Jurnalul Oficial al Uniunii Europene

L 72

Anul 58

Ediția în limba română **Legislație** 17 martie 2015

Cuprins

RO

Actele ale căror titluri sunt tipărite cu caractere drepte sunt acte de gestionare curentă adoptate în cadrul politicii agricole și care au, în general, o perioadă de valabilitate limitată.

Titlurile celorlalte acte sunt tipărite cu caractere aldine și sunt precedate de un asterisc.

II

(Acte fără caracter legislativ)

REGULAMENTE

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2015/434 AL COMISIEI

din 16 martie 2015

de stabilire a valorilor forfetare de import pentru fixarea prețului de intrare pentru anumite fructe și legume

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) nr. 1308/2013 al Parlamentului European și al Consiliului din 17 decembrie 2013 de instituire a unei organizări comune a piețelor produselor agricole și de abrogare a Regulamentelor (CEE) nr. 922/72, (CEE) nr. 234/79, (CE) nr. 1037/2001 și (CE) nr. 1234/2007 ale Consiliului ([1]),

având în vedere Regulamentul de punere în aplicare (UE) nr. 543/2011 al Comisiei din 7 iunie 2011 de stabilire a normelor de aplicare a Regulamentului (CE) nr. 1234/2007 al Consiliului în sectorul fructelor și legumelor și în sectorul fructelor și legumelor procesate ([2]), în special articolul 136 alineatul (1),

întrucât:

(1) Regulamentul de punere în aplicare (UE) nr. 543/2011 prevede, ca urmare a rezultatelor negocierilor comerciale multilaterale din cadrul Rundei Uruguay, criteriile pentru stabilirea de către Comisie a valorilor forfetare de import din țări terțe pentru produsele și perioadele menționate în partea A din anexa XVI la regulamentul respectiv.

(2) Valoarea forfetară de import se calculează în fiecare zi lucrătoare, în conformitate cu articolul 136 alineatul (1) din Regulamentul de punere în aplicare (UE) nr. 543/2011, ținând seama de datele zilnice variabile. Prin urmare, prezentul regulament trebuie să intre în vigoare la data publicării în *Jurnalul Oficial al Uniunii Europene*,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Valorile forfetare de import prevăzute la articolul 136 din Regulamentul de punere în aplicare (UE) nr. 543/2011 sunt stabilite în anexa la prezentul regulament.

([1]) JO L 347, 20.12.2013, p. 671.
([2]) JO L 157, 15.6.2011, p. 1.

Articolul 2

Prezentul regulament intră în vigoare la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 16 martie 2015.

Pentru Comisie,
pentru președinte
Jerzy PLEWA
Director general pentru agricultură și dezvoltare rurală

ANEXĂ

Valorile forfetare de import pentru fixarea prețului de intrare pentru anumite fructe și legume

(EUR/100 kg)

Codul NC	Codul țării terțe ([1])	Valoarea forfetară de import
0702 00 00	EG	65,8
	MA	84,9
	TR	86,4
	ZZ	79,0
0707 00 05	JO	229,9
	MA	183,9
	TR	185,1
	ZZ	199,6
0709 93 10	MA	119,5
	TR	192,4
	ZZ	156,0
0805 10 20	EG	45,8
	IL	72,7
	MA	56,7
	TN	57,3
	TR	63,6
	ZZ	59,2
0805 50 10	TR	61,4
	ZZ	61,4
0808 10 80	BR	70,9
	CA	81,0
	CL	100,9
	CN	91,1
	MK	25,2
	US	166,1
	ZZ	89,2
0808 30 90	AR	112,0
	CL	133,2
	US	124,8
	ZA	103,5
	ZZ	118,4

([1]) Nomenclatura țărilor stabilită prin Regulamentul (UE) nr. 1106/2012 al Comisiei din 27 noiembrie 2012 de punere în aplicare a Regulamentului (CE) nr. 471/2009 al Parlamentului European și al Consiliului privind statisticile comunitare privind comerțul exterior cu țările terțe, în ceea ce privește actualizarea nomenclatorului țărilor și teritoriilor (JO L 328, 28.11.2012, p. 7). Codul „ZZ" desemnează „alte origini".

DECIZII

DECIZIA (UE) 2015/435 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI

din 17 decembrie 2014

privind mobilizarea marjei pentru situații neprevăzute

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Acordul interinstituțional din 2 decembrie 2013 dintre Parlamentul European, Consiliu și Comisie privind disciplina bugetară, cooperarea în chestiuni bugetare și buna gestiune financiară ([1]), în special punctul 14,

având în vedere propunerea Comisiei Europene,

întrucât:

(1) Articolul 13 din Regulamentul (UE, Euratom) nr. 1311/2013 al Consiliului ([2]) instituie o marjă pentru situații neprevăzute de până la 0,03 % din venitul național brut al Uniunii.

(2) În conformitate cu articolul 6 din regulamentul menționat, Comisia a calculat valoarea absolută a marjei pentru situații neprevăzute pentru anul 2014 ([3]).

(3) După examinarea tuturor celorlalte posibilități financiare de reacție la situațiile neprevăzute care au apărut după stabilirea, pentru prima dată, în februarie 2013, a plafonului de plăți în cadrul CFM pentru 2014, se constată că este necesar să se mobilizeze marja pentru situații neprevăzute pentru a se completa creditele de plată din bugetul general al Uniunii Europene pentru exercițiul financiar 2014, peste plafonul de plăți.

(4) În mobilizarea marjei pentru situații neprevăzute ar trebui inclusă suma de 350 de milioane EUR sub formă de credite de plată, în așteptarea unui acord privind plățile pentru alte instrumente speciale.

(5) Având în vedere situația excepțională din exercițiul financiar curent, este îndeplinită condiția pentru instituirea unui instrument ultim de reacție prevăzut la articolul 13 alineatul (1) din Regulamentul (UE, Euratom) nr. 1311/2013.

(6) Pentru a se asigura conformitatea cu articolul 13 alineatul (3) din Regulamentul (UE, Euratom) nr. 1311/2013, Comisia ar trebui să prezinte o propunere privind compensarea sumei în cauză prin plafoanele de plăți prevăzute în cadrul CFM pentru unul sau mai multe exerciții financiare viitoare, ținând seama în mod corespunzător de acordul privind plățile destinate altor instrumente speciale și fără a aduce atingere prerogativelor instituționale ale Comisiei,

([1]) JO C 373, 20.12.2013, p. 1.
([2]) Regulamentul (UE, Euratom) nr. 1311/2013 al Consiliului din 2 decembrie 2013 de stabilire a cadrului financiar multianual pentru perioada 2014-2020 (JO L 347, 20.12.2013, p. 884).
([3]) Comunicarea Comisiei către Consiliu și Parlamentul European din 20 decembrie 2013 privind ajustarea tehnică a cadrului financiar pentru 2014 în funcție de evoluțiile VNB [COM(2013) 928].

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

În cadrul bugetului general al Uniunii Europene pentru exercițiul financiar 2014, marja pentru situații neprevăzute se utilizează pentru a se asigura suma de 3 168 233 715 EUR în credite de plată peste plafonul de plăți al cadrului financiar multianual.

Articolul 2

Suma de 2 818 233 715 EUR se compensează, în trei tranșe, cu marjele plafoanelor de plăți aferente exercițiilor financiare următoare:

(a) 2018: 939 411 200 EUR;

(b) 2019: 939 411 200 EUR;

(c) 2020: 939 411 315 EUR.

Comisia este invitată să prezinte în timp util o propunere privind suma rămasă de 350 de milioane EUR.

Articolul 3

Prezenta decizie se publică în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Strasbourg, 17 decembrie 2014.

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*
M. SCHULZ	B. DELLA VEDOVA

DECIZIA (UE) 2015/436 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI

din 17 decembrie 2014

privind mobilizarea Fondului de solidaritate al Uniunii Europene

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (CE) nr. 2012/2002 al Consiliului din 11 noiembrie 2002 de instituire a Fondului de solidaritate al Uniunii Europene ([1]), în special articolul 4 alineatul (3),

având în vedere Acordul interinstituțional din 2 decembrie 2013 dintre Parlamentul European, Consiliu și Comisie privind disciplina bugetară, cooperarea în chestiuni bugetare și buna gestiune financiară ([2]), în special punctul 11,

având în vedere propunerea Comisiei Europene,

întrucât:

(1) Uniunea Europeană a instituit Fondul de solidaritate al Uniunii Europene („fondul") pentru a-și exprima solidaritatea față de populația din regiunile afectate de dezastre.

(2) Articolul 10 din Regulamentul (UE, Euratom) nr. 1311/2013 al Consiliului ([3]) permite mobilizarea fondului în limita unui plafon anual de 500 de milioane EUR (la prețurile din 2011).

(3) Regulamentul (CE) nr. 2012/2002 conține dispozițiile care permit mobilizarea fondului.

(4) Italia a depus o cerere de mobilizare a fondului ca urmare a producerii de inundații în această țară.

(5) Grecia a depus o cerere de mobilizare a fondului ca urmare a producerii unui cutremur în această țară.

(6) Slovenia a depus o cerere de mobilizare a fondului ca urmare a furtunilor de gheață care au avut loc în această țară.

(7) Croația a depus o cerere de mobilizare a fondului ca urmare a furtunilor de gheață, urmate de inundații, care au avut loc în această țară,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

În cadrul bugetului general al Uniunii Europene pentru exercițiul financiar 2014, se mobilizează din Fondul de solidaritate al Uniunii Europene suma de 46 998 528 EUR în credite de angajament.

În cadrul bugetului general al Uniunii Europene pentru exercițiul financiar 2015, se mobilizează din Fondul de solidaritate al Uniunii Europene suma de 46 998 528 EUR în credite de plată.

Articolul 2

Prezenta decizie se publică în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Strasbourg, 17 decembrie 2014.

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*
M. SCHULZ	B. DELLA VEDOVA

([1]) JO L 311, 14.11.2002, p. 3.
([2]) JO C 373, 20.12.2013, p. 1.
([3]) Regulamentul (UE, Euratom) nr. 1311/2013 al Consiliului din 2 decembrie 2013 de stabilire a cadrului financiar multianual pentru perioada 2014-2020 (JO L 347, 20.12.2013, p. 884).

DECIZIA (UE) 2015/437 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI

din 17 decembrie 2014

privind mobilizarea Fondului de solidaritate al Uniunii Europene

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (CE) nr. 2012/2002 al Consiliului din 11 noiembrie 2002 de instituire a Fondului de solidaritate al Uniunii Europene ([1]), în special articolul 4 alineatul (3),

având în vedere Acordul interinstituțional din 2 decembrie 2013 dintre Parlamentul European, Consiliu și Comisie privind disciplina bugetară, cooperarea în chestiuni bugetare și buna gestiune financiară ([2]), în special punctul 11,

având în vedere propunerea Comisiei Europene,

întrucât:

(1) Uniunea Europeană a instituit Fondul de solidaritate al Uniunii Europene („fondul"), pentru a-și exprima solidaritatea față de populația din regiunile afectate de dezastre.

(2) Articolul 10 din Regulamentul (UE, Euratom) nr. 1311/2013 al Consiliului ([3]) permite mobilizarea fondului în limita unui plafon anual de 500 de milioane EUR (la prețurile din 2011).

(3) Regulamentul (CE) nr. 2012/2002 conține dispozițiile care permit mobilizarea fondului.

(4) Serbia a depus o cerere de mobilizare a fondului ca urmare a inundațiilor care au avut loc în această țară.

(5) Croația a depus o cerere de mobilizare a fondului ca urmare a inundațiilor care au avut loc în această țară.

(6) Bulgaria a depus o cerere de mobilizare a fondului ca urmare a inundațiilor care au avut loc în această țară,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

În cadrul bugetului general al Uniunii Europene pentru exercițiul financiar 2014, se mobilizează din Fondul de solidaritate al Uniunii Europene suma de 79 726 440 EUR în credite de angajament.

În cadrul bugetului general al Uniunii Europene pentru exercițiul financiar 2015, se mobilizează din Fondul de solidaritate al Uniunii Europene suma de 79 726 440 EUR în credite de plată.

Articolul 2

Prezenta decizie se publică în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Strasbourg, 17 decembrie 2014.

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*
M. SCHULZ	B. DELLA VEDOVA

([1]) JO L 311, 14.11.2002, p. 3.
([2]) JO C 373, 20.12.2013, p. 1.
([3]) Regulamentul (UE, Euratom) nr. 1311/2013 al Consiliului din 2 decembrie 2013 de stabilire a cadrului financiar multianual pentru perioada 2014-2020 (JO L 347, 20.12.2013, p. 884).

DECIZIA (UE) 2015/438 A CONSILIULUI

din 2 martie 2015

de stabilire a poziției care urmează să fie adoptată în numele Uniunii Europene în cadrul Comitetului mixt instituit în temeiul Acordului dintre Uniunea Europeană și Ucraina privind facilitarea eliberării vizelor, cu privire la adoptarea orientărilor comune pentru punerea în aplicare a acordului

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 77 alineatul (2) litera (a) coroborat cu articolul 218 alineatul (9),

având în vedere propunerea Comisiei Europene,

întrucât:

(1) Articolul 12 din Acordul dintre Uniunea Europeană și Ucraina privind facilitarea eliberării vizelor ([1]) (denumit în continuare „acordul") instituie un comitet mixt. În conformitate cu articolul menționat, Comitetul mixt monitorizează, în special, punerea în aplicare a acordului.

(2) Acordul între Uniunea Europeană și Ucraina de modificare a acordului între Comunitatea Europeană și Ucraina privind facilitarea eliberării vizelor ([2]) (denumit în continuare „acordul de modificare") a intrat în vigoare la 1 iulie 2013.

(3) Regulamentul (CE) nr. 810/2009 al Parlamentului European și al Consiliului ([3]) a instituit procedurile și condițiile de eliberare a vizelor de tranzit sau de ședere planificată pe teritoriul statelor membre cu o durată de maximum 90 de zile în orice perioadă de 180 de zile.

(4) În limita responsabilităților care îi revin, Comitetul mixt a subliniat necesitatea unor orientări comune pentru a se asigura o punere în aplicare pe deplin armonizată a acordului de către consulatele statelor membre și pentru clarificarea relației dintre dispozițiile acordului și dispozițiile prevăzute de părțile contractante care se aplică în continuare cu privire la aspecte legate de vize care nu sunt reglementate de acord.

(5) Comitetul mixt a adoptat astfel de orientări prin Decizia nr. 1/2009 din 25 noiembrie 2009. Orientările respective ar trebui adaptate la noile dispoziții ale acordului introduse de acordul de modificare și la modificările survenite în dreptul intern al Uniunii privind politica în domeniul vizelor. Din motive de claritate, este oportun ca respectivele orientări să fie înlocuite.

(6) Este oportun să se stabilească poziția care urmează să fie adoptată în numele Uniunii în cadrul Comitetului mixt în ceea ce privește adoptarea orientărilor comune pentru punerea în aplicare a acordului,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Poziția care urmează să fie adoptată în numele Uniunii în cadrul Comitetului mixt instituit prin articolul 12 din Acordul între Uniunea Europeană și Ucraina privind facilitarea eliberării vizelor, cu privire la adoptarea unor orientări comune pentru punerea în aplicare a acordului se bazează pe proiectul de decizie a Comitetului mixt atașat la prezenta decizie.

([1]) JO L 332, 18.12.2007, p. 68.
([2]) JO L 168, 20.6.2013, p. 11.
([3]) Regulamentul (CE) nr. 810/2009 al Parlamentului European și al Consiliului din 13 iulie 2009 privind instituirea unui Cod comunitar de vize (Codul de vize) (JO L 243, 15.9.2009, p. 1).

Articolul 2

Prezenta decizie intră în vigoare la data adoptării.

Adoptată la Bruxelles, 2 martie 2015.

Pentru Consiliu
Președintele
D. REIZNIECE-OZOLA

PROIECT

DECIZIA NR. …/2014 A COMITETULUI MIXT INSTITUIT PRIN ACORDUL DINTRE UNIUNEA EUROPEANĂ ȘI UCRAINA PRIVIND FACILITAREA ELIBERĂRII VIZELOR

din …

cu privire la adoptarea orientărilor comune pentru punerea în aplicare a acordului

COMITETUL MIXT,

având în vedere Acordul dintre Uniunea Europeană și Ucraina privind facilitarea eliberării vizelor (denumit în continuare „acordul"), în special articolul 12,

întrucât acordul a intrat în vigoare la 1 ianuarie 2008,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Orientările comune pentru punerea în aplicare a Acordului dintre Uniunea Europeană și Ucraina privind facilitarea eliberării vizelor sunt stabilite în anexa la prezenta decizie.

Articolul 2

Decizia nr. 1/2009 a Comitetului mixt se abrogă.

Articolul 3

Prezenta decizie intră în vigoare la data adoptării.

Adoptată la …

Pentru Uniunea Europeană *Pentru Ucraina*

ANEXĂ

ORIENTĂRI COMUNE PENTRU PUNEREA ÎN APLICARE A ACORDULUI DINTRE UNIUNEA EUROPEANĂ ȘI UCRAINA PRIVIND FACILITAREA ELIBERĂRII VIZELOR

Scopul acordului dintre Uniunea Europeană și Ucraina privind facilitarea eliberării vizelor, care a intrat în vigoare la 1 ianuarie 2008, astfel cum a fost modificat prin Acordul dintre Uniunea Europeană și Ucraina din 23 iulie 2012, care a intrat în vigoare la 1 iulie 2013 (denumit în continuare „acordul"), este de a facilita, pe bază de reciprocitate, procedurile de eliberare a vizelor pentru cetățenii ucraineni pentru o ședere planificată de cel mult 90 de zile într-un interval de 180 de zile.

Acordul stabilește, pe bază de reciprocitate, drepturile și obligațiile cu caracter obligatoriu din punct de vedere juridic în vederea simplificării procedurilor de eliberare a vizelor pentru cetățenii ucraineni.

Scopul prezentelor orientări, adoptate de Comitetul mixt instituit prin articolul 12 din acord (denumit în continuare „Comitetul mixt"), este de a asigura o punere în aplicare corectă și armonizată a dispozițiilor acordului de către misiunile diplomatice și oficiile consulare ale statelor membre. Prezentele orientări nu fac parte din acord și, prin urmare, nu sunt obligatorii din punct de vedere juridic. Cu toate acestea, este recomandabil ca personalul diplomatic și consular să le urmeze în mod consecvent la punerea în aplicare a dispozițiilor acordului.

Aceste orientări sunt destinate să fie actualizate pentru a ține seama de experiența punerii în aplicare a acordului sub responsabilitatea Comitetului mixt. Orientările adoptate de Comitetul mixt la 25 noiembrie 2009 au fost adaptate în conformitate cu Acordul dintre Uniunea Europeană și Ucraina de modificare a Acordului dintre Comunitatea Europeană și Ucraina privind facilitarea eliberării vizelor (denumit în continuare „acordul de modificare"), precum și în conformitate cu noua legislație a Uniunii, cum ar fi Regulamentul (CE) nr. 810/2009 al Parlamentului European și al Consiliului ([1]) (Codul de vize).

I. ASPECTE GENERALE

1.1. **Scopul și domeniul de aplicare**

Articolul 1 din acord prevede: „Scopul prezentului acord este de a facilita eliberarea vizelor pentru cetățenii ucraineni, pentru o perioadă de ședere de până la 90 de zile, în decurs de 180 de zile."

Acordul se aplică tuturor cetățenilor ucraineni care solicită o viză de scurtă ședere, indiferent de țara în care își au reședința.

Articolul 1 alineatul (2) din acord prevede: „Ucraina poate reintroduce obligația de a deține viză doar pentru cetățenii sau anumite categorii de cetățeni din toate statele membre și nu pentru cetățenii sau anumite categorii de cetățeni din state membre distincte. În cazul în care Ucraina reintroduce obligativitatea vizelor pentru cetățenii UE sau pentru anumite categorii de cetățeni UE, aceleași facilități acordate în baza prezentului acord cetățenilor ucraineni se aplică în mod automat cetățenilor UE în cauză, pe bază de reciprocitate."

Potrivit deciziilor adoptate de guvernul ucrainean, începând cu 1 mai 2005 sau, respectiv, cu 1 ianuarie 2008, cetățenii UE sunt exonerați de obligația de a deține viză atunci când călătoresc în Ucraina pentru o perioadă de până la 90 de zile sau când tranzitează teritoriul Ucrainei. Această dispoziție nu aduce atingere dreptului guvernului ucrainean de a modifica deciziile respective.

1.2. **Domeniul de aplicare al acordului**

Articolul 2 din acord prevede:

> „(1) Facilitățile referitoare la vize prevăzute în prezentul acord se aplică cetățenilor Ucrainei numai în măsura în care aceștia nu sunt scutiți de obligativitatea vizelor în temeiul actelor cu putere de lege și al reglementărilor administrative ale Uniunii Europene sau ale statelor membre, în temeiul prezentului acord sau al altor acorduri internaționale.
>
> (2) În domeniile care nu sunt acoperite de prevederile prezentului acord, ca, de exemplu, refuzul de eliberare a unei vize, recunoașterea documentelor de călătorie, dovada mijloacelor suficiente de subzistență, refuzul intrării și măsurile de expulzare, se aplică după caz legislația națională a Ucrainei, cea a statelor membre sau legislația Uniunii Europene."

([1]) Regulamentul (CE) nr. 810/2009 al Parlamentului European și al Consiliului din 13 iulie 2009 privind instituirea unui Cod comunitar de vize (Codul de vize) (JO L 243, 15.9.2009, p. 1).

Fără a aduce atingere articolului 10 (care prevede exonerarea titularilor de pașapoarte diplomatice și pașapoarte de serviciu biometrice din Ucraina de obligația de a deține viză), acordul nu afectează normele existente privind obligațiile în materie de vize și exonerarea de obligația de a deține viză. De exemplu, articolul 4 din Regulamentul nr. 539/2001 al Consiliului ([1]) permite statelor membre să exonereze de obligația de a deține viză, printre alte categorii, echipajele civile ale aeronavelor și navelor.

Normele Schengen și, după caz, legislația națională continuă să se aplice în cazul tuturor aspectelor nereglementate de acord, cum ar fi refuzul de eliberare a unei vize, recunoașterea documentelor de călătorie, dovada mijloacelor suficiente de subzistență, refuzul intrării și măsurile de expulzare. Acest lucru se aplică și normelor Schengen care determină statul membru Schengen responsabil pentru prelucrarea unei cereri de viză. Prin urmare, cetățenii ucraineni ar trebui în continuare să solicite viză la consulatul statului membru care este destinația principală a călătoriei; în cazul în care nu există o destinație principală, cetățenii ucraineni ar trebui să solicite viză la consulatul statului membru al primei intrări în spațiul Schengen.

Chiar dacă condițiile prevăzute în acord sunt îndeplinite, de exemplu, solicitantul de viză face dovada documentelor justificative privind scopul călătoriei pentru categoriile prevăzute la articolul 4, se poate totuși refuza eliberarea vizei dacă nu sunt îndeplinite condițiile prevăzute la articolul 5 din Regulamentul (CE) nr. 562/2006 al Parlamentului European și al Consiliului ([2]) (Codul frontierelor Schengen), și anume dacă persoana nu este în posesia unui document de călătorie valabil, dacă a fost emisă o semnalare în SIS, dacă persoana este considerată o amenințare pentru ordinea publică, securitatea internă etc.

Se aplică în continuare alte posibilități de flexibilitate permise în Codul de vize în ceea ce privește eliberarea vizelor. De exemplu, vizele cu intrări multiple cu un termen de valabilitate îndelungat – de până la cinci ani – pot fi eliberate altor categorii de persoane decât cele menționate la articolul 5 din acord dacă sunt îndeplinite condițiile prevăzute în Codul de vize [a se vedea articolul 24 alineatul (2) din Codul de vize). În mod similar, dispozițiile cuprinse în Codul de vize care permit eliminarea sau reducerea taxei de viză vor continua să se aplice (a se vedea punctul II.2.1.1.).

1.3. **Tipurile de vize care intră în domeniul de aplicare al acordului**

Articolul 3 litera (d) din acord definește „viza” drept „o autorizație eliberată de un stat membru sau o decizie adoptată de un astfel de stat, care este necesară în scopul:

— de a intra pe teritoriul unuia sau al mai multor state membre în vederea unei șederi de cel mult 90 de zile în total;

— de a intra pe teritoriului unuia sau al mai multor state membre în vederea tranzitării acestuia.”

Acordul acoperă următoarele tipuri de viză:

— vizele de tip „C” (vize de scurtă ședere).

Facilitățile oferite de acord se aplică atât în cazul vizelor uniforme valabile pentru întregul teritoriu al statelor membre, cât și al vizelor cu valabilitate teritorială limitată (VTL).

1.4. **Calcularea duratei de ședere autorizate de o viză și, în special, modul în care se determină perioada de șase luni**

Recenta modificare a Codului frontierelor Schengen a redefinit noțiunea de „scurtă ședere”. Definiția actuală este următoarea: „90 de zile în orice perioadă de 180 de zile, ceea ce implică luarea în considerare a ultimei perioade de 180 de zile precedente fiecărei zile de ședere”.

Data intrării se calculează ca prima zi de ședere pe teritoriul statelor membre și data de ieșire se calculează ca ultima zi de ședere pe teritoriul statelor membre. Termenul „orice” presupune aplicarea unei perioade de referință „mobile” de 180 de zile; aceasta înseamnă că trebuie calculată retroactiv fiecare zi de ședere din ultima perioadă de 180 de zile, pentru a se verifica dacă cerința privind durata de ședere de 90 de zile în decursul unei perioade de 180 de zile continuă să fie îndeplinită. Aceasta înseamnă că o absență pe o perioadă neîntreruptă de 90 zile permite o nouă ședere de până la 90 de zile.

Definiția a intrat în vigoare la 18 octombrie 2013. Calculatorul este disponibil online la următoarea adresă: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/border-crossing/index_en.htm

([1]) Regulamentul (CE) nr. 539/2001 al Consiliului din 15 martie 2001 de stabilire a listei țărilor terțe ai căror resortisanți trebuie să dețină viză pentru trecerea frontierelor externe și a listei țărilor terțe ai căror resortisanți sunt exonerați de această obligație (JO L 81, 21.3.2001, p. 1).

([2]) Regulamentul (CE) nr. 562/2006 al Parlamentului European și al Consiliului din 15 martie 2006 de instituire a unui Cod comunitar privind regimul de trecere a frontierelor de către persoane (Codul Frontierelor Schengen) (JO L 105, 13.4.2006, p. 1).

Exemplu de calculare a șederii pe baza noii definiții:

O persoană care deține o viză cu intrări multiple valabilă 1 an (18.4.2014 – 18.4.2015) intră pentru prima dată pe teritoriul unui stat membru la 19.4.2014 pentru o ședere de 3 zile. Apoi, aceasta intră din nou la 18.6.2014 pentru o ședere de 86 de zile. Care este situația persoanei în cauză la aceste date? Când i se va dreptul de a intra din nou pe teritoriul statelor membre?

La 11.9.2014: în cursul ultimelor 180 de zile (16.3.2014 – 11.9.2014), persoana în cauză a rămas pe teritoriul statelor membre timp de 3 de zile (19 – 21.4.2014), urmate de alte 86 de zile (18.6.2014 – 11.9.2014) = 89 de zile = Nu a depășit durata maximă de ședere autorizată. Persoana poate să mai rămână pe teritoriul statelor membre cel mult 1 zi.

Începând de la 16.10.2014: persoana ar putea intra pe teritoriul unui stat membru pentru o ședere de 3 zile suplimentare [la 16.10.2014, șederea din 19.4.2014 nu mai este relevantă (se situează în afara perioadei de 180 de zile); la 17.10.2014, șederea din 20.4.2014 nu mai este relevantă (se situează în afara perioadei de 180 de zile etc.).

Începând de la 15.12.2014: persoana ar putea intra pe teritoriul unui stat membru pentru o ședere de 86 de zile suplimentare [la 15.12.2014, șederea din 18.6.2014 nu mai este relevantă (se situează în afara perioadei de 180 de zile); la 16.12.2014, șederea din 19.6.2014 nu mai este relevantă etc.)].

1.5. **Situația în privința statelor membre care nu aplică încă integral acquis-ul Schengen, a statelor membre care nu participă la politica comună a UE în domeniul vizelor și a țărilor asociate**

Statele membre care au aderat la Uniune în 2004 (Republica Cehă, Estonia, Cipru, Letonia, Lituania, Ungaria, Malta, Polonia, Slovenia și Slovacia), în 2007 (Bulgaria și România) și în 2013 (Croația) au obligații în temeiul acordului din momentul intrării sale în vigoare.

Numai Bulgaria, Croația, Cipru și România nu aplică încă integral acquis-ul Schengen. Aceste țări vor continua să elibereze vize naționale cu o valabilitate limitată la propriul lor teritoriu național. Când vor aplica integral acquis-ul Schengen, aceste state membre vor continua să aplice acordul.

Legislația națională continuă să se aplice în cazul tuturor aspectelor care nu sunt reglementate de acord până la data aplicării integrale a acquis-ului Schengen de către statele membre respective. Începând de la acea dată, se vor aplica normele Schengen/legislația națională în cazul aspectelor care nu sunt reglementate de acord.

Bulgaria, Croația, Cipru și România sunt autorizate să recunoască permisele de ședere, vizele de tip „D” și vizele de scurtă ședere eliberate de statele membre Schengen și de țările asociate pentru șederile de scurtă durată pe teritoriul lor.

În conformitate cu articolul 21 din Convenția de punere în aplicare a Acordului Schengen din 14 iunie 1985 privind eliminarea treptată a controalelor la frontierele comune, toate statele Schengen trebuie să recunoască vizele de lungă ședere și permisele de ședere eliberate de fiecare dintre ele ca fiind valabile pentru șederi de scurtă durată pe teritoriile celorlalte state Schengen. Statele membre Schengen acceptă permisele de ședere, vizele de tip „D” și vizele de scurtă ședere ale țărilor asociate pentru intrarea și ședera de scurtă durată și viceversa.

Acordul nu se aplică Danemarcei, Irlandei și Regatului Unit, însă cuprinde declarații comune cu privire la disponibilitatea statelor membre respective de a încheia acorduri bilaterale privind facilitarea eliberării vizelor cu Ucraina.

La 1 martie 2009 a intrat în vigoare un acord bilateral între Danemarca și Ucraina privind facilitarea eliberării vizelor. Nu au avut loc negocieri privind facilitarea eliberării vizelor între Ucraina și, respectiv Irlanda și Regatul Unit.

Cu toate că aceste țări sunt asociate spațiului Schengen, acordul nu se aplică Islandei, Liechtensteinului, Norvegiei și Elveției, însă cuprinde declarații comune cu privire la disponibilitatea țărilor Schengen respective de a încheia acorduri bilaterale privind facilitarea eliberării vizelor cu Ucraina.

Norvegia a semnat un acord bilateral privind facilitarea eliberării vizelor la 13 februarie 2008. Acordul respectiv a intrat în vigoare la 1 septembrie 2011.

Elveția a finalizat negocierile referitoare la un acord bilateral privind facilitarea eliberării vizelor în noiembrie 2011. Islanda a anunțat că au fost lansate negocierile cu Ucraina.

1.6. **Acordul/acorduri bilaterale**

Articolul 13 alineatul (1) din acord prevede:

„(1) De la intrarea sa în vigoare, prezentul acord are întâietate în fața prevederilor oricărui acord sau aranjament bilateral sau multilateral încheiat între un stat membru și Ucraina, în măsura în care prevederile acordurilor sau ale aranjamentelor se referă la domenii reglementate de prezentul acord.”

De la data intrării în vigoare a acordului, dispozițiile acordurilor bilaterale în vigoare dintre statele membre și Ucraina cu privire la aspectele abordate în acord încetează să se mai aplice. În conformitate cu legislația Uniunii, statele membre trebuie să ia măsurile necesare pentru a elimina incompatibilitățile dintre acordurile lor bilaterale și acord.

Cu toate acestea, articolul 13 alineatul (2) din acord prevede:

„(2) Dispozițiile acordurilor sau ale înțelegerilor bilaterale dintre diferitele state membre și Ucraina, încheiate înainte de intrarea în vigoare a prezentului acord, care prevăd exonerarea titularilor de pașapoarte de serviciu nebiometrice de obligația de a deține viză, se aplică în continuare fără a aduce atingere dreptului statelor membre în cauză sau al Ucrainei de a denunța sau de a suspenda aceste acorduri sau înțelegeri bilaterale."

Următoarele state membre au semnat un acord bilateral cu Ucraina care prevede exonerarea titularilor de pașapoarte de serviciu de obligația de a deține viză: Bulgaria, Croația, Cipru, Letonia, Lituania, Ungaria, Polonia, România și Slovacia.

În conformitate cu articolul 13 alineatul (1) din acord, în măsura în care aceste acorduri bilaterale reglementează cazul titularilor de pașapoarte de serviciu biometrice, articolul 10 alineatul (2) din acordare prioritate față de acordurile bilaterale respective. În conformitate cu articolul 13 alineatul (2) din acord, aceste acorduri bilaterale, care au fost încheiate înainte de intrarea în vigoare a acordului de modificare, continuă să se aplice în măsura în care reglementează cazul titularilor de pașapoarte de serviciu nebiometrice, fără a aduce atingere dreptului statelor membre în cauză sau al Ucrainei de a denunța sau de a suspenda aceste acorduri sau înțelegeri bilaterale. Exonerarea de obligația de a deține viză acordată de un stat membru titularilor de pașapoarte de serviciu nebiometrice se aplică numai pentru călătoriile pe teritoriul statului membru respectiv și nu pentru călătoriile pe teritoriul altor state membre Schengen.

În cazul în care un stat membru a încheiat un acord sau o înțelegere bilaterală cu Ucraina cu privire la aspecte care nu sunt reglementate de acord, această exonerare va continua să se aplice și după intrarea în vigoare a acordului.

1.7. **Declarația Comunității Europene privind accesul solicitanților de vize și armonizarea informațiilor privind procedurile de eliberare a vizelor de scurtă ședere și documentele necesare pentru depunerea cererii de viză de scurtă ședere**

În conformitate cu această declarație a Comunității Europene, atașată la acord, au fost elaborate informații de bază comune privind accesul solicitanților de vize la misiunile diplomatice și oficiile consulare ale statelor membre, privind procedurile și condițiile de eliberare a vizelor, precum și privind valabilitatea vizelor eliberate, în scopul asigurării faptului că solicitanții de viză primesc informații coerente și uniforme. Aceste informații sunt disponibile pe pagina de internet a delegației UE în Ucraina: http://eeas.europa.eu/delegations/ukraine/index_en.htm

Se solicită misiunilor diplomatice și oficiilor consulare ale statelor membre să disemineze aceste informații pe scară largă (pe panourile de informare, prin broșuri, pe site-uri internet etc.) și să difuzeze, de asemenea, informații precise privind condițiile de eliberare a vizelor, reprezentarea statelor membre în Ucraina și lista UE armonizată a documentelor justificative necesare.

II. ORIENTĂRI PRIVIND DISPOZIȚII SPECIFICE

2.1. **Norme care se aplică tuturor solicitanților de viză**

Important: se reamintește faptul că facilitățile menționate mai jos referitoare la taxele de procesare, durata procedurilor de prelucrare a cererilor de viză, călătoriile în cazul în care documentele sunt pierdute sau furate și prelungirea vizelor în circumstanțe excepționale se aplică tuturor solicitanților de viză și titularilor de viză ucraineni.

2.1.1. *Taxa de procesare a vizelor*

Articolul 6 alineatul (1) din acord prevede:

„Taxa pentru procesarea cererilor de viză depuse de cetățenii ucraineni este de 35 EUR. Suma menționată mai sus poate fi modificată în conformitate cu procedura prevăzută la articolul 14 alineatul (4)."

În conformitate cu articolul 6 alineatul (1), taxa pentru procesarea unei cereri de viză este de 35 EUR. Această taxă se va aplica tuturor solicitanților de viză ucraineni (inclusiv turiștilor) și se referă la vizele de scurtă ședere, indiferent de numărul de intrări. Taxa se aplică, de asemenea, în cazul cererilor de viză depuse la frontierele externe.

Articolul 6 alineatul (2) din acord prevede:

„În cazul în care Ucraina reintroduce obligativitatea vizelor pentru cetățenii UE, taxa de viză percepută de Ucraina nu depășește 35 EUR sau suma convenită în cazul în care taxa este modificată în conformitate cu procedura prevăzută la articolul 14 alineatul (4)."

Articolul 6 alineatul (3) din acord prevede:

„Statele membre percep o taxă de 70 EUR pentru procesarea vizelor în cazurile în care, pe baza distanței dintre locul de reședință al solicitantului și locul în care a fost depusă cererea, solicitantul a cerut să se ia o decizie cu privire la cerere în termen de trei zile de la depunerea acesteia și consulatul a acceptat să ia o decizie în termen de trei zile."

Se percepe o taxă de 70 EUR pentru procesarea cererilor de viză în cazurile în care cererea de viză și documentele justificative au fost depuse de către solicitantul de viză al cărui loc de reședință se știe că se află în oblastul în care statul membru în care solicitantul dorește să călătorească nu are reprezentanță consulară (dacă în oblastul respectiv nu există niciun consulat, niciun centru de vize, nici consulate ale statelor membre care au încheiat acorduri de reprezentare cu statul membru în care solicitantul dorește să călătorească) și în cazul în care misiunea diplomatică sau oficiul consular a fost de acord să ia o decizie privind cererea de viză în termen de trei zile. Dovada locului de reședință al solicitantului de viză este furnizată în cadrul formularului de cerere de viză.

În principiu, obiectivul articolului 6 alineatul (3) din acord este de a facilita solicitarea unei vize de către solicitanții care locuiesc la o distanță mare de un consulat. În cazul în care este necesară o călătorie îndelungată pentru a depune o cerere de viză, scopul este de a o elibera rapid, astfel încât solicitantul să poată primi viza fără a mai fi nevoit să facă încă o dată aceeași călătorie îndelungată.

Din motivele menționate mai sus, în cazurile în care timpul „standard" de procesare a unei cereri de viză de către o anumită misiune diplomatică sau un anumit oficiu consular este de trei zile sau mai puțin, se percepe taxa de viză standard de 35 EUR.

Pentru misiunile diplomatice și oficiile consulare care au un sistem de programare, perioada de timp pentru obținerea unei programări nu trebuie considerată ca făcând parte din timpul de procesare (a se vedea, de asemenea, II. 2.1.2).

Articolul 6 alineatul (4) din acord prevede:

„(4) Fără a aduce atingere alineatului (5), sunt scutite de plata taxelor pentru procesarea cererilor de viză următoarele categorii de persoane:

(a) pentru rudele apropiate – soț/soție, copii (inclusiv copii adoptați), părinți (inclusiv tutori), bunici și nepoți – care vizitează cetățeni ucraineni aflați în situație de ședere legală pe teritoriul statelor membre sau cetățeni ai Uniunii Europene care au reședința pe teritoriul statului membru ai căror resortisanți sunt".

(NB. Acest punct reglementează situația rudelor ucrainene apropiate care călătoresc în statele membre pentru a vizita cetățeni ucraineni aflați în situație de ședere legală în statele membre sau cetățeni ai Uniunii Europene care au reședința pe teritoriul statului membru ai cărui resortisanți sunt. Solicitanților de viză ucraineni care sunt membri de familie ai unui cetățean al Uniunii, în înțelesul articolului 5 alineatul (2) din Directiva 2004/38/CE a Parlamentului European și a Consiliului ([1]), li se eliberează vize gratuit, în cel mai scurt termen și pe baza unei proceduri accelerate.)

„(b) pentru membrii delegațiilor oficiale care, ca urmare a unei invitații oficiale adresate Ucrainei, participă la reuniuni, consultări, negocieri sau programe de schimb, precum și la evenimente organizate pe teritoriul unuia dintre statele membre de către organizații interguvernamentale;

(c) membrii guvernelor și ai parlamentelor naționale și regionale, ai curților constituționale și curților supreme, dacă aceștia nu sunt scutiți de obligativitatea vizelor prin prezentul acord;

(d) elevii, studenții instituțiilor universitare și postuniversitare și profesorii însoțitori, care călătoresc în scopul efectuării unor studii sau în scopuri educaționale;

(e) persoanele cu dizabilități și persoanele care le însoțesc, dacă este cazul"; (N.B. Pentru a beneficia de scutirea de taxă, trebuie prezentate documente justificative care să demonstreze că fiecare solicitant de viză se încadrează la această categorie.)

„(f) persoanele care au prezentat documente care dovedesc necesitatea călătoriei în scopuri umanitare, inclusiv pentru urmarea unui tratament medical urgent, precum și persoana însoțitoare, sau persoanele care participă la funeraliile unei rude apropiate sau vizitează o rudă apropiată care este grav bolnavă;

(g) participanții la evenimente sportive internaționale și persoanele însoțitoare"; (N.B. Sunt acoperite numai persoanele însoțitoare care călătoresc în capacitate profesională; suporterii nu sunt considerați drept persoane însoțitoare.)

([1]) Directiva 2004/38/CE a Parlamentului European și a Consiliului din 29 aprilie 2004 privind dreptul la liberă circulație și ședere pe teritoriul statelor membre pentru cetățenii Uniunii și membrii familiilor acestora, de modificare a Regulamentului (CEE) nr. 1612/68 și de abrogare a Directivelor 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE și 93/96/CEE (JO L 158, 30.4.2004, p. 77).

„(h) persoanele care participă la activități științifice, culturale și artistice, inclusiv programe de schimb între universități și de altă natură;

(i) participanții la programe oficiale de schimb organizate de orașe înfrățite și de alte entități municipale;

(j) jurnaliștii și personalul tehnic care îi însoțește în scop profesional"; [N.B. La această literă se încadrează jurnaliștii care fac obiectul articolului 4 alineatul (1) litera (e) din acord].

„(k) pensionari"; (N.B. Pentru a beneficia de scutirea de taxă pentru această categorie, solicitanții de viză trebuie să prezinte documente justificative care să le demonstreze statutul de pensionari.)

„(l) conducătorii auto care prestează servicii de transport internațional de mărfuri și pasageri către teritoriile statelor membre, cu vehicule înregistrate în Ucraina;

(m) membri ai echipajului trenului, precum și ai echipajului responsabil de vagoanele frigorifice și de locomotivele trenurilor internaționale, care călătoresc pe teritoriile statelor membre;

(n) copiii cu vârsta sub 18 ani și copiii aflați în întreținere, cu vârsta sub 21 de ani." (N.B. Pentru a beneficia de scutirea de taxă pentru această categorie, solicitanții de viză trebuie să prezinte documente justificative care să le demonstreze vârsta și, în plus – dacă au sub 21 de ani – faptul că se află în întreținere.);

„(o) reprezentanții comunităților religioase;

(p) membrii profesiilor liberale care participă la expoziții, conferințe, simpozioane, seminare internaționale sau la alte evenimente similare organizate pe teritoriul statelor membre;

(q) participanții în vârstă de cel mult 25 de ani la seminare, conferințe, evenimente sportive, culturale sau educaționale, organizate de organizații nonprofit;

(r) reprezentanții organizațiilor societății civile care efectuează călătorii în scopul formării educaționale sau în scopul participării la seminare și conferințe, inclusiv în cadrul programelor de schimb;

(s) pentru participanții la programe oficiale de cooperare transfrontalieră ale Uniunii Europene, cum ar fi cele din cadrul Instrumentului european de vecinătate și parteneriat (IEVP).

Primul paragraf se aplică, de asemenea, atunci când scopul călătoriei este tranzitul."

Articolul 6 alineatul (4) al doilea paragraf din acord se aplică numai dacă scopul călătoriei către țara terță este echivalent cu unul dintre scopurile enumerate la articolul 6 alineatul (4) literele (a)-(s) din acord, de exemplu dacă tranzitul este necesar pentru a participa la un seminar, a vizita membri de familie, a participa la un program de schimb al organizațiilor societății civile etc. în țara terță.

Categoriile de persoane menționate mai sus sunt scutite integral de taxă. În plus, în conformitate cu articolul 16 alineatul (6) din Codul de vize, „în cazuri particulare, se poate renunța la perceperea taxei de viză sau valoarea acesteia poate fi redusă dacă acest lucru contribuie la promovarea unor interese de ordin cultural sau sportiv, precum și a unor interese din domeniul politicii externe, al politicii de dezvoltare și alte domenii de interes public vital sau din motive umanitare".

Totuși, această regulă nu poate fi aplicată pentru a scuti solicitanții de taxa de 70 EUR pentru procesarea vizei în situații individuale în care cererea de viză și documentele justificative au fost depuse de către solicitantul de viză al cărui loc de reședință se știe că se află departe de misiunea diplomatică sau oficiul consular al statului membru și care se încadrează într-una din categoriile scutite de plata taxei de viză, enumerate la articolul 6 alineatul (4) din acord.

Ar trebui reamintit, de asemenea, faptul că categoriile de persoane scutite de plata taxei de viză ar putea totuși plăti o taxă pentru servicii în cazul în care un stat membru cooperează cu un prestator extern de servicii.

Articolul 6 alineatul (5) din acord prevede:

„(5) Dacă un stat membru cooperează cu un prestator extern de servicii în vederea eliberării vizelor, prestatorul extern de servicii poate percepe o taxă pentru servicii. Această taxă este proporțională cu costurile suportate de prestatorul extern de servicii în îndeplinirea sarcinilor sale și nu depășește 30 EUR. Statele membre mențin posibilitatea, pentru toți solicitanții, de a-și depune cererile direct la consulatele lor. În cazul în care solicitanții sunt obligați să obțină o programare pentru depunerea unei cereri, programarea se face, de regulă, într-un termen de două săptămâni de la data solicitării acesteia."

Menținerea posibilității ca toate categoriile de solicitanți să-și depună cererile direct la consulat și nu prin intermediul unui prestator extern de servicii presupune că ar trebui să existe o posibilitate reală de alegere între aceste două opțiuni. Chiar dacă accesul direct nu trebuie să fie organizat în condiții identice sau similare celor aplicabile în cazul accesului la prestatorul de servicii, condițiile respective nu ar trebui să facă accesul direct imposibil în practică. Chiar dacă se acceptă ca perioada de așteptare pentru obținerea unei programări să fie diferită în cazul accesului direct, aceasta nu trebuie să fie atât de lungă încât să facă accesul direct imposibil în practică.

2.1.2. *Durata procedurilor pentru procesarea cererilor de viză*

Articolul 7 din acord prevede:

„(1) Misiunile diplomatice și oficiile consulare ale statelor membre iau o decizie privind cererea de eliberare a vizei în termen de 10 zile calendaristice de la data primirii cererii și a documentelor necesare pentru eliberarea vizei.

(2) Perioada de timp pentru luarea deciziei privind cererea de viză se poate prelungi până la 30 de zile calendaristice în cazuri individuale, mai ales atunci când este necesară o analiză detaliată a cererii.

(3) În cazuri de urgență, perioada de timp pentru luarea deciziei privind o cerere de viză se poate reduce la două zile lucrătoare sau mai puțin."

O decizie privind cererea de viză se ia, în principiu, în termen de 10 zile calendaristice de la data primirii cererii de viză complete și a documentelor justificative.

Această perioadă poate fi prelungită până la 30 de zile calendaristice atunci când este necesară o analiză detaliată, de exemplu, pentru consultarea autorităților centrale.

Toate aceste termene încep să curgă numai din momentul în care dosarul de cerere este complet, adică de la data primirii cererii de viză și a documentelor justificative.

Pentru misiunile diplomatice și oficiile consulare care au un sistem de programare, perioada de timp pentru obținerea unei programări nu trebuie considerată ca făcând parte din timpul de procesare. La stabilirea programării, ar trebui să se țină seama de posibila situație de urgență invocată de solicitantul de viză în vederea punerii în aplicare a articolului 7 alineatul (3) din acord. De regulă, programările ar trebui să se facă într-un termen de două săptămâni de la data solicitării programării [a se vedea articolul 6 alineatul (5) din acord]. Un termen mai îndelungat ar trebui să fie o excepție, inclusiv în perioadele foarte aglomerate. Comitetul mixt va monitoriza cu atenție acest aspect. Statele membre depun toate eforturile pentru a se asigura că programările solicitate de membrii delegațiilor oficiale din Ucraina pentru a depune cereri la misiunile diplomatice și oficiile consulare sunt fixate cât mai curând posibil, de preferință în termen de două zile lucrătoare, în cazurile urgente în care invitația a fost transmisă cu întârziere.

Decizia privind reducerea perioadei de timp pentru luarea unei decizii cu privire la o cerere de viză, astfel cum se menționează la articolul 7 alineatul (3) din acord, este luată de către funcționarul consular.

2.1.3. *Prelungirea vizei în circumstanțe excepționale*

Articolul 9 din acord prevede:

„Cetățenii Ucrainei care nu pot părăsi teritoriul statului membru la data menționată pe viză din motive de forță majoră beneficiază gratuit de prelungirea vizei, în conformitate cu legislația aplicată de statul de destinație, pentru întreaga perioadă necesară întoarcerii acestora în statul de reședință."

În ceea ce privește posibilitatea de a extinde durata de valabilitate a vizelor în cazuri de forță majoră, de exemplu în cazul internării într-un spital din motive neprevăzute/pentru o boală subită/în caz de accident, dacă titularul vizei nu are posibilitatea de a părăsi teritoriul statului membru până la data menționată pe viză, se aplică dispozițiile articolului 33 alineatul (1) din Codul de vize în măsura în care sunt compatibile cu acordul (de exemplu, viza prelungită trebuie să rămână o viză uniformă, permițând intrarea pe teritoriul tuturor statelor membre Schengen pentru care viza era valabilă la data eliberării). Cu toate acestea, în temeiul acordului, prelungirea vizei se efectuează gratuit în caz de forță majoră.

2.2. **Norme care se aplică anumitor categorii de solicitanți de viză**

2.2.1. *Documente justificative privind scopul călătoriei*

Pentru toate categoriile de persoane enumerate la articolul 4 alineatul (1) din acord, inclusiv pentru conducătorii auto care prestează servicii de transport internațional de mărfuri și pasageri, vor fi necesare numai documentele justificative indicate privind scopul călătoriei. Pentru aceste categorii de solicitanți nu se solicită alte documente privind scopul ședерii. Astfel cum se menționează la articolul 4 alineatul (3) din acord, nu se va mai cere altă justificare, invitație sau validare referitoare la scopul călătoriei.

Dacă, în cazuri individuale, persistă îndoieli cu privire la scopul real al călătoriei, solicitantul vizei este invitat la un interviu (suplimentar) detaliat la sediul ambasadei/consulatului, unde poate fi chestionat în legătură cu scopul real al vizitei sau intenția solicitantului de a se întoarce – a se vedea articolul 21 alineatul (8) din Codul de vize. În astfel de cazuri individuale, solicitantul de viză poate furniza documente suplimentare sau funcționarul consular le poate cere, în mod excepțional. Comitetul mixt va monitoriza îndeaproape acest aspect.

Pentru categoriile de persoane care nu sunt menționate la articolul 4 alineatul (1) din acord, normele actuale continuă să se aplice în ceea ce privește documentele care fac dovada scopului călătoriei. Același lucru este valabil și pentru documentele referitoare la consimțământul părinților pentru călătoria copiilor cu vârsta sub 18 ani.

Normele Schengen sau legislația națională se aplică în cazul aspectelor care nu fac obiectul dispozițiilor acordului, cum ar fi recunoașterea documentelor de călătorie, asigurarea medicală de călătorie, garanțiile privind întoarcerea în țara de origine și mijloacele de subzistență suficiente (a se vedea punctul I.1.2.).

În conformitate cu „Declarația Uniunii Europene privind documentele necesare pentru depunerea cererii de viză de scurtă ședere”, anexată la acordul de modificare, „Uniunea Europeană va stabili o listă armonizată a documentelor justificative, în conformitate cu articolul 48 alineatul (1) litera (a) din Codul de vize, în scopul de a se asigura că solicitanților de viză din Ucraina li se cere să depună, în principiu, aceleași documente justificative”; consulatele statelor membre, care acționează în cadrul cooperării locale Schengen, sunt invitate să se asigure că solicitanții de viză ucraineni primesc informații de bază coerente și uniforme și că trebuie să depună, în principiu, aceleași documente justificative, indiferent de consulatul statului membru în care depun cererea.

În principiu, cererea inițială sau adeverința prevăzută la articolul 4 alineatul (1) din acord sunt prezentate împreună cu cererea de viză. Cu toate acestea, consulatul poate începe procesarea cererii de viză pe baza documentelor transmise prin fax sau a copiilor cererii ori ale adeverinței. Totuși, consulatul poate solicita documentul original în cazul unei prime cereri și solicită documentul original în cazuri individuale în care există îndoieli.

întrucât listele autorităților de mai jos cuprind uneori și numele persoanei care poate semna cererile/adeverințele relevante, autoritățile ucrainene ar trebui să informeze cooperarea locală Schengen atunci când aceste persoane sunt înlocuite.

Articolul 4 din acord prevede că:

„(1) Pentru următoarele categorii de cetățeni ai Ucrainei, sunt suficiente următoarele documente pentru justificarea scopului călătoriei pe teritoriul celeilalte părți:

(a) pentru membrii delegațiilor oficiale care, ca urmare a unei invitații oficiale adresate Ucrainei, participă la reuniuni, consultări, negocieri sau programe de schimb, precum și la evenimente organizate pe teritoriul unuia dintre statele membre de către organizații interguvernamentale:

— o scrisoare emisă de o autoritate ucraineană, care să confirme că solicitantul este un membru al delegației sale care călătorește pe teritoriul celeilalte părți în scopul participării la evenimentele menționate anterior, scrisoare însoțită de o copie a invitației oficiale”.

Numele solicitantului trebuie să fie indicat în scrisoarea emisă de autoritatea competentă, care să confirme că persoana face parte din delegația care călătorește pe teritoriul celeilalte părți în scopul de a participa la reuniunea oficială. Numele solicitantului nu trebuie în mod obligatoriu să fie indicat în invitația oficială de participare la reuniune, deși acest lucru ar putea fi valabil atunci când invitația oficială se adresează unei anumite persoane.

Această dispoziție se aplică membrilor delegațiilor oficiale, indiferent de tipul de pașaport (pașaport de serviciu nebiometric sau pașaport obișnuit) pe care îl dețin;

„(b) pentru oamenii de afaceri și reprezentanții organizațiilor de afaceri:

— o solicitare scrisă din partea unei persoane juridice sau societăți comerciale gazdă sau din partea unui birou sau filială a unei astfel de persoane juridice sau societăți comerciale, din partea unor autorități locale și naționale ale statelor membre sau a comitetelor de organizare a târgurilor și a expozițiilor, a conferințelor și a simpozioanelor organizate pe teritoriile statelor membre;

(c) pentru conducătorii auto care prestează servicii de transport internațional de mărfuri și pasageri către teritoriile statelor membre, cu vehicule înmatriculate în Ucraina:

— o cerere scrisă din partea asociației naționale a transportatorilor din Ucraina care prestează servicii de transport rutier internațional, în care să se precizeze scopul, durata, destinația (destinațiile) și frecvența călătoriilor".

Autoritățile competente care furnizează servicii de transport rutier internațional și sunt responsabile pentru precizarea scopului, duratei, destinației (destinațiilor) și a frecvenței călătoriilor efectuate de conducătorii auto care furnizează servicii de transport internațional de mărfuri și pasageri către teritoriile statelor membre, cu vehicule înmatriculate în Ucraina, sunt următoarele:

1. Asociația transportatorilor rutieri internaționali din Ucraina (AsMAP/„АсМАП")

Adresa poștală a AsMAP:

11, Shorsa str.

Kiev, 03150, Ucraina

Funcționari autorizați să semneze cererile:

Kostiuchenko Leonid – Președintele AsMAP din Ucraina;

Dokil' Leonid – Vicepreședintele AsMAP din Ucraina;

Kuchynskiy Yurii – Vicepreşedintele AsMAP din Ucraina.

2. Întreprinderea de stat „Serviciul privind transportul rutier internațional" (SE „SIRC")

Adresa poștală a SE „SIRC":

57, av. Nauka

Kiev, 03083, Ucraina

Tel. +38 044 524 21 01

Fax +38 044 524 00 70

Funcționari autorizați să semneze cererile:

Tkachenko Anatolij – Directorul SE „SIRC";

Neronov Oleksandr – Prim-director adjunct al SE „SIRC".

3. Uniunea pentru transport rutier și logistică din Ucraina

Adresa poștală a Uniunii pentru transport rutier și logistică din Ucraina:

28, Predslavinska str.

Kiev, 03150, Ucraina

Tel./fax +38 044 528 71 30/+38 044 528 71 46/+38 044 529 44 40

Funcționarul autorizat să semneze cererile:

Lypovskiy Vitalij – Președintele Uniunii pentru transport rutier și logistică din Ucraina

4. Asociația ucraineană a transportatorilor de autovehicule (AAAC)(Всеукраїнська асоціація автомобільних перевізників)

Adresa poștală a AAAC:

139, Velyka Vasylkivska str.

Kiev, 03150, Ucraina

Tel./fax: +38044-538-75-05, +38044-529-25-21

Funcționari autorizați să semneze cererile:

Reva Vitalii (Віталій Рева) – Președintele AAAC

Glavatskyi Petro (Петро Главатський) – Vicepreşedintele AAAC

e-mail: vaap@i.com.ua

5. Asociația ucraineană a transportatorilor de autovehicule (AAAC) (Всеукраїнська асоціація автомобільних перевізників)

   Adresa poștală a AAAC:

   3, Rayisy Okipnoyi str.

   Kiev, 02002, Ucraina

   Tel./fax: +38044-517-44-31, +38044-516-47-26

   Funcționari autorizați să semneze cererile:

   Vakulenko Volodymyr (Вакуленко Володимир Михайлович) – Vicepreședintele AAAC

6. Întreprinderea ucraineană de stat „Ukrinteravtoservice” (Українське державне підприємство по обслуговуванню іноземних та вітчизняних автотранспортних засобів „Укрінтеравтосервіс”)

   Adresa poștală a întreprinderii ucrainene de stat „Ukrinteravtoservice”:

   57, av. Nauky

   Kiev, 03083, Ucraina

   Funcționari autorizați să semneze cererile:

   Dobrohod Serhii (Доброход Сергій Олександрович) – Director general al întreprinderii ucrainene de stat „Ukrinteravtoservice” (telefon: +38 044 524-09-99; telefon mobil: +38 050 463-89-32);

   Kubalska Svitlana (Кубальська Світлана Сергіївна) – Director general adjunct al întreprinderii ucrainene de stat „Ukrinteravtoservice” (telefon: +38 044 524-09-99; telefon mobil: +38 050 550-82-62);

Luând în considerare problemele actuale cu această categorie de solicitanți de viză, Comitetul mixt monitorizează îndeaproape punerea în aplicare a acestei dispoziții;

„(d) pentru membri ai echipajului trenului, precum și ai echipajului responsabil de vagoanele frigorifice și de locomotivele trenurilor internaționale, care călătoresc pe teritoriile statelor membre:

— o solicitare scrisă din partea companiei de căi ferate competente din Ucraina, în care se specifică scopul, durata și frecvența călătoriilor”.

Autoritatea competentă în domeniul transporturilor feroviare din Ucraina este Administrația de Stat a Transportului Feroviar din Ucraina („Ukrzaliznytsia”/„Укрзалізниця”).

Adresa poștală a „Ukrzaliznytsia”:

5-7 Tverskaya str.
Kiev, 03680, Ucraina

Potrivit repartizării competențelor din conducerea „Ukrzaliznytsia”, funcționarii responsabili cu furnizarea de informații privind scopul, durata și frecvența călătoriilor efectuate de membri ai echipajului trenului, precum și ai echipajului responsabil de vagoanele frigorifice și de locomotivele trenurilor internaționale, care călătoresc pe teritoriile statelor membre sunt:

Bolobolin Serhii (Болоболін Сергій Петрович) – Prim-director general al Ukrzaliznytsia (telefon: +38 044 465 00 10);

Serhiyenko Mykola (Сергієнко Микола Іванович) – Prim-director general adjunct al Ukrzaliznytsia (telefon: +38 044 465 00 01);

Zhurakivskyy Vitaliy (Жураківський Віталій Олександрович) – Prim-director general adjunct al Ukrzaliznytsia (telefon: +38 044 465 00 41);

Slipchenko Oleksiy (Сліпченко Олексій Леонтійович) – Director general adjunct al Ukrzaliznytsia (telefon: +38 044 465 00 14);

Naumenko Petro (Науменко Петро Петрович) – Director general adjunct al Ukrzaliznytsia (telefon: +38 044 465 00 12);

Chekalov Pavlo (Чекалов Павло Леонтійович) – Director general adjunct al Ukrzaliznytsia (telefon: +38 044 465 00 13);

Matviiv Igor – șeful departamentului „Relații internaționale” al Ukrzaliznytsia (telefon: +38 044 465 04 25);

„(e) pentru jurnaliști și personalul tehnic care îi însoțește în scop profesional:

— un certificat sau un alt document eliberat de o organizație profesională sau de angajatorul solicitantului, din care să reiasă faptul că persoana în cauză este un jurnalist calificat și în care să se indice că scopul călătoriei este desfășurarea unei activități de natură jurnalistică sau din care să reiasă faptul că persoana în cauză este membru al personalului tehnic care îl însoțește pe jurnalist în scop profesional”.

Această categorie nu include jurnaliștii independenți.

Trebuie prezentat certificatul sau documentul din care să reiasă faptul că solicitantul este un jurnalist profesionist, precum și documentul original eliberat de angajatorul acestuia în care să se indice că scopul călătoriei este desfășurarea unei activități de natură jurnalistică sau din care să reiasă faptul că persoana în cauză este membru al personalului tehnic care îl însoțește pe jurnalist în scop profesional.

Organizația profesională competentă din Ucraina care poate demonstra că persoana în cauză este un jurnalist calificat este:

1. Uniunea națională a jurnaliștilor din Ucraina (NUJU) („Національна спілка журналістів україни”, НСЖУ).

   NUJU eliberează angajaților calificați din domeniul mass-media legitimații naționale de jurnalist profesionist și legitimații internaționale de presă după modelul standard stabilit de Federația Internațională a Jurnaliștilor.

   Adresa poștală a NUJU:

   27-a Khreschatyk str.

   Kiev, 01001, Ucraina

   Persoana autorizată a NUJU:

   Nalyvaiko Oleg Igorovych (Наливайко Олег Ігорович) – șeful NUJU

   Telefon/Fax: +38044-234-20-96; +38044-234-49-60; +38044-234-52-09

   e-mail: spilka@nsju.org; admin@nsju.org.

2. Uniunea independentă a mass-mediei din Ucraina (IMUU) Незалежна медіа-профспілка України.

   Adresa poștală a IMUU:

   Office 25,

   27 – A, Khreshchatyk Str.,

   Kiev, 01001, Ucraina

   Persoanele autorizate:

   Lukanov Yurii (Луканов Юрій Вадимович) – Directorul IMUU

   Vynnychuk Oksana (Оксана Винничук) – Secretar executiv al IMUU

   Telefon + 38 050 356 57 58

   e-mail: secretar@profspilka.org.ua;

„(f) pentru persoanele care participă la activități științifice, culturale și artistice, inclusiv programe de schimb între universități și de altă natură:

— o invitație scrisă din partea unei organizații-gazdă de a participa la aceste activități;

(g) pentru elevii, studenții instituțiilor universitare și postuniversitare și profesorii însoțitori care efectuează călătorii de studii sau educaționale, inclusiv în cadrul programelor de schimb, precum și al altor activități conexe educației școlare:

— o invitație scrisă sau o adeverință de înscriere din partea universității, colegiului sau școlii-gazdă, carnete de student sau certificate privind cursurile care vor fi urmate”.

Un carnet de student nu poate fi acceptat ca document justificativ pentru scopul călătoriei decât dacă este emis de universitatea, colegiul sau școala gazdă în care urmează să se desfășoare studiile sau formarea educațională;

„(h) pentru participanții la evenimente sportive internaționale și persoanele care îi însoțesc în calitate profesională:

— o invitație scrisă din partea organizației-gazdă: autorități competente, federații sportive și comitete olimpice naționale ale statelor membre”.

Lista persoanelor însoțitoare în cazul evenimentelor sportive internaționale se va limita la persoanele care însoțesc sportivul/sportiva în scop profesional: antrenori, maseuri, manager, personal medical și șeful clubului sportiv. Suporterii nu sunt considerați drept persoane însoțitoare;

„(i) pentru participanții la programe oficiale de schimb organizate de orașe înfrățite și de alte entități municipale:

— o invitație scrisă din partea șefilor administrației/primarilor acestor orașe sau ai altor entități municipale”.

Șefii administrației/primarii orașelor sau ai altor entități municipale care au competența de a elibera invitația scrisă sunt șefii administrației/primarii orașelor sau ai entităților municipale în care urmează să se desfășoare activitatea programului de înfrățire. Această categorie include numai înfrățirile oficiale;

„(j) pentru rudele apropiate – soț/soție, copii (inclusiv copii adoptați), părinți (inclusiv tutori), bunici și nepoți – care vizitează cetățeni ucraineni aflați în situație de ședere legală pe teritoriul statelor membre sau cetățeni ai Uniunii Europene care au reședința pe teritoriul statului membru ai căror resortisanți sunt:

— o invitație scrisă din partea gazdei”.

Această literă reglementează situația rudelor ucrainene apropiate care călătoresc în statele membre pentru a vizita cetățeni ucraineni aflați în situație de ședere legală în statele membre sau cetățeni ai Uniunii Europene care au reședința pe teritoriul statului membru ai cărui resortisanți sunt.

Autenticitatea semnăturii persoanei care face invitația trebuie dovedită de autoritatea competentă în conformitate cu legislația națională a țării de reședință.

Este necesar, de asemenea, să se facă dovada șederii legale a persoanei care face invitația și a legăturii de familie; de exemplu, împreună cu invitația scrisă din partea gazdei, se furnizează copii ale documentelor care explică statutul acesteia, cum ar fi o fotocopie a permisului de rezidență, și care confirmă legăturile de familie.

Această dispoziție se aplică, de asemenea, rudelor personalului care lucrează la misiuni diplomatice și consulate, care călătoresc pentru a efectua o vizită de familie de până la 90 de zile pe teritoriul statelor membre, însă nu este necesar să se facă dovada șederii legale și a legăturilor de familie.

În conformitate cu Declarația Uniunii Europene privind facilitățile acordate membrilor de familie, anexată la acordul de modificare, „în scopul facilitării mobilității unui număr mai mare de persoane care au legături de familie (în special frați și surori, precum și copiii acestora) cu cetățeni ucraineni aflați în situație de ședere legală pe teritoriile statelor membre sau cu cetățeni ai Uniunii Europene care au reședința pe teritoriul statului membru ai căror resortisanți sunt, Uniunea Europeană invită oficiile consulare ale statelor membre să utilizeze pe deplin posibilitățile existente în cadrul Codului de vize cu privire la facilitarea eliberării vizelor pentru această categorie de persoane, posibilități care includ, în special, simplificarea documentelor justificative cerute solicitanților de viză, scutirea de taxele de prelucrare și, dacă este cazul, eliberarea de vize cu intrări multiple”;

„(k) pentru rudele care participă la ceremonii funerare:

— un document oficial care să confirme decesul, precum și gradul de rudenie sau alt tip de legătură dintre solicitant și decedat”.

Acordul nu specifică țara ale cărei autorități ar trebui să elibereze documentul oficial menționat mai sus: țara în care se va desfășura ceremonia funerară sau țara în care locuiește persoana care dorește să participe la ceremonia funerară. Ar trebui să se accepte posibilitatea ca autoritățile competente din ambele țări să poată elibera un astfel de document oficial.

Trebuie prezentat documentul oficial menționat anterior care confirmă decesul, precum și gradul de rudenie sau alt tip de legătură dintre solicitant și decedat, de exemplu, certificatul de naștere și/sau de căsătorie;

„(l) pentru vizitarea cimitirelor militare și civile:

— un document oficial care să confirme existența și conservarea mormântului, precum și legătura de familie sau alt tip de legătură dintre solicitant și decedat”.

Acordul nu specifică dacă documentul oficial menționat mai sus ar trebui să fie eliberat de autoritățile: din țara în care este situat cimitirul sau de autoritățile din țara în care persoana care dorește să viziteze cimitirul își are reședința. Ar trebui să se accepte posibilitatea ca autoritățile competente din ambele țări să poată elibera un astfel de document oficial.

Trebuie prezentat documentul oficial menționat anterior care să confirme existența și conservarea mormântului, precum și gradul de rudenie sau alt tip de legătură dintre solicitant și decedat.

În conformitate cu declarația Comunității Europene privind eliberarea vizelor de scurtă ședere pentru vizitarea cimitirelor militare și civile atașată la acord, de regulă, vizele de scurtă ședere pentru persoanele care vizitează cimitirele militare și civile se eliberează pentru o perioadă de până la 14 zile;

„(m) pentru persoanele care călătoresc din motive medicale și pentru persoanele care trebuie să le însoțească:

— un document oficial din partea instituției medicale, care să confirme necesitatea îngrijirii medicale în această instituție și necesitatea de a fi însoțit, precum și dovada mijloacelor financiare suficiente pentru achitarea tratamentului medical".

Trebuie prezentat documentul din partea instituției medicale, care să confirme necesitatea îngrijirii medicale în această instituție, și dovada mijloacelor financiare suficiente pentru achitarea tratamentului medical; acest document ar trebui, de asemenea, să confirme necesitatea ca persoanele în cauză să fie însoțite;

„(n) pentru reprezentanții organizațiilor societății civile atunci când efectuează călătorii în scopul formării educaționale sau în scopul participării la seminare și conferințe, inclusiv în cadrul programelor de schimb:

— o invitație scrisă din partea organizației-gazdă, o confirmare că persoana în cauză reprezintă organizația societății civile și certificatul de la registrul competent privind înființarea organizației respective, eliberat de o autoritate de stat, în conformitate cu legislația națională".

Documentul care dovedește înregistrarea în Ucraina a unei organizații a societății civile este o scrisoare emisă de Serviciul de înregistrare de Stat din Ucraina, care preia informațiile relevante din Registrul asociațiilor publice;

„(o) pentru membrii profesiilor liberale care participă la expoziții, conferințe, simpozioane, seminare internaționale sau la alte evenimente similare organizate pe teritoriul statelor membre:

— o invitație scrisă din partea organizației-gazdă care să confirme că persoana în cauză participă la eveniment;

(p) pentru reprezentanții comunităților religioase:

— o invitație scrisă din partea comunității religioase înregistrate în Ucraina, în care să se precizeze scopul, durata și frecvența călătoriilor".

Documentul care dovedește înregistrarea în Ucraina a unei comunități religioase este un extras din Registrul de stat unificat al persoanelor juridice și al întreprinzătorilor individuali care arată că forma organizațională și juridică a unei entități juridice este aceea a unei comunități religioase;

„(q) pentru participanții la programe oficiale de cooperare transfrontalieră ale Uniunii Europene, cum ar fi cele din cadrul Instrumentului european de vecinătate și parteneriat (IEVP):

— o invitație scrisă din partea organizației-gazdă."

Important: Acordul nu creează nicio normă nouă privind răspunderea persoanelor fizice sau juridice care emit invitații scrise. Dreptul UE/național respectiv se aplică în cazul emiterii unor astfel de invitații false.

2.2.2. *Eliberarea vizelor cu intrări multiple*

În cazul în care solicitantul de viză trebuie să călătorească în mod frecvent sau regulat pe teritoriul statelor membre, se eliberează vize de scurtă ședere pentru mai multe vizite, cu condiția ca durata totală a acestor vizite să nu depășească 90 de zile într-un interval de 180 de zile.

Articolul 5 alineatul (1) din acord prevede:

„(1) Misiunile diplomatice și oficiile consulare ale statelor membre eliberează vize cu intrări multiple cu un termen de valabilitate de cinci ani pentru următoarele categorii de persoane:

(a) membrii guvernelor și ai parlamentelor naționale și regionale, membrii Curților Constituționale și membrii Curților Supreme, procurorii naționali și regionali și adjuncții acestora în exercitarea atribuțiilor care le revin, în cazul în care nu sunt exonerați de obligația de a deține viză în temeiul prezentului acord;

(b) membrii permanenți ai delegațiilor oficiale care, în urma invitațiilor oficiale adresate Ucrainei, participă în mod regulat la reuniuni, consultări, negocieri sau programe de schimb, precum și la evenimente organizate de organizații interguvernamentale pe teritoriul statelor membre;

(c) soții/soțiile și copiii (inclusiv copiii adoptați), care nu depășesc vârsta de 21 de ani sau care sunt în îngrijire, și părinții (inclusiv tutorii) care vizitează cetățeni ucraineni aflați în situație de ședere legală pe teritoriul statelor membre sau cetățeni ai Uniunii Europene care au reședința pe teritoriul statului membru ai căror resortisanți sunt;

(d) oamenii de afaceri și reprezentanții organizațiilor de afaceri care călătoresc în mod regulat în statele membre;

(e) jurnaliștii și personalul tehnic care îi însoțește în scop profesional.

Prin derogare de la primul paragraf, atunci când necesitatea sau intenția de a călători în mod frecvent sau regulat este vădit limitată la o perioadă mai scurtă, termenul de valabilitate al vizei cu intrări multiple este limitat la perioada respectivă, în special atunci când:

— în cazul persoanelor menționate la litera (a), durata funcției deținute;

— în cazul persoanelor menționate la litera (b), durata statutului de membru permanent al unei delegații oficiale;

— în cazul persoanelor menționate la litera (c), perioada de valabilitate a autorizației de ședere legală a cetățenilor ucraineni aflați în situație de ședere legală în Uniunea Europeană;

— în cazul persoanelor menționate la litera (d), durata statutului de reprezentant al organizației de afaceri sau durata contractului de muncă;

— în cazul persoanelor menționate la litera (e), durata contractului de muncă

este mai mică de cinci ani."

Pentru aceste categorii de persoane, luând în considerare statutul lor profesional sau legătura de rudenie cu un cetățean ucrainean aflat în situație de ședere legală pe teritoriile statelor membre sau cu un cetățean al Uniunii Europene care are reședința pe teritoriul statului membru al cărui resortisant este, este justificat să se elibereze, de regulă, o viză cu intrări multiple cu o perioadă de valabilitate de cinci ani. În versiunea inițială a acordului, expresia „cu termen de valabilitate de până la cinci ani" lăsa consulatelor o marjă de apreciere în a decide perioada de valabilitate a vizei, stabilind numai durata maximă de valabilitate. În acordul de modificare, această marjă de apreciere a dispărut, odată cu noua formulare „cu un termen de valabilitate de cinci ani", care stipulează că, dacă solicitantul îndeplinește toate cerințele de la articolul 5 alineatul (1) din acord, „misiunile diplomatice și oficiile consulare ale statelor membre eliberează vize cu intrări multiple cu un termen de valabilitate de cinci ani".

Pentru persoanele care intră sub incidența articolului 5 alineatul (1) litera (a) din acord trebuie să se furnizeze o confirmare a statutului lor profesional și a duratei mandatului acestora.

Această dispoziție nu se aplică persoanelor care intră sub incidența articolului 5 alineatul (1) litera (a) din acord dacă acestea sunt exonerate de obligația de a deține viză în temeiul acordului, și anume dacă sunt titulari de pașapoarte diplomatice sau de pașapoarte de serviciu biometrice.

Pentru persoanele care intră sub incidența articolului 5 alineatul (1) litera (b) din acord trebuie prezentată dovada privind statutul de membru al delegației și necesitatea de a participa în mod regulat la reuniuni, consultări, negocieri sau programe de schimb.

Pentru persoanele care intră sub incidența articolului 5 alineatul (1) litera (c) din acord trebuie prezentată dovada șederii legale a persoanei care face invitația (a se vedea punctul II.2.2.1).

Pentru persoanele care intră sub incidența articolului 5 alineatul (1) literele (d) și (e) din acord trebuie prezentată o confirmare a statutului lor profesional și a duratei activităților acestora.

Articolul 5 alineatul (2) din acord prevede:

„(2) Misiunile diplomatice și oficiile consulare ale statelor membre eliberează vize cu intrări multiple cu un termen de valabilitate de un an pentru următoarele categorii de persoane, cu condiția ca pe parcursul anului precedent acestea să fi obținut cel puțin o viză și să o fi utilizat în conformitate cu legislația statului vizitat privind intrarea și șederea:

(a) conducătorii auto care prestează servicii de transport internațional de mărfuri și pasageri către teritoriile statelor membre, cu vehicule înregistrate în Ucraina;

(b) membri ai echipajului trenului, precum și ai echipajului responsabil de vagoanele frigorifice și de locomotivele trenurilor internaționale, care călătoresc pe teritoriile statelor membre;

(c) persoanele care participă la activități științifice, culturale și artistice, inclusiv programe de schimb între universități și alte tipuri de programe de schimb, care călătoresc în mod regulat în statele membre;

(d) participanții la manifestări sportive internaționale și persoanele care îi însoțesc în scop profesional;

(e) participanții la programe oficiale de schimb organizate de orașe înfrățite și de alte entități municipale;

(f) reprezentanții organizațiilor societății civile care călătoresc în mod regulat în statele membre în scopul formării educaționale sau în scopul participării la seminare și conferințe, inclusiv în cadrul programelor de schimb;

(g) pentru participanții la programe oficiale de cooperare transfrontalieră ale Uniunii Europene, cum ar fi cele din cadrul Instrumentului european de vecinătate și parteneriat (IEVP);

(h) studenții instituțiilor universitare și postuniversitare care efectuează în mod regulat călătorii de studii sau de formare educațională, inclusiv în cadrul programelor de schimb;

(i) pentru reprezentanții comunităților religioase:

(j) membrii profesiilor liberale care participă la expoziții, conferințe, simpozioane, seminare internaționale sau la alte evenimente similare organizate pe teritoriul statelor membre;

(k) persoanele care trebuie să călătorească în mod regulat din motive medicale și persoanele care trebuie să le însoțească.

Prin derogare de la primul paragraf, atunci când necesitatea sau intenția de a călători în mod frecvent sau regulat este vădit limitată la o perioadă mai scurtă, termenul de valabilitate al vizei cu intrări multiple este limitat la perioada respectivă."

În versiunea inițială a acordului, expresia „cu termen de valabilitate de până la un an" lăsa consulatelor o marjă de apreciere în a decide perioada de valabilitate a vizei, stabilind numai durata maximă de valabilitate. În acordul de modificare, această marjă de apreciere a dispărut, odată cu noua formulare „cu un termen de valabilitate de un an", care stipulează că, dacă solicitantul îndeplinește toate cerințele de la articolul 5 alineatul (2) din acord, „misiunile diplomatice și oficiile consulare ale statelor membre eliberează vize cu intrări multiple cu un termen de valabilitate de un an". Se remarcă faptul că vizele cu intrări multiple valabile timp de un an, cu condiția ca în anul precedent (12 luni) solicitantul de viză să fi obținut cel puțin o viză Schengen și să o fi utilizat în conformitate cu legislația statului (statelor) vizitat(e) privind intrarea și șederea (de exemplu, persoana să nu fi depășit perioada legală de ședere) și dacă există motive pentru a solicita o viză cu intrări multiple. Viza Schengen obținută în anul precedent poate fi o viză eliberată de un stat Schengen, altul decât cel în care solicitantul a cerut noua viză. În cazurile în care nu se justifică eliberarea unei vize valabile timp de un an (de exemplu, dacă durata programului de schimb este mai mică de un an sau dacă persoana nu are nevoie să călătorească în mod frecvent sau regulat pentru un an complet), durata de valabilitate a vizei va fi mai mică de un an, cu condiția ca celelalte cerințe pentru eliberarea vizei să fie îndeplinite.

Articolul 5 alineatele (3) și (4) din acord prevăd:

„(3) Misiunile diplomatice și oficiile consulare ale statelor membre eliberează vize cu intrări multiple cu un termen de valabilitate de cel puțin doi ani și de cel mult cinci ani pentru categoriile de persoane menționate la alineatul (2) din prezentul articol, cu condiția ca în ultimii doi ani acestea să fi utilizat vizele cu intrări multiple de un an în conformitate cu legislația statului vizitat privind intrarea și ședera, cu excepția cazului în care necesitatea sau intenția de a călători în mod frecvent sau regulat este vădit limitată la o perioadă mai scurtă, situație în care termenul de valabilitate al vizei cu intrări multiple este limitat la perioada respectivă.

(4) Perioada totală de ședere pe teritoriul statelor membre a persoanelor la care se face referire la alineatele (1) – (3) ale prezentului articol nu trebuie să depășească 90 de zile, în decurs de 180 de zile."

Vizele cu intrări multiple valabile de la doi la cinci ani se eliberează categoriilor menționate la articolul 5 alineatul (2) din acord, cu condiția ca în ultimii doi ani acestea să fi utilizat vizele Schengen cu intrări multiple de un an în conformitate cu legislația statului (statelor) vizitat(e) privind intrarea și ședera pe teritoriul respectiv, și ca necesitatea de a călători în mod frecvent sau regulat să nu fie vădit limitată la o perioadă mai scurtă. Trebuie remarcat faptul că o viză cu o valabilitate de la doi la cinci ani se eliberează numai dacă solicitantului de viză i s-au eliberat două vize valabile timp de un an (și nu mai puțin) în cursul celor doi ani precedenți și dacă solicitantul a utilizat aceste vize în conformitate cu legislația statului (statelor) vizitat(e) privind intrarea și ședera pe teritoriul respectiv. Misiunile diplomatice și oficiile consulare hotărăsc, pe baza evaluării fiecărei cereri de viză, perioada de valabilitate a acestor vize, și anume de la doi la cinci ani.

În ceea ce privește definirea criteriilor de la articolul 5 alineatul (2) din acord: „cu condiția ca … să existe motive pentru solicitarea unei vize cu intrări multiple” și de la articolul 5 alineatul (3) din acord: „cu condiția ca … motivele pentru solicitarea unei vize cu intrări multiple să fie în continuare valabile”, pentru eliberarea acestui tip de vize se aplică criteriile prevăzute la articolul 24 alineatul (2) litera (a) din Codul de vize, și anume faptul că persoana trebuie să călătorească frecvent într-unul sau mai multe state membre, de exemplu pentru afaceri.

Nu există nicio obligație de a elibera o viză cu intrări multiple dacă solicitantul nu a utilizat o viză anterioară. Cu toate acestea, o astfel de viză poate fi eliberată dacă solicitantul nu a utilizat viza anterioară din cauza unor circumstanțe independente de voința sa, de exemplu, în cazul unui șofer de camion, o perioadă lungă de absență de la locul de muncă din motive de boală.

A se vedea punctul II.2.2.1. privind documentele care justifică scopul călătoriei pentru eliberarea vizelor cu intrări multiple pentru categoriile menționate la articolul 5 din acord.

2.2.3. *Titularii de pașapoarte diplomatice și de serviciu*

Articolul 10 din acord prevede:

„(1) Cetățenii Ucrainei, posesori de pașapoarte diplomatice valabile, pot intra, ieși și tranzita fără viză teritoriile statelor membre.

(2) Cetățenii ucraineni care sunt titulari de pașapoarte de serviciu biometrice valabile pot intra, ieși și tranzita fără viză teritoriile statelor membre.

(3) Persoanele menționate la alineatele (1) și (2) ale prezentului articol pot sta pe teritoriul statelor membre pentru o perioadă de ședere de până la 90 de zile, în decurs de 180 de zile.”

Acordurile sau înțelegerile bilaterale existente privind exonerarea titularilor de pașapoarte de serviciu nebiometrice de obligația de a deține viză continuă să se aplice, cu excepția cazului în care acestea au fost denunțate sau suspendate (a se vedea punctul I.1.6).

Detașarea diplomaților în statele membre nu este reglementată de acord. Se aplică procedura de acreditare obișnuită.

III. STATISTICI

Pentru a permite Comitetului mixt să monitorizeze eficient acordul, misiunile diplomatice și oficiile consulare ale statelor membre trebuie să transmită Comisiei, o dată la șase luni, statistici care să se refere, în măsura posibilului, și să precizeze pentru fiecare lună:

— tipurile de vize eliberate diferitelor categorii de persoane care fac obiectul acordului;

— numărul de refuzuri de a elibera viză diferitelor categorii de persoane care fac obiectul acordului;

— procentul solicitanților chemați la un interviu personal, pe categorii de persoane;

— numărul de vize cu intrări multiple de cinci ani eliberate resortisanților ucraineni (pe țară);

— procentul vizelor eliberate gratuit diferitelor categorii de persoane care fac obiectul acordului.

DECIZIA (PESC) 2015/439 A CONSILIULUI

din 16 martie 2015

de prelungire a mandatului Reprezentantului Special al Uniunii Europene pentru Sahel

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind Uniunea Europeană, în special articolul 33 și articolul 31 alineatul (2),

având în vedere propunerea Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate,

întrucât:

(1) La 18 martie 2013, Consiliul a adoptat Decizia 2013/133/PESC [1] de numire a domnului Michel Dominique REVEYRAND-DE MENTHON în calitate de Reprezentant Special al Uniunii Europene (RSUE) pentru Sahel. Mandatul RSUE a fost prelungit prin Decizia 2014/130/PESC [2] a Consiliului și urmează să expire la 28 februarie 2015.

(2) Mandatul RSUE ar trebui să fie prelungit pentru o perioadă suplimentară de opt luni.

(3) RSUE își va duce la îndeplinire mandatul în contextul unei situații care s-ar putea deteriora și care ar putea aduce atingere realizării obiectivelor acțiunii externe a Uniunii prevăzute la articolul 21 din tratat,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Reprezentantul Special al Uniunii Europene

(1) Mandatul domnului Michel Dominique REVEYRAND-DE MENTHON în calitate de RSUE pentru regiunea Sahel se prelungește până la 31 octombrie 2015. Mandatul RSUE poate fi încheiat mai devreme, în cazul în care Consiliul decide astfel, la propunerea Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate (ÎR).

(2) În sensul mandatului RSUE, regiunea Sahel este definită ca incluzând preocuparea primordială a Strategiei UE pentru securitate și dezvoltare în Sahel („strategia"), și anume Burkina Faso, Ciad, Mali, Mauritania și Niger. În ceea ce privește aspectele cu implicații regionale mai extinse, RSUE va conlucra, după caz, cu alte țări și entități regionale sau internaționale din afara regiunii Sahel, precum și din Africa de Vest și din Golful Guineei, după caz.

(3) Având în vedere necesitatea unei abordări la nivel regional a provocărilor interdependente cu care se confruntă regiunea, RSUE pentru Sahel își desfășoară activitatea în strânsă consultare cu alți RSUE relevanți, printre care RSUE pentru regiunea Mediteranei de sud, RSUE pentru drepturile omului și RSUE pentru Uniunea Africană.

Articolul 2

Obiective de politică

(1) Mandatul RSUE se întemeiază pe obiectivul de politică al Uniunii în ceea ce privește contribuția activă a Sahelului la eforturile regionale și internaționale pentru o pace durabilă, securitate și dezvoltare în regiune. De asemenea RSUE urmărește sporirea calității, intensității și impactului angajamentului multilateral al Uniunii în Sahel.

(2) RSUE contribuie la dezvoltarea și aplicarea tuturor aspectelor pe care le îmbracă acțiunea Uniunii, în special în domeniile de politică, securitate și dezvoltare, printre care și strategia, precum și la coordonarea tuturor instrumentelor de acțiune ale Uniunii.

(3) Inițial se va acorda prioritate Republicii Mali și stabilizării sale pe termen lung și dimensiunilor regionale ale conflictului existent în Mali.

---

[1] Decizia 2013/133/PESC a Consiliului din 18 martie 2013 de numire a Reprezentantului Special al Uniunii Europene pentru Sahel (JO L 75, 19.3.2013, p. 29).

[2] Decizia 2014/130/PESC a Consiliului din 10 martie 2014 de prelungire a mandatului Reprezentantului Special al Uniunii Europene pentru Sahel (JO L 71, 12.3.2014, p. 14).

(4) În ceea ce privește Mali, obiectivele de politică ale Uniunii urmăresc să promoveze, prin utilizarea coordonată și eficace a tuturor instrumentelor sale, revenirea la Mali pe calea păcii, reconcilierii, securității și dezvoltării. Ar trebui acordată atenția cuvenită statelor Burkina Faso și Niger, în special în perspectiva alegerilor din aceste țări.

Articolul 3

Mandat

(1) În vederea realizării obiectivelor de politică ale Uniunii în ce privește Sahelul, mandatul RSUE este:

(a) să contribuie activ la coordonarea și dezvoltarea ulterioară a abordării cuprinzătoare a Uniunii privind criza regională, pe baza strategiei sale, urmărind să consolideze coerența și eficiența globale ale activităților Uniunii în Sahel, mai ales în Mali;

(b) să se implice, împreună cu toate părțile interesate relevante din regiune, guverne, autorități regionale existente, organizații internaționale și regionale, societatea civilă și diaspora, în urmărirea obiectivelor Uniunii și să contribuie la o mai bună înțelegere a rolului pe care Uniunea îl are în Sahel;

(c) să reprezinte Uniunea în cadrul forumurilor internaționale și publice relevante, inclusiv în cadrul Grupului de sprijin și monitorizare a situației din Mali și să asigure vizibilitate sprijinului acordat de Uniune în domeniul gestionării crizelor și al prevenirii conflictelor, printre care și Misiunii militare a Uniunii Europene pentru a contribui la instruirea forțelor armate maliene (EUTM Mali) și Misiunii PSAC a Uniunii Europene în Niger (EUCAP Sahel Niger);

(d) să coopereze strâns cu Organizația Națiunilor Unite (ONU), în special cu Reprezentantul Special al Secretarului General pentru Africa Occidentală și cu Reprezentantul Special al Secretarului General pentru Mali, cu Uniunea Africană (UA), în special cu Înaltul Reprezentant al UA pentru Mali și Sahel, cu Comunitatea economică a statelor Africii occidentale (ECOWAS) și cu alte părți interesate de la nivel național, regional și internațional, inclusiv alți trimiși speciali pentru Sahel, precum și cu alte organisme relevante în zona Maghreb;

(e) să monitorizeze îndeaproape dimensiunea regională și transfrontalieră a crizei, printre care și aspectele precum terorismul, traficul de armament, fluxurile migratorii și de refugiați, precum și fluxurile financiare aferente, în strânsă cooperare cu coordonatorul UE pentru lupta împotriva terorismului, la aplicarea în continuare a Strategiei UE de combatere a terorismului;

(f) să mențină contacte politice constante la nivel înalt cu țările din regiune afectate de terorism și criminalitate internațională în vederea garantării unei abordări consecvente și cuprinzătoare și a asigurării rolului fundamental al Uniunii în cadrul eforturilor internaționale de combatere a terorismului și criminalității internaționale. În cadrul acestor se include sprijinul activ acordat de Uniune pentru consolidarea capacităților regionale în domeniul securității și garantarea abordării corespunzătoare a cauzelor terorismului și criminalității internaționale în Sahel;

(g) să urmărească îndeaproape efectele politice și de securitate ale crizelor umanitare în regiune;

(h) să contribuie, în ceea ce privește Mali, la eforturile regionale și internaționale de facilitare a soluționării crizei din Mali, în special revenirea deplină la o situație de normalitate constituțională și guvernare pe întregul teritoriu, precum și un dialog național credibil și deschis tuturor care să ducă la o soluționare politică durabilă;

(i) să promoveze consolidarea instituțională, reforma în domeniul securității, precum și construcția unei păci durabile și reconcilierea în Mali;

(j) să contribuie la punerea în aplicare a politicii Uniunii cu privire la drepturile omului în regiune, în cooperare cu RSUE pentru drepturile omului, inclusiv a liniilor directoare ale UE cu privire la drepturile omului, în special a liniilor directoare ale UE privind copiii și conflictele armate, precum și privind violența împotriva femeilor și fetelor și combaterea tuturor formelor de discriminare a acestora, și a politicii Uniunii privind femeile, pacea și securitatea, inclusiv prin monitorizarea și raportarea evoluțiilor, precum și prin formularea de recomandări în acest sens, și să mențină contacte regulate cu autoritățile relevante din Mali și din regiune, cu Biroul Procurorului Curții Penale Internaționale, Oficiul Înaltului Comisar al Națiunilor Unite pentru Drepturile Omului și cu apărătorii drepturilor omului și observatorii din regiune;

(k) să urmărească și să raporteze cu privire la respectarea rezoluțiilor Consiliului de Securitate ONU (RCSONU) relevante, în special RCSONU 2056 (2012), 2071 (2012), 2085 (2012) și 2100 (2013).

(2) În scopul îndeplinirii mandatului său, RSUE, între altele:

(a) consiliază și raportează în ceea ce privește definirea pozițiilor Uniunii în forurile regionale și internaționale, în scopul promovării și consolidării proactive a abordării cuprinzătoare a Uniunii privind criza din Sahel;

(b) menține perspectiva globală a activităților Uniunii și cooperează strâns cu delegațiile Uniunii implicate.

Articolul 4

Executarea mandatului

(1) RSUE are răspunderea îndeplinirii mandatului său sub autoritatea ÎR.

(2) Comitetul politic și de securitate (COPS) menține o legătură privilegiată cu RSUE și este principalul punct de contact al RSUE cu Consiliul. COPS furnizează RSUE orientări strategice și îndrumare politică în cadrul mandatului, fără a aduce atingere responsabilităților ÎR.

(3) RSUE își desfășoară activitatea în strânsă coordonare cu Serviciul European de Acțiune Externă (SEAE) și cu departamentele relevante ale acestuia, în special cu coordonatorul pentru regiunea Sahel.

Articolul 5

Finanțare

(1) Valoarea de referință financiară destinată să acopere cheltuielile aferente mandatului RSUE pentru perioada 1 martie 2015-31 octombrie 2015 este de 900 000 EUR.

(2) Cheltuielile sunt gestionate în conformitate cu procedurile și normele aplicabile bugetului general al Uniunii.

(3) Gestionarea cheltuielilor face obiectul unui contract între RSUE și Comisie. RSUE răspunde în fața Comisiei pentru toate cheltuielile.

Articolul 6

Constituirea și componența echipei

(1) În limitele mandatului său și ale mijloacelor financiare aferente puse la dispoziție, RSUE răspunde de constituirea echipei sale. Echipa dispune de competențele necesare în chestiuni politice și de securitate specifice, conform mandatului. RSUE informează prompt Consiliul și Comisia cu privire la componența echipei sale.

(2) Statele membre, instituțiile Uniunii și SEAE pot propune detașarea de personal care să lucreze cu RSUE. Remunerarea personalului detașat pe lângă RSUE este asigurată de respectivul stat membru, de instituția Uniunii în cauză ori de SEAE. Experții detașați de statele membre pe lângă instituțiile Uniunii sau SEAE pot, de asemenea, să fie repartizați pe lângă RSUE. Personalul internațional angajat este format din resortisanți ai statelor membre.

(3) Toți membrii personalului detașat rămân sub autoritatea administrativă a statului membru din care provin sau a instituției Uniunii care i-a detașat ori a SEAE, își duc la îndeplinire sarcinile și acționează în interesul mandatului RSUE.

(4) Personalul RSUE este amplasat în același loc cu departamentele relevante ale SEAE sau cu delegațiile relevante ale Uniunii, în vederea asigurării coerenței și consecvenței activităților lor respective.

Articolul 7

Privilegiile și imunitățile RSUE și ale personalului RSUE

Privilegiile, imunitățile și alte garanții necesare îndeplinirii și bunei desfășurări a misiunii RSUE, precum și a membrilor personalului RSUE se stabilesc împreună cu partea-gazdă sau părțile-gazdă, după caz. Statele membre și SEAE oferă tot sprijinul necesar în acest sens.

Articolul 8

Securitatea informațiilor UE clasificate

RSUE și membrii echipei acestuia respectă principiile și standardele minime de securitate stabilite prin Decizia 2013/488/UE a Consiliului ([1]).

([1]) Decizia 2013/488/UE a Consiliului din 23 septembrie 2013 privind normele de securitate pentru protecția informațiilor UE clasificate (JO L 274, 15.10.2013, p. 1).

Articolul 9

Accesul la informații și asistență logistică

(1) Statele membre, Comisia, SEAE și Secretariatul General al Consiliului garantează accesul RSUE la toate informațiile relevante.

(2) Delegațiile Uniunii și/sau statele membre, după caz, furnizează asistență logistică în regiune.

Articolul 10

Securitate

În conformitate cu politica Uniunii privind securitatea personalului cu atribuții operaționale desfășurat în afara Uniunii în temeiul titlului V din tratat, RSUE ia toate măsurile a căror aplicare este rezonabilă, conform mandatului său și pe baza condițiilor de securitate din regiunea geografică pentru care este responsabil, pentru a asigura securitatea întregului personal aflat sub directa sa autoritate, în special prin:

(a) elaborarea unui plan de securitate specific, pe baza orientărilor primite din partea SEAE, care să includă măsuri de securitate fizice, organizaționale și procedurale specifice, destinate gestionării deplasării personalului în condiții de siguranță către zona geografică și în interiorul acesteia și gestionării incidentelor de securitate, precum și un plan de urgență și de evacuare aferent misiunii;

(b) asigurarea faptului că întreg personalul desfășurat în afara Uniunii beneficiază de asigurare pentru un grad înalt de risc, necesară în condițiile specifice zonei geografice;

(c) asigurarea faptului că toți membrii echipei care urmează să fie desfășurați în afara Uniunii, inclusiv personalul contractat la nivel local, au participat, înainte de sosirea în zona de misiune sau după aceasta, la cursuri adecvate de instruire în domeniul securității, pe baza clasificărilor de risc atribuite zonei geografice;

(d) asigurarea punerii în aplicare a tuturor recomandărilor convenite, formulate ca urmare a evaluărilor periodice privind securitatea, și transmiterea către Consiliu, ÎR și Comisie a unor rapoarte scrise cu privire la punerea în aplicare a acestora și la alte aspecte legate de securitate, în cadrul rapoartelor intermediare și al celui privind executarea mandatului.

Articolul 11

Raportare

(1) RSUE prezintă periodic rapoarte ÎR și COPS. De asemenea, RSUE prezintă rapoarte grupurilor de lucru ale Consiliului, dacă este necesar. Rapoartele periodice sunt difuzate prin rețeaua COREU. RSUE poate furniza rapoarte Consiliului Afaceri Generale. În conformitate cu articolul 36 din tratat, RSUE poate fi implicat în activitatea de informare a Parlamentului European.

(2) RSUE raportează cu privire la cea mai adecvată modalitate de desfășurare a inițiativelor Uniunii, printre care contribuția Uniunii la reforme și în ceea ce privește aspectele politice ale proiectelor de dezvoltare relevante ale Uniunii, în coordonare cu delegațiile Uniunii în regiune.

Articolul 12

Coordonarea cu alți actori din UE

(1) În cadrul Strategiei, RSUE contribuie la unitatea, coerența și eficacitatea acțiunii politice și diplomatice a Uniunii și asigură sprijin pentru implicarea semnificativă a tuturor instrumentelor Uniunii și acțiunilor statelor membre, în vederea realizării obiectivelor de politică ale Uniunii.

(2) Activitățile RSUE se coordonează cu cele ale delegațiilor Uniunii și cu cele ale Comisiei, precum și cu cele ale altor RSUE activi în regiune. RSUE informează periodic misiunile statelor membre și delegațiile Uniunii în regiune.

(3) Pe teren se menține o strânsă legătură cu șefii delegațiilor Uniunii și cu șefii de misiune ai statelor membre. RSUE, în strânsă cooperare cu delegațiile relevante ale Uniunii, oferă orientări politice la nivel local șefilor misiunilor EUCAP Sahel Niger și EUCAP Sahel Mali, precum și comandantului misiunii EUTM Mali. RSUE, comandantul misiunii EUTM Mali, comandantul operației civile EUCAP Sahel Niger și cel al EUCAP Sahel Mali se consultă reciproc în funcție de necesități.

Articolul 13

Revizuire

Punerea în aplicare a prezentei decizii și coerența acesteia cu alte contribuții din partea Uniunii în regiune fac obiectul unei revizuiri periodice. RSUE prezintă Consiliului, ÎR și Comisiei un raport cuprinzător privind executarea mandatului până la sfârșitul lunii august 2015.

Articolul 14

Intrare în vigoare

Prezenta decizie intră în vigoare la data adoptării.

Se aplică de la 1 martie 2015.

Adoptată la Bruxelles, 16 martie 2015.

Pentru Consiliu
Președintele
F. MOGHERINI

DECIZIA (PESC) 2015/440 A CONSILIULUI

din 16 martie 2015

de prelungire a mandatului Reprezentantului Special al Uniunii Europene pentru Cornul Africii

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind Uniunea Europeană, în special articolul 33 și articolul 31 alineatul (2),

având în vedere propunerea Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate,

întrucât:

(1) La 8 decembrie 2011, Consiliul a adoptat Decizia 2011/819/PESC ([1]) de numire a domnului Alexander RONDOS în calitate de Reprezentant Special al Uniunii Europene (RSUE) pentru Cornul Africii. Mandatul RSUE urmează să expire la 28 februarie 2015.

(2) Mandatul RSUE ar trebui prelungit în continuare până la 31 octombrie 2015.

(3) RSUE își va executa mandatul în contextul unei situații care s-ar putea deteriora și care ar putea aduce atingere realizării obiectivelor acțiunii externe a Uniunii prevăzute la articolul 21 din tratat,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Reprezentantul Special al Uniunii Europene

Mandatul domnului Alexander RONDOS în calitate de RSUE pentru Cornul Africii se prelungește până la 31 octombrie 2015. Consiliul poate decide ca mandatul RSUE să se încheie mai devreme, pe baza unei evaluări din partea Comitetului politic și de securitate (COPS) și a unei propuneri din partea Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate (ÎR).

În sensul mandatului RSUE, Cornul Africii cuprinde Republica Djibouti, Statul Eritreea, Republica Federală Democrată Etiopia, Republica Kenya, Republica Federală Somalia, Republica Sudan, Republica Sudanul de Sud și Republica Uganda. În ceea ce privește aspectele cu implicații regionale mai extinse, RSUE inițiază contacte cu țări și entități regionale din afara Cornului Africii, după caz.

Articolul 2

Obiective de politică

(1) Mandatul RSUE se întemeiază pe obiectivele de politică ale Uniunii în ceea ce privește Cornul Africii, astfel cum au fost stabilite în cadrul său strategic adoptat la 14 noiembrie 2011 și în concluziile relevante ale Consiliului, și anume de a contribui în mod activ la eforturile regionale și internaționale în vederea realizării coexistenței pașnice și a păcii, securității și dezvoltării durabile în interiorul și în rândul țărilor din regiune. RSUE are ca obiectiv suplimentar sporirea calității, a intensității, a impactului și a vizibilității angajamentului pluridimensional al Uniunii în Cornul Africii.

(2) Obiectivele de politică includ, printre altele:

(a) continuarea stabilizării situației din Somalia, în special din perspectiva unei dimensiuni regionale;

(b) coexistența pașnică a Sudanului și a Sudanului de Sud ca două state viabile și prospere cu structuri politice robuste și responsabile;

(c) soluționarea conflictelor actuale și evitarea conflictelor potențiale dintre țările din regiune sau în interiorul acestora;

(d) sprijinirea cooperării regionale la nivel politic, de securitate și economic.

([1]) Decizia 2011/819/PESC a Consiliului din 8 decembrie 2011 de numire a Reprezentantului Special al Uniunii Europene pentru Cornul Africii (JO L 327, 9.12.2011, p. 62).

Articolul 3

Mandat

(1) În vederea realizării obiectivelor de politică ale UE în ceea ce privește Cornul Africii, mandatul RSUE constă în:

(a) implicarea, împreună cu toate părțile interesate relevante din regiune, guverne, autorități regionale, organizații internaționale și regionale, societatea civilă și diaspora, în vederea urmăririi obiectivelor Uniunii și a contribuției la o mai bună înțelegere a rolului pe care Uniunea îl are în regiune;

(b) reprezentarea Uniunii în forurile internaționale relevante, după caz, și asigurarea vizibilității sprijinului acordat de Uniune în vederea gestionării crizelor, precum și a soluționării și a prevenirii conflictelor;

(c) încurajarea și sprijinirea cooperării politice și de securitate eficace și a integrării economice din regiune prin parteneriatul Uniunii cu Uniunea Africană (UA), precum și cu organizațiile regionale, în special cu Agenția Interguvernamentală pentru Dezvoltare (IGAD);

(d) urmărirea evoluțiilor politice din regiune și contribuția la dezvoltarea politicii Uniunii cu privire la regiune, inclusiv în ceea ce privește Somalia, Sudan, Sudanul de Sud, problema granițelor dintre Etiopia și Eritreea și punerea în aplicare a Acordului de la Alger, Inițiativa bazinului Nilului și alte aspecte din regiune care au impact asupra securității, stabilității și prosperității sale;

(e) în ceea ce privește Somalia și acționând în strânsă coordonare cu Trimisul special al UE pentru Somalia și cu partenerii regionali și internaționali relevanți, inclusiv cu Reprezentantul Special al Secretarului General al Organizației Națiunilor Unite (ONU) pentru Somalia și cu UA, contribuția activă la acțiuni și inițiative care duc la stabilizarea și la acordurile post-tranziție suplimentare cu Somalia, cu accent pe promovarea unei abordări coordonate și coerente la nivel internațional în ceea ce privește Somalia, construirea unor bune relații de vecinătate și sprijinirea dezvoltării sectorului de securitate în Somalia, inclusiv prin intermediul misiunii militare a Uniunii Europene destinate să contribuie la instruirea forțelor de securitate somaleze (EUTM Somalia), forțele navale aflate sub comanda Uniunii Europene (EUNAVFOR Atalanta), misiunea Uniunii Europene referitoare la consolidarea capacităților maritime regionale în statele din Cornul Africii (EUCAP NESTOR) și al sprijinului continuu pe care Uniunea îl acordă Misiunii Uniunii Africane în Somalia (AMISOM), în strânsă cooperare cu statele membre;

(f) în ceea ce privește Sudanul și Sudanul de Sud și în strânsă cooperare cu șefii respectivi ai delegațiilor Uniunii, contribuția la coerența și la eficacitatea politicii Uniunii cu privire la Sudan și la Sudanul de Sud și sprijinirea coexistenței lor pașnice, în special prin intermediul punerii în aplicare a Acordurilor de la Addis Abeba și al soluționării chestiunilor încă nerezolvate Acordului global de pace, inclusiv Abyei, al soluțiilor politice la conflictele în desfășurare, în special din Darfur, Kordofanul de Sud și Nilul Albastru, al consolidării instituționale în Sudanul de Sud și al reconcilierii naționale. În această privință, RSUE contribuie la o abordare internațională coerentă în strânsă cooperare cu UA și în special cu Grupul la nivel înalt de punere în aplicare al UA pentru Sudan (AUHIP), cu ONU și cu alte părți interesate regionale și internaționale;

(g) urmărirea îndeaproape a provocărilor transfrontaliere care afectează Cornul Africii, inclusiv terorismul, radicalizarea, securitatea maritimă și pirateria, criminalitatea organizată, traficul de arme, fluxurile de refugiați și de migranți și eventualele consecințe politice și de securitate ale crizelor umanitare;

(h) promovarea accesului umanitar în întreaga regiune;

(i) contribuția la punerea în aplicare a Deciziei 2011/168/PESC a Consiliului [1] și a politicii Uniunii în domeniul drepturilor omului, în cooperare cu RSUE pentru drepturile omului, inclusiv a liniilor directoare ale UE cu privire la drepturile omului, în special a liniilor directoare ale UE privind copiii și conflictele armate, precum și a liniilor directoare privind violența împotriva femeilor și combaterea tuturor formelor de discriminare la adresa femeilor, și a politicii Uniunii referitoare la Rezoluția 1325 (2000) a Consiliului de Securitate al ONU, inclusiv prin monitorizarea și raportarea evoluțiilor, precum și formularea de recomandări în acest sens.

(2) În scopul îndeplinirii mandatului, RSUE, printre altele:

(a) consiliază și raportează în ceea ce privește definirea pozițiilor Uniunii în forurile internaționale, după caz, în scopul promovării proactive a unei abordări politice consecvente a Uniunii în privința Cornului Africii;

(b) menține o viziune de ansamblu asupra tuturor activităților Uniunii.

[1] Decizia 2011/168/PESC a Consiliului din 21 martie 2011 privind Curtea Penală Internațională și de abrogare a Poziției comune 2003/444/PESC (JO L 76, 22.3.2011, p. 56).

Articolul 4

Executarea mandatului

(1) RSUE răspunde de executarea mandatului, acționând sub autoritatea ÎR.

(2) COPS menține o legătură privilegiată cu RSUE și reprezintă principalul punct de contact al RSUE cu Consiliul. COPS furnizează RSUE orientări strategice și îndrumare politică în cadrul mandatului, fără a aduce atingere competențelor ÎR.

(3) RSUE își desfășoară activitatea în strânsă coordonare cu Serviciul European de Acțiune Externă (SEAE) și cu departamentele relevante ale acestuia, cu delegațiile Uniunii din regiune și cu Comisia.

Articolul 5

Finanțare

(1) Valoarea de referință financiară destinată acoperirii cheltuielilor aferente mandatului RSUE pentru perioada 1 martie 2015-31 octombrie 2015 este de 1 770 000 EUR.

(2) Cheltuielile sunt gestionate în conformitate cu procedurile și normele aplicabile bugetului general al Uniunii.

(3) Gestionarea cheltuielilor face obiectul unui contract între RSUE și Comisie. RSUE răspunde în fața Comisiei pentru toate cheltuielile.

Articolul 6

Constituirea și componența echipei

(1) În limitele mandatului său și ale mijloacelor financiare aferente puse la dispoziție, RSUE răspunde de constituirea echipei sale. Echipa dispune de competențele necesare în chestiuni politice și de securitate specifice, conform mandatului. RSUE informează în mod prompt și regulat Consiliul și Comisia cu privire la componența echipei sale.

(2) Statele membre, instituțiile Uniunii și SEAE pot propune detașarea de personal care să lucreze cu RSUE. Remunerarea personalului detașat este asigurată de statul membru, de instituția Uniunii în cauză ori de SEAE, după caz. Experții detașați de statele membre pe lângă instituțiile Uniunii sau SEAE pot, de asemenea, să fie repartizați pe lângă RSUE. Personalul internațional contractat este format din resortisanți ai statelor membre.

(3) Toți membrii personalului detașat rămân sub autoritatea administrativă a statului membru din care provin sau a instituției Uniunii care i-a detașat ori a SEAE, își duc la îndeplinire sarcinile și acționează în interesul mandatului RSUE.

(4) Personalul RSUE este amplasat în același loc cu departamentele relevante ale SEAE sau cu delegațiile relevante ale Uniunii, pentru a contribui la coerența și consecvența activităților lor respective.

Articolul 7

Privilegiile și imunitățile RSUE și ale personalului RSUE

Privilegiile, imunitățile și alte garanții necesare îndeplinirii și bunei desfășurări a misiunii RSUE, precum și ale membrilor personalului RSUE se stabilesc împreună cu țările-gazdă, după caz. Statele membre și SEAE oferă tot sprijinul necesar în acest sens.

Articolul 8

Securitatea informațiilor UE clasificate

RSUE și membrii echipei sale respectă principiile și standardele minime de securitate stabilite prin Decizia 2013/488/UE a Consiliului ([1]).

([1]) Decizia 2013/488/UE a Consiliului din 23 septembrie 2013 privind normele de securitate pentru protecția informațiilor UE clasificate (JO L 274, 15.10.2013, p. 1).

Articolul 9

Accesul la informații și asistență logistică

(1) Statele membre, Comisia, SEAE și Secretariatul General al Consiliului garantează accesul RSUE la toate informațiile relevante.

(2) Delegațiile Uniunii în regiune și statele membre, după caz, furnizează asistență logistică în regiune.

Articolul 10

Securitate

În conformitate cu politica Uniunii privind securitatea personalului cu atribuții operaționale desfășurat în afara Uniunii în temeiul titlului V din tratat, RSUE ia toate măsurile a căror aplicare este rezonabilă, în conformitate cu mandatul RSUE și cu condițiile de securitate din regiunea geografică pentru care este responsabil, pentru a asigura securitatea întregului personal aflat sub directa autoritate a RSUE, în special prin:

(a) elaborarea unui plan de securitate specific misiunii, pe baza îndrumărilor SEAE, care să prevadă măsuri de securitate fizice, organizaționale și procedurale specifice misiunii, prin care să se reglementeze gestionarea deplasării personalului în condiții de siguranță către zona de misiune și în interiorul acesteia și gestionarea incidentelor de securitate și care să includă un plan de urgență și un plan de evacuare pentru misiune;

(b) asigurarea faptului că întregul personal desfășurat în afara Uniunii beneficiază de asigurare pentru un grad înalt de risc, necesară în condițiile specifice zonei de misiune;

(c) asigurarea faptului că toți membrii echipei RSUE care urmează să fie desfășurați în afara Uniunii, inclusiv personalul contractat la nivel local, au participat, înainte de sosire sau la sosirea în zona de misiune, la cursuri adecvate de instruire în domeniul securității, pe baza clasificărilor de risc atribuite zonei de misiune de către SEAE;

(d) asigurarea punerii în aplicare a tuturor recomandărilor formulate de comun acord ca urmare a evaluărilor periodice privind securitatea și transmiterea către Consiliu, ÎR și Comisie a unor rapoarte scrise cu privire la punerea în aplicare a acestora și la alte aspecte legate de securitate, în cadrul rapoartelor privind progresele înregistrate și privind executarea mandatului.

Articolul 11

Raportare

(1) RSUE prezintă ÎR și COPS, periodic, rapoarte verbale și scrise. De asemenea, RSUE prezintă rapoarte grupurilor de lucru ale Consiliului, dacă este necesar. Rapoartele periodice sunt difuzate prin rețeaua COREU. RSUE poate prezenta rapoarte Consiliului Afaceri Externe. În conformitate cu articolul 36 din tratat, RSUE poate fi implicat în activitatea de informare a Parlamentului European.

(2) RSUE raportează cu privire la cea mai bună modalitate de urmărire a inițiativelor Uniunii, cum ar fi contribuția Uniunii la reforme și includerea aspectelor politice ale proiectelor de dezvoltare relevante ale Uniunii, în coordonare cu delegațiile Uniunii din regiune.

Articolul 12

Coordonare

(1) RSUE contribuie la unitatea, coerența și eficacitatea acțiunilor Uniunii și la asigurarea faptului că toate instrumentele Uniunii și acțiunile statelor membre sunt angajate într-un mod coerent pentru a atinge obiectivele de politică ale Uniunii. Activitățile RSUE se coordonează cu cele ale delegațiilor Uniunii și ale Comisiei, precum și cu cele ale altor RSUE activi în regiune, în special cu cele ale RSUE pentru UA. RSUE furnizează periodic informări misiunilor statelor membre și delegațiilor Uniunii din regiune.

(2) Pe teren, se menține o strânsă legătură cu șefii delegațiilor Uniunii și cu șefii de misiune ai statelor membre. Aceștia depun toate eforturile pentru a susține RSUE în executarea mandatului său. RSUE, în strânsă cooperare cu delegațiile relevante ale Uniunii, oferă orientări politice la nivel local comandantului forței EUNAVFOR Atalanta, comandantului misiunii UE EUTM Somalia și șefului misiunii EUCAP NESTOR. RSUE, comandantul operației UE și comandantul operației civile se consultă reciproc în funcție de necesități.

(3) RSUE colaborează îndeaproape cu autoritățile din țările în cauză, cu ONU, UA, IGAD, cu alte părți interesate de pe plan național, regional și internațional, precum și cu societatea civilă din regiune.

Articolul 13

Revizuirea

Punerea în aplicare a prezentei decizii și coerența acesteia cu alte contribuții ale Uniunii în regiune se revizuiește în mod periodic. RSUE prezintă Consiliului, ÎR și Comisiei un raport cuprinzător privind executarea mandatului până la 31 august 2015.

Articolul 14

Intrarea în vigoare

Prezenta decizie intră în vigoare la data adoptării.

Se aplică de la 1 martie 2015.

Adoptată la Bruxelles, 16 martie 2015.

Pentru Consiliu
Președintele
F. MOGHERINI

DECIZIA (PESC) 2015/441 A CONSILIULUI

din 16 martie 2015

de modificare și prelungire a Deciziei 2010/96/PESC privind o misiune militară a Uniunii Europene pentru a contribui la instruirea forțelor de securitate somaleze

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind Uniunea Europeană, în special articolul 42 alineatul (4) și articolul 43 alineatul (2),

având în vedere propunerea Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate,

întrucât:

(1) La 15 februarie 2010, Consiliul a adoptat Decizia 2010/96/PESC ([1]). Mandatul misiunii militare a UE se încheie la 31 martie 2015.

(2) Conferința de la Bruxelles privind Somalia, care a avut loc la 16 septembrie 2013, a oferit baza pentru Pactul privind Somalia și a declanșat un mecanism destinat coordonării și asumării responsabilității somaleze prin intermediul grupului operativ „New Deal" pentru Somalia.

(3) Pe parcursul reuniunii internaționale găzduite în comun de Regatul Unit și Somalia, care a avut loc la Londra la 18 septembrie 2014, Guvernul Federal a conturat calea Ministerului Apărării în direcția dezvoltării armatei naționale somaleze până în 2019 și cerințele sale imediate.

(4) Ca urmare a revizuirii strategice din octombrie 2014, mandatul misiunii militare a UE ar trebui să fie prelungit până la 31 decembrie 2016.

(5) În conformitate cu articolul 5 din Protocolul nr. 22 privind poziția Danemarcei, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Danemarca nu participă la elaborarea și la punerea în aplicare a deciziilor și a acțiunilor Uniunii care au implicații în materie de apărare. Danemarca nu participă la punerea în aplicare a prezentei decizii și nu contribuie, prin urmare, la finanțarea acestei misiuni.

(6) Mandatul misiunii militare a UE ar trebui din nou prelungită cu un mandat adaptat,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Decizia 2010/96/PESC se modifică după cum urmează:

1. La articolul 1, alineatul (2) se înlocuiește cu următorul text:

„(2) Pentru a realiza obiectivele stabilite la alineatul (1), misiunea militară a UE este desfășurată în Somalia pentru a aborda atât consolidarea instituțională în sectorul apărării prin consiliere strategică, cât și sprijinul direct pentru armata națională somaleză prin instruire, consiliere și mentorat. În limitele mijloacelor și capabilităților sale, misiunea militară a UE este pregătită și pentru a oferi sprijin altor actori ai Uniunii în punerea în aplicare a mandatelor lor respective în domeniul securității și apărării în Somalia."

2. Articolul 3 se înlocuiește cu următorul text:

„Articolul 3

Desemnarea comandamentului misiunii

(1) Comandamentul misiunii este amplasat în Somalia, la aeroportul internațional Mogadiscio din Mogadiscio. Acesta îndeplinește atât funcțiile de comandament al operației, cât și pe cele de comandament al forței.

(2) Comandamentul misiunii include un birou de legătură și de sprijin la Nairobi și o celulă de sprijin la Bruxelles."

([1]) Decizia 2010/96/PESC a Consiliului din 15 februarie 2010 privind o misiune militară a Uniunii Europene pentru a contribui la instruirea forțelor de securitate somaleze (JO L 44, 19.2.2010, p. 16).

3. La articolul 7, alineatul (4) se înlocuiește cu următorul text:

„(4) În limitele mijloacelor și capabilităților sale, misiunea militară a UE acționează în strânsă cooperare cu alți actori internaționali în regiune, în special Organizația Națiunilor Unite și AMISOM, în conformitate cu cerințele convenite ale Guvernului federal al Somaliei."

4. La articolul 10 se adaugă următorul alineat:

„(5) Valoarea de referință financiară pentru costurile comune ale misiunii militare a UE pentru perioada cuprinsă între 1 aprilie 2015 și 31 decembrie 2016 este de 17 507 399 EUR. Procentajul acestei valori de referință menționate la articolul 25 alineatul (1) din ATHENA este de 30 %, iar procentajul pentru angajament menționat la articolul 32 alineatul (3) din ATHENA este de 90 %."

5. Se introduce următorul articol:

„Articolul 10b

Celula de proiecte

(1) Misiunea militară a UE dispune de o celulă de proiecte pentru identificarea și punerea în aplicare a proiectelor care urmează să fie finanțate de statele membre sau statele terțe și care sunt coerente cu obiectivele misiunii și contribuie la îndeplinirea mandatului.

(2) Sub rezerva alineatului (3), comandantul misiunii UE este autorizat să recurgă la contribuții financiare din partea statelor membre sau a statelor terțe pentru a pune în aplicare proiecte identificate drept completare a altor acțiuni ale misiunii militare a UE într-un mod coerent. Într-un astfel de caz, comandantul misiunii UE încheie un acord cu statele respective, care vizează în special procedurile specifice pentru soluționarea eventualelor plângeri formulate de părți terțe cu privire la prejudicii suferite în urma acțiunilor sau omisiunilor comandantului misiunii UE în utilizarea fondurilor furnizate de către statele respective.

În niciun caz statele contribuitoare nu pot angaja răspunderea Uniunii sau a ÎR în urma acțiunilor sau omisiunilor comandantului misiunii UE în utilizarea fondurilor furnizate de către statele respective.

(3) COPS își dă acordul cu privire la acceptarea unei contribuții financiare din partea statelor terțe în beneficiul celulei de proiecte."

6. Articolul 11 se modifică după cum urmează:

(a) la alineatul (1), cuvintele introductive se înlocuiesc cu „ÎR este autorizat să comunice statelor terțe asociate prezentei decizii, după caz și în conformitate cu nevoile misiunii, informații UE clasificate generate în scopul misiunii, în conformitate cu Decizia 2013/488/UE a Consiliului (*):

(*) Decizia 2013/488/UE a Consiliului din 23 septembrie 2013 privind normele de securitate pentru protecția informațiilor UE clasificate (JO L 274, 15.10.2013, p. 1).";

(b) la alineatele (2) și (3), cuvintele „Decizia 2011/292/UE" se înlocuiesc cu „Decizia 2013/488/UE".

7. La articolul 12, alineatele (2) și (3) se înlocuiesc cu următorul text:

„(2) Mandatul misiunii militare a UE se încheie la 31 decembrie 2016.

(3) Prezenta decizie se abrogă începând cu data închiderii comandamentului UE, a biroului de legătură și de sprijin din Nairobi și a celulei de sprijin din Bruxelles, în conformitate cu planurile aprobate pentru încetarea misiunii militare a UE și fără a aduce atingere procedurilor privind auditul și prezentarea situațiilor financiare ale misiunii militare a UE, prevăzute în ATHENA."

Articolul 2

Prezenta decizie intră în vigoare la data adoptării.

Se aplică de la 1 aprilie 2015.

Adoptată la Bruxelles, 16 martie 2015.

Pentru Consiliu

Președintele

F. MOGHERINI

DECIZIA (PESC) 2015/442 A CONSILIULUI

din 16 martie 2015

privind lansarea Misiunii de consiliere militară PSAC a Uniunii Europene în Republica Centrafricană (EUMAM RCA) și de modificare a Deciziei (PESC) 2015/78

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind Uniunea Europeană, în special articolul 42 alineatul (4) și articolul 43 alineatul (2),

având în vedere Decizia (PESC) 2015/78 a Consiliului din 19 ianuarie 2015 privind o misiune de consiliere militară PSAC a Uniunii Europene în Republica Centrafricană (EUMAM RCA) ([1]), în special articolul 4,

având în vedere propunerea Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate,

întrucât:

(1) La 19 ianuarie 2015, Consiliul a adoptat Decizia (PESC) 2015/78.

(2) La 9 februarie 2015, Consiliul a aprobat regulile de angajare pentru EUMAM RCA.

(3) La 6 martie 2015, Consiliul a aprobat planul de misiune pentru EUMAM RCA.

(4) La 11 martie 2015, Comitetul politic și de securitate a primit favorabil scrisoarea comandantului misiunii referitoare la recomandarea de a lansa EUMAM RCA, precum și calendarul preconizat pentru declararea capacității operaționale inițiale a EUMAM RCA.

(5) EUMAM RCA ar trebui lansată la 16 martie 2015.

(6) În conformitate cu articolul 5 din Protocolul nr. 22 privind poziția Danemarcei, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Danemarca nu participă la elaborarea și la punerea în aplicare a deciziilor și acțiunilor Uniunii care au implicații în materie de apărare. Prin urmare, Danemarca nu participă la punerea în aplicare a prezentei decizii și, ca atare, nu contribuie la finanțarea prezentei misiuni,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Misiunea de consiliere militară PSAC a Uniunii Europene în Republica Centrafricană (EUMAM RCA) se lansează la 16 martie 2015.

Articolul 2

Comandantul misiunii UE EUMAM RCA este autorizat să înceapă imediat executarea misiunii.

Articolul 3

La articolul 4 din decizia (PESC) 2015/78, alineatul (2) se înlocuiește cu următorul text:

„(2) EUMAM RCA se lansează printr-o decizie a Consiliului la data recomandată de comandantul misiunii, în urma aprobării planului misiunii și, dacă este necesar, a unor reguli de angajare suplimentare.”

([1]) JO L 13, 20.1.2015, p. 8.

Articolul 4

Prezenta decizie intră în vigoare la data adoptării.

Adoptată la Bruxelles, 16 martie 2015.

Pentru Consiliu
Președintele
F. MOGHERINI

DECIZIA (UE, Euratom) 2015/443 A COMISIEI

din 13 martie 2015

privind securitatea în cadrul Comisiei

COMISIA EUROPEANĂ,

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

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

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

întrucât:

(1) Obiectivul de securitate în cadrul Comisiei constă în a permite Comisiei să își desfășoare activitatea într-un mediu de siguranță și securitate prin stabilirea unei abordări coerente și integrate cu privire la securitatea sa, asigurând niveluri adecvate de protecție a persoanelor, activelor și informațiilor, proporțional cu riscurile identificate, precum și obținerea, în timp util, a unor rezultate eficiente în materie de securitate.

(2) Comisia, la fel ca și alte organisme internaționale, se confruntă cu amenințări și provocări importante în domeniul securității, în special în ceea ce privește terorismul, atacurile cibernetice și spionajul politic și comercial.

(3) Comisia Europeană a lansat, împreună cu guvernele Belgiei, Luxemburgului și Italiei ([1]), instrumente privind aspectele legate de securitate pentru principalele sale locații. Aceste instrumente confirmă faptul că Comisia este responsabilă pentru securitatea sa.

(4) Pentru a asigura securitatea persoanelor, a activelor și a informațiilor, Comisia poate fi nevoită să ia măsuri în domenii protejate prin drepturile fundamentale astfel cum sunt consacrate în Carta drepturilor fundamentale și în Convenția europeană a drepturilor omului și astfel cum sunt recunoscute de Curtea de Justiție a Uniunii Europene.

(5) Prin urmare, orice astfel de măsură ar trebui să fie justificată de importanța interesului pe care este menită să îl protejeze, să fie proporțională și să asigure respectarea deplină a drepturilor fundamentale, în special a dreptului la viață privată și la protecția datelor.

(6) În cadrul unui sistem care sprijină supremația legii și respectarea drepturilor fundamentale, Comisia trebuie să depună eforturi pentru asigurarea unui nivel corespunzător de securitate pentru personalul, activele și informațiile sale, care să îi permită să își desfășoare activitățile, fără limitarea drepturilor fundamentale mai mult decât este strict necesar.

(7) Securitatea în cadrul Comisiei se bazează pe principiile legalității, transparenței, proporționalității și responsabilității.

(8) Membrii personalului autorizat să ia măsuri de securitate nu ar trebui să fie dezavantajați sub nicio formă ca urmare a desfășurării acțiunilor, cu excepția cazului în care au acționat în afara domeniului de aplicare al mandatului lor sau au încălcat legislația și, prin urmare, în acest sens, prezenta decizie trebuie considerată drept regulament de serviciu în sensul Statutului funcționarilor.

(9) Comisia ar trebui să ia inițiativele corespunzătoare pentru a-și încuraja și consolida propria cultură a securității, prin asigurarea unei implementări mai eficiente a securității, îmbunătățirea guvernanței în materie de siguranță, consolidarea în continuare a rețelelor și a cooperării cu autoritățile relevante la nivel internațional, european și național, și prin îmbunătățirea activităților de monitorizare și control privind punerea în aplicare a măsurilor de securitate.

(10) Înființarea Serviciului European de Acțiune Externă (SEAE), ca organ autonom din punct de vedere funcțional al Uniunii, a avut un impact semnificativ asupra intereselor în materie de securitate ale Comisiei și acest lucru impune, prin urmare, ca SEAE și Comisia să stabilească norme și proceduri de cooperare în ceea ce privește siguranța și securitatea, în special în ceea ce privește îndeplinirea de către Comisie a responsabilităților privind obligația de diligență față de personalul Comisiei din delegațiile Uniunii.

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

(11) Politica de securitate a Comisiei ar trebui să fie pusă în aplicare într-un mod care să fie coerent cu alte procese și proceduri interne care pot implica elemente de securitate. Printre acestea se numără, în special, gestionarea continuității activității care are drept scop menținerea funcțiilor critice ale Comisiei în cazul unei întreruperi operaționale, precum și sistemul general de alertă rapidă ARGUS, pentru coordonarea crizelor multisectoriale.

(12) În pofida măsurilor care sunt deja în vigoare la data adoptării prezentei decizii și au fost notificate Autorității Europene pentru Protecția Datelor ([1]), orice măsură adoptată în temeiul prezentei decizii care implică prelucrarea datelor cu caracter personal trebuie să facă obiectul unor norme de punere în aplicare în conformitate cu articolul 21, care stabilește garanții corespunzătoare pentru persoanele vizate.

(13) Prin urmare, este necesar ca Comisia să revizuiască, să actualizeze și să consolideze baza de reglementare existentă privind securitatea din cadrul Comisiei.

(14) Prin urmare, Decizia (94) 2129 a Comisiei ([2]) ar trebui abrogată.

ADOPTĂ PREZENTA DECIZIE:

CAPITOLUL 1

DISPOZIȚII GENERALE

Articolul 1

Definiții

În sensul prezentei decizii, se aplică următoarele definiții:

1. „active” înseamnă toate bunurile mobile și imobile și proprietățile deținute de Comisie;

2. „departament al Comisiei” înseamnă fie o direcție generală sau un serviciu al Comisiei, fie un cabinet al unui membru al Comisiei;

3. „sistem informatic și de comunicații” sau „SIC” înseamnă orice sistem care permite manipularea informațiilor în format electronic, inclusiv toate activele necesare funcționării sale, precum și infrastructura, organizarea, personalul și resursele informaționale;

4. „control al riscurilor” înseamnă orice măsură de securitate despre care se poate presupune, în mod rezonabil, că va controla în mod efectiv un risc la adresa securității prin prevenire, atenuare, evitare sau transfer;

5. „situație de criză” înseamnă o situație, un eveniment, un incident sau o stare de urgență (sau o succesiune sau o combinație a acestora) care reprezintă o amenințare serioasă sau imediată la adresa securității în cadrul Comisiei, indiferent de originea lor;

6. „date” înseamnă informații într-o formă care permite ca acestea să fie comunicate, înregistrate sau prelucrate;

7. „membrul Comisiei responsabil de securitate” înseamnă un membru al Comisiei în subordinea căruia se află Direcția Generală Resurse Umane și Securitate;

8. „date cu caracter personal” înseamnă datele cu caracter personal astfel cum sunt definite la articolul 2 litera (a) din Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului ([3]);

9. „incinte” înseamnă orice bunuri imobile sau bunuri asimilate acestora și aflate în proprietatea Comisiei;

10. „prevenirea riscurilor” înseamnă măsurile de securitate despre care se poate presupune, în mod rezonabil, că vor împiedica, întârzia sau pune capăt unui risc care amenință securitatea.

11. „risc la adresa securității” înseamnă combinația dintre nivelul de amenințare, nivelul de vulnerabilitate și impactul posibil al unui eveniment;

12. „securitate în cadrul Comisiei” înseamnă securitatea persoanelor, a activelor și a informațiilor în cadrul Comisiei și, în special, integritatea fizică a persoanelor și a activelor, integritatea, confidențialitatea și disponibilitatea informațiilor și a sistemelor de comunicații și informații, precum și desfășurarea neobstrucționată a activităților Comisiei;

([1]) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

([2]) Decizia C(94) 2129 a Comisiei din 8 septembrie 1994 privind sarcinile Oficiului de securitate.

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

13. „măsură de securitate" înseamnă orice măsură luată în conformitate cu prezenta decizie în scopul controlării riscurilor la adresa securității;

14. „Statutul funcționarilor" înseamnă Statutul funcționarilor Uniunii Europene, prevăzut de Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului ([1]) și de actele de modificare a acestuia;

15. „amenințare la adresa securității" înseamnă o împrejurare sau un agent despre care se poate presupune, în mod rezonabil, că va avea efecte negative asupra securității în cazul în care nu se iau măsuri de răspuns și control;

16. „amenințare imediată la adresa securității" înseamnă o amenințare la adresa securității care apare fără vreo avertizare în acest sens sau în contextul unei avertizări cu foarte puțin timp înainte de apariție, și

17. „amenințare majoră la adresa securității" înseamnă o amenințare la adresa securității despre care se poate presupune, în mod rezonabil, că va duce la pierderea de vieți omenești, vătămări sau lezări grave, daune semnificative aduse proprietății, compromiterea unor informații extrem de sensibile, perturbarea sistemelor informatice sau a capacităților operaționale esențiale ale Comisiei;

18. „vulnerabilitate" înseamnă un punct slab de orice natură despre care se poate presupune, în mod rezonabil, că va avea efecte negative asupra securității în cadrul Comisiei în cazul în care este expus uneia sau mai multor amenințări.

Articolul 2

Obiectul

(1) Prezenta decizie stabilește obiectivele, principiile de bază, organizarea și responsabilitățile în materie de securitate în cadrul Comisiei.

(2) Prezenta decizie se aplică tuturor departamentelor Comisiei și în toate incintele acesteia. Personalul Comisiei din delegațiile Uniunii se va supune normelor de securitate pentru Serviciul European de Acțiune Externă ([2]).

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

(4) Dispozițiile prezentei decizii se aplică fără a aduce atingere Deciziei 2002/47/CE, CECO, Euratom a Comisiei ([3]) și Deciziei 2004/563/CE, Euratom a Comisiei ([4]), deciziilor C(2006) 1623 ([5]) și C(2006) 3602 ([6]) ale Comisiei.

CAPITOLUL 2

PRINCIPII

Articolul 3

Principii de securitate în cadrul Comisiei

(1) Punerea în aplicare a prezentei decizii de către Comisie se desfășoară în conformitate cu tratatele și îndeosebi cu Carta drepturilor fundamentale și Protocolul nr. 7 privind privilegiile și imunitățile Uniunii Europene, cu instrumentele la care se face referire în considerentul 2, cu toate normele de drept intern aplicabile, precum și cu condițiile prevăzute în prezenta decizie. În cazul în care este necesar, se va emite o notificare de securitate în sensul articolului 21 alineatul (2) care să ofere orientări în acest sens.

(2) Securitatea în cadrul Comisiei se bazează pe principiile legalității, transparenței, proporționalității și responsabilității.

(3) Principiul legalității se referă la necesitatea de a menține strict în cadrul juridic punerea în aplicare a prezentei decizii și de a respecta cerințele legale.

([1]) Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului din 29 februarie 1968 de stabilire a Statutului funcționarilor Comunităților Europene și a Regimului aplicabil celorlalți agenți ai Comunităților Europene și de instituire de măsuri speciale aplicabile temporar funcționarilor Comisiei (regim aplicabil altor categorii de angajați) (JO L 56, 4.3.1968, p. 1).

([2]) 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 (2013/C 190/01) (JO C 190, 29.6.2013, p. 1).

([3]) Decizia 2002/47/CE, CECO, Euratom a Comisiei din 23 ianuarie 2002 de modificare a regulamentului de procedură (JO L 21, 24.1.2002, p. 23) însoțită de anexa referitoare la dispozițiile privind gestionarea documentelor.

([4]) Decizia 2004/563/CE a Comisiei, Euratom din 7 iulie 2004 de modificare a regulamentului său de procedură (JO L 251, 27.7.2004, p. 9) însoțită de anexa referitoare la dispozițiile privind documentele electronice și digitalizate.

([5]) C(2006) 1623 din 21 aprilie 2006 de stabilire a unei politici armonizate în materie de sănătate și securitate la locul de muncă pentru toți membrii personalului Comisiei Europene.

([6]) C(2006) 3602 din 16 august 2006 privind securitatea sistemelor informaționale utilizate de Comisia Europeană.

(4) Toate măsurile de securitate sunt luate într-un climat de deschidere, cu excepția cazului în care se poate presupune, în mod rezonabil, că acest lucru va compromite efectul măsurii în cauză. Destinatarii unei măsuri de securitate sunt informați în prealabil cu privire la motivele și impactul măsurii, cu excepția cazului în care se poate presupune, în mod rezonabil, că efectul măsurii va fi afectat de transmiterea acestor informații. În acest caz, informațiile respective sunt transmise destinatarului măsurii de securitate după încetarea riscului care amenință efectul măsurii de securitate.

(5) Departamentele Comisiei se asigură că aspectele de securitate sunt luate în considerare de la începutul elaborării și punerii în aplicare a politicilor, deciziilor, programelor, proiectelor și activităților Comisiei pentru care acestea sunt responsabile. Pentru a proceda astfel, vor fi implicați, încă din primele stadii ale preparativelor, Direcția Generală Resurse Umane și Securitate, în ceea ce privește aspectele generale, și responsabilul principal cu securitatea informațiilor Comisiei, în ceea ce privește sistemele IT.

(6) Comisia urmărește, după caz, să coopereze cu autoritățile competente ale statului-gazdă, ale altor state membre și ale altor instituții, agenții sau organe ale UE, în cazul în care acest lucru este fezabil, ținând seama de măsurile luate sau planificate de autoritățile respective pentru a aborda riscurile de securitate în cauză.

Articolul 4

Obligația de conformitate

(1) Conformitatea cu dispozițiile prezentei decizii și normele sale de punere în aplicare, precum și cu măsurile și instrucțiunile de securitate furnizate de personalul autorizat este obligatorie.

(2) Nerespectarea normelor de securitate poate atrage răspunderea disciplinară, în conformitate cu tratatele, Statutul funcționarilor, sancțiunile contractuale și/sau acțiunile în justiție prevăzute de actele cu putere de lege și dispozițiile administrative naționale.

CAPITOLUL 3

ASIGURAREA SECURITĂȚII

Articolul 5

Personalul autorizat

(1) Numai personalului autorizat pe baza unui mandat nominativ, conferit de către directorul general al DG Resurse Umane și Securitate, având în vedere sarcinile care le revin, i se poate acorda competența de a adopta una sau mai multe dintre următoarele măsuri:

1. portul armelor de mână;

2. desfășurarea unor anchete de securitate, astfel cum se menționează la articolul 13;

3. adoptarea unor măsuri de securitate, astfel cum se menționează la articolul 12, conform mandatului.

(2) Mandatele menționate la alineatul (1) se conferă pe o durată care nu depășește perioada în care persoana în cauză deține postul sau funcția pentru care i s-a acordat mandatul respectiv. Acestea se acordă în conformitate cu dispozițiile aplicabile prevăzute la articolul 3 alineatul (1).

(3) În ceea ce privește personalul autorizat, prezenta decizie constituie un regulament de serviciu în sensul articolului 21 din Statutul funcționarilor.

Articolul 6

Dispoziții generale privind măsurile de securitate

(1) Atunci când ia măsuri de securitate, Comisia se asigură, în special, în măsura în care acest lucru este posibil în mod rezonabil, că:

(a) solicită sprijin sau asistență numai din partea statului implicat, cu condiția ca acesta să fie un stat membru al Uniunii Europene sau, în caz contrar, să fie parte la Convenția europeană a drepturilor omului sau să garanteze drepturi care să fie cel puțin echivalente cu drepturile garantate prin această convenție;

(b) transferă informații cu privire la o persoană numai către acei destinatari, alții decât instituțiile și organele comunitare, care nu se supun legislației naționale adoptate în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului ([1]), în conformitate cu articolul 9 din Regulamentul (CE) nr. 45/2001;

([1]) Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (JO L 281, 23.11.1995, p. 31).

(c) în cazul în care o persoană reprezintă o amenințare la adresa securității, orice măsură de securitate trebuie să fie îndreptată împotriva persoanei respective, căreia i se poate impune obligația de a suporta costurile aferente. Aceste măsuri de securitate pot fi îndreptate împotriva altor persoane numai în cazul în care este necesar să se țină sub control o amenințare imediată sau importantă la adresa securității și dacă sunt îndeplinite următoarele condiții:

(a) nu este posibil să se ia măsurile preconizate împotriva persoanei care reprezintă o amenințare la adresa securității sau aceste măsuri riscă să nu fie eficace;

(b) Comisia nu poate controla amenințarea la adresa securității prin propriile sale acțiuni sau nu pot face acest lucru în timp util;

(c) măsura nu constituie un pericol disproporționat pentru alte persoane și drepturile lor.

(2) Direcția Securitate din cadrul Direcției Generale Resurse Umane și Securitate elaborează o prezentare generală a măsurilor de securitate care pot presupune emiterea unui ordin judecătoresc, în conformitate cu actele cu putere de lege și normele administrative ale statelor membre în care se află incinte ale Comisiei.

(3) Direcția de Securitate din cadrul Direcției Generale Resurse Umane și Securitate poate recurge la un contractant care să efectueze, sub conducerea și supravegherea Direcției de Securitate, sarcini legate de asigurarea securității.

Articolul 7

Măsuri de securitate cu privire la persoane

(1) Se asigură un nivel adecvat de protecție a persoanelor aflate în incintele Comisiei, ținându-se seama de cerințele de securitate și siguranță.

(2) În cazul existenței unor riscuri majore de securitate, Direcția Generală Resurse Umane și Securitate oferă protecție personală membrilor Comisiei sau altor agenți în situația în care o evaluare a riscului a evidențiat că o astfel de protecție este necesară pentru a asigura siguranța și securitatea acestora.

(3) În cazul unor riscuri majore de securitate, Comisia poate dispune evacuarea incintelor sale.

(4) Victimele accidentelor sau atacurilor care au avut loc în incintele Comisiei beneficiază de asistență.

(5) Pentru a preveni și a controla riscurile la adresa securității, membrii personalului autorizat pot efectua verificări ale antecedentelor persoanelor cărora li se aplică prezenta decizie, pentru a stabili dacă faptul că acestor persoane li se permite accesul în incintele sau la informațiile Comisiei prezintă o amenințare la adresa securității. În acest scop și în conformitate cu Regulamentul (CE) nr. 45/2001 și dispozițiile la care se face referire în articolul 3 alineatul (1), membrii personalului autorizat pot:

(a) utiliza orice sursă de informare de care dispune Comisia, ținând seama de fiabilitatea sursei de informare;

(b) avea acces la dosarul de personal sau la datele personale de care dispune Comisia cu privire la persoanele pe care le-a angajat sau pe care intenționează să le angajeze sau referitoare la membrii personalului contractanților, atunci când acest lucru se justifică în mod corespunzător.

Articolul 8

Măsuri de securitate cu privire la securitatea fizică și activele fixe

(1) Securitatea activelor trebuie să fie asigurată prin aplicarea unor măsuri adecvate de protecție fizică și tehnică și a procedurilor corespunzătoare, denumite în continuare „securitate fizică”, creându-se un sistem organizat pe mai multe niveluri.

(2) În temeiul prezentului articol se pot adopta măsuri în vederea protejării persoanelor sau a informațiilor la nivelul Comisiei, precum și pentru protejarea activelor.

(3) Obiectivele securității fizice sunt următoarele:

— prevenirea actelor de violență îndreptate împotriva membrilor Comisiei sau a persoanelor care intră sub incidența prezentei decizii;

— prevenirea spionajului și a interceptării informațiilor sensibile sau clasificate;

— prevenirea furturilor, a actelor de vandalism, sabotaj și a altor acțiuni violente care vizează vătămarea sau distrugerea clădirilor și activelor Comisiei;

— să permită efectuarea unor investigații și anchete cu privire la incidentele de securitate, inclusiv prin controale vizând fișierele de control al intrărilor și ieșirilor, monitorizarea prin intermediul televiziunii cu circuit închis (CCTV), înregistrările convorbirilor telefonice și ale unor date similare, astfel cum se menționează la articolul 22 alineatul (2) de mai jos și alte surse de informații.

(4) Securitatea fizică trebuie să includă:

— o politică de acces care se aplică tuturor persoanelor sau vehiculelor care solicită accesul la incintele Comisiei, inclusiv la locurile de parcare;

— un sistem de control al accesului care să cuprindă agenți de securitate, echipament și măsuri tehnice, sisteme de informații sau o combinație a tuturor acestor elemente.

(5) Pentru a asigura securitatea fizică, pot fi întreprinse următoarele acțiuni:

— înregistrarea persoanelor, a vehiculelor, a bunurilor și a echipamentelor care intră sau ies din incintele Comisiei;

— efectuarea de controale de identitate în incintele Comisiei;

— efectuarea de controale ale vehiculelor, bunurilor și echipamentelor cu ajutorul unor mijloace vizuale sau tehnice;

— împiedicarea accesului persoanelor, vehiculelor și bunurilor neautorizate în incintele Comisiei.

Articolul 9

Măsuri de securitate cu privire la informații

(1) Securitatea informațiilor se referă la toate informațiile gestionate de Comisie.

(2) Securitatea informațiilor, indiferent de forma acestora, trebuie să se caracterizeze printr-un echilibru între transparență, proporționalitate, responsabilitate și eficiență, pe de o parte, și necesitatea de a proteja informațiile împotriva accesului, a utilizării, a divulgării, a modificării sau a distrugerii neautorizate, pe de altă parte.

(3) Securitatea informațiilor are ca scop protejarea confidențialității, a integrității și a disponibilității acestora.

(4) Prin urmare, trebuie să se utilizeze proceduri de management al riscurilor pentru a clasifica activele informaționale și a se elabora măsuri, proceduri și standarde de securitate proporționale,, inclusiv măsuri de atenuare.

(5) Aceste principii generale care stau la baza securității informațiilor se aplică în special în ceea ce privește:

(a) „informațiile clasificate ale Uniunii Europene" (denumite în continuare IUEC), și anume orice informații sau materiale desemnate ca atare printr-o clasificare în materie de securitate a UE a căror divulgare neautorizată ar putea cauza prejudicii de diferite grade intereselor Uniunii Europene sau ale unora sau mai multor state membre;

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

(6) Informațiile sensibile neclasificate fac obiectul normelor privind operațiunile de manipulare și păstrare a acestora. Aceste informații pot fi transmise numai acelor persoane cărora li se aplică principiul „necesității de a cunoaște". Atunci când se consideră că acest lucru este necesar pentru protecția efectivă a caracterului lor confidențial, aceste informații trebuie să fie identificate printr-un marcaj de securitate și prin instrucțiuni de manipulare corespunzătoare, aprobate de directorul general al DG Resurse Umane și Securitate. Atunci când sunt gestionate sau păstrate în sisteme informatice și de comunicații, aceste informații trebuie să fie protejate, de asemenea, în conformitate cu Decizia (2006) 3602 a Comisiei, cu normele de aplicare a acesteia și cu standardele corespunzătoare.

(7) Orice persoană responsabilă de compromiterea sau pierderea IUEC sau a unor informații sensibile neclasificate, care sunt identificate ca atare în normele privind manipularea și păstrarea acestora, este pasibilă de măsuri disciplinare, în conformitate cu Statutul funcționarilor. Aceste măsuri disciplinare nu aduc atingere niciunei alte proceduri contencioase sau penale puse în aplicare de către autoritățile naționale competente ale statelor membre în conformitate cu actele cu putere de lege și normele lor administrative și nici căilor de atac contractuale.

[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).

Articolul 10

Măsuri de securitate cu privire la sistemele informatice și de comunicații

(1) Toate sistemele informatice și de comunicații („SIC") utilizate de Comisie sunt conforme cu politica de securitate privind sistemele de informații ale Comisiei, prevăzută în Decizia C (2006) 3602 a Comisiei, în normele de aplicare a acesteia și în standardele de securitate corespunzătoare.

(2) Serviciile Comisiei care dețin, gestionează sau utilizează SIC permit accesul instituțiilor, al agențiilor, al organelor Uniunii sau al altor organizații la aceste sisteme, numai cu condiția ca aceste instituții, agenții, organe ale Uniunii sau alte organizații să fie în măsură să ofere o asigurare rezonabilă că sistemele lor informatice sunt protejate la un nivel echivalent cu cel al politicii Comisiei privind securitatea sistemelor informatice, prevăzută în Decizia C (2006) 3602 a Comisiei, în normele de aplicare a acesteia și în standardele de securitate corespunzătoare. Comisia monitorizează respectarea acestor cerințe, și, în caz de neconformitate gravă sau neconformare persistentă, are dreptul să interzică accesul.

Articolul 11

Analiza criminalistică în materie de securitate cibernetică

Direcției Generale Resurse Umane și Securitate îi revine în special responsabilitatea efectuării de analize criminalistice tehnice în cooperare cu departamentele competente ale Comisiei, în sprijinul anchetelor de securitate prevăzute la articolul 13, referitoare la contrainformații, scurgerea de date, atacuri cibernetice și securitatea sistemelor informatice.

Articolul 12

Măsuri de securitate cu privire la persoane și obiecte

(1) Pentru a asigura securitatea în cadrul Comisiei și pentru a preveni și a controla riscurile, membrii personalului autorizat în temeiul articolului 5 pot lua, în conformitate cu principiile prevăzute la articolul 3, printre altele, una sau mai multe dintre următoarele măsuri de securitate:

(a) securizarea spațiilor și a probelor, inclusiv prin intermediul fișierelor-jurnal de control al accesului și ieșirilor și al imaginilor CCTV în cazul unor incidente sau comportamente care pot duce la proceduri administrative, disciplinare, civile sau penale;

(b) un număr limitat de măsuri vizând persoanele care prezintă o amenințare la adresa securității, inclusiv să ordone persoanelor să părăsească incintele Comisiei, să însoțească persoanele atunci când părăsesc incintele Comisiei, să interzică persoanelor accesul în incintele Comisiei pe o perioadă de timp stabilită în conformitate cu criteriile care urmează a fi definite în normele de punere în aplicare;

(c) un număr limitat de măsuri referitoare la obiecte care prezintă o amenințare la adresa securității, inclusiv eliminarea, confiscarea și distrugerea obiectelor;

(d) efectuarea de percheziții în incintele Comisiei, inclusiv în birourile situate în aceste incinte;

(e) efectuarea de controale având ca obiect sistemele informatice și de comunicare și echipamentele, datele privind traficul telefonic și de telecomunicații, fișierele-jurnal, conturile de utilizator etc.;

(f) alte măsuri de securitate specifice cu efect similar, în scopul de a preveni sau de a controla riscurile la adresa securității, în special în contextul drepturilor de care beneficiază Comisia în calitate de proprietar sau angajator, în conformitate cu legile naționale aplicabile.

(2) În situații excepționale, membrii personalului din Direcția Securitate din cadrul Direcției Generale Resurse Umane și Securitate, autorizați în conformitate cu articolul 5, pot lua orice măsuri urgente necesare, în strictă conformitate cu principiile stabilite la articolul 3. Cât mai curând posibil după luarea măsurilor respective, aceștia îl informează în acest sens pe directorul Direcției Securitate, care va solicita un mandat corespunzător din partea directorului general al Direcției Generale Resurse Umane și Securitate, confirmând măsurile adoptate și autorizând luarea oricăror altor acțiuni necesare, și cooperează, după caz, cu autoritățile naționale competente.

(3) Măsurile de securitate adoptate în temeiul prezentului articol trebuie consemnate în momentul adoptării sau, în cazul unui risc imediat sau al unei situații de criză, într-un termen rezonabil după adoptarea lor. În acest din urmă caz, documentația trebuie să includă, de asemenea, elementele care au stat la baza evaluării referitoare la existența unui risc imediat sau a unei situații de criză. Documentația poate fi concisă, dar ar trebui să fie întocmită într-un mod care să îi permită persoanei care face obiectul măsurii să își exercite dreptul la apărare și la protecția datelor cu caracter personal, în conformitate cu Regulamentul (CE) nr. 45/2001, și care să permită efectuarea unui control cu privire la legalitatea măsurii. Nicio informație cu privire la măsurile de securitate specifice vizând un membru al personalului nu figurează în dosarul personal al persoanei în cauză.

(4) Atunci când ia măsuri de securitate în temeiul literei (b), Comisia se asigură, de asemenea, că persoana în cauză are posibilitatea de a contacta un avocat sau o persoană de încredere și că i se aduce la cunoștință faptul că are dreptul să se adreseze Autorității Europene pentru Protecția Datelor.

Articolul 13

Anchetele

(1) Fără a aduce atingere articolului 86 și anexei IX din Statutul funcționarilor sau oricăror acorduri speciale încheiate între Comisie și SEAE, precum acordul special privind obligația de diligență față de personalul Comisiei care își desfășoară activitatea în delegațiile Uniunii, încheiat la 28 mai 2014 între Direcția Generală Resurse Umane și Securitate a Comisiei Europene și Serviciul European de Acțiune Externă, pot fi efectuate anchete privind securitatea:

(a) în cazul unor incidente care afectează securitatea la nivelul Comisiei, inclusiv în cazul unor presupuse infracțiuni;

(b) în cazul unor eventuale scurgeri de informații, al utilizării necorespunzătoare sau al compromiterii informațiilor sensibile neclasificate, a informațiilor UE clasificate (IUEC) sau a datelor clasificate ale Euratom;

(c) în contextul activităților de contrainformații și de contracarare a terorismului;

(d) în cazul unor incidente cibernetice grave.

(2) Decizia de a desfășura o anchetă privind securitatea este luată de către directorul general al DG Resurse Umane și Securitate care este, de asemenea, destinatarul raportului de anchetă.

(3) Anchetele privind securitatea sunt efectuate numai de către membrii specializați ai personalului din cadrul Direcției Generale Resurse Umane și Securitate, autorizați în mod corespunzător în conformitate cu articolul 5.

(4) Personalul autorizat își exercită în mod independent atribuțiile cu privire la anchetele privind securitatea, astfel cum se specifică în mandat, și deține competențele enumerate la articolul 12.

(5) Membrii personalului autorizat care au competența de a desfășura anchete privind securitatea pot colecta informații din toate sursele disponibile referitoare la orice contravenții sau infracțiuni comise în incintele Comisiei sau în care sunt implicate persoanele menționate la articolul 2 alineatul (3), fie în calitate de victimă, fie ca autori ai unor astfel de infracțiuni.

(6) Direcția Generală Resurse Umane și Securitate informează autoritățile competente din statul membru gazdă sau din oricare alt stat membru în cauză, dacă este cazul și, în special, dacă anchetele au oferit indicii cu privire la faptul că s-ar fi comis o infracțiune. În acest context, Direcția Generală Resurse Umane și Securitate poate, în cazul în care este oportun sau necesar, să ofere sprijin autorităților din statul membru gazdă sau din oricare alt stat membru implicat.

(7) În cazul incidentelor cibernetice grave, Direcția Generală Informatică colaborează îndeaproape cu Direcția Generală Resurse Umane și Securitate pentru acordarea de sprijin privind toate aspectele tehnice. Direcția Generală Resurse Umane și Securitate decide, după consultarea Direcției Generale Informatică, să informeze, atunci când este oportun, autoritățile competente din țara gazdă sau din oricare alt stat membru implicat. Serviciile de coordonare a incidentelor din cadrul Centrului de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile europene („CERT-UE") sunt utilizate pentru acordarea de sprijin altor instituții și agenții ale UE care pot fi afectate.

(8) Anchetele privind securitatea sunt documentate.

Articolul 14

Delimitarea competențelor în ceea ce privește anchetele privind securitatea și alte tipuri de investigații

(1) În cazul în care Direcția de Securitate din cadrul Direcției Generale Resurse Umane și Securitate efectuează anchete privind securitatea, astfel cum se prevede la articolul 13, și dacă aceste anchete intră în sfera de competență a Oficiului European de Luptă Antifraudă (OLAF) sau a Oficiului de investigație și de disciplină al Comisiei (IDOC), aceasta ia imediat legătura cu organismele respective, cu scopul, în special, de a nu compromite acțiunile ulterioare ale OLAF sau ale IDOC. După caz, Direcția de Securitate din cadrul Direcției Generale Resurse Umane și Securitate invită OLAF sau IDOC să participe la anchetă.

(2) Efectuarea anchetelor privind securitatea menționate la articolul 13 nu aduce atingere competențelor OLAF și IDOC, astfel cum sunt prevăzute în normele care reglementează aceste organisme. Direcției de Securitate din cadrul Direcției Generale Resurse Umane și Securitate i se poate solicita acordarea de asistență tehnică în cadrul anchetelor inițiate de OLAF sau de IDOC.

(3) Direcției Securitate din cadrul Direcției Generale Resurse Umane și Securitate i se poate solicita acordarea de asistență agenților OLAF atunci când intră în incintele Comisiei, în conformitate cu articolul 3 alineatul (5) și cu articolul 4 alineatul (4) din Regulamentul 883/2013 al Parlamentului European și al Consiliului ([1]), pentru a le facilita

([1]) Regulamentul (UE, Euratom) nr. 883/2013 al Parlamentului European și al Consiliului din 11 septembrie 2013 privind investigațiile efectuate de Oficiul European de Luptă Antifraudă (OLAF) și de abrogare a Regulamentului (CE) nr. 1073/1999 al Parlamentului European și al Consiliului și a Regulamentului (Euratom) nr. 1074/1999 al Consiliului (JO L 248, 18.9.2013, p. 1).

sarcinile. Direcția Securitate aduce aceste cereri de asistență la cunoștința Secretarului General și a directorului general al Direcției Generale Resurse Umane și Securitate sau, în cazul în care aceste anchete se desfășoară în spațiile Comisiei ocupate de membrii săi sau de către Secretarul General, a președintelui Comisiei Europene și a comisarului responsabil pentru resurse umane.

(4) Fără a aduce atingere articolului 22 litera (a) din Statutul funcționarilor, dacă un caz este susceptibil de a intra atât în competența Direcției Securitate din cadrul Direcției Generale Resurse Umane și Securitate, cât și în competența IDOC, în momentul în care aduce acest lucru la cunoștința directorului general al DG Resurse Umane, în conformitate cu articolul 13, Direcția Securitate examinează, în stadiul cel mai timpuriu posibil, dacă există motive care justifică sesizarea IDOC cu privire la această problemă. Se consideră că acest stadiu a fost atins atunci când o amenințare imediată la adresa securității a luat sfârșit. Directorul general al DG Resurse Umane și Securitate ia o decizie cu privire la această chestiune.

(5) În situația în care un caz un caz este susceptibil de a intra atât în competența Direcției Securitate din cadrul Direcției Generale Resurse Umane și Securitate, cât și în competența OLAF, Direcția Securitate aduce imediat acest lucru la cunoștința directorului general al DG Resurse Umane și Securitate și îl informează, în acest sens, în stadiul cel mai timpuriu posibil, pe directorul general al OLAF. Se consideră că acest stadiu a fost atins atunci când o amenințare imediată la adresa securității a luat sfârșit.

Articolul 15

Inspecții de securitate

(1) Direcția Generală Resurse Umane și Securitate efectuează inspecții de securitate pentru a verifica respectarea de către serviciile Comisiei și de către cetățeni a prezentei decizii și a normelor de aplicare a acesteia și pentru a formula recomandări atunci când consideră că acest lucru este necesar.

(2) Atunci când este cazul, Direcția Generală Resurse Umane și Securitate efectuează inspecții de securitate și vizite de monitorizare sau de evaluare a securității, pentru a verifica dacă securitatea personalului Comisiei, a bunurilor și a informațiilor care intră în sfera de responsabilitate a instituțiilor, a agențiilor sau a altor organisme ale Uniunii, a statelor membre, a țărilor terțe sau a organizațiilor internaționale sunt protejate în mod corespunzător, în conformitate cu norme, reglementări și standarde de securitate care sunt cel puțin echivalente cu cele ale Comisiei. Atunci când este oportun și în spiritul bunei cooperări între administrații, aceste inspecții de securitate includ, de asemenea, inspecțiile efectuate în contextul schimbului de informații clasificate cu alte instituții, organe și agenții ale Uniunii, cu statele membre, cu state terțe sau cu organizații internaționale.

(3) Prezentul articol se aplică, *mutatis mutandis*, personalului Comisiei din delegațiile Uniunii, fără a aduce atingere acordurilor speciale încheiate între Comisie și SEAE, precum acordul special privind obligația de diligență față de personalul Comisiei care își desfășoară activitatea în delegațiile Uniunii, încheiat la 28 mai 2014 între Direcția Generală Resurse Umane și Securitate a Comisiei Europene și Serviciul European de Acțiune Externă.

Articolul 16

Niveluri de alertă și gestionarea situațiilor de criză

(1) Direcția Generală Resurse Umane și Securitate este responsabilă atât pentru punerea în aplicare a unor măsuri adecvate pentru nivelurile de alertă, pentru a anticipa sau a răspunde amenințărilor și incidentelor care afectează securitatea în spațiile Comisiei, cât și pentru măsurile necesare pentru gestionarea situațiilor de criză.

(2) Măsurile corespunzătoare nivelurilor de alertă menționate la alineatul (1) sunt proporționale cu nivelul de amenințare la adresa securității. Nivelurile de alertă trebuie să fie definite în strânsă colaborare cu serviciile competente ale celorlalte instituții, agenții și organe ale Uniunii și ale statului membru sau statelor membre în care sunt situate sediile Comisiei.

(3) Direcția Generală Resurse Umane și Securitate este punctul de contact pentru nivelurile de alertă și gestionarea situațiilor de criză.

CAPITOLUL 4

ORGANIZARE

Articolul 17

Responsabilitățile generale ale serviciilor Comisiei

(1) Responsabilitățile Comisiei menționate în prezenta decizie sunt exercitate de Direcția Generală Resurse Umane și Securitate, sub autoritatea și responsabilitatea membrului Comisiei responsabil de securitate.

(2) Acordurile specifice în ceea ce privește securitatea cibernetică sunt definite în Decizia (2006) 3602.

(3) Responsabilitățile privind punerea în aplicare a prezentei decizii și normele de punere în aplicare a acesteia, precum și asigurarea respectării zilnice a acestora pot fi delegate altor departamente ale Comisiei, ori de câte ori asigurarea descentralizată a serviciilor de securitate oferă câștiguri importante în materie de eficiență, resurse sau timp, de exemplu datorită localizării geografice a serviciilor în cauză.

(4) În cazul în care se aplică alineatul (3), Direcția Generală Resurse Umane și Securitate și, după caz, directorul general al DG Informatică încheie acorduri cu anumite departamente din cadrul Comisiei, care stabilesc roluri și responsabilități clare privind punerea în aplicare și monitorizarea politicilor de securitate.

Articolul 18

Direcția Generală Resurse Umane și Securitate

(1) Direcției Generale Resurse Umane și Securitate îi revin, în special, următoarele responsabilități:

1. elaborarea politicii de securitate a Comisiei, a normelor de punere în aplicare și a notificărilor de securitate;
2. colectarea de informații în vederea evaluării amenințărilor și a riscurilor la adresa securității și cu privire la toate problemele care pot afecta securitatea în spațiile Comisiei;
3. furnizarea de supraveghere electronică și protecție în toate spațiile de lucru ale Comisiei, ținând seama în mod corespunzător de evaluările amenințărilor și dovezile privind desfășurarea unor activități neautorizate care deservesc interesele Comisiei;
4. punerea la dispoziția serviciilor și a personalului Comisiei a unui serviciu de urgență permanent (24 de ore/7 zile) pentru toate aspectele legate de siguranță și securitate;
5. punerea în aplicare a măsurilor de securitate menite să reducă riscurile la adresa securității și dezvoltarea și menținerea unui sistem informatic și de comunicații adecvat pentru a acoperi necesitățile operaționale ale acesteia, în special în domeniile controlului accesului fizic, al administrării autorizațiilor de securitate și al manipulării informațiilor sensibile și clasificate ale UE;
6. acțiuni de conștientizare, organizarea de exerciții și antrenamente și oferirea de cursuri de pregătire și de servicii de consiliere cu privire la toate aspectele legate de securitate în spațiile Comisiei, în vederea promovării unei culturi a securității și a creării unei echipe de membri ai personalului pregătiți în mod corespunzător în materie de securitate.

(2) Direcția Generală Resurse Umane și Securitate asigură, fără a aduce atingere competențelor și responsabilităților altor servicii ale Comisiei, legătura cu următoarele servicii externe:

1. serviciile de securitate ale celorlalte instituții, agenții și organe ale Uniunii, cu privire la chestiuni legate de securitatea persoanelor, a bunurilor și a informațiilor în spațiile Comisiei;
2. serviciile de securitate, de informații și de evaluare a amenințărilor, inclusiv cu autoritățile naționale de securitate, din state membre, țări terțe și din cadrul unor organizații sau instituții internaționale, cu privire la chestiuni care afectează securitatea persoanelor, a activelor și a informațiilor în spațiile Comisiei;
3. poliția și alte servicii de urgență, cu privire la toate chestiunile obișnuite și urgente care afectează securitatea Comisiei;
4. autoritățile responsabile cu securitatea din cadrul altor instituții, agenții și organe ale Uniunii, din state membre și țări terțe, în domeniul combaterii atacurilor cibernetice cu un impact potențial asupra securității Comisiei;
5. în ceea ce privește primirea, evaluarea și difuzarea de informații referitoare la amenințările reprezentate de terorism și de activitățile de spionaj care afectează securitatea Comisiei;
6. în ceea ce privește aspectele referitoare la informații clasificate, astfel cum se specifică în continuare în Decizia (UE, Euratom) 2015/444 a Comisiei ([1]).

(3) Direcția Generală Resurse Umane și Securitate este responsabilă pentru securitatea transmiterii informațiilor efectuate în temeiul prezentului articol, inclusiv pentru transmiterea de date cu caracter personal.

Articolul 19

Grupul de experți pe probleme de securitate din cadrul Comisiei (ComSEG)

Se înființează Grupul de experți pe probleme de securitate din cadrul Comisiei, având drept mandat consilierea Comisiei, după caz, cu privire la chestiuni legate de politica de securitate internă și, în special, cu privire la protejarea informațiilor clasificate ale UE.

([1]) Decizia (UE, Euratom) 2015/444 a Comisiei din 13 martie 2015 privind normele de securitate pentru protecția informațiilor UE clasificate (a se vedea pagina 53 din prezentul Jurnal Oficial)

Articolul 20

Ofițeri locali de securitate (LSO)

(1) Fiecare departament sau cabinet al Comisiei numește un ofițer local de securitate (LSO), care acționează ca principal punct de contact între serviciul său și Direcția Generală Resurse Umane și Securitate cu privire la toate aspectele legate de securitate în spațiile Comisiei. Dacă este necesar, pot fi numiți unul sau mai mulți adjuncți ai LSO. Funcția de LSO est îndeplinită de un funcționar sau un agent temporar.

(2) În calitate de principal punct de contact privind securitatea în departamentul sau cabinetul Comisiei pe care îl reprezintă, LSO raportează periodic Direcției Generale Resurse Umane și Securitate și superiorilor săi ierarhici cu privire la problemele de securitate cu care se confruntă departamentul Comisiei din care face parte și aduce imediat la cunoștința acestora orice incidente legate de securitate, inclusiv pe cele care ar putea compromite informațiile IUEC sau informațiile sensibile neclasificate.

(3) În ceea ce privește aspectele legate de securitatea sistemelor informatice și de comunicații, LSO ține legătura cu ofițerii locali de securitate informatică (LISO) din cadrul departamentului Comisiei pe care îl reprezintă, ale cărui rol și responsabilități sunt prevăzute în Decizia C (2006) 3602 a Comisiei.

(4) Acesta contribuie la activitățile de formare și conștientizare în domeniul securității care răspund nevoilor specifice ale personalului, ale contractanților și ale altor persoane care acționează sub autoritatea departamentului Comisiei din care acesta face parte.

(5) La cererea Direcției Generale Resurse Umane și Securitate, în cazul apariției unor riscuri majore care amenință securitatea sau în situații de urgență, ofițerului local de securitate LSO i se pot atribui sarcini specifice. Directorul general sau directorul de resurse umane din cadrul Direcției Generale din care face parte LSO este informat cu privire la aceste sarcini specifice de către Direcția Generală Resurse Umane și Securitate.

(6) Responsabilitățile LSO nu aduc atingere rolului și responsabilităților atribuite ofițerilor locali de securitate informatică (LISO), responsabililor cu sănătatea și securitatea, ofițerilor de control ai registraturii (RCO) sau oricărei alte funcții care implică responsabilități în materie de securitate sau siguranță. LSO ține legătura cu persoanele menționate pentru a asigura o abordare coerentă și consecventă a politicii de securitate și un flux eficient de informații cu privire la aspectele legate de securitate în spațiile Comisiei.

(7) Atunci când LSO transmite informații superiorilor săi imediați, acesta are acces direct la directorul său general sau la șeful său de serviciu. LSO deține un certificat de securitate care să îi permite accesul la informațiile UE clasificate, cel puțin până la nivelul SECRET UE/EU SECRET.

(8) În vederea promovării schimbului de informații și a celor mai bune practici, Direcția Generală Resurse Umane și Securitate organizează, cel puțin de două ori pe an, o conferință a LSO. Participarea LSO la aceste conferințe este obligatorie.

CAPITOLUL 5

PUNEREA ÎN APLICARE

Articolul 21

Norme de punere în aplicare și notificări în materie de securitate

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

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

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

CAPITOLUL 6

DISPOZIȚII DIVERSE ȘI DISPOZIȚII FINALE

Articolul 22

Prelucrarea datelor cu caracter personal

(1) Comisia prelucrează datele cu caracter personal necesare pentru punerea în aplicare a prezentei decizii în conformitate cu Regulamentul (CE) nr. 45/2001.

(2) În pofida măsurilor deja în vigoare la data adoptării prezentei decizii, notificate Autorității Europene pentru Protecția Datelor ([1]), orice măsură adoptată în temeiul prezentei decizii care implică prelucrarea de date cu caracter personal, de exemplu date referitoare la fișierele privind intrările și ieșirile, înregistrări TVCI, înregistrări ale unor convorbiri telefonice cu serviciile de permanență sau centrele de expediere și date similare, care sunt necesare din motive de securitate sau pentru a interveni în situații de criză, trebuie să facă obiectul unor norme de punere în aplicare în conformitate cu articolul 21, care să stabilească garanții corespunzătoare pentru persoanele vizate.

(3) Directorul general al Direcției Generale Resurse Umane și Securitate este responsabil pentru securitatea oricărei operațiuni de prelucrare a datelor cu caracter personal efectuate în cadrul prezentei decizii.

(4) Normele și procedurile de punere în aplicare menționate se adoptă după consultarea responsabilului cu protecția datelor și a Autorității Europene pentru Protecția Datelor, în conformitate cu Regulamentul (CE) nr. 45/2001.

Articolul 23

Transparență

Prezenta decizie și normele de punere în aplicare a acesteia sunt aduse la cunoștința personalului Comisiei și a tuturor persoanelor cărora li se aplică aceste dispoziții.

Articolul 24

Abrogarea deciziilor anterioare

Decizia (94) 2129 se abrogă.

Articolul 25

Intrarea în vigoare

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

Adoptată la Bruxelles, 13 martie 2015.

Pentru Comisie

Președintele

Jean-Claude JUNCKER

([1]) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

DECIZIA (UE, Euratom) 2015/444 A COMISIEI

din 13 martie 2015

privind normele de securitate pentru protecția informațiilor UE clasificate

COMISIA EUROPEANĂ,

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

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

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

întrucât:

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

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

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

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

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

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

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

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

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

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

(8) Dispoziția din prezenta decizie nu aduce atingere:

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

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

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

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

ADOPTĂ PREZENTA DECIZIE:

CAPITOLUL 1

PRINCIPII DE BAZĂ ȘI STANDARDE MINIME

Articolul 1

Definiții

În sensul prezentei decizii, se aplică următoarele definiții:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

([4]) Regulamentul (CEE, Euratom) nr. 354/83 al Consiliului din 1 februarie 1983 privind deschiderea către public a arhivelor istorice ale Comunității Economice Europene și ale Comunității Europene a Energiei Atomice (JO L 43, 15.2.1983, p. 1)

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

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

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

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

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

Articolul 2

Obiect și domeniu de aplicare

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

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

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

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

Articolul 3

Definiția IUEC, a clasificărilor și a marcajelor de securitate

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

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

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

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

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

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

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

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

Articolul 4

Gestionarea clasificărilor

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

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

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

Articolul 5

Protecția informațiilor clasificate

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

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

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

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

Articolul 6

Managementul riscului de securitate

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

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

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

Articolul 7

Punerea în aplicare a prezentei decizii

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

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

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

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

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

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

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

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

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

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

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

Articolul 8

Încălcări ale securității și compromiterea IUEC

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

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

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

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

(5) Se iau toate măsurile corespunzătoare pentru:

(a) a informa emitentul;

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

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

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

(e) a notifica autorităților competente acțiunea întreprinsă.

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

CAPITOLUL 2

SECURITATEA PERSONALULUI

Articolul 9

Definiții

În sensul prezentului capitol, se aplică definițiile următoare:

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

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

   (a) au nevoie să le cunoască;

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

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

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

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

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

Articolul 10

Principii de bază

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

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

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

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

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

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

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

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

Articolul 11

Procedura de autorizare de securitate

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Evidențele referitoare la permisiunile de securitate și la autorizările de securitate

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

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

Reînnoirea autorizărilor de securitate

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

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

Articolul 12

Informări cu privire la autorizarea de securitate

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

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

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

Articolul 13

Autorizările temporare de securitate

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

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

Articolul 14

Participarea la reuniunile clasificate organizate de Comisie

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

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

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

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

Articolul 15

Acces potențial la IUEC

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

CAPITOLUL 3

SECURITATEA FIZICĂ CE VIZEAZĂ PROTEJAREA INFORMAȚIILOR CLASIFICATE

Articolul 16

Principii de bază

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

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

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

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

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

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

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

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

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

Articolul 17

Cerințe și măsuri de securitate fizică

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

(a) nivelul de clasificare al IUEC;

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

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

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

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

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

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

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

Articolul 18

Echipamente destinate protecției fizice a IUEC

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

(a) zone administrative; și

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

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

(3) Pentru zonele administrative:

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

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

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

(4) Pentru zonele securizate:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(e) orice alte măsuri și proceduri relevante.

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

Articolul 19

Măsuri de protecție fizică pentru gestionarea și păstrarea IUEC

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

(a) într-o zonă securizată;

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

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

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

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

(a) într-o zonă securizată;

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

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

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

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

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

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

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

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

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

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

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

sau

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

Articolul 20

Gestionarea cheilor și a combinațiilor de cifruri utilizate pentru protecția IUEC

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

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

(a) la primirea unui nou container;

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

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

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

(e) cel puțin la fiecare 12 luni.

CAPITOLUL 4

MANAGEMENTUL INFORMAȚIILOR CLASIFICATE ALE UE

Articolul 21

Principii de bază

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

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

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

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

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

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

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

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

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

Articolul 22

Clasificări și marcaje

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

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

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

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

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

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

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

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

CONFIDENTIEL UE/EU CONFIDENTIAL

Fără anexă/anexe RESTREINT UE/EU RESTRICTED

Articolul 23

Marcaje

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

(a) un element de identificare care desemnează emitentul;

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

(c) marcaje de comunicare;

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

Articolul 24

Marcaje de clasificare abreviate

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

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

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

Articolul 25

Crearea IUEC

(1) La crearea unui document UE clasificat:

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

(b) fiecare pagină este numerotată;

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

(d) documentul este datat;

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

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

Articolul 26

Reducerea nivelului de clasificare și declasificarea IUEC

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

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

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

Articolul 27

Sistemul de registraturi IUEC din cadrul Comisiei

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

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

— registratură IUEC locală a Secretariatului General al Comisiei;

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

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

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

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

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

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

Articolul 28

Ofițerul de control al registraturii

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

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

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

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

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

— verifică periodic necesitatea menținerii clasificării informațiilor;

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

Articolul 29

Înregistrarea IUEC din motive de securitate

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

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

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

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

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

Articolul 30

Copierea și traducerea documentelor clasificate ale UE

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

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

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

Articolul 31

Transportul IUEC

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

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

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

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

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

  — între clădiri ale Comisiei situate în același stat membru;

  — în Uniune;

  — din Uniune către teritoriul unui stat terț; și

  — sunt adaptate la caracteristicile și forma IUEC.

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

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

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

— modul de prezentare al IUEC;

— contramăsurile tehnice pentru IUEC transportate pe suporturi electronice;

— orice altă măsură procedurală, fizică sau electronică;

— procedurile de înregistrare;

— recurgerea la personalul de securitate autorizat.

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

Articolul 32

Distrugerea IUEC

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

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

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

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

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

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

Articolul 33

Distrugerea IUEC în situații de urgență

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

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

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

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

CAPITOLUL 5

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

Articolul 34

Principii de bază ale asigurării informațiilor

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

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

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

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

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

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

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

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

Articolul 35

Definiții

În sensul prezentului capitol se folosesc următoarele definiții:

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

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

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

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

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

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

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

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

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

Articolul 36

SIC care gestionează IUEC

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

— autoritate AI (AAI);

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

— autoritate TEMPEST (AT);

— autoritatea de aprobare criptografică (AAC);

— autoritate de distribuție criptografică (ADC);

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

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

Articolul 37

Acreditarea unui SIC care gestionează IUEC

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

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

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

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

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

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

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

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

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

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

(b) de a audita sau inspecta SCI;

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

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

Articolul 38

Situații de urgență

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

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

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

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

(3) Informațiile clasificate transmise în împrejurările enunțate la alineatul (1) nu poartă niciun marcaj sau indicație care să le distingă de orice informații neclasificate sau care pot fi protejate cu ajutorul unui produs de criptare disponibil. Destinatarilor le este notificat fără întârziere nivelul de clasificare, prin alte mijloace.

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

CAPITOLUL 6

SECURITATE INDUSTRIALĂ

Articolul 39

Principii de bază

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

(a) în cadrul contractelor clasificate, de către:

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

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

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

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

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

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

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

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

Articolul 40

Definiții

În sensul prezentului capitol, se aplică următoarele definiții:

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

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

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

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

Articolul 41

Procedura aplicabilă contractelor sau acordurilor de grant clasificate

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

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

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

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

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

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

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

Articolul 42

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

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

Instrucțiuni de securitate pentru program sau proiect (ISP)

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

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

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

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

Anexa de securitate

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

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

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

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

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

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

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

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

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

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

Articolul 43

Accesul la IUEC al personalului contractanților și al beneficiarilor

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

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

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

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

Articolul 44

Autorizarea de securitate industrială

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

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

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

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

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

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

Articolul 45

Dispoziții referitoare la contractele clasificate și la acordurile de grant clasificate

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

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

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

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

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

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

Articolul 46

Dispoziții specifice referitoare la contractele clasificate

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

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

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

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

Articolul 47

Vizite legate de contractele clasificate

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

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

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

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

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

Articolul 48

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

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

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

(3) Pentru transportul ca marfă al materialelor clasificate, se aplică următoarele principii în stabilirea măsurilor de securitate:

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

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

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

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

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

Articolul 49

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

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

Articolul 50

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

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

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

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

CAPITOLUL 7

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

Articolul 51

Principii de bază

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

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

Articolul 52

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

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

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

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

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

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

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

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

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

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

Articolul 53

Schimbul de IUEC cu statele membre

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

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

Articolul 54

Schimbul de IUEC cu state terțe și organizații internaționale

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

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

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

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

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

Articolul 55

Acordurile privind securitatea informațiilor

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

(2) Acordurile privind securitatea informațiilor:

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

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

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

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

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

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

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

(a) cadrul normativ aplicabil pentru protecția informațiilor clasificate;

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

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

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

Articolul 56

Acorduri administrative

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

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

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

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

Articolul 57

Comunicarea ad-hoc excepțională a IUEC

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

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

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

CAPITOLUL 8

DISPOZIȚII FINALE

Articolul 58

Înlocuirea deciziei anterioare

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

Articolul 59

Informațiile clasificate create înainte de intrarea în vigoare a prezentei decizii

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

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

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

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

Articolul 60

Norme de punere în aplicare și notificări de securitate

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

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

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

Articolul 61

Intrarea în vigoare

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

Adoptată la Bruxelles, 13 martie 2015.

Pentru Comisie

Președintele

Jean-Claude JUNCKER

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

ANEXA I

ECHIVALENȚA CLASIFICĂRILOR DE SECURITATE

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

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

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

([2]) Germania: VS = Verschlusssache.

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

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

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

ANEXA II

LISTA ABREVIERILOR

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

ANEXA III

LISTA AUTORITĂȚILOR NAȚIONALE DE SECURITATE

BELGIA

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

BULGARIA

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

REPUBLICA CEHĂ

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

DANEMARCA

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

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

GERMANIA

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

ESTONIA

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

GRECIA

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

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

SPANIA

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

FRANȚA

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

CROAȚIA

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

IRLANDA

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

ITALIA

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

CIPRU

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

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

LETONIA

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

LITUANIA

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

LUXEMBURG

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

UNGARIA

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

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

MALTA

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

ȚĂRILE DE JOS

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

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

AUSTRIA

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

POLONIA

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

PORTUGALIA

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

ROMÂNIA

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

SLOVENIA

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

SLOVACIA

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

FINLANDA

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

SUEDIA

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

REGATUL UNIT

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

ISSN 1977-0782 (ediție electronică)
ISSN 1830-3625 (ediție tipărită)

Oficiul pentru Publicații al Uniunii Europene
2985 Luxemburg
LUXEMBURG

RO