5. Informațiilor clasificate care provin de la statele membre și care fac obiectul unor schimburi cu SEAE li se atribuie același nivel de protecție precum IUEC care au nivelul de clasificare echivalent. Un tabel de echivalență este prezentat în apendicele B la prezenta decizie.

6. Clasificarea de securitate și, dacă este cazul, data sau evenimentul specific după care nivelul acesteia poate fi redus sau clasificarea poate fi anulată se indică în mod clar și corect, indiferent dacă IUEC se prezintă sub formă tipărită, orală, electronică sau sub orice altă formă.

7. Anumite părți dintr-un document (și anume, pagini, paragrafe, 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.

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 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.

10. Nivelul de clasificare al scrisorilor sau notelor care însoțesc documente atașate trebuie să fie același cu cel mai ridicat nivel al documentelor atașate. Emitentul indică clar, prin folosirea unui marcaj corespunzător, nivelul de clasificare pe care scrisorile 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

11. În afară de marcajele clasificărilor de securitate stabilite la articolul 2 alineatul (2) din anexa A, IUEC pot purta marcaje suplimentare, precum:

(a) un element de identificare care desemnează emitentul;

(b) orice tip de 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.

12. Dacă se decide comunicarea unor IUEC către un stat terț sau către o organizație internațională, informațiile clasificate în cauză se transmit de către Direcția SEAE responsabilă de securitate; acestea poartă un marcaj de comunicare care indică statul terț destinatar sau organizația internațională destinatară.

13. Autoritatea de securitate a SEAE urmează să adopte o listă de marcaje autorizate.

Marcaje de clasificare abreviate

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

15. În interiorul documentelor UE clasificate pot fi utilizate următoarele abrevieri standard pentru a indica nivelul de clasificare al unor secțiuni sau porțiuni de text mai mici de o pagină:

TRES 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

16. La crearea unui document al 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 acesta este marcat ca atare;

(d) documentul este datat;

(e) pe documentele clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior se înscrie numărul exemplarului pe fiecare pagină, în cazul în care acestea urmează să fie distribuite în mai multe exemplare.

17. În cazul acelor IUEC cărora nu li se poate aplica punctul 16, se iau alte măsuri corespunzătoare în conformitate cu orientările de securitate convenite în temeiul prezentei decizii.

Scăderea nivelului de clasificare și declasificarea IUEC

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

19. SEAE reexaminează în mod periodic IUEC pe care le deține, pentru a evalua necesitatea menținerii nivelului de clasificare. SEAE stabilește un sistem de reexaminare, 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 dacă emitentul a indicat de la început un termen anume la care informațiilor trebuie să li se scadă automat nivelul de clasificare sau la care acestea trebuie declasificate automat și dacă informațiile au fost marcate în consecință.

III. ÎNREGISTRAREA IUEC DIN MOTIVE DE SECURITATE

20. La sediu se creează un registru central. Pentru fiecare entitate organizațională din cadrul SEAE în care sunt manipulate IUEC se creează un registru responsabil subordonat registrului central, pentru a se asigura faptul că IUEC sunt manipulate în conformitate cu prezenta decizie. Registrele se amenajează ca zone securizate, astfel cum se definește în anexa A.

Fiecare delegație a Uniunii își stabilește propriul registru al IUEC.

Autoritatea de securitate a SEAE desemnează un șef al acestor registre.

21. În sensul prezentei decizii, înregistrarea din motive de securitate (denumită în continuare „înregistrarea") înseamnă aplicarea unor proceduri prin care se înregistrează ciclul de viață al informațiilor, inclusiv diseminarea și distrugerea acestora. În cazul unui SIC, procedurile de înregistrare pot fi efectuate prin procese din cadrul respectivului SIC.

22. Toate materialele clasificate CONFIDENTIEL UE/EU CONFIDENTIAL și la un nivel superior sunt înregistrate ori de câte ori parvin unei entități organizaționale sau părăsesc entitatea respectivă, inclusiv delegațiilor Uniunii. Informațiile clasificate TRES SECRET UE/EU TOP SECRET sunt înregistrate în registre speciale.

23. Registrul central constituie, la sediul SEAE, principalul punct de intrare și de ieșire pentru schimburile de informații clasificate cu state terțe și organizații internaționale. În acesta se păstrează evidența tuturor schimburilor de astfel de informații.

24. Autoritatea de securitate a SEAE aprobă orientările de securitate privind înregistrarea IUEC în scopuri de securitate, în conformitate cu articolul 14 din prezenta decizie.

Registrele TRES SECRET UE/EU TOP SECRET

25. Registrul central de la sediul SEAE este desemnat ca autoritate centrală de primire și de expediere a informațiilor clasificate TRES SECRET UE/EU TOP SECRET. Dacă este necesar, pot fi desemnate registre subordonate care să trateze astfel de informații în scopul înregistrării.

26. Aceste registre subordonate nu pot transmite documente clasificate TRES SECRET UE/EU TOP SECRET direct altor registre subordonate aceluiași registru central TRES SECRET UE/EU TOP SECRET sau în exterior fără aprobarea expresă și scrisă a acestuia din urmă.

IV. COPIEREA ȘI TRADUCEREA DOCUMENTELOR UE CLASIFICATE

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

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

29. Măsurile de securitate aplicabile documentului original se aplică copiilor și traducerilor acestuia. Copiile documentelor clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior se realizează numai de către un registru (subordonat) relevant cu ajutorul unui copiator securizat. Copiile trebuie înregistrate.

V. TRANSPORTUL IUEC

30. Pentru transportul IUEC se respectă măsurile de protecție prevăzute la punctele 32-42. În cazul în care IUEC sunt transportate pe suporturi electronice și fără a aduce atingere articolului 7 alineatul (4) din anexa A, măsurile de protecție prevăzute mai jos pot fi completate de contramăsuri tehnice adecvate stabilite de autoritatea de securitate a SEAE, astfel încât riscul pierderii sau compromiterii lor să fie redus la minimum.

31. Autoritatea de securitate a SEAE emite instrucțiuni privind transportul IUEC în conformitate cu prezenta decizie.

În interiorul unei clădiri sau al unui grup autonom de clădiri

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

33. În interiorul unei clădiri sau al unui grup autonom de clădiri, informațiile clasificate TRES SECRET UE/EU TOP SECRET sunt transportate de către persoane care dețin un certificat de securitate corespunzător și într-un plic securizat pe care este înscris numai numele destinatarului.

În UE

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

35. 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 A II;

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

(iii) persoanele să dețină un certificat de securitate pentru nivelul corespunzător și să fie informate cu privire la responsabilitățile pe care le au în materie de securitate;

(iv) persoanelor să li se acorde 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 aplice măsuri de protecție corespunzătoare în conformitate cu cerințele minime care trebuie prevăzute în orientările de securitate convenite în temeiul articolului 21 alineatul (1) din prezenta decizie.

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

36. Materialele clasificate CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET (de exemplu, echipamente sau aparate) care nu pot fi transportate prin mijloacele prevăzute la punctul 34 sunt transportate ca marfă de către societăți comerciale de curierat, în conformitate cu anexa A V.

37. Transportul informațiilor clasificate TRES 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 sau între entități ale UE situate în state terțe

38. IUEC transportate din UE către teritoriul unui stat terț sau între entități ale UE situate în state terțe sunt astfel ambalate încât să fie protejate împotriva divulgării neautorizate.

39. Transportul informațiilor clasificate CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET din UE către teritoriul unui stat terț și transportul oricăror informații clasificate până la nivelul SECRET UE/EU SECRET între entități ale UE situate în state terțe se efectuează prin unul dintre 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 în care este consemnat pachetul și care 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 A II;

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

(v) persoanele să dețină un certificat de securitate pentru nivelul corespunzător și să fie informate cu privire la responsabilitățile pe care le au în materie de securitate.

40. Transportul informațiilor clasificate CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET și 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 10 alineatul (2) din anexa A.

41. Informațiile clasificate RESTREINT UE/EU RESTRICTED pot fi, de asemenea, transportate din UE către teritoriul unui stat terț prin intermediul serviciilor poștale sau al serviciilor de curierat comercial.

42. Transportul informațiilor clasificate TRES SECRET UE/EU TOP SECRET din UE către teritoriul unui stat terț sau între entități ale UE situate în state terțe se efectuează prin curier militar sau diplomatic.

VI. DISTRUGEREA IUEC

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

44. Documentele care trebuie înregistrate în conformitate cu articolul 7 alineatul (2) din anexa A 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.

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

46. Gestionarul registrului 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 timp de cel puțin zece ani în cazul documentelor TRES SECRET UE/EU TOP SECRET și de cel puțin cinci ani în cazul documentelor CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET.

47. Documentele clasificate, inclusiv cele clasificate RESTREINT UE/EU RESTRICTED, sunt distruse prin metode care îndeplinesc standardele relevante ale UE sau standardele 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.

48. Distrugerea suporturilor informatice de stocare utilizate pentru IUEC se realizează în conformitate cu procedurile aprobate de către autoritatea de securitate a SEAE.

VII. INSPECȚII DE SECURITATE

Inspecții de securitate ale SEAE

49. În conformitate cu articolul 16 din prezenta decizie, inspecțiile de securitate ale SEAE cuprind:

(a) inspecții de securitate generale prin care se analizează nivelul de securitate general la sediul central al SEAE, în cadrul delegațiilor Uniunii și în toate incintele accesorii sau conexe, în special în scopul de a se evalua eficacitatea măsurilor de securitate puse în aplicare pentru protejarea intereselor în materie de securitate a SEAE;

(b) inspecții privind securitatea IUEC prin care se evaluează, de obicei în vederea unei acreditări, eficacitatea măsurilor puse în aplicare pentru protecția IUEC la sediul central al SEAE și în cadrul delegațiilor Uniunii.

Mai precis, aceste inspecții se efectuează, printre altele, pentru:

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

(ii) sublinierea importanței securității și a unei gestionări eficace a riscurilor de securitate în interiorul entităților inspectate;

(iii) recomandarea unor contramăsuri în scopul de a atenua impactul specific al pierderii confidențialității, integrității sau disponibilității informațiilor clasificate; și

(iv) consolidarea programelor de formare și de sensibilizare în domeniul securității desfășurate de autoritățile de securitate.

Efectuarea inspecțiilor de securitate ale SEAE și rapoartele de inspecție

50. Inspecțiile de securitate ale SEAE se efectuează de către o echipă de inspecție din cadrul Direcției SEAE responsabilă de securitate și, atunci când este necesar, cu sprijinul experților în materie de securitate din alte instituții ale UE sau din statele membre.

Echipa de inspecție are acces la toate amplasamentele în care se manipulează IUEC, în special la registre și la punctele de prezență ale SIC.

51. În cadrul delegațiilor Uniunii, inspecțiile de securitate ale SEAE pot fi efectuate, ori de câte ori este necesar, cu sprijinul responsabililor cu securitatea de la ambasadele statelor membre situate în țările terțe.

52. Înainte de sfârșitul fiecărui an calendaristic, autoritatea de securitate a SEAE adoptă un program de inspecții de securitate în cadrul SEAE pentru anul următor.

53. Autoritatea de securitate a SEAE poate organiza, ori de câte ori este necesar, inspecții de securitate care nu sunt prevăzute în programul sus-menționat.

54. La sfârșitul inspecției de securitate, entității inspectate i se prezintă principalele concluzii și recomandări. Ulterior, echipa de inspecție întocmește un raport de inspecție. În cazurile în care s-au propus măsuri corective și recomandări, în raport se includ suficiente detalii pentru a sprijini concluziile la care s-a ajuns. Raportul este înaintat autorității de securitate a SEAE și directorului entității inspectate.

Sub responsabilitatea Direcției SEAE responsabilă de securitate se elaborează un raport periodic care ilustrează principalele concluzii desprinse în urma inspecțiilor desfășurate într-o perioadă specificată și care este analizat de Comitetul de securitate al SEAE.

Efectuarea inspecțiilor de securitate în cadrul agențiilor și organelor UE instituite în temeiul titlului V capitolul 2 din TUE și rapoartele de inspecție

55. Direcția SEAE responsabilă de securitate poate, după caz, desemna experți colaboratori care să participe la echipele comune de inspecție ale UE care efectuează inspecții în agențiile și organele UE instituite în temeiul titlului V capitolul 2 din TUE.

Lista de control pentru inspecțiile de securitate ale SEAE

56. Direcția SEAE responsabilă de securitate elaborează și actualizează o listă de control pentru inspecțiile de securitate, cuprinzând aspectele care urmează să fie verificate în cursul unei inspecții de securitate a SEAE. Lista de control respectivă este înaintată Comitetului de securitate al SEAE.

57. 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 de comun acord cu entitatea inspectată. Aceasta nu face parte din raportul de inspecție.

ANEXA A IV

PROTECȚIA IUEC MANIPULATE ÎN SIC

I. INTRODUCERE

1. Prezenta anexă conține dispoziții pentru punerea în aplicare a articolului 8 din anexa A.

2. Următoarele proprietăți și concepte referitoare la asigurarea informațiilor (AI) sunt esențiale pentru securitatea și funcționarea corectă a operațiilor derulate în sistemele informatice și de comunicații (SIC):

Autenticitate:	garanția faptului că informațiile sunt autentice și provin din surse de bună credință;
Disponibilitate:	proprietatea informațiilor de a putea fi accesate și utilizate la cerere de către o entitate autorizată;
Confidențialitate:	proprietatea informațiilor de a nu fi divulgate persoanelor, entităților sau proceselor neautorizate;
Integritate:	proprietate care constă în garantarea acurateței și a exhaustivității informațiilor și activelor;
Nerepudiere:	capacitatea de a dovedi că o acțiune sau un 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 manipulează IUEC. Cerințele detaliate pentru punerea în aplicare a acestor dispoziții sunt definite în orientările de securitate privind AI.

Gestionarea riscurilor de securitate

4. Gestionarea riscurilor de securitate face parte integrantă din definirea, dezvoltarea, utilizarea și întreținerea SIC. Gestionarea riscurilor (evaluarea, tratarea, acceptarea și comunicarea) se efectuează, ca proces iterativ, în comun de către reprezentanți ai proprietarilor de sisteme, ai autorităților responsabile cu proiectul, ai autorităților responsabile cu funcționarea și ai autorităților de aprobare în materie de securitate, utilizând un proces de evaluare a riscurilor confirmat, transparent și care poate fi pe deplin înțeles. Domeniul de acoperire al SIC și al activelor sale este definit clar în momentul inițierii procesului de gestionare a riscurilor.

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

6. Rolul gestionării riscurilor de securitate este de a aplica un set de măsuri de securitate care duc la un echilibru satisfăcător între cerințele utilizatorului și riscurile reziduale de securitate.

7. Cerințele specifice, scara și gradul de detaliere pe care autoritatea relevantă de acreditare în materie de securitate (AAS) le stabilește pentru acreditarea unui SIC sunt proporționale cu riscurile evaluate, ținând seama de toți factorii relevanți, inclusiv de nivelul de clasificare al IUEC manipulate în cadrul SIC. Acreditarea implică o declarație formală privind riscurile reziduale și acceptarea riscurilor reziduale 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. Rolul și interacțiunea fiecărui actor implicat într-un SIC în ceea ce privește securitatea se stabilesc clar pentru fiecare fază a ciclului de viață.

10. Orice SIC, inclusiv măsurile sale de securitate tehnice și de altă natură, face obiectul unor teste de securitate în cursul procesului de acreditare, pentru a se garanta obținerea nivelului corespunzător de asigurare privind măsurile de securitate puse în aplicare și pentru 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 atunci când apar situații 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. SEAE cooperează cu SGC, Comisia și statele membre pentru elaborarea celor mai bune practici în materie de protecție a IUEC manipulate într-un SIC. Orientările privind bunele practici conțin 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 manipulate într-un 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 sunt operate de SEAE și în care sunt manipulate IUEC.

Apărarea în profunzime

16. În scopul atenuării riscurilor la adresa SIC, sunt puse în aplicare o serie de măsuri de securitate tehnice și de altă natură, 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 număr cât mai mic de informații sau de active ale unui SIC și să împiedice daunele ulterioare; și

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

Gradul de strictețe și de aplicabilitate al acestor măsuri de securitate este determinat în urma unei evaluări a riscurilor.

17. Autoritățile competente ale SEAE 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 părți terțe 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 necesare pentru îndeplinirea cerințelor operaționale.

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

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

Sensibilizare la asigurarea informațiilor

21. Sensibilizarea la riscurile 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 lipsurile în materie de securitate ar putea produce pagube semnificative SIC și întregii organizații;

(b) că din interconectivitate și interdependență ar putea rezulta pagube potențiale pentru alții; și

(c) care este responsabilitatea și răspunderea fiecăruia pentru securitatea SIC, în funcție de rolul pe care îl au în cadrul sistemelor și al proceselor.

22. Pentru a se garanta înțelegerea responsabilităților în materie de securitate, tot personalul implicat, inclusiv personalul de conducere de nivel superior și utilizatorii SIC, urmează cursuri obligatorii de formare și de sensibilizare în domeniul AI.

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 gestionare a riscurilor și în conformitate cu politicile și orientările de securitate relevante.

24. Nivelul de asigurare se verifică prin utilizarea unor procese și metodologii recunoscute 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 autoritate națională de aprobare criptografică (AAC) a unui stat membru.

26. Înainte de a fi recomandate pentru aprobare de către AAC a SEAE, în conformitate cu articolul 8 alineatul (5) din prezenta decizie, aceste produse criptografice trebuie să treacă cu succes o evaluare de către o a doua parte, efectuată de o autoritate de autorizare calificată (AQUA) a unui stat membru neimplicat în proiectarea sau fabricarea echipamentului. Gradul de detaliere al evaluării efectuate de o a doua parte depinde de nivelul maxim de clasificare avut în vedere al IUEC care urmează să fie protejate prin aceste produse.

27. Dacă acest lucru este justificat din motive operaționale specifice, AAC a SEAE poate, la recomandarea Comitetului de securitate al Consiliului, 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 8 alineatul (5) din prezenta decizie.

28. O AQUA este o AAC 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. Înaltul Reprezentant aprobă o politică de securitate privind calificarea și aprobarea produselor de securitate IT necriptografice.

Transmiterea în interiorul zonelor securizate

30. Fără a aduce atingere dispozițiilor prezentei decizii, în cazul în care transmiterea IUEC este limitată la zonele securizate sau la zonele administrative, se poate recurge la o distribuție necriptată sau la o criptare la nivel inferior, pe baza rezultatului unui proces de gestionare a riscurilor și cu condiția obținerii aprobării AAS.

Interconectări securizate ale SIC

31. În sensul prezentei decizii, o interconectare reprezintă conectarea directă a două sau a mai multor 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 legate de activități sau operaționale pentru astfel de interconectări sunt stabilite și aprobate de autoritățile competente;

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

    (c) sunt puse în aplicare servicii de protecție a perimetrului (*Boundary Protection Services*, BPS) la periferia tuturor SIC.

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

    Atunci când rețeaua neprotejată sau publică este utilizată numai ca suport și datele sunt criptate prin intermediul unui produs criptografic aprobat în conformitate cu articolul 8 alineatul (5) din prezenta decizie, o astfel de conexiune nu este considerată ca fiind o interconectare.

35. Este interzisă interconectarea directă sau în cascadă a unui SIC acreditat să manipuleze informații TRES 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 a SEAE.

37. Suporturilor informatice de stocare le poate fi scăzut nivelul de clasificare sau acestea pot fi declasificate în conformitate cu orientările de securitate care urmează să fie stabilite în temeiul articolului 8 alineatul (2) din prezenta decizie.

Situații de urgență

38. Fără a aduce atingere dispozițiilor prezentei decizii, procedurile specifice descrise în continuare pot fi aplicate, pentru o perioadă limitată, într-o situație de urgență, cum ar fi crizele, conflictele sau situațiile de război iminente sau efective sau în 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 dispun de echipamentele de criptare necesare sau nu dispun de niciun echipament de criptare; și

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

40. Informațiile clasificate transmise în împrejurările enunțate la punctul 39 nu poartă niciun marcaj și nicio indicație care să le distingă de informații care sunt 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 39, se înaintează un raport ulterior Direcției SEAE responsabilă de securitate și, prin intermediul acesteia, Comitetului de securitate al SEAE. În acest raport se vor preciza cel puțin expeditorul, destinatarul și inițiatorul fiecărei IUEC.

III. FUNCȚII ȘI AUTORITĂȚI DE ASIGURARE A INFORMAȚIILOR

42. În SEAE se stabilesc următoarele funcții în materie de 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 (AAI)

43. AAI este responsabilă cu:

(a) elaborarea orientărilor de securitate privind AI și monitorizarea eficacității și pertinenței acestora;

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

(c) asigurarea faptului că măsurile AI selectate pentru protejarea IUEC respectă orientările relevante care reglementează eligibilitatea și selecția acestora;

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

(e) coordonarea cursurilor de formare și sensibilizare în domeniul AI;

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

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

Autoritatea TEMPEST

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

Autoritatea de aprobare criptografică (AAC)

45. AAC este responsabilă cu asigurarea conformității produselor criptografice cu orientările privind criptografierea aferente. Aceasta aprobă produse criptografice de protecție a IUEC până la un anumit nivel de clasificare în mediul lor operațional.

Autoritatea de distribuție criptografică (ADC)

46. ADC este responsabilă cu:

(a) gestionarea și evidența materialului criptografic al UE;

(b) garantarea aplicării unor proceduri adecvate și a stabilirii unor canale adecvate pentru evidența, manipularea 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 (AAS)

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

(a) asigurarea respectării de către SIC a orientărilor de securitate relevante, furnizarea unei declarații de aprobare a SIC în vederea manipulării IUEC până la un anumit nivel de clasificare în mediul lor operațional, stabilirea clauzelor și a condițiilor de acreditare, precum și a criteriilor pe baza cărora este necesară o reaprobare;

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

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

(d) examinarea și aprobarea documentației de securitate, inclusiv a declarațiilor privind gestionarea riscurilor și riscurile reziduale, a declarațiilor privind cerințele de securitate specifice sistemului (denumite în continuare „CSSS"), a documentației de verificare a aplicării securității și a procedurilor operaționale de securitate (denumite în continuare „SecOP"), și asigurarea conformității acestei documentații de securitate cu normele și orientările de securitate ale SEAE;

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

(f) definirea cerințelor de securitate (precum nivelul certificatelor de securitate a personalului) pentru pozițiile sensibile în relație cu SIC;

(g) susținerea alegerii unor produse criptografice și TEMPEST omologate care sunt 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 gestionarea riscurilor de securitate, în special a riscurilor reziduale, și la clauzele și condițiile declarației de aprobare.

48. AAS din cadrul SEAE este responsabilă cu acreditarea tuturor SIC care funcționează în domeniul de competență al SEAE.

Consiliul de acreditare în probleme de securitate (CAS)

49. Un CAS mixt este responsabil cu acreditarea SIC din domeniul de competență atât al AAS din cadrul SEAE, cât și al AAS din statele membre. Acesta este compus dintr-un reprezentant al AAS din fiecare stat membru, iar la lucrările sale participă un reprezentant al AAS din cadrul SGC și al Comisiei. 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 din cadrul SEAE. 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 al SEAE rapoarte periodice cu privire la activitățile sale și îi notifică toate declarațiile de acreditare.

Autoritatea operațională de asigurare a informațiilor

50. Autoritatea operațională însărcinată cu AI pentru fiecare sistem este responsabilă de:

(a) elaborarea unei documentații de securitate, în conformitate cu orientările de securitate, în special a declarației privind cerințele de securitate specifice sistemului (**CSSS**), inclusiv a declarației privind riscurile reziduale, a procedurilor operaționale de securitate (**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 faptul că acestea sunt instalate, configurate și întreținute în siguranță, în conformitate cu documentația de securitate relevantă;

(c) participarea la selectarea măsurilor și dispozitivelor de securitate TEMPEST, dacă sunt necesare în cadrul CSSS, și garantarea că acestea sunt instalate și întreținute în siguranță în cooperare cu AT;

(d) monitorizarea punerii în aplicare și a aplicării SecOP și, dacă este cazul, delegarea responsabilităților în materie de securitate operațională proprietarului sistemului;

(e) gestionarea și manipularea produselor criptografice, asigurarea custodiei elementelor criptografice și a elementelor controlate și, dacă este cazul, asigurarea generării de variabile criptografice;

(f) efectuarea unor analize, reexaminări și teste de securitate, în special pentru elaborarea rapoartelor relevante de evaluare a riscurilor, astfel cum solicită AAS;

(g) organizarea unei formări privind AI specifice fiecărui SIC;

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

ANEXA A V

SECURITATEA INDUSTRIALĂ

I. INTRODUCERE

1. Prezenta anexă conține dispoziții pentru punerea în aplicare a articolului 9 din anexa A. 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 atribuite de SEAE.

2. Autoritatea de securitate a SEAE aprobă orientări privind securitatea industrială în care sunt indicate în special cerințe detaliate referitoare la certificatele de securitate industrială (CSI), anexele de securitate, vizite, transmiterea și transportul IUEC.

II. ELEMENTELE DE SECURITATE DINTR-UN CONTRACT CLASIFICAT

Ghidul clasificărilor de securitate (GCS)

3. Înainte de a lansa o invitație de participare la licitație sau de a atribui un contract clasificat, SEAE, în calitate de autoritate contractantă, stabilește clasificarea de securitate a informațiilor care urmează să fie furnizate ofertanților și contractanților, precum și clasificarea de securitate a informațiilor care urmează să fie create de contractant. În acest scop, SEAE 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, SEAE 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 al contractului nu poate să fie mai scăzut decât cel mai ridicat nivel de clasificare al oricăruia dintre elementele sale; și

(c) atunci când este cazul, SEAE ia legătura cu ANS/ASD 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 ghidului clasificărilor de securitate.

Anexa de securitate (AS)

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

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

Instrucțiuni de securitate pentru program/proiect (ISP)

7. În funcție de domeniul de aplicare al programelor sau al proiectelor care implică accesarea, manipularea sau păstrarea IUEC, pot fi elaborate instrucțiuni de securitate pentru program/proiect (ISP) specifice de către autoritatea contractantă desemnată să gestioneze respectivul program sau proiect. ISP necesită aprobarea de către ANS/ASD sau de către oricare altă autoritate de securitate competentă din statele membre participante la program/proiect și pot conține cerințe de securitate suplimentare.

III. CERTIFICATUL DE SECURITATE INDUSTRIALĂ (CSI)

8. Direcția SEAE responsabilă de securitate solicită ANS/ASD sau altei autorități de securitate competente din statul membru în chestiune să acorde un CSI 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 localurile proprii. Contractanților, subcontractanților și potențialilor contractanți sau subcontractanți nu le sunt furnizate IUEC și nici nu le sunt acordate drepturi de acces la acestea înainte ca SEAE să fi primit dovada unui CSI.

9. Atunci când este cazul, SEAE, în calitate de autoritate contractantă, înștiințează ANS/ASD competentă 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 un 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.

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

11. SEAE, în calitate de autoritate contractantă, solicită ANS/ASD sau oricărei alte autorități de securitate competente care a eliberat un CSI să îi comunice eventualele informații nefavorabile care afectează CSI. În cazul subcontractelor, ANS/ASD sau orice altă autoritate de securitate competentă este informată în mod corespunzător.

12. Retragerea unui CSI de către ANS/ASD sau de către orice altă autoritate de securitate competentă constituie un motiv suficient pentru ca SEAE, în calitate de autoritate contractantă, să rezilieze un contract clasificat sau să excludă un ofertant din competiție.

IV. CERTIFICATELE DE SECURITATE A PERSONALULUI (CSP) PENTRU CONTRACTANȚI

13. Toți membrii personalului contractanților care au nevoie de acces la IUEC clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior trebuie să dețină un certificat de securitate corespunzător, iar accesul acestora la informații trebuie să fie determinat de necesitatea de a cunoaște. Pentru accesul la IUEC clasificate RESTREINT UE/EU RESTRICTED nu este necesar un CSP, însă trebuie să existe necesitatea de cunoaște.

14. Cererile de CSP pentru personalul unui contractant se înaintează ANS/ASD responsabilă pentru entitatea respectivă.

15. SEAE le pune în vedere contractanților care doresc să angajeze un resortisant al unui stat terț într-un post care presupune accesul la IUEC că este de responsabilitatea ANS/ASD a statului membru în care își are sediul și este înregistrat angajatorul să stabilească dacă persoanei respective i se poate acorda accesul la astfel de informații, în conformitate cu prezenta decizie, și să confirme că înainte de acordarea unui astfel de acces este necesar să se fi obținut consimțământul emitentului.

V. CONTRACTE ȘI SUBCONTRACTE CLASIFICATE

16. Atunci când IUEC sunt furnizate unui ofertant în etapa precontractuală, invitația de participare la licitație trebuie să conțină o dispoziție prin care ofertanții care nu depun o ofertă sau care nu sunt selectați sunt obligați să restituie toate documentele clasificate într-un termen specificat.

17. Odată ce un contract sau un subcontract clasificat a fost atribuit, SEAE, în calitate de autoritate contractantă, notifică ANS/ASD sau oricărei alte autorități de securitate competente de care ține contractantul sau subcontractantul respectiv dispozițiile în materie de securitate ale contractului clasificat.

18. În cazul rezilierii sau al ajungerii la termen a acestor contracte, SEAE, în calitate de autoritate contractantă (și/sau ANS/ASD sau orice altă autoritate de securitate competentă, după cum este necesar, în cazul subcontractelor) notifică de îndată acest lucru ANS/ASD sau oricărei alte autorități de securitate competente a statului membru în care este înregistrat contractantul sau subcontractantul.

19. În general, contractantul sau subcontractantul are obligația de a înapoia autorității contractante, la rezilierea sau la ajungere la termen a contractului sau a subcontractului clasificat, toate IUEC pe care le deține.

20. Dispozițiile specifice privind distrugerea IUEC în timpul executării contractului sau la rezilierea sau ajungerea la termen a acestuia sunt prevăzute în AS.

21. În cazul în care contractantul sau subcontractantul este autorizat să păstreze IUEC după rezilierea sau încetarea unui contract, standardele minime cuprinse în prezenta decizie trebuie respectate în continuare și confidențialitatea IUEC trebuie protejată de către contractant sau subcontractant.

22. Condițiile pe care trebuie să le îndeplinească contractantul pentru a putea subcontracta sunt menționate în invitația de participare la licitație și în contract.

23. Un contractant obține permisiunea SEAE, 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 și care nu a încheiat un acord privind securitatea informațiilor cu UE.

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

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

VI. VIZITE PRIVIND CONTRACTELE CLASIFICATE

26. În cazul în care SEAE, contractanții necesită acces la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET în incintele subcontractanților sau invers, în scopul executării unui contract clasificat, vizitele sunt organizate în colaborare cu ANS/ASD sau cu orice altă autoritate de securitate competentă implicată. Acest lucru nu aduce atingere dreptului ANS/ASD de a conveni asupra unei proceduri prin care astfel de vizite pot fi organizate direct, în cadrul unor proiecte specifice.

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

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

VII. TRANSMITEREA ȘI TRANSPORTUL IUEC

29. În ceea ce privește transmiterea IUEC prin mijloace electronice, se aplică dispozițiile relevante ale articolului 8 din anexa A și ale anexei A IV.

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

31. Pentru transportul ca marfă al materialelor clasificate se aplică următoarele principii la 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) pentru societățile care asigură transportul se obține un CSI de nivel corespunzător dacă activitatea de transport presupune și depozitarea informațiilor clasificate în localurile contractanților. În toate cazurile, personalul care se ocupă de transportul respectiv deține certificate de securitate corespunzătoare, în conformitate cu anexa A I;

(d) înaintea oricărei deplasări transfrontaliere de materiale clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET, expeditorul întocmește un plan de transport care trebuie aprobat de SEAE împreună cu, atunci când este cazul, ANS/ASD ale expeditorului și ale destinatarului sau cu orice altă autoritate de securitate competentă implicată;

(e) transporturile se realizează, în măsura posibilului, pe rute directe și se finalizează pe atât de rapid pe cât o permit împrejurările;

(f) atunci când este posibil, ar trebui să se aleagă numai rute care trec prin state membre. Rutele care trec prin alte state decât statele membre ar trebui alese numai cu autorizația SEAE sau a oricărei alte autorități de securitate competente atât din statul expeditorului, cât și din cel al destinatarului.

VIII. TRANSFERUL IUEC CĂTRE CONRACTANȚII AFLAȚI ÎN STATE TERȚE

32. IUEC sunt transferate contractanților și subcontractanților aflați în state terțe care sunt părți la un acord de securitate în curs de valabilitate semnat cu UE, în conformitate cu măsurile de securitate convenite între SEAE, în calitate de autoritate contractantă, și ANS/ASD din statul terț în care este înregistrat contractantul.

IX. MANIPULAREA ȘI PĂSTRAREA IUEC CLASIFICATE RESTREINT UE/EU RESTRICTED

33. SEAE, în calitate de autoritate contractantă, împreună cu, după caz, ANS/ASD a statului membru, are dreptul să efectueze vizite în localurile contractanților/subcontractanților în temeiul clauzelor contractuale, în scopul de a verifica dacă s-au aplicat măsurile de securitate relevante pentru protecția IUEC la nivelul RESTREINT UE/EU RESTRICTED, astfel cum se prevede în contract.

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

35. În cazul contractelor atribuite de SEAE care conțin informații clasificate RESTREINT UE/EU RESTRICTED, contractanții sau subcontractanții și personalul acestora nu au obligația de a deține CSI sau CSP.

36. SEAE, în calitate de autoritate contractantă, analizează răspunsurile la invitațiile de participare la licitații 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 al dispozițiilor administrative naționale.

37. Condițiile pe care trebuie să le îndeplinească contractantul pentru a putea subcontracta trebuie să fie conforme cu punctele 22-24.

38. Atunci când contractul prevede manipularea unor informații clasificate RESTREINT UE/EU RESTRICTED într-un SIC operat de un contractant, SEAE, 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 riscurile evaluate, luându-se în considerare toți factorii relevanți. Domeniul de acreditare al unui astfel de SIC este convenit de autoritatea contractantă cu ANS/ASD competentă.

ANEXA A VI

SCHIMBUL DE INFORMAȚII CLASIFICATE CU STATE TERȚE ȘI ORGANIZAȚII INTERNAȚIONALE

I. INTRODUCERE

1. Prezenta anexă conține dispoziții pentru punerea în aplicare a articolului 10 din anexa A.

II. CADRE CARE REGLEMENTEAZĂ SCHIMBUL DE INFORMAȚII CLASIFICATE

2. SEAE poate schimba IUEC cu state terțe sau cu organizații internaționale în conformitate cu articolul 10 alineatul (1) din anexa A.

Pentru sprijinirea ÎR în îndeplinirea responsabilităților stabilite la articolul 218 din TFUE:

(a) SEAE stabilește, prin departamentul său geografic sau tematic relevant și în consultare cu Direcția SEAE responsabilă de securitate, dacă este necesar să existe un schimb de IUEC pe termen lung cu statul terț sau cu organizația internațională în chestiune;

(b) Direcția SEAE responsabilă de securitate prezintă ÎR, după ce s-a consultat cu departamentul geografic relevant din cadrul SEAE și dacă este cazul, proiectele de texte care urmează să fie propuse Consiliului în temeiul articolului 218 alineatele (3), (5) și (6) din TFUE;

(c) Direcția SEAE responsabilă de securitate sprijină ÎR la conducerea negocierilor, în coordonare cu serviciile relevante ale Comisiei și ale Secretariatului General al Consiliului;

(d) în ceea ce privește acordurile sau convențiile încheiate cu state terțe și având ca obiect participarea acestora la operațiunile de gestionare a crizelor desfășurate în cadrul PSAC, astfel cum se menționează la articolul 10 alineatul (1) litera (c) din anexa A, Direcția de planificare și de gestionare a crizelor din cadrul SEAE prezintă ÎR, după ce s-a consultat cu serviciile relevante ale SEAE și dacă este cazul, proiectele de texte care urmează să fie propuse Consiliului în temeiul articolului 218 alineatele (3), (5) și (6) din TFUE și sprijină ÎR la conducerea negocierilor, în coordonare cu serviciile relevante ale SEAE și ale Secretariatului General al Consiliului.

3. Atunci când în acordurile privind securitatea informațiilor se prevede că Direcția SEAE responsabilă de securitate – în coordonare cu Direcția de securitate din cadrul Direcției Generale Resurse Umane și Securitate a Comisiei și cu Oficiul de securitate al Secretariatului General al Consiliului – și autoritatea de securitate competentă a statului terț sau a organizației internaționale în cauză au obligația de a conveni asupra unor modalități tehnice de punere în aplicare, respectivele modalități trebuie să țină seama de nivelul de protecție prevăzut de regulamentele, structurile și procedurile de securitate existente în statul terț sau în cadrul organizației internaționale în cauză.

4. Atunci când există o necesitate pe termen lung pentru SEAE de a schimba informații clasificate, în principiu, cel mult la nivelul RESTREINT UE/EU RESTRICTED cu un stat terț sau cu o organizație internațională și când s-a stabilit că partea în cauză nu deține un sistem de securitate suficient de dezvoltat care să îi permită încheierea unui acord privind securitatea informațiilor, ÎR poate, după ce a primit avizul favorabil unanim al Comitetului de securitate al SEAE, în conformitate cu articolul 15 alineatul (5) din prezenta decizie, să încheie un acord administrativ cu autoritățile de securitate competente ale statului terț sau ale organizației internaționale în cauză.

5. Nu este permis schimbul de IUEC prin mijloace electronice cu un stat terț sau cu o organizație internațională, cu excepția cazului în care acest lucru este prevăzut în mod explicit în acordul privind securitatea informațiilor sau în acordul administrativ.

6. În temeiul acordurilor administrative privind schimbul de informații clasificate, SEAE și statul terț sau organizația internațională desemnează fiecare un registru ca principal punct de intrare și de ieșire a informațiilor clasificate care fac obiectul schimbului. Pentru SEAE, acesta va fi registrul central al SEAE.

7. În general, acordurile administrative iau forma unui schimb de scrisori.

III VIZITE DE EVALUARE

8. Vizitele de evaluare menționate la articolul 17 din prezenta decizie sunt efectuate de comun acord cu statul terț sau cu organizația internațională în cauză; ele vizează:

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

(b) eventualele particularități ale actelor cu putere de lege, ale dispozițiilor administrative, ale politicilor și ale procedurilor în domeniul securității care sunt în vigoare în statul terț sau se aplică organizației internaționale și care pot avea un impact asupra nivelului maxim de informații clasificate care pot fi schimbate;

(c) măsurile și procedurile de securitate în vigoare pentru protecția informațiilor clasificate; și

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

9. Nu este permis schimbul de IUEC înainte ca vizita de evaluare să fi fost efectuată și ca nivelul la care informațiile clasificate pot fi schimbate între părți să fi fost stabilit, pe baza echivalenței nivelului de protecție care va fi atribuit informațiilor respective.

Dacă, în așteptarea acestei vizite de evaluare, ÎR este informat cu privire la existenta unor motive excepționale sau urgente pentru schimbul de informații clasificate, SEAE:

(a) solicită, în primul rând, consimțământul scris al emitentului, pentru a stabili că nu există obiecții cu privire la comunicarea informațiilor;

(b) sesizează autoritatea de securitate a SEAE, care poate hotărî comunicarea informațiilor, cu condiția să se fi obținut avizul favorabil unanim al statelor membre, astfel cum sunt reprezentate în Comitetul de securitate al SEAE.

Dacă SEAE nu poate stabili cine este emitentul, autoritatea de securitate a SEAE își asumă responsabilitatea emitentului după obținerea avizului favorabil unanim al Comitetului de securitate al SEAE.

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

10. Atunci când pentru schimbul de informații clasificate cu un stat terț sau cu o organizație internațională există un cadru în conformitate cu articolul 10 alineatul (1) din anexa A, decizia ca SEAE să comunice IUEC unui stat terț sau unei organizații internaționale este adoptată de autoritatea de securitate a SEAE, care poate delega această competență unor înalți funcționari ai SEAE sau altor persoane aflate sub conducerea sa.

11. Dacă SEAE nu este emitentul informațiilor clasificate care urmează a fi comunicate, și nici al materialelor-sursă pe care aceste informații le-ar putea conține, SEAE solicită, mai întâi, consimțământul scris al emitentului, în scopul de a stabili că nu există obiecții cu privire la comunicarea informațiilor respective. Dacă SEAE nu poate stabili cine este emitentul, autoritatea de securitate a SEAE își asumă responsabilitatea emitentului după obținerea avizului favorabil unanim al statelor membre, astfel cum sunt reprezentate în Comitetul de securitate al SEAE.

V. COMUNICAREA AD HOC EXCEPȚIONALĂ A IUEC

12. Atunci când nu există niciunul dintre cadrele menționate la articolul 10 alineatul (1) din anexa A și când interesele UE sau interesele unuia sau mai multor state membre ale acesteia cer comunicarea de IUEC din motive politice, operaționale sau urgente, IUEC pot fi comunicate, în mod excepțional, unui stat terț sau unei organizații internaționale după întreprinderea următoarelor acțiuni.

După ce s-a asigurat că sunt îndeplinite condițiile prevăzute la punctul 11 de mai sus, Direcția SEAE responsabilă de securitate:

(a) în măsura posibilului, verifică împreună cu autoritățile de securitate ale statului terț sau ale organizației internaționale în cauză dacă reglementările, structurile și procedurile de securitate ale acestora sunt astfel concepute încât 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 al SEAE să formuleze, pe baza informațiilor disponibile, un aviz privind încrederea care poate fi acordată reglementărilor, structurilor și procedurilor de securitate ale statului terț sau ale organizației internaționale căreia urmează să îi fie comunicate IUEC;

(c) sesizează autoritatea de securitate a SEAE, care poate hotărî comunicarea informațiilor, cu condiția să se fi obținut avizul favorabil unanim al statelor membre, astfel cum sunt reprezentate în Comitetul de securitate al SEAE.

13. Dacă nu există niciunul dintre cadrele menționate la articolul 10 alineatul (1) din anexa A, partea terță în cauză se angajează, în scris, să protejeze IUEC în mod corespunzător.

Apendicele A

Definiții

În sensul prezentei decizii, se aplică următoarele definiții:

„Acreditare” 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 activitățile sale și pentru continuitatea acestora, inclusiv resursele informaționale care sprijină misiunea organizației.

„Autorizație de acces la IUEC” înseamnă o autorizație din partea Autorității de securitate a SEAE care este obținută în conformitate cu prezenta decizie în urma eliberării unui CSP de către autoritățile competente ale unui stat membru și care certifică 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 – a se vedea articolul 2 din anexa A I.

„Încălcare” înseamnă o acțiune sau o omisiune a unei persoane, care contravine normelor de securitate prevăzute în prezenta decizie și/sau politicilor sau orientărilor în materie de securitate care stabilesc măsurile necesare pentru punerea în aplicare a acesteia.

„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.

„Contract clasificat” înseamnă un contract încheiat de SEAE 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.

„Subcontract clasificat” înseamnă un contract încheiat de un contractant al SEAE 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.

„Sistem informatic și de comunicații” (SIC) înseamnă orice sistem care permite manipularea informațiilor în format electronic. Un sistem informatic și de comunicații cuprinde toate activele necesare pentru a funcționa, inclusiv infrastructura, organizarea, personalul și resursele informaționale – a se vedea articolul 8 alineatul (2) din anexa A.

„Compromiterea IUEC” înseamnă divulgarea totală sau parțială a IUEC unor persoane sau entități neautorizate – a se vedea articolul 9 alineatul (2).

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

„Produse criptografice” înseamnă algoritmii criptografici, modulele criptografice hardware și software și produsele care cuprind modalitățile de instalare și documentația aferentă, precum și materialul de criptare.

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

„Declasificare” înseamnă eliminarea clasificării de securitate.

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

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

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

„Scădere a nivelului de clasificare” înseamnă atribuirea unui nivel de clasificare de securitate inferior celui anterior.

„Informații UE clasificate” (IUEC) înseamnă orice informații sau materiale desemnate ca atare printr-o clasificare de securitate a UE a căror divulgare neautorizată ar putea cauza prejudicii de diferite grade intereselor Uniunii Europene sau ale unuia sau mai multor state membre – a se vedea articolul 2 litera (f).

„Certificat de securitate industrială” (CSI) înseamnă o decizie administrativă a ANS sau ASD conform căreia, în ceea ce privește securitatea, un local poate oferi un nivel de protecție adecvat IUEC clasificate cu un anumit nivel de clasificare a securității, iar personalul său care are nevoie de acces la IUEC deține 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.

„Manipularea” 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, transmiterea și păstrarea.

„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 care este responsabilă în mod corespunzător de protecția acesteia.

„Entitate industrială sau de altă natură” înseamnă o entitate implicată în livrarea de bunuri, executarea de lucrări sau prestarea de servicii. Aceasta poate fi o entitate care desfășoară activități în domeniul industriei, al comerțului, al serviciilor, al științei, al cercetării, al educației sau al dezvoltării sau o persoană care desfășoară activități independente.

„Securitate industrială” înseamnă 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 – a se vedea articolul 9 alineatul (1) din anexa A.

„Asigurarea informațiilor” (AI) în domeniul sistemelor informatice și de comunicații înseamnă încrederea în faptul că aceste sisteme vor proteja informațiile pe care le manipulează și că ele vor funcționa așa cum trebuie, când trebuie și sub controlul unor utilizatori legitimi. O AI eficace asigură grade adecvate de confidențialitate, integritate, disponibilitate, nerepudiere și autenticitate. AI se bazează pe un proces de gestionare a riscurilor – a se vedea articolul 8 alineatul (1) din anexa A.

„Interconectare” înseamnă, în sensul prezentei decizii, conectarea directă a două sau a mai multor sisteme IT în scopul partajării datelor și a altor resurse informaționale (de exemplu, de comunicații) în mod unidirecțional sau multidirecțional – a se vedea anexa A IV punctul 31.

„Gestionarea informațiilor clasificate” înseamnă aplicarea unor măsuri administrative pentru a controla IUEC pe durata ciclului lor de viață, în vederea completării măsurilor prevăzute la articolele 5, 6 și 8, contribuind astfel la descurajarea, detectarea și remedierea compromiterii sau pierderii deliberate sau accidentale de astfel de informații. Aceste măsuri se referă, în special, la crearea, înregistrarea, copierea, traducerea, transportul, manipularea, păstrarea și distrugerea IUEC – a se vedea articolul 7 alineatul (1) din anexa A.

„Material” înseamnă orice document sau orice aparat sau echipament deja fabricat sau în curs de fabricație.

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

„Securitatea personalului” înseamnă aplicarea unor măsuri prin care se garantează că accesul la IUEC este acordat numai persoanelor:

— în cazul cărora există necesitatea de a cunoaște;

— care, pentru accesul la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior, au primit certificatul de securitate pentru nivelul corespunzător sau sunt autorizate în alt mod corespunzător în temeiul funcțiilor deținute în conformitate cu actele cu putere de lege și dispozițiile administrative naționale; și

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

a se vedea articolul 5 alineatul (1) din anexa A.

„Certificatul de securitate a personalului” (CSP) pentru accesul la IUEC înseamnă o declarație a unei autorități competente a unui stat membru făcută după încheierea unei investigații de securitate efectuate de autoritățile competente ale unui stat membru, care certifică faptul că unei persoane îi poate fi acordat accesul la IUEC până la un nivel precizat (CONFIDENTIEL UE/EU CONFIDENTIAL sau superior), 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”.

„Certificarea autorizării de securitate a personalului” (CASP) înseamnă un certificat eliberat de o autoritate competentă care stabilește că o persoană deține certificatul de securitate și deține un CSP național valabil sau o autorizație de acces la IUEC valabilă emisă de șeful Direcției responsabile de securitate care indică nivelul IUEC la care este permis accesul persoanei respective (CONFIDENTIEL UE/EU CONFIDENTIAL sau superior), data de valabilitate a CSP relevant și data de expirare a certificării.

„Securitate fizică” înseamnă aplicarea unor măsuri de protecție fizică și tehnică în vederea descurajării accesului neautorizat la IUEC – a se vedea articolul 6 din anexa A.

„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.

„Înregistrare” înseamnă aplicarea unor proceduri prin care se înregistrează ciclul de viață al informațiilor, inclusiv diseminarea și distrugerea acestora – a se vedea punctul 21 din anexa A III.

„Riscuri reziduale” înseamnă riscuri care persistă după punerea în aplicare a măsurilor de securitate, având în vedere că nu toate amenințările sunt contracarate și că nu toate vulnerabilitățile pot fi eliminate.

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

„Acceptarea riscurilor” înseamnă decizia de a accepta, după tratarea riscurilor, existența în continuare a unui risc rezidual.

„Evaluarea riscurilor” înseamnă identificarea amenințărilor și a vulnerabilităților și efectuarea analizei riscurilor conexe, și anume analiza probabilității și a impactului.

„Comunicarea riscurilor” cuprinde sensibilizarea comunităților de utilizatori ai SIC la riscuri, informarea autorităților de aprobare cu privire la aceste riscuri și raportarea lor către autoritățile operaționale.

„Procesul de gestionare a riscurilor” înseamnă întregul proces de identificare, control și reducere la minimum a evenimentelor incerte care pot afecta securitatea unei organizații sau a oricăruia dintre sistemele pe care aceasta le folosește. Procesul acoperă ansamblul activităților legate de riscuri, inclusiv evaluarea, tratarea, acceptarea și comunicarea.

„Tratarea riscurilor” constă în atenuarea, eliminarea sau reducerea riscurilor (prin combinarea adecvată a măsurilor de ordin tehnic, fizic, organizațional sau procedural), transferul sau monitorizarea riscurilor.

„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 contractului care necesită protecție de securitate – a se vedea secțiunea II din anexa A V.

„Ghid al clasificărilor de securitate” (GCS) înseamnă un document care descrie elementele clasificate ale unui program sau contract, precizând nivelurile aplicabile de clasificare de securitate. GCS poate fi extins pe toată durata programului sau a contractului respectiv, iar informațiile pot face obiectul unei reclasificări sau al unei scăderi a nivelului de securitate. Atunci când există, GCS face parte din AS – a se vedea secțiunea II din anexa A V.

„Investigație de securitate” înseamnă procedurile de investigare derulate de autoritatea competentă a unui stat membru, în conformitate cu actele cu putere de lege și dispozițiile administrative naționale ale statului membru în cauză, pentru a garanta că nu există informații defavorabile care ar putea 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).

„Proceduri operaționale de securitate” (SecOP) înseamnă descrierea modului de punere în aplicare a politicii de securitate care urmează să fie adoptat, descrierea procedurilor operaționale care trebuie respectate și descrierea responsabilităților care revin personalului.

„Informații sensibile neclasificate” înseamnă informațiile sau materialele pe care SEAE trebuie să le protejeze ca urmare a obligațiilor juridice stabilite prin tratate sau prin actele adoptate pentru punerea în aplicare a acestora și/sau ca urmare a caracterului lor sensibil. Informațiile sensibile neclasificate includ, fără a se limita la acestea, informațiile sau materialele care fac obiectul obligației de păstrare a secretului profesional, astfel cum sunt menționate la articolul 339 din TFUE, informațiile care fac obiectul intereselor protejate în conformitate cu articolul 4 din Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului ([1]), citit în coroborare cu jurisprudența relevantă a Curții de Justiție a Uniunii Europene, și datele cu caracter personal care intră sub incidența Regulamentului (CE) nr. 45/2001.

„Declarație privind cerințele de securitate specifice sistemului” (CSSS) înseamnă un set obligatoriu de principii de securitate care trebuie respectate și de cerințe de securitate detaliate care trebuie puse în aplicare; acest set stă la baza procesului de certificare și acreditare a SIC.

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

„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.

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

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

Apendicele B

Echivalența clasificărilor de securitate

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

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

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

([2]) Germania: VS = Verschlusssache.

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

([4]) Suedia: marcajele clasificării de securitate din rândul de sus sunt utilizate de către autoritățile din domeniul apărării, în timp ce marcajele din rândul de jos sunt utilizate de către alte autorități.

([5]) Regatul Unit manipulează și protejează IUEC marcate „CONFIDENTIEL UE/EU CONFIDENTIAL” în conformitate cu cerințele în materie de protecție a securității pentru UK SECRET.

ISSN 1977-1029 (ediție electronică)
ISSN 1830-3668 (ediție tipărită)

Oficiul pentru Publicații al Uniunii Europene
2985 Luxemburg
LUXEMBURG

RO