Journal officiel de l'Union européenne

L 72

Édition de langue française

Législation

58e année

17 mars 2015

Sommaire

FR

Les actes dont les titres sont imprimés en caractères maigres sont des actes de gestion courante pris dans le cadre de la politique agricole et ayant généralement une durée de validité limitée.

Les actes dont les titres sont imprimés en caractères gras et précédés d'un astérisque sont tous les autres actes.

II

(Actes non législatifs)

RÈGLEMENTS

RÈGLEMENT D'EXÉCUTION (UE) 2015/434 DE LA COMMISSION

du 16 mars 2015

établissant les valeurs forfaitaires à l'importation pour la détermination du prix d'entrée de certains fruits et légumes

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) nº 1308/2013 du Parlement européen et du Conseil du 17 décembre 2013 portant organisation commune des marchés des produits agricoles et abrogeant les règlements (CEE) nº 922/72, (CEE) nº 234/79, (CE) nº 1037/2001 et (CE) nº 1234/2007 du Conseil ([1]),

vu le règlement d'exécution (UE) nº 543/2011 de la Commission du 7 juin 2011 portant modalités d'application du règlement (CE) nº 1234/2007 du Conseil en ce qui concerne les secteurs des fruits et légumes et des fruits et légumes transformés ([2]), et notamment son article 136, paragraphe 1,

considérant ce qui suit:

(1) Le règlement d'exécution (UE) nº 543/2011 prévoit, en application des résultats des négociations commerciales multilatérales du cycle d'Uruguay, les critères pour la fixation par la Commission des valeurs forfaitaires à l'importation des pays tiers, pour les produits et les périodes figurant à l'annexe XVI, partie A, dudit règlement.

(2) La valeur forfaitaire à l'importation est calculée chaque jour ouvrable, conformément à l'article 136, paragraphe 1, du règlement d'exécution (UE) nº 543/2011, en tenant compte des données journalières variables. Il importe, par conséquent, que le présent règlement entre en vigueur le jour de sa publication au *Journal officiel de l'Union européenne*,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Les valeurs forfaitaires à l'importation visées à l'article 136 du règlement d'exécution (UE) nº 543/2011 sont fixées à l'annexe du présent règlement.

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

Article 2

Le présent règlement entre en vigueur le jour de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 16 mars 2015.

Par la Commission,
au nom du président,
Jerzy PLEWA
Directeur général de l'agriculture et du développement rural

ANNEXE

Valeurs forfaitaires à l'importation pour la détermination du prix d'entrée de certains fruits et légumes

(EUR/100 kg)

Code NC	Code des pays tiers (1)	Valeur forfaitaire à l'importation
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) Nomenclature des pays fixée par le règlement nº 1106/2012 de la Commission du 27 novembre 2012 portant application du règlement (CE) nº 471/2009 du Parlement européen et du Conseil concernant les statistiques communautaires relatives au commerce extérieur avec les pays tiers, en ce qui concerne la mise à jour de la nomenclature des pays et territoires (JO L 328 du 28.11.2012, p. 7). Le code «ZZ» représente «autres origines».

DÉCISIONS

DÉCISION (UE) 2015/435 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 17 décembre 2014

relative à la mobilisation de la marge pour imprévus

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu l'accord interinstitutionnel du 2 décembre 2013 entre le Parlement européen, le Conseil et la Commission sur la discipline budgétaire, la coopération en matière budgétaire et la bonne gestion financière ([1]), et notamment son point 14,

vu la proposition de la Commission européenne,

considérant ce qui suit:

(1) L'article 13 du règlement (UE, Euratom) nº 1311/2013 du Conseil ([2]) a instauré une marge pour imprévus pouvant atteindre 0,03 % du revenu national brut de l'Union.

(2) Conformément à l'article 6 dudit règlement, la Commission a calculé le montant en valeur absolue de cette marge pour imprévus pour l'exercice 2014 ([3]).

(3) Après avoir examiné toutes les autres possibilités financières de faire face aux circonstances imprévues qui ont surgi après que le plafond des paiements du cadre financier pluriannuel pour 2014 a été établi pour la première fois en février 2013, il apparaît nécessaire de mobiliser la marge pour imprévus disponible pour compléter les crédits de paiement inscrits dans le budget général de l'Union européenne pour l'exercice 2014, au-delà du plafond des paiements.

(4) Un montant de 350 millions d'EUR en crédits de paiement devrait être inclus dans la mobilisation de la marge pour imprévus, en attendant qu'un accord intervienne sur les paiements concernant d'autres instruments spéciaux.

(5) Compte tenu de la situation très particulière qui s'est présentée cette année, la condition de «dernier recours» mentionnée à l'article 13, paragraphe 1, du règlement (UE, Euratom) nº 1311/2013 est remplie.

(6) Afin d'assurer le respect de l'article 13, paragraphe 3, du règlement (UE, Euratom) nº 1311/2013, la Commission devrait présenter une proposition sur la compensation du montant concerné dans les plafonds des paiements du CFP pour un ou deux exercices financiers futurs, compte dûment tenu de l'accord sur les paiements concernant d'autres instruments spéciaux, et sans préjudice des prérogatives institutionnelles de la Commission,

([1]) JO C 373 du 20.12.2013, p. 1.
([2]) Règlement (UE, Euratom) nº 1311/2013 du Conseil du 2 décembre 2013 fixant le cadre financier pluriannuel pour la période 2014-2020 (JO L 347 du 20.12.2013, p. 884).
([3]) Communication de la Commission au Conseil et au Parlement européen du 20 décembre 2013 concernant l'ajustement technique du cadre financier pour 2014 à l'évolution du RNB [COM(2013) 928].

ONT ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Dans le cadre du budget général de l'Union européenne établi pour l'exercice 2014, un montant de 3 168 233 715 EUR en crédits de paiement est mobilisé au titre de la marge pour imprévus, au-delà du plafond des paiements du cadre financier pluriannuel.

Article 2

Le montant de 2 818 233 715 EUR est compensé, en trois tranches, sur les marges sous les plafonds des paiements pour les exercices suivants:

a) 2018: 939 411 200 EUR;

b) 2019: 939 411 200 EUR;

c) 2020: 939 411 315 EUR.

La Commission est invitée à présenter sans tarder une proposition concernant le montant restant de 350 millions d'EUR.

Article 3

La présente décision est publiée au *Journal officiel de l'Union européenne*.

Fait à Strasbourg, le 17 décembre 2014.

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*
M. SCHULZ	B. DELLA VEDOVA

DÉCISION (UE) 2015/436 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 17 décembre 2014

relative à la mobilisation du Fonds de solidarité de l'Union européenne

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (CE) n° 2012/2002 du Conseil du 11 novembre 2002 instituant le Fonds de solidarité de l'Union européenne ([1]), et notamment son article 4, paragraphe 3,

vu l'accord interinstitutionnel du 2 décembre 2013 entre le Parlement européen, le Conseil et la Commission sur la discipline budgétaire, la coopération en matière budgétaire et la bonne gestion financière ([2]), et notamment son point 11,

vu la proposition de la Commission européenne,

considérant ce qui suit:

(1) L'Union européenne a créé un Fonds de solidarité de l'Union européenne (ci-après dénommé le «Fonds») pour exprimer sa solidarité à l'égard de la population de régions touchées par des catastrophes.

(2) L'article 10 du règlement (UE, Euratom) n° 1311/2013 du Conseil ([3]) permet la mobilisation du Fonds à concurrence d'un plafond annuel de 500 000 000 EUR (aux prix de 2011).

(3) Le règlement (CE) n° 2012/2002 contient les dispositions permettant la mobilisation du Fonds.

(4) L'Italie a présenté une demande d'intervention du Fonds concernant des inondations.

(5) La Grèce a présenté une demande d'intervention du Fonds concernant un tremblement de terre.

(6) La Slovénie a présenté une demande d'intervention du Fonds concernant des tempêtes de verglas.

(7) La Croatie a présenté une demande d'intervention du Fonds concernant des tempêtes de verglas suivies d'inondations,

ONT ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Dans le cadre du budget général de l'Union européenne établi pour l'exercice 2014, une somme de 46 998 528 EUR en crédits d'engagement est mobilisée au titre du Fonds de solidarité de l'Union européenne.

Dans le cadre du budget général de l'Union européenne établi pour l'exercice 2015, une somme de 46 998 528 EUR en crédits de paiement est mobilisée au titre du Fonds de solidarité de l'Union européenne.

Article 2

La présente décision est publiée au *Journal officiel de l'Union européenne*.

Fait à Strasbourg, le 17 décembre 2014.

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*
M. SCHULZ	B. DELLA VEDOVA

([1]) JO L 311 du 14.11.2002, p. 3.
([2]) JO C 373 du 20.12.2013, p. 1.
([3]) Règlement (UE, Euratom) n° 1311/2013 du Conseil du 2 décembre 2013 fixant le cadre financier pluriannuel pour la période 2014-2020 (JO L 347 du 20.12.2013, p. 884).

DÉCISION (UE) 2015/437 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 17 décembre 2014

relative à la mobilisation du Fonds de solidarité de l'Union européenne

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (CE) n° 2012/2002 du Conseil du 11 novembre 2002 instituant le Fonds de solidarité de l'Union européenne ([1]), et notamment son article 4, paragraphe 3,

vu l'accord interinstitutionnel du 2 décembre 2013 entre le Parlement européen, le Conseil et la Commission sur la discipline budgétaire, la coopération en matière budgétaire et la bonne gestion financière ([2]), et notamment son point 11,

vu la proposition de la Commission européenne,

considérant ce qui suit:

(1) L'Union européenne a créé un Fonds de solidarité de l'Union européenne (ci-après dénommé le «Fonds») pour exprimer sa solidarité à l'égard de la population de régions touchées par des catastrophes.

(2) L'article 10 du règlement (UE, Euratom) n° 1311/2013 du Conseil ([3]) permet la mobilisation du Fonds à concurrence d'un plafond annuel de 500 000 000 EUR (aux prix de 2011).

(3) Le règlement (CE) n° 2012/2002 contient les dispositions permettant la mobilisation du Fonds.

(4) La Serbie a présenté une demande d'intervention du Fonds concernant des inondations.

(5) La Croatie a présenté une demande d'intervention du Fonds concernant des inondations.

(6) La Bulgarie a présenté une demande d'intervention du Fonds concernant des inondations,

ONT ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Dans le cadre du budget général de l'Union européenne établi pour l'exercice 2014, une somme de 79 726 440 EUR en crédits d'engagement est mobilisée au titre du Fonds de solidarité de l'Union européenne.

Dans le cadre du budget général de l'Union européenne établi pour l'exercice 2015, une somme de 79 726 440 EUR en crédits de paiement est mobilisée au titre du Fonds de solidarité de l'Union européenne.

Article 2

La présente décision est publiée au *Journal officiel de l'Union européenne*.

Fait à Strasbourg, le 17 décembre 2014.

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*
M. SCHULZ	B. DELLA VEDOVA

([1]) JO L 311 du 14.11.2002, p. 3.
([2]) JO C 373 du 20.12.2013, p. 1.
([3]) Règlement (UE, Euratom) n° 1311/2013 du Conseil du 2 décembre 2013 fixant le cadre financier pluriannuel pour la période 2014-2020 (JO L 347 du 20.12.2013, p. 884).

DÉCISION (UE) 2015/438 DU CONSEIL

du 2 mars 2015

établissant la position à prendre au nom de l'Union européenne au sein du comité mixte institué par l'accord entre l'Union européenne et l'Ukraine visant à faciliter la délivrance de visas, en ce qui concerne l'adoption de lignes directrices communes pour la mise en œuvre de cet accord

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 77, paragraphe 2, point a), en liaison avec l'article 218, paragraphe 9,

vu la proposition de la Commission européenne,

considérant ce qui suit:

(1) L'article 12 de l'accord entre l'Union européenne et l'Ukraine visant à faciliter la délivrance de visas ([1]) (ci-après dénommé «accord») institue un comité mixte. Il prévoit que le comité mixte est notamment chargé de suivre la mise en œuvre de l'accord.

(2) L'accord entre l'Union européenne et l'Ukraine portant modification de l'accord entre la Communauté européenne et l'Ukraine visant à faciliter la délivrance de visas ([2]) (ci-après dénommé «accord modificatif») est entré en vigueur le 1er juillet 2013.

(3) Le règlement (CE) nº 810/2009 du Parlement européen et du Conseil ([3]) a fixé les procédures et conditions de délivrance des visas pour les transits ou les séjours prévus sur le territoire des États membres d'une durée maximale de 90 jours sur toute période de 180 jours.

(4) Dans le cadre de sa mission, le comité mixte a constaté la nécessité d'établir des lignes directrices communes afin d'assurer une mise en œuvre entièrement harmonisée de l'accord dans les consulats des États membres et de clarifier la relation entre les dispositions de l'accord et celles des parties contractantes qui continuent de s'appliquer aux questions de visas non couvertes par l'accord.

(5) Par sa décision nº 1/2009, le comité mixte a adopté de telles lignes directrices le 25 novembre 2009. Ces lignes directrices devraient être adaptées aux nouvelles dispositions de l'accord introduites par l'accord modificatif et aux évolutions du droit interne de l'Union relatif à la politique des visas. Par souci de clarté, il convient de remplacer ces lignes directrices.

(6) Il convient de fixer la position à prendre, au nom de l'Union, au sein du comité mixte en ce qui concerne l'adoption de lignes directrices communes pour la mise en œuvre de l'accord,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

La position à prendre au nom de l'Union au sein du comité mixte institué par l'article 12 de l'accord entre l'Union européenne et l'Ukraine visant à faciliter la délivrance de visas, en ce qui concerne l'adoption de lignes directrices communes pour la mise en œuvre de l'accord, est fondée sur le projet de décision du comité mixte joint à la présente décision.

([1]) JO L 332 du 18.12.2007, p. 68.
([2]) JO L 168 du 20.6.2013, p. 11.
([3]) Règlement (CE) nº 810/2009 du Parlement européen et du Conseil du 13 juillet 2009 établissant un code communautaire des visas (code des visas) (JO L 243 du 15.9.2009, p. 1).

Article 2

La présente décision entre en vigueur le jour de son adoption.

Fait à Bruxelles, le 2 mars 2015.

Par le Conseil
Le président
D. RIEZNIECE-OZOLA

PROJET DE

DÉCISION Nº …./2014 DU COMITÉ MIXTE INSTITUÉ PAR L'ACCORD ENTRE L'UNION EUROPÉENNE ET L'UKRAINE VISANT À FACILITER LA DÉLIVRANCE DE VISAS

du …

en ce qui concerne l'adoption de lignes directrices communes pour la mise en œuvre de l'accord

LE COMITÉ MIXTE,

vu l'accord conclu entre l'Union européenne et l'Ukraine visant à faciliter la délivrance de visas (ci-après dénommé «accord»), et notamment son article 12,

considérant que l'accord est entré en vigueur le 1er janvier 2008,

DÉCIDE:

Article premier

Les lignes directrices communes pour la mise en œuvre de l'accord entre l'Union européenne et l'Ukraine visant à faciliter la délivrance de visas sont établies dans l'annexe à la présente décision.

Article 2

La décision nº 1/2009 du comité mixte est abrogée.

Article 3

La présente décision entre en vigueur le jour de son adoption.

Fait le …, à ….

Par l'Union européenne *Par l'Ukraine*

ANNEXE

LIGNES DIRECTRICES COMMUNES POUR LA MISE EN ŒUVRE DE L'ACCORD ENTRE L'UNION EUROPÉENNE ET L'UKRAINE, VISANT À FACILITER LA DÉLIVRANCE DE VISAS

L'accord entre l'Union européenne et l'Ukraine visant à faciliter la délivrance de visas, entré en vigueur le 1er janvier 2008, tel que modifié par l'accord entre l'Union européenne et l'Ukraine du 23 juillet 2012, entré en vigueur le 1er juillet 2013, (ci-après dénommé «accord»), a pour objectif de faciliter, sur une base de réciprocité, les procédures de délivrance de visas aux citoyens de l'Ukraine pour des séjours dont la durée prévue n'excède pas 90 jours, par période de 180 jours.

L'accord établit, sur une base de réciprocité, des droits et des obligations juridiquement contraignants, en vue de simplifier les procédures de délivrance de visas aux citoyens ukrainiens.

Les présentes lignes directrices, adoptées par le comité mixte institué par l'article 12 de l'accord (ci-après dénommé «comité mixte»), visent à garantir une application correcte et harmonisée des dispositions de l'accord par les missions diplomatiques et les postes consulaires des États membres. Les présentes lignes directrices ne font pas partie de l'accord et ne sont donc pas juridiquement contraignantes. Il est toutefois vivement recommandé aux membres du personnel diplomatique et consulaire de les observer systématiquement lorsqu'ils mettent en œuvre les dispositions de l'accord.

Il est prévu que les présentes lignes directrices soient mises à jour en fonction de l'expérience acquise dans la mise en œuvre de l'accord, sous la responsabilité du comité mixte. Les lignes directrices adoptées par le comité mixte, le 25 novembre 2009, ont été adaptées conformément à l'accord entre l'Union européenne et l'Ukraine portant modification de l'accord entre la Communauté européenne et l'Ukraine visant à faciliter la délivrance de visas (ci-après dénommé «accord modificatif»), et à la nouvelle législation de l'Union, telle que le règlement (CE) no 810/2009 du Parlement européen et du Conseil [1] (ci-après dénommé «code des visas»).

I. GÉNÉRALITÉS

1.1. **Objet et champ d'application**

L'article 1er de l'accord dispose: «Le présent accord vise à faciliter la délivrance de visas aux citoyens de l'Ukraine pour des séjours dont la durée prévue n'excède pas 90 jours, par période de 180 jours».

L'accord s'applique à tous les citoyens Ukrainiens qui demandent un visa de court séjour, quel que soit le pays dans lequel ils résident.

L'article 1er, paragraphe 2, de l'accord dispose: «L'Ukraine ne peut réintroduire d'obligation de visa que pour les ressortissants, ou certaines catégories de ressortissants, de tous les États membres et non pour les ressortissants, ou certaines catégories de ressortissants, d'États membres particuliers. Si l'Ukraine réintroduisait l'obligation de visa pour les citoyens de l'Union européenne ou certaines catégories de ces citoyens, les mesures visant à faciliter la délivrance de visas prévues dans le présent accord en faveur des citoyens ukrainiens s'appliqueraient automatiquement et de manière identique, sur une base de réciprocité, aux citoyens de l'Union.».

Conformément aux décisions prises par le gouvernement ukrainien, tous les citoyens de l'Union sont dispensés de l'obligation de visa pour leurs voyages en Ukraine d'une durée ne dépassant pas 90 jours, depuis le 1er mai 2005, ou pour leur transit par le territoire ukrainien, depuis le 1er janvier 2008. Cette disposition n'affecte pas le droit du gouvernement ukrainien de modifier ces décisions.

1.2. **Champ d'application de l'accord**

L'article 2 de l'accord dispose:

> «1. Les mesures visant à faciliter la délivrance de visas prévues dans le présent accord s'appliquent aux citoyens de l'Ukraine dans la seule mesure où ceux-ci ne sont pas dispensés de l'obligation de visa par les dispositions législatives, réglementaires et administratives de l'Union européenne ou de ses États membres, par le présent accord ou par d'autres accords internationaux.
>
> 2. Le droit national de l'Ukraine ou des États membres, ou le droit de l'Union européenne, s'applique aux questions qui ne relèvent pas des dispositions du présent accord, comme le refus de délivrer un visa, la reconnaissance des documents de voyage, la preuve de moyens de subsistance suffisants, le refus d'entrée et les mesures d'expulsion.».

[1] Règlement (CE) no 810/2009 du Parlement européen et du Conseil du 13 juillet 2009 établissant un code communautaire des visas (code des visas) (JO L 243 du 15.9.2009, p. 1).

Sans préjudice de son article 10 (qui exempte de l'obligation de visa les titulaires de passeports diplomatiques et de passeports de service biométriques ukrainiens), l'accord ne modifie pas la réglementation en vigueur en matière d'obligation et d'exemption de visa. Par exemple, l'article 4 du règlement (CE) nº 539/2001 du Conseil ([1]) permet aux États membres d'exonérer de l'obligation de visa, entre autres catégories, les équipages civils des avions et des navires.

Les règles de Schengen et, le cas échéant, le droit national demeurent applicables à toutes les questions non couvertes par l'accord, comme le refus de délivrer un visa, la reconnaissance des documents de voyage, la preuve de moyens de subsistance suffisants, le refus d'entrée et les mesures d'expulsion. Il en est de même des règles de Schengen déterminant l'État membre Schengen responsable du traitement de la demande de visa. Les citoyens ukrainiens devraient donc toujours demander un visa au consulat de l'État membre constituant la principale destination de leur voyage; s'il n'y a pas de destination principale, ils devraient s'adresser au consulat de l'État membre par lequel ils entrent en premier dans l'espace Schengen.

Même si les conditions prévues dans l'accord sont réunies, par exemple, si les preuves documentaires de l'objet du voyage pour les catégories visées à l'article 4 sont fournies par le demandeur de visa, la délivrance du visa peut être refusée si les conditions prévues à l'article 5 du règlement (CE) nº 562/2006 du Parlement européen et du Conseil ([2]) (ci-après dénommé «code frontières Schengen») ne sont pas remplies, c'est-à-dire si la personne n'est pas en possession d'un document de voyage en cours de validité, fait l'objet d'un signalement dans le SIS, est considérée comme constituant une menace pour l'ordre public, la sécurité intérieure, etc.

Les autres possibilités d'assouplissement des procédures de délivrance de visas autorisées par le code des visas restent applicables. Par exemple, des visas à entrées multiples de longue durée — jusqu'à cinq ans — peuvent être délivrés à des catégories de personnes autres que celles visées à l'article 5 de l'accord, pourvu que les conditions prévues dans le code des visas soient remplies (voir article 24, paragraphe 2, du code des visas). De même, les dispositions du code des visas autorisant l'exonération ou la réduction des droits de visa resteront applicables (voir point II.2.1.1.).

1.3. **Types de visas relevant du champ d'application de l'accord**

L'article 3, point d), de l'accord définit le «visa» comme «une autorisation délivrée ou une décision prise par un État membre, qui est nécessaire à:

— l'entrée pour un séjour envisagé dans cet État membre ou dans plusieurs États membres, pour une période dont la durée totale n'excède pas 90 jours,

— l'entrée pour traverser le territoire de cet État membre ou de plusieurs États membres;».

Le type de visa suivant est couvert par l'accord:

— visas «C» (visas de court séjour).

Les mesures de facilitation prévues par l'accord s'appliquent à la fois aux visas uniformes valables pour l'ensemble du territoire des États membres et aux visas à validité territoriale limitée (VTL).

1.4. **Calcul de la durée de séjour autorisée par un visa, en particulier mode de détermination de la période de six mois**

La récente modification du code frontières Schengen a redéfini la notion de court séjour. La définition actuelle est la suivante: «90 jours sur toute période de 180 jours, ce qui implique d'examiner la période de 180 jours précédant chaque jour de séjour».

Le jour d'entrée et le jour de sortie corresponderont respectivement au premier et au dernier jour de séjour sur le territoire des États membres. L'adjectif «toute» suppose l'application d'une période de référence «mobile» de 180 jours, ce qui consiste à remonter dans le temps en comptant chaque jour du séjour couvert par la dernière période de 180 jours, afin de vérifier si la condition de 90 jours sur toute période de 180 jours continue d'être remplie. Cela signifie qu'une absence pendant une période ininterrompue de 90 jours ouvre droit à un nouveau séjour d'une durée maximale de 90 jours.

Cette définition est entrée en vigueur le 18 octobre 2013. La calculette peut être consultée en ligne à l'adresse suivante: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/border-crossing/index_en.htm

([1]) Règlement (CE) nº 539/2001 du Conseil du 15 mars 2001 fixant la liste des pays tiers dont les ressortissants sont soumis à l'obligation de visa pour franchir les frontières extérieures des États membres et la liste de ceux dont les ressortissants sont exemptés de cette obligation (JO L 81 du 21.3.2001, p. 1).

([2]) Règlement (CE) nº 562/2006 du Parlement européen et du Conseil du 15 mars 2006 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes (code frontières Schengen) (JO L 105 du 13.4.2006, p. 1).

Exemple de calcul de la durée d'un séjour sur la base de la nouvelle définition:

Une personne titulaire d'un visa à entrées multiples valable un an (du 18.4.2014 au 18.4.2015) entre sur le territoire des États membres pour la première fois le 19.4.2014 et y séjourne trois jours. Puis elle y entre de nouveau le 18.6.2014 et y séjourne 86 jours. Quelle est la situation à ces dates précises? Quand cette personne sera-t-elle autorisée à entrer à nouveau sur le territoire des États membres?

Le 11.9.2014: au cours des 180 derniers jours (du 16.3.2014 au 11.9.2014), la personne avait séjourné 3 jours (du 19 au 21.4.2014) plus 86 jours (du 18.6.2014 — 11.9.2014), soit 89 jours, donc pas de dépassement de la durée de séjour autorisée. La personne peut encore séjourner un jour.

À partir du 16.10.2014: la personne pourrait entrer pour un séjour de 3 jours supplémentaires (le 16.10.2014, le séjour du 19.4.2014 n'est plus pris en compte (en dehors du délai de 180 jours); le 17.10.2014, le séjour du 20.4.2014 n'est plus à prendre en compte (en dehors de la période 180 jours, etc.).

À partir du 15.12.2014: la personne pourrait entrer pour un séjour de 86 jours supplémentaires [le 15.12.2014, le séjour du 18.6.2014 n'est plus pris en compte (en dehors du délai de 180 jours); le 16.12.2014, le séjour du 19.6.2014 n'est plus à prendre en compte, etc.].

1.5. **Situation concernant les États membres ne mettant pas encore en œuvre l'intégralité de l'acquis de Schengen, les États membres ne participant pas à la politique commune de l'Union européenne dans le domaine des visas, et les pays associés.**

Les États membres qui ont adhéré à l'Union en 2004 (République Tchèque, Estonie, Chypre, Lettonie, Lituanie, Hongrie, Malte, Pologne, Slovénie et Slovaquie,), en 2007 (Bulgarie et Roumanie) et en 2013 (Croatie) sont liés par l'accord dès son entrée en vigueur.

Seules la Bulgarie, la Croatie, Chypre et la Roumanie ne mettent pas encore en œuvre l'intégralité de l'acquis de Schengen. Elles continueront à délivrer des visas nationaux d'une validité limitée à leur propre territoire national. Ces États membres continueront à appliquer l'accord lorsqu'ils mettront en œuvre l'intégralité de l'acquis de Schengen.

Le droit national reste applicable à toutes les questions non couvertes par l'accord jusqu'à la date de mise en œuvre de l'intégralité de l'acquis de Schengen par ces États membres. À partir de cette date, les règles de Schengen/les législations nationales s'appliqueront aux questions non régies par l'accord.

La Bulgarie, la Croatie, Chypre et la Roumanie sont autorisées à reconnaître les titres de séjour, les visas de type D et les visas de court séjour délivrés par les États de l'espace Schengen et les pays associés pour des courts séjours sur leur territoire.

Conformément à l'article 21 de la convention d'application de l'accord de Schengen du 14 juin 1985 relatif à la suppression graduelle des contrôles aux frontières communes, tous les États Schengen doivent reconnaître les visas de long séjour et les titres de séjour délivrés par les autres États Schengen comme valables pour de courts séjours sur leurs territoires respectifs. Les États membres Schengen acceptent les titres de séjour, les visas de type D et les visas de court séjour des pays associés pour l'entrée et les courts séjours, et vice-versa.

L'accord ne s'applique pas au Danemark, à l'Irlande et au Royaume-Uni, mais comporte des déclarations communes soulignant qu'il serait souhaitable que ces États membres concluent avec l'Ukraine des accords bilatéraux visant à faciliter la délivrance de visas.

Un accord bilatéral visant à faciliter la délivrance de visas entre le Danemark et l'Ukraine est entré en vigueur le 1er mars 2009. Aucune négociation visant à faciliter la délivrance de visas n'a eu lieu entre l'Ukraine et, respectivement l'Irlande et le Royaume-Uni.

L'accord ne s'applique pas à l'Islande, au Liechtenstein, à la Norvège et à la Suisse,, même si ces pays sont associés à Schengen, mais il comporte des déclarations communes soulignant qu'il serait souhaitable que ces États Schengen concluent avec l'Ukraine des accords bilatéraux visant à faciliter la délivrance de visas.

La Norvège a signé un accord bilatéral visant à faciliter la délivrance de visas le 13 février 2008. Cet accord est entré en vigueur le 1er septembre 2011.

La Suisse a finalisé les négociations en vue d'un accord bilatéral visant à faciliter la délivrance de visas en novembre 2011. L'Islande a indiqué que les négociations avec l'Ukraine avaient commencé.

1.6. **L'accord/les accords bilatéraux**

L'article 13, paragraphe 1, de l'accord dispose:

> «1. À partir de son entrée en vigueur, le présent accord prime les dispositions de toute convention ou de tout accord bilatéral(e) ou multilatéral(e) conclu(e) entre un État membre et l'Ukraine, dans la mesure où ces dispositions traitent de questions régies par le présent accord.».

À compter de l'entrée en vigueur de l'accord, les dispositions des accords bilatéraux en vigueur entre les États membres et l'Ukraine sur les questions couvertes par l'accord ont cessé de s'appliquer. Conformément au droit de l'Union, les États membres doivent prendre les mesures nécessaires pour éliminer les incompatibilités entre leurs accords bilatéraux et l'accord.

Toutefois, l'article 13, paragraphe 2, de l'accord dispose:

> «2. Les dispositions d'accords ou d'arrangements bilatéraux conclus entre des États membres particuliers et l'Ukraine avant l'entrée en vigueur du présent accord, qui prévoient une exemption de l'obligation de visa pour les titulaires de passeports de service non biométriques continuent à s'appliquer sans préjudice du droit des États membres concernés ou de l'Ukraine de dénoncer ou de suspendre ces accords ou arrangements bilatéraux.».

Les États membres suivants ont un accord bilatéral avec l'Ukraine prévoyant l'exemption de l'obligation de visa pour les titulaires de passeports de service: Bulgarie, Croatie, Chypre, Lettonie, Lituanie, Hongrie, Pologne, Roumanie et Slovaquie.

Conformément à l'article 13, paragraphe 1de l'accord, dans la mesure où ces accords bilatéraux concernent les titulaires d'un passeport de service biométrique, l'article 10, paragraphe 2, de l'accord prévaut sur ces accords bilatéraux. Conformément à l'article 13, paragraphe 2 de l'acccord, ces accords bilatéraux conclus avant l'entrée en vigueur de l'accord modificatif, dans la mesure où ils concernent des titulaires de passeports de service non biométriques, continuent à s'appliquer sans préjudice du droit des États membres concernés ou de l'Ukraine de dénoncer ou de suspendre ces accords ou arrangements bilatéraux. L'exemption de l'obligation de visa accordée par un État membre aux titulaires de passeports de service non biométriques s'applique uniquement pour les voyages effectués sur le territoire de cet État membre, et non pour les voyages à destination des autres États membres Schengen.

Au cas où un État membre aurait conclu avec l'Ukraine une convention ou un accord bilatéral sur des questions non couvertes par l'accord, cette exemption resterait applicable après l'entrée en vigueur de l'accord.

1.7. **Déclaration de la Communauté européenne relative à l'accès des demandeurs de visa et à l'harmonisation des informations à connaître sur les procédures de délivrance de visas de court séjour et sur les documents à fournir à l'appui d'une demande de visa de court séjour**

Conformément à cette déclaration de la Communauté européenne jointe à l'accord, des informations de base communes sur l'accès des demandeurs de visa aux missions diplomatiques et postes consulaires des États membres, sur les procédures et conditions de délivrance d'un visa et sur la validité des visas délivrés ont été rédigées à l'intention des demandeurs pour assurer la cohérence et l'uniformité des informations qui leur sont communiquées. Ces informations sont disponibles sur le site internet de la délégation de l'Union européenne en Ukraine: http://eeas.europa.eu/delegations/ukraine/index_en.htm

Les missions diplomatiques et les postes consulaires des États membres sont invités à assurer une large diffusion de ces informations (sur les tableaux d'affichage, sous la forme de dépliants, sur l'internet, etc.), ainsi qu'à diffuser des informations précises sur les conditions de délivrance des visas, sur la représentation des États membres en Ukraine et sur la liste harmonisée de l'Union européenne de pièces justificatives requises.

II. LIGNES DIRECTRICES CONCERNANT CERTAINES DISPOSITIONS

2.1. **Règles applicables à tous les demandeurs de visa**

Important: il est rappelé que les mesures de facilitation mentionnées ci-dessous, relatives au droit prélevé pour le traitement des demandes de visa, à la durée des procédures de traitement des demandes, au départ en cas de perte ou de vol de documents, et à la prolongation du visa dans des circonstances exceptionnelles, s'appliquent à tous les demandeurs de visa et titulaires de visa ukrainiens.

2.1.1. *Droit prélevé pour le traitement des demandes de visa*

L'article 6, paragraphe 1, de l'accord dispose:

> «Le droit prélevé pour le traitement des demandes de visa des citoyens ukrainiens est de 35 EUR. Ce montant peut être revu en appliquant la procédure prévue à l'article 14, paragraphe 4.».

Aux termes de l'article 6, paragraphe 1, le droit prélevé pour le traitement d'une demande de visa est de 35 EUR. Ce droit s'applique à tous les demandeurs de visa ukrainiens (y compris les touristes) et concerne les visas de court séjour, indépendamment du nombre d'entrées. Il s'applique également aux demandes de visa présentées aux frontières extérieures.

L'article 6, paragraphe 2, de l'accord dispose:

> «Si l'Ukraine réintroduisait l'obligation de visa pour les citoyens de l'Union européenne, le droit de visa prélevé ne serait pas supérieur à 35 EUR ou au montant convenu après révision intervenant conformément à la procédure prévue à l'article 14, paragraphe 4.».

L'article 6, paragraphe 3, de l'accord dispose:

> «Les États membres prélèvent un droit de 70 EUR pour le traitement des demandes de visa lorsque, compte tenu de la distance entre son lieu de résidence et le lieu où la demande a été présentée, le demandeur a demandé qu'une décision sur la demande soit prise dans un délai de trois jours à compter de sa présentation et que le consulat a accepté de prendre une décision dans un délai de trois jours.».

Un droit de 70 EUR sera perçu pour le traitement des demandes de visa lorsque la demande et les pièces justificatives sont soumises par un demandeur de visa dont le lieu de résidence est notoirement situé dans l'oblast dans lequel l'État membre vers lequel le demandeur souhaite se rendre n'a pas de représentation consulaire (s'il n'y a pas, dans cet oblast, de consulat, de centre des visas, ni les consulats des États membres ayant conclu des accords de représentation avec l'État membre vers lequel le demandeur souhaite se rendre), et lorsque la représentation diplomatique ou consulaire a accepté de se prononcer sur la demande de visa dans les trois jours. La preuve du lieu de résidence du demandeur de visa est fournie dans le formulaire de demande de visa.

En principe, l'article 6, paragraphe 3 de l'accord, vise à faciliter l'introduction d'une demande de visa par les demandeurs vivant à grande distance du consulat. Si un long voyage est nécessaire pour introduire la demande de visa, l'objectif est de le délivrer rapidement, afin de permettre au demandeur de l'obtenir sans devoir entreprendre le même long voyage une seconde fois.

Pour les raisons précitées, lorsque la durée «normale» du traitement d'une demande de visa par une mission diplomatique ou un poste consulaire donné est égale ou inférieure à trois jours, le droit de visa normal de 35 EUR est perçu.

Pour les missions diplomatiques et les postes consulaires qui appliquent un système de rendez-vous, le délai nécessaire pour obtenir un rendez-vous n'est pas comptabilisé dans la durée de traitement (voir également II. 2.1.2).

L'article 6, paragraphe 4, de l'accord dispose:

> «4. Sans préjudice des dispositions du paragraphe 5, les catégories de personnes suivantes sont exonérées des droits de visa:
>
> a) les parents proches — conjoints, enfants (y compris adoptifs), parents (y compris parents ayant la garde légale), grands-parents et petits-enfants — de citoyens de l'Ukraine en séjour régulier sur le territoire d'un État membre ou de citoyens de l'Union européenne résidant sur le territoire de l'État membre dont ils sont ressortissants;»

(N.B.: ce point régit la situation des parents proches ukrainiens qui se rendent dans un État membre afin de rendre visite à des citoyens ukrainiens en séjour régulier dans l'État membre ou à des citoyens de l'Union européenne qui résident sur le territoire de l'État membre dont ils sont ressortissants. Les demandeurs de visa ukrainiens qui sont membres de la famille d'un citoyen de l'Union, au sens de l'article 5, paragraphe 2, de la directive 2004/38/CE du Parlement européen et du Conseil ([1]), obtiendront leur visa sans frais, dans les meilleurs délais et dans le cadre d'une procédure accélérée.)

> «b) les membres de délégations officielles qui, à la suite d'une invitation officielle adressée à l'Ukraine, participent à des réunions, consultations, négociations ou programmes d'échange ainsi qu'à des événements ayant lieu sur le territoire de l'un des États membres à l'initiative d'organisations intergouvernementales;
>
> c) les membres des gouvernements et parlements nationaux et régionaux et les membres des cours constitutionnelles et suprêmes, lorsque ces personnes ne sont pas dispensées de l'obligation de visa par le présent accord;
>
> d) les écoliers, les étudiants, les étudiants de troisième cycle et les enseignants accompagnateurs qui entreprennent des voyages d'études ou à but éducatif;
>
> e) les personnes handicapées et la personne les accompagnant, le cas échéant;» (N.B. pour pouvoir bénéficier de l'exonération du droit de visa, il est nécessaire de fournir la preuve que les demandeurs de visa relèvent tous de cette catégorie.)
>
> «f) les personnes qui ont présenté des documents attestant la nécessité de leur voyage pour raisons de santé ou familiales, y compris pour recevoir un traitement médical urgent, auquel cas la personne les accompagnant est aussi exonérée de droit de visa, ou pour assister aux obsèques d'un parent proche, ou pour rendre visite à un parent proche gravement malade;
>
> g) les participants à des manifestations sportives internationales et les personnes les accompagnant;» (N.B. seuls les accompagnateurs voyageant à titre professionnel sont couverts; les supporters ne sont pas donc considérés comme des accompagnateurs.)

([1]) Directive 2004/38/CE du Parlement européen et du Conseil du 29 avril 2004 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres, modifiant le règlement (CEE) n° 1612/68 et abrogeant les directives 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE et 93/96/CEE (JO L 158 du 30.4.2004, p. 77).

«h) les personnes participant à des activités scientifiques, culturelles et artistiques, y compris des programmes d'échanges universitaires ou autres;

i) les participants à des programmes d'échange officiels organisés par des villes jumelées et d'autres entités municipales;

j) les journalistes et le personnel technique les accompagnant à titre professionnel; (N.B. les journalistes couverts par l'article 4, paragraphe 1, point e) de l'accord sont couverts par ce point).

k) les retraités;» (N.B.: pour pouvoir bénéficier de l'exonération du droit de visa pour cette catégorie, les demandeurs de visa doivent présenter un document attestant leur statut de retraité.)

«l) les conducteurs fournissant des services de transport international de marchandises et de passagers vers le territoire des États membres dans des véhicules immatriculés en Ukraine;

m) le personnel de wagons, wagons frigorifiques et locomotives de trains internationaux circulant vers le territoire des États membres;

n) les enfants de moins de 18 ans et les enfants à charge de moins de 21 ans.» (N.B. pour pouvoir bénéficier de l'exonération du droit de visa pour cette catégorie, les demandeurs de visa doivent présenter un document attestant leur âge et — s'ils ont moins de 21 ans — leur qualité de personne à charge).

«o) les représentants de communautés religieuses;

p) les membres de professions libérales participant à des foires, à des conférences, à des symposiums et à des séminaires internationaux ou à d'autres événements similaires ayant lieu sur le territoire des États membres;

q) les participants, âgés au maximum de 25 ans, à des séminaires, des conférences ou des manifestations sportives, culturelles ou éducatives organisés par des organisations à but non lucratif;

r) les représentants d'organisations de la société civile qui entreprennent des voyages à but éducatif ou se rendent à des séminaires ou à des conférences, y compris dans le cadre de programmes d'échange;

s) les participants à des programmes officiels de coopération transfrontalière de l'Union européenne, par exemple dans le cadre de l'instrument européen de voisinage et de partenariat (IEVP);

Le premier alinéa s'applique également lorsque l'objet du voyage est le transit.».

Le deuxième alinéa de l'article 6, paragraphe 4 de l'accord ne s'applique que si l'objet du voyage vers le pays tiers est équivalent à l'un des objets énumérés à l'article 6, paragraphe 4, points a) à s) de l'accord, par exemple si le transit est nécessaire pour participer à un séminaire, rendre visite à des membres de la famille, participer à un programme d'échange d'organisations de la société civile, etc. dans le pays tiers.

Les catégories de personnes susmentionnées sont totalement exonérées du droit. En outre, aux termes de l'article 16, paragraphe 6, du code des visas, «dans certains cas individuels, le montant des droits du visa peut être réduit ou ne pas être perçu, lorsque cette mesure sert à promouvoir des intérêts culturels ou sportifs ou des intérêts dans le domaine de la politique étrangère, de la politique de développement, d'autres domaines d'intérêt général essentiel, ou lorsqu'elle répond à des considérations humanitaires.».

Toutefois, ce principe ne peut pas être appliqué pour supprimer, dans des cas individuels, le droit de 70 EUR pour le traitement de la demande de visa, lorsque cette dernière et les pièces justificatives sont soumises par un demandeur de visa dont on sait que le lieu de résidence est éloigné de la représentation diplomatique ou consulaire de l'État membre et qui appartient à l'une des catégories exemptées du droit de visa figurant à l'article 6, paragraphe 4, de l'accord.

Il convient également de rappeler que les catégories de personnes exemptées de droits de visa pourraient se voir appliquer des frais de service dans le cas où un État membre coopère avec un prestataire de services extérieur.

L'article 6, paragraphe 5, de l'accord dispose:

«5. Si un État membre coopère avec un prestataire de services extérieur en vue de la délivrance d'un visa, ce prestataire de services extérieur peut facturer des frais pour ses services. Ces frais sont proportionnels aux coûts engagés par le prestataire pour la réalisation de ses tâches et ne peuvent dépasser 30 EUR. Les États membres maintiennent la possibilité, pour tous les demandeurs, d'introduire directement leur demande auprès de leur consulat. Si les demandeurs sont tenus d'obtenir un rendez-vous pour l'introduction d'une demande, celui-ci se déroule, en règle générale, dans un délai de deux semaines à compter de la date à laquelle il a été demandé.».

Maintenir la possibilité, pour toutes les catégories de demandeurs de visa, de déposer leur demande directement au consulat, au lieu de s'adresser à un prestataire de services extérieur, suppose qu'ils puissent véritablement choisir entre ces deux possibilités. Si l'accès direct ne doit pas obligatoirement être organisé dans des conditions identiques ou analogues à celles qui sont attachées à l'accès à un prestataire de services, il ne doit pas être subordonné à des conditions qui le rendent impossible en pratique. Même s'il est admissible que le délai d'attente pour obtenir un rendez-vous soit différent pour l'accès direct, la longueur du délai ne doit pas rendre cet accès impossible dans la pratique.

2.1.2. *Durée des procédures de traitement des demandes de visa*

L'article 7 de l'accord dispose:

> «1. Les missions diplomatiques et les postes consulaires des États membres prennent la décision de délivrer ou non un visa dans un délai de dix jours de calendrier suivant la réception de la demande de visa et des documents requis aux fins de sa délivrance.
>
> 2. Le délai imparti pour prendre une décision sur une demande de visa peut être étendu à trente jours de calendrier, notamment lorsqu'un examen complémentaire de la demande se révèle nécessaire.
>
> 3. En cas d'urgence, le délai imparti pour prendre une décision sur une demande de visa peut être ramené à deux jours ouvrables, voire moins.».

Une décision relative à la demande de visa sera arrêtée, en principe, dans les 10 jours calendrier suivant la date de réception de la demande de visa complète et des pièces justificatives.

Ce délai peut être porté à 30 jours calendrier au maximum lorsqu'un examen complémentaire se révèle nécessaire — par exemple, pour consulter les autorités centrales.

Tous ces délais ne commencent à courir que lorsque le dossier de demande est complet, c'est-à-dire à compter de la date de réception de la demande de visa et des pièces justificatives.

Pour les missions diplomatiques et les postes consulaires qui appliquent un système de rendez-vous, le délai nécessaire pour obtenir un rendez-vous n'est pas comptabilisé dans la durée de traitement. Lors de la fixation du rendez-vous, il convient de tenir compte de l'éventuelle urgence invoquée par le demandeur de visa en vue de l'application de l'article 7, paragraphe 3 de l'accord. Les rendez-vous se déroulent, en règle générale, dans un délai de deux semaines à compter de la date à laquelle ils ont été demandés (voir article 6, paragraphe 5 de l'accord). Un délai plus long devrait être une exception, même en période de pointe. Le comité mixte suivra cette question de près. Les États membres veillent à ce que les rendez-vous fixés à la demande des membres de délégations officielles de l'Ukraine pour le dépôt des demandes auprès des missions diplomatiques et des postes consulaires interviennent le plus rapidement possible, de préférence dans un délai de deux jours ouvrables, en cas d'urgence lorsque l'invitation a été envoyée tardivement.

La décision de réduire le délai imparti pour prendre une décision sur une demande de visa au sens de l'article 7, paragraphe 3 de l'accord, est prise par l'agent consulaire.

2.1.3. *Prorogation du visa dans des circonstances exceptionnelles*

L'article 9 de l'accord dispose:

> «Les citoyens de l'Ukraine qui, pour des raisons de force majeure, n'ont pas la possibilité de quitter le territoire des États membres à la date indiquée par leur visa voient celui-ci prorogé gratuitement, conformément à la législation appliquée par l'État hôte, pour toute la période nécessaire à leur retour dans leur État de résidence.».

En ce qui concerne la possibilité de proroger la validité du visa dans des cas de force majeure (par exemple, en cas d'hospitalisation due à des motifs imprévus/une maladie soudaine/un accident), où le titulaire du visa n'a pas la possibilité de quitter le territoire de l'État membre au plus tard à la date indiquée sur le visa, les dispositions de l'article 33, paragraphe 1, du code des visas s'appliquent pour autant qu'elles soient compatibles avec l'accord (par exemple, le visa prorogé doit rester un visa uniforme, autorisant l'entrée sur le territoire de tous les États membres de Schengen pour lesquels il était valable à la date de sa délivrance). L'accord prévoit toutefois que la prorogation du visa est effectuée gratuitement en cas de force majeure.

2.2. **Règles applicables à certaines catégories de demandeurs de visa**

2.2.1. *Preuves documentaires de l'objet du voyage*

Pour toutes les catégories de personnes énumérées à l'article 4, paragraphe 1 de l'accord, y compris les conducteurs fournissant des services de transport international de marchandises et de passagers, seules les preuves documentaires mentionnées seront exigées en ce qui concerne l'objet du voyage. Aucun autre document concernant l'objet du séjour ne doit être demandé pour ces catégories de demandeurs. Conformément à l'article 4, paragraphe 3 de l'accord, aucune autre justification, invitation ou validation concernant l'objet du voyage ne sera exigée.

Si, dans des cas individuels, il subsiste des doutes quant à l'objet réel du voyage, le demandeur de visa sera convié à un entretien (supplémentaire) approfondi à l'ambassade/au consulat, où il pourra être interrogé sur l'objet effectif de son séjour ou sur son intention de retourner dans son pays de provenance — voir article 21, paragraphe 8, du code des visas. Dans ce cas, des documents supplémentaires peuvent être fournis par le demandeur de visa ou demandés, à titre exceptionnel, par l'agent consulaire. Le comité mixte suivra cette question de près.

Pour les catégories de personnes non mentionnées à l'article 4, paragraphe 1 de l'accord, les règles actuelles relatives aux documents attestant l'objet du voyage restent applicables. Il en va de même des documents concernant l'autorisation parentale pour les voyages d'enfants âgés de moins de 18 ans.

Les règles de Schengen ou les législations nationales s'appliquent aux questions non couvertes par les dispositions de l'accord, comme la reconnaissance des documents de voyage, l'assurance médicale de voyage et les garanties relatives au retour et aux moyens de subsistance suffisants (voir I.1.2.).

Dans le droit fil de la déclaration de l'Union européenne sur les justificatifs à produire à l'appui d'une demande de visa de court séjour jointe à l'accord, «[l]'Union européenne établira une liste harmonisée des justificatifs à produire, conformément à l'article 48, paragraphe 1, point a), du code des visas, afin de veiller à ce que les demandeurs en Ukraine soient tenus de produire, en principe, les mêmes justificatifs». Les consulats des États membres, agissant dans le cadre de la coopération locale au titre de Schengen, sont invités à veiller à ce que demandeurs ukrainiens reçoivent des informations de base cohérentes et uniformes et soient tenus de fournir, en principe, les mêmes justificatifs quel que soit le consulat de l'État membre dans lequel ils introduisent leur demande.

En principe, l'original de la demande ou du document requis par l'article 4, paragraphe 1 de l'accord, sera joint à la demande de visa. Toutefois, le consulat peut commencer à traiter la demande de visa à partir de télécopies ou de copies de la demande ou du document. Le consulat peut néanmoins réclamer le document original s'il s'agit d'une première demande, et il le feradans des cas individuels en cas de doute.

Étant donné que les listes des autorités ci-dessous contiennent parfois aussi le nom de la personne qui peut signer les demandes/attestations, les autorités ukrainiennes devraient informer la coopération locale au titre de Schengen lorsque ces personnes sont remplacées.

L'article 4 de l'accord dispose:

«1. Pour les catégories suivantes de citoyens de l'Ukraine, les documents énumérés ci-après suffisent à justifier l'objet du voyage sur le territoire de l'autre partie:

a) pour les membres de délégations officielles qui, à la suite d'une invitation officielle adressée à l'Ukraine, participent à des réunions, consultations, négociations ou programmes d'échange ainsi qu'à des événements ayant lieu sur le territoire de l'un des États membres à l'initiative d'organisations intergouvernementales:

— une lettre délivrée par une autorité ukrainienne confirmant que le demandeur est membre de sa délégation se rendant sur le territoire de l'autre partie pour participer aux événements susmentionnés, accompagnée d'une copie de l'invitation officielle;»

Le nom du demandeur doit être mentionné dans la lettre délivrée par l'autorité compétente confirmant que la personne appartient à la délégation qui se rend sur le territoire de l'autre partie pour participer à une réunion officielle. Le nom du demandeur ne doit pas nécessairement être mentionné dans l'invitation officielle à la réunion, même si tel peut être le cas lorsque l'invitation officielle est adressée à une personne en particulier.

Cette disposition s'applique aux membres des délégations officielles quel que soit le passeport (de service non biométrique, ou ordinaire) dont ils sont titulaires.

«b) pour les hommes et femmes d'affaires et les représentants d'entreprises:

— une invitation écrite émanant d'une personne morale ou société hôte, ou d'un bureau ou d'une filiale de celle-ci, ou des autorités nationales ou locales d'un État membre, ou d'un comité d'organisation de foires, conférences et symposiums commerciaux et industriels tenus sur le territoire d'un État membre;»

«c) pour les chauffeurs fournissant des services de transport international de marchandises et de passagers vers le territoire des États membres dans des véhicules immatriculés en Ukraine:

— une demande écrite émanant de l'association nationale des transporteurs ukrainiens assurant des transports internationaux par route, indiquant l'objet, la durée, la ou les destinations et la fréquence des voyages;»

Les autorités compétentes qui prévoient les transports internationaux par route et sont responsables d'établir l'objet, la durée, la ou les destinations et la fréquence des voyages des chauffeurs fournissant des services de transport international de marchandises et de passagers vers le territoire des États membres dans des véhicules immatriculés en Ukraine, sont les suivantes:

1. Association des transporteurs routiers internationaux d'Ukraine (AsMAP/«АсМАП»)

   L'adresse postale de AsMAP est la suivante:

   11, Shorsa str.

   Kiev, 03150, Ukraine

   Les fonctionnaires habilités à signer les demandes sont les suivants:

   Kostiuchenko Leonid — président de l'AsMAP d'Ukraine;

   Dokil' Leonid — vice-président de l'AsMAP d'Ukraine;

   Kuchynskiy Yurii — vice-président de l'AsMAP d'Ukraine;

2. Entreprise d'État «Service de transport routier international» (SE «SIRC»)

   L'adresse postale du SE «SIRC» est la suivante:

   57, av. Nauka

   Kiev, 03083, Ukraine

   Téléphone +38 044 524 21 01

   Fax +38 044 524 00 70

   Les fonctionnaires habilités à signer les demandes sont les suivants:

   Tkachenko Anatolij — directeur du SE «SIRC»;

   Neronov Oleksandr — premier directeur adjoint du SE «SIRC».

3. L'Union ukrainienne des transports routiers et de la logistique

   L'adresse postale de l'Union ukrainienne des transports routiers et de la logistique est la suivante:

   28, Predslavinska str.

   Kiev, 03150, Ukraine

   Téléphone/Fax + 38 044 528 71 30/+ 38 044 528 71 46/+ 38 044 529 44 40

   Le fonctionnaire habilité à signer les demandes est le suivant:

   Lypovskiy Vitalij — président de l'Union

4. Association panukrainienne des transporteurs automobiles (AAAC) (Всеукраїнська асоціація автомобільних перевізників)

   L'adresse postale de l'AAAC est la suivante:

   139, Velyka Vasylkivska str.

   Kiev, 03150, Ukraine

   Téléphone/Fax +38044-538-75-05, +38044-529-25-21

   Les fonctionnaires habilités à signer les demandes sont les suivants:

   Reva Vitalii (Віталій Рева) — président de l'AAAC

   Glavatskyi Petro (Петро Главатський) — vice-président de l'AAAC

   e-mail: vaap@i.com.ua

5. Association panukrainienne des transporteurs automobiles (AAAC) (Всеукраїнська асоціація автомобільних перевізників)

   L'adresse postale de l'AAAC est la suivante:

   3, Rayisy Okipnoyi str.

   Kiev 02002, Ukraine

   Téléphone/Fax +38044-517-44-31, +38044-516-47-26

   Les fonctionnaires habilités à signer les demandes sont les suivants:

   Vakulenko Volodymyr (Вакуленко Володимир Михайлович) — vice-président de l'AAAC

6. Entreprise d'État ukrainienne «Ukrinteravtoservice» (Українське державне підприємство по обслуговуванню іноземних та вітчизняних автотранспортних засобів «Укрінтеравтосервіс»)

   L'adresse postale de l'entreprise d'État Ukrainienne «Ukrinteravtoservice»:

   57, av. Nauky

   Kiev, 03083, Ukraine

   Les fonctionnaires habilités à signer les demandes sont les suivants:

   Dobrohod Serhii (Доброход Сергій Олександрович) — directeur général de l'entreprise d'État ukrainienne «Ukrinteravtservice» (téléphone: +38 044 524-09-99; portable: +38 050 463-89-32);

   Kubalska Svitlana (Кубальська Світлана Сергіївна) — directeur général adjoint de l'entreprise d'État ukrainienne «Ukrinteravtoservice» (téléphone: +38 044 524-09-99; portable: +38 050 550-82-62);

Compte tenu des problèmes actuellement enregistrés avec cette catégorie de demandeurs de visa, le comité mixte suivra de près la mise en œuvre de cette disposition.

«d) pour le personnel de wagons, wagons frigorifiques et locomotives de trains internationaux circulant vers le territoire des États membres:

— une demande écrite émanant de la société de chemins de fer ukrainienne compétente, indiquant l'objet, la durée et la fréquence des voyages.»

L'autorité compétente dans le domaine des transports ferroviaires en Ukraine est l'administration nationale des transports ferroviaires d'Ukraine («Ukrzaliznytsia»/«Укрзалізниця»).

L'adresse postale de l'«Ukrzaliznytsia» est la suivante:

5-7 Tverskaya str.
Kiev 03680, Ukraine

Conformément à la répartition des responsabilités dans la direction de «Ukrzaliznytsia», les fonctionnaires compétents chargés de communiquer les informations relatives à l'objet, la durée et la fréquence des voyages du personnel des trains, des wagons frigorifiques et des locomotives de trains internationaux circulant vers le territoire des États membres sont les suivants:

Bolobolin Serhii (Болоболін Сергій Петрович) — premier directeur général d'Ukrzaliznytsia (téléphone: +38 044 465 00 10);

Serhiyenko Mykola (Сергієнко Микола Іванович) — premier directeur général adjoint d'Ukrzaliznytsia (téléphone: + 38 044 465 00 01);

Zhurakivskyy Vitaliy (Жураківський Віталій Олександрович) — premier directeur général adjoint d'Ukrzaliznytsia (téléphone: + 38 044 465 00 41);

Slipchenko Oleksiy (Сліпченко Олексій Леонтійович) — directeur général adjoint d'Ukrzaliznytsia (téléphone: +38 044 465 00 14);

Naumenko Petro (Науменко Петро Петрович) — directeur général adjoint d'Ukrzaliznytsia (téléphone: +38 044 465 00 12);

Chekalov Pavlo (Чекалов Павло Леонтійович) — directeur général adjoint d'Ukrzaliznytsia (téléphone: +38 044 465 00 13);

Matviiv Igor — chef du département des relations internationales d'Ukrzaliznytsia (téléphone: + 38 044 465 04 25).

«e) pour les journalistes et le personnel technique les accompagnant à titre professionnel:

— un certificat ou un autre document délivré par une organisation professionnelle ou par l'employeur du demandeur, attestant que la personne concernée est un journaliste qualifié et indiquant que le voyage a pour objet la réalisation d'un travail journalistique, ou attestant que la personne est membre du personnel technique accompagnant le journaliste à titre professionnel;»

Cette catégorie ne couvre pas les journalistes indépendants.

Le certificat ou autre document attestant que le demandeur est un journaliste qualifié et le document original établi par son employeur attestant que le voyage a pour objet la réalisation d'un travail journalistique ou que la personne est membre du personnel technique accompagnant le journaliste à titre professionnel doivent être présentés.

L'organisation professionnelle ukrainienne compétente pour attester que la personne concernée est un journaliste qualifié est la suivante:

1. Union nationale des journalistes d'Ukraine (NUJU) («Національна Спілка журналістів України», НСЖУ).

   La NUJU délivre aux employés des médias qualifiés les cartes nationales de journaliste professionnel et les cartes de presse internationales établies sur le modèle fixé par la Fédération internationale des journalistes.

   L'adresse postale de la NUJU est la suivante:

   27-a Khreschatyk str.

   Kiev, 01001, Ukraine

   La personne autorisée de la NUJU est la suivante:

   Nalyvaiko Oleg Igorovych (Наливайко Олег Ігорович) — directeur de la NUJU

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

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

2. Union des médias indépendants d'Ukraine (IMUU) («Незалежна медіа-профспілка України»).

   L'adresse postale est la suivante:

   Office 25,

   27-A, Khreshchatyk Str.

   Kiev, 01001, Ukraine

   Les personnes autorisées sont les suivantes:

   Lukanov Yurii (Луканов Юрій Вадимович) — directeur de l'IMUU

   Vynnychuk Oksana (Оксана Винничук) — secrétaire exécutif de l'IMUU

   Téléphone + 38 050 356 57 58

   Courrier électronique: secretar@profspilka.org.ua

«f) pour les personnes participant à des activités scientifiques, culturelles et artistiques, y compris des programmes d'échanges universitaires ou autres:

— une invitation écrite à participer à ces activités, émanant de l'organisation hôte;

g) pour les écoliers, les étudiants, les étudiants de troisième cycle et les enseignants accompagnateurs qui entreprennent des voyages d'études ou à but éducatif, y compris dans le cadre de programmes d'échanges ou d'activités parascolaires:

— une invitation écrite ou un certificat d'inscription délivré(e) par l'école primaire ou secondaire, l'université ou la faculté hôte, ou une carte d'étudiant, ou un certificat concernant les cours auxquels les visiteurs doivent assister;»

Une carte d'étudiant ne peut être acceptée comme justificatif de l'objet du voyage que si elle est délivrée par l'université ou la faculté hôte où les études ou la formation scolaire doivent avoir lieu.

«h) pour les participants à des manifestations sportives internationales et les personnes les accompagnant à titre professionnel:

— une invitation écrite émanant de l'organisation hôte: autorités compétentes, fédérations sportives nationales et comités nationaux olympiques des États membres;»

La liste des accompagnateurs lors de manifestations sportives internationales sera limitée aux accompagnateurs des sportifs agissant à titre professionnel: entraîneurs, masseurs, managers, personnel médical et présidents de club. Les supporters ne sont pas considérés comme des accompagnateurs.

«i) pour les participants à des programmes d'échange officiels organisés par des villes jumelées et d'autres entités municipales:

— une invitation écrite émanant du chef de l'administration/du maire de ces villes ou autres entités municipales;»

Le chef de l'administration/maire de la commune/ville ou d'une autre entité municipale, compétent pour émettre l'invitation écrite, est le chef de l'administration/maire de la commune/ville hôte dans laquelle l'activité de jumelage va avoir lieu. Cette catégorie couvre uniquement les jumelages officiels.

«j) pour les parents proches — le conjoint, les enfants (y compris adoptifs), les parents (y compris les personnes ayant la garde légale), les grands-parents et les petits-enfants — rendant visite à des ressortissants ukrainiens en séjour régulier sur le territoire des États membres ou à des citoyens de l'Union européenne résidant sur le territoire de l'État membre dont ils sont ressortissants;

— une invitation écrite émanant de la personne hôte;»

Ce point régit la situation des parents proches ukrainiens qui se rendent dans un État membre afin de rendre visite à des citoyens ukrainiens en séjour régulier dans cet État membre ou à des citoyens de l'Union européenne qui résident sur le territoire de l'État membre dont ils sont ressortissants.

L'authenticité de la signature de la personne qui invite doit être attestée par l'autorité compétente conformément à la législation nationale du pays de résidence.

Il est également nécessaire d'attester la légalité du séjour de la personne invitante, ainsi que le lien familial, en joignant, par exemple, à l'invitation écrite émanant de la personne hôte, des copies de documents témoignant de son statut, comme une photocopie du titre de séjour, et confirmant les liens familiaux.

Cette disposition s'applique également aux membres de la famille du personnel des missions diplomatiques et des consulats effectuant une visite familiale de 90 jours au maximum sur le territoire des États membres, hormis la nécessité d'attester la légalité du séjour et les liens de parenté.

Conformément à la déclaration de l'Union européenne concernant les mesures visant à faciliter la délivrance de visas pour les membres de la famille, jointe à l'accord modificatif, «[a]fin de faciliter les déplacements d'un plus grand nombre de personnes ayant des liens familiaux (notamment les frères et sœurs et leurs enfants) avec des ressortissants ukrainiens en séjour régulier sur le territoire des États membres ou des citoyens de l'Union résidant sur le territoire de l'État membre dont ils sont ressortissants, l'Union européenne invite les représentations consulaires des États membres à utiliser pleinement les possibilités actuelles offertes par le code des visas pour faciliter la délivrance de visas à cette catégorie de personnes, notamment en simplifiant les preuves documentaires exigées des demandeurs, en les exonérant des droits perçus pour le traitement des demandes et, si nécessaire, en leur délivrant des visas à entrées multiples».

«k) pour les personnes se rendant aux obsèques d'un membre de leur famille:

— un document officiel confirmant le décès, ainsi que l'existence d'un lien de parenté ou autre entre le demandeur et le défunt;»

L'accord ne précise pas le pays dont les autorités doivent délivrer le document officiel susmentionné, à savoir s'il s'agit du pays où les obsèques ont lieu ou du pays où réside la personne qui souhaite se rendre aux obsèques. Il y a lieu d'admettre que les autorités compétentes des deux pays peuvent délivrer ce document officiel.

Le document officiel susmentionné confirmant le décès ainsi que l'existence d'un lien de parenté ou autre entre le demandeur et le défunt doit être présenté; il peut s'agir, par exemple, d'un certificat de naissance ou de mariage.

«l) pour les personnes souhaitant se rendre dans un cimetière militaire ou civil:

— un document officiel confirmant l'existence et le maintien de la tombe concernée, ainsi que l'existence d'un lien de parenté ou autre entre le demandeur et le défunt.»

L'accord ne précise pas si le document officiel susvisé doit être délivré par les autorités du pays où le cimetière est situé ou par celles du pays où réside la personne qui souhaite se rendre dans ce cimetière. Il y a lieu d'admettre que les autorités compétentes des deux pays peuvent délivrer ce document officiel.

Le document officiel susmentionné confirmant l'existence et la préservation de la tombe ainsi que du lien de parenté ou d'un autre lien entre le demandeur et le défunt doit être présenté.

Conformément à la déclaration de la Communauté européenne relative à la délivrance de visas de court séjour aux fins de visites dans un cimetière militaire ou civil jointe à l'accord, en principe, les visas de court séjour pour les personnes souhaitant se rendre dans un cimetière civil ou militaire seront délivrés pour une durée de 14 jours maximum.

«m) pour les personnes en visite pour des raisons médicales et les personnes qui doivent les accompagner:

— un document officiel de l'établissement médical confirmant la nécessité d'y suivre un traitement et d'être accompagné, et la preuve de moyens financiers suffisants pour payer ce traitement médical;»

Le document officiel de l'établissement médical confirmant la nécessité d'y suivre un traitement et la preuve de moyens financiers suffisants pour payer ce traitement médical seront présentés; il devrait également confirmer la nécessité d'être accompagné.

«n) pour les représentants d'organisations de la société civile qui entreprennent des voyages à but éducatif, se rendent à des séminaires ou à des conférences, y compris dans le cadre de programmes d'échange:

— une demande écrite émanant de l'organisation hôte, une confirmation que la personne représente l'organisation de la société civile et le certificat d'établissement de l'organisation en question émanant du registre ad hoc, délivré par une autorité nationale conformément à la législation nationale;»

Le document prouvant l'enregistrement en Ukraine d'une organisation de la société civile est une lettre délivrée par le service national ukrainien d'enregistrement contenant les données issues du registre des associations publiques.

«o) pour les membres des professions libérales participant à des foires, des conférences, des symposiums et des séminaires internationaux ou à d'autres événements analogues ayant lieu sur le territoire d'un État membre:

— une demande écrite émanant de l'organisation hôte, confirmant que la personne concernée participe à la manifestation;

p) pour les représentants des communautés religieuses:

— une demande écrite émanant d'une communauté religieuse enregistrée en Ukraine, indiquant l'objet, la durée et la fréquence des voyages;»

Le document prouvant l'enregistrement en Ukraine d'une communauté religieuse est un extrait du registre national unifié des entités juridiques et des entrepreneurs individuels, contenant des informations montrant que l'organisation et la forme juridique d'une entité juridique sont celles d'une communauté religieuse.

«q) pour les participants à des programmes officiels de coopération transfrontalière de l'Union européenne, par exemple dans le cadre de l'instrument européen de voisinage et de partenariat (IEVP):

— une invitation écrite émanant de l'organisation hôte.»

Important: l'accord ne crée aucune nouvelle règle de responsabilité pour les personnes physiques ou morales dont émanent les demandes écrites. Les législations nationales et de l'Union européenne respectives s'appliquent en cas de faux.

2.2.2. *Délivrance de visas à entrées multiples*

Lorsque le demandeur de visa doit se rendre fréquemment ou régulièrement sur le territoire des États membres, un visa de court séjour sera délivré pour plusieurs visites à condition que la durée totale de celles-ci n'excède pas 90 jours par période de 180 jours.

L'article 5, paragraphe 1 de l'accord dispose:

«1. Les missions diplomatiques et les postes consulaires des États membres délivrent des visas à entrées multiples, d'une durée de validité de cinq ans, aux catégories de personnes suivantes:

a) les membres des gouvernements et parlements nationaux et régionaux, ainsi que les membres des cours constitutionnelles et suprêmes, les procureurs nationaux et régionaux et leurs adjoints, dans l'exercice de leurs fonctions, sous réserve que ces personnes ne soient pas exemptées de l'obligation de visa par le présent accord;

b) les membres permanents de délégations officielles qui, à la suite d'invitations officielles adressées à l'Ukraine, participent régulièrement à des réunions, consultations, négociations ou programmes d'échange ainsi qu'à des événements ayant lieu sur le territoire des États membres à l'initiative d'organisations intergouvernementales;

c) les conjoints, les enfants (y compris adoptifs) n'ayant pas encore atteint l'âge de 21 ans ou étant à charge et les parents (y compris les personnes ayant la garde légale) qui rendent visite à des ressortissants ukrainiens en séjour régulier sur le territoire des États membres ou à des citoyens de l'Union européenne qui résident sur le territoire de l'État membre dont ils sont ressortissants;

d) les hommes et femmes d'affaires et les représentants d'entreprises se rendant régulièrement dans les États membres;

e) les journalistes et le personnel technique les accompagnant à titre professionnel.

Par dérogation au premier alinéa, lorsque le besoin ou l'intention de voyager fréquemment ou régulièrement est manifestement limitée à une durée plus courte, la validité du visa à entrées multiples est limitée à cette durée, en particulier lorsque:

— dans le cas des personnes visées au point a), la durée de leur mandat,

— dans le cas des personnes visées au point b), la durée de validité de leur statut de membre permanent d'une délégation officielle,

— dans le cas des personnes visées au point c), la durée de validité de l'autorisation de séjour des ressortissants ukrainiens en séjour régulier dans l'Union européenne,

— dans le cas des personnes visées au point d), la durée de validité de leur statut de représentant de l'entreprise ou de leur contrat de travail,

— dans le cas des personnes visées au point e), la durée de validité de leur contrat de travail

est inférieure à cinq ans.»

Pour ces catégories de personnes, compte tenu de leur statut professionnel ou de leur lien familial avec un citoyen ukrainien en séjour régulier sur le territoire d'un État membre ou avec un citoyen de l'Union européenne résidant sur le territoire de l'État membre dont il est ressortissant, il est justifié de délivrer, en principe, un visa à entrées multiples d'une durée de validité de cinq ans. Dans la version initiale de l'accord, en n'établissant qu'une durée maximale de validité, l'expression «d'une durée de validité pouvant aller jusqu'à cinq ans» laissait aux consulats toute latitude pour décider de la durée de validité du visa. Dans le cadre de l'accord modificatif, cette latitude a disparu avec la nouvelle formulation «d'une durée de validité de cinq ans», en précisant que, dans l'hypothèse où le demandeur satisfait à toutes les exigences de l'article 5, paragraphe 1 de l'accord, «les missions diplomatiques et les postes consulaires des États membres délivrent des visas à entrées multiples, d'une durée de validité de cinq ans».

Pour les personnes relevant de l'article 5, paragraphe 1, point a) de l'accord, la confirmation de leur statut professionnel et de la durée de leur mandat devrait être apportée.

Cette disposition ne s'appliquera pas aux personnes relevant de l'article 5, paragraphe 1, point a) de l'accord, si elles sont exemptées de l'obligation de visa par l'accord, c'est-à-dire si elles sont titulaires d'un passeport diplomatique ou d'un passeport de service biométrique.

Pour les personnes relevant de l'article 5, paragraphe 1, point b), la preuve de leur statut permanent de membre de la délégation et de la nécessité qu'elles participent régulièrement à des réunions, à des consultations, à des négociations ou à des programmes d'échanges doit être fournie.

Pour les personnes relevant de l'article 5, paragraphe 1, point c), la preuve de la légalité du séjour de la personne qui invite doit être fournie (voir point II.2.2.1 ci-dessus).

Pour les personnes relevant de l'article 5, paragraphe 1, point d) et e) de l'accord, la preuve de leur statut professionnel et de la durée de leur mandat doit être fournie.

L'article 5, paragraphe 2 de l'accord dispose:

«2. Les missions diplomatiques et les postes consulaires des États membres délivrent des visas à entrées multiples d'une durée de validité d'un an aux catégories de personnes suivantes, sous réserve que, durant l'année précédant la demande, ces personnes aient obtenu au moins un visa et qu'elles l'aient utilisé dans le respect de la législation régissant l'entrée et le séjour sur le territoire de l'État hôte:

a) les conducteurs fournissant des services de transport international de marchandises et de passagers vers le territoire des États membres dans des véhicules immatriculés en Ukraine;

b) le personnel de wagons, wagons frigorifiques et locomotives de trains internationaux circulant vers le territoire des États membres;

c) les personnes participant à des activités scientifiques, culturelles et artistiques, y compris des programmes d'échange universitaires ou autres, qui se rendent régulièrement dans les États membres;

d) les participants à des manifestations sportives internationales et les personnes les accompagnant à titre professionnel;

e) les participants à des programmes d'échange officiels organisés par des villes jumelées et d'autres entités municipales;

f) les représentants d'organisations de la société civile se rendant régulièrement dans les États membres dans un but éducatif ou participant à des séminaires ou à des conférences, y compris dans le cadre de programmes d'échange;

g) les participants à des programmes officiels de coopération transfrontalière de l'Union européenne, par exemple dans le cadre de l'instrument européen de voisinage et de partenariat (IEVP);

h) les étudiants, y compris de troisième cycle, qui entreprennent régulièrement des voyages d'étude ou à but éducatif, y compris dans le cadre de programmes d'échange;

i) les représentants de communautés religieuses;

j) les membres de professions libérales participant à des foires, à des conférences, à des symposiums et à des séminaires internationaux ou à d'autres événements similaires ayant lieu sur le territoire des États membres;

k) les personnes en visite régulière pour des raisons médicales et celles qui doivent les accompagner.

Par dérogation au premier alinéa, lorsque le besoin ou l'intention de voyager fréquemment ou régulièrement est manifestement limitée à une durée plus courte, la validité du visa à entrées multiples est limitée à cette durée.»

Dans la version initiale de l'accord, en n'établissant qu'une durée maximale de validité, l'expression «d'une durée de validité pouvant aller jusqu'à un an» laissait aux consulats toute latitude pour décider de la durée de validité du visa. Dans le cadre de l'accord modificatif, cette latitude a disparu avec le nouveau libellé «d'une durée de validité d'un an», disposant que si le demandeur remplit l'ensemble des conditions de l'article 5, paragraphe 2 de l'accord, «les missions diplomatiques et les postes consulaires des États membres délivrent des visas à entrées multiples d'une durée de validité d'un an». Il y a lieu de noter que des visas à entrées multiples valables un an seront délivrés aux catégories susmentionnées sous réserve qu'au cours de l'année précédente (12 mois), le demandeur de visa ait obtenu au moins un visa Schengen, qu'il l'ait utilisé conformément à la législation régissant l'entrée et le séjour dans l'État ou les États hôtes (en n'ayant pas dépassé la durée de séjour autorisée, par exemple) et qu'il ait des raisons de demander un visa à entrées multiples. Le visa Schengen obtenu au cours de l'année précédente peut avoir été délivré par un autre État Schengen que celui dans lequel le demandeur a demandé le nouveau visa. Lorsque la délivrance d'un visa valable un an ne se justifie pas (par exemple, si la durée du programme d'échange est inférieure à un an ou que la personne n'a pas à voyager fréquemment ou régulièrement pendant toute une année), la validité du visa sera inférieure à une année, pourvu que les autres conditions de délivrance du visa soient remplies.

L'article 5, paragraphes 3 et 4 de l'accord dispose:

«3. Les missions diplomatiques et les postes consulaires des États membres délivrent des visas à entrées multiples d'une durée de validité minimale de deux ans et maximale de cinq ans aux catégories de personnes visées au paragraphe 2, sous réserve que, durant les deux années précédant la demande, ces personnes aient utilisé leur visa à entrées multiples d'une durée d'un an dans le respect de la législation régissant l'entrée et le séjour sur le territoire de l'État hôte, sauf lorsque le besoin ou l'intention de voyager fréquemment ou régulièrement sont manifestement limités à une durée plus courte, auquel cas la validité du visa à entrées multiples est limitée à cette durée.

4. La durée totale du séjour des personnes visées aux paragraphes 1 à 3 du présent article sur le territoire des États membres ne peut excéder 90 jours par période de 180 jours.».

Des visas à entrées multiples valables de deux à cinq ans seront délivrés aux catégories mentionnées à l'article 5, paragraphe 2 de l'accord, sous réserve qu'au cours des deux années précédentes, ces personnes aient utilisé leur visa Schengen à entrées multiples d'une durée d'un an dans le respect de la législation régissant l'entrée et le séjour sur le territoire du ou des États hôtes et que le besoin de voyager fréquemment ou régulièrement ne soit pas manifestement limité à une durée plus courte. Il y a lieu de noter qu'un visa d'une durée de validité de deux à cinq ans ne sera délivré que si le demandeur de visa a obtenu deux visas d'une durée de validité d'un an — et non d'une durée inférieure — au cours des deux années précédentes et s'il les a utilisés dans le respect de la législation régissant l'entrée et le séjour sur le territoire du ou des États hôtes. Les missions diplomatiques et les postes consulaires des États membres détermineront, sur la base d'une évaluation de chaque demande de visa, la durée de validité de ces visas — à savoir entre deux et cinq ans.

En ce qui concerne la définition des critères visés à l'article 5, paragraphe 2 de l'accord («sous réserve que […] elles aient des raisons de solliciter un visa à entrées multiples»), et à l'article 5, paragraphe 3 de l'accord («sous réserve que […] leurs raisons de solliciter un visa à entrées multiples soient toujours valables»), les critères fixés à l'article 24, paragraphe 2, du code des visas pour la délivrance de ce type de visa sont applicables, à savoir, la personne a besoin de se rendre fréquemment dans un ou plusieurs États membres, par exemple dans le cadre de voyages d'affaires.

Il n'y a pas d'obligation de délivrer un visa à entrées multiples si le demandeur n'a pas utilisé un visa antérieur. Néanmoins, un tel visa peut être délivré si la non-utilisation du visa précédent est due à des circonstances indépendantes de la volonté du demandeur; par exemple, un chauffeur de camion longuement absent de son travail pour cause de maladie.

En ce qui concerne les documents attestant l'objet du voyage pour la délivrance de visas à entrées multiples pour les catégories visées à l'article 5 de l'accord, voir II.2.2.1.

2.2.3. *Titulaires de passeports diplomatiques et de service.*

L'article 10 de l'accord dispose:

> «1. Les citoyens de l'Ukraine titulaires de passeports diplomatiques en cours de validité peuvent entrer sur le territoire des États membres, le quitter et le traverser sans visa.
>
> 2. Les ressortissants ukrainiens qui sont titulaires de passeports de service biométriques en cours de validité peuvent entrer sur le territoire des États membres, le quitter et le traverser sans visa.
>
> 3. Les personnes mentionnées aux paragraphes 1 et 2 du présent article peuvent séjourner sur le territoire des États membres pour une durée n'excédant pas 90 jours par période de 180 jours.»

Les accords ou arrangements bilatéraux existants prévoyant l'exemption de l'obligation de visa pour les titulaires de passeports de service non biométriques continueront à s'appliquer, à moins d'être dénoncés ou suspendus (voir I 1.6).

L'affectation de diplomates dans les États membres n'est pas régie par l'accord. La procédure d'accréditation habituelle s'applique.

III. STATISTIQUES

Afin de permettre au comité mixte institué d'assurer un contrôle efficace de l'accord, les missions diplomatiques et les postes consulaires des États membres doivent fournir à la Commission, tous les six mois, des statistiques, avec ventilation mensuelle, concernant notamment, si possible:

— les types de visas délivrés aux différentes catégories de personnes couvertes par l'accord,

— le nombre de refus de visas pour les différentes catégories de personnes couvertes par l'accord,

— pour chaque catégorie de personnes, le pourcentage de demandeurs convoqués à un entretien personnel,

— les visas à entrées multiples valables cinq ans délivrés à des ressortissants ukrainiens (par pays),

— les pourcentages de visas délivrés gratuitement aux différentes catégories de personnes couvertes par l'accord.

DÉCISION (PESC) 2015/439 DU CONSEIL

du 16 mars 2015

prorogeant le mandat du représentant spécial de l'Union européenne pour le Sahel

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur l'Union européenne, et notamment son article 33 et son article 31, paragraphe 2,

vu la proposition du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité,

considérant ce qui suit:

(1) Le 18 mars 2013, le Conseil a adopté la décision 2013/133/PESC [1] portant nomination de M. Michel Dominique REVEYRAND — DE MENTHON en tant que représentant spécial de l'Union européenne (RSUE) pour le Sahel. Le mandat du RSUE a été prorogé par la décision 2014/130/PESC du Conseil [2] et vient à expiration le 28 février 2015.

(2) Il y a lieu de proroger le mandat du RSUE pour une nouvelle période de huit mois.

(3) Le RSUE exécutera son mandat dans le contexte d'une situation susceptible de se détériorer et de compromettre la réalisation des objectifs de l'action extérieure de l'Union énoncés à l'article 21 du traité,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Représentant spécial de l'Union européenne

1. Le mandat de M. Michel Dominique REVEYRAND — DE MENTHON en tant que RSUE pour le Sahel est prorogé jusqu'au 31 octobre 2015. Le mandat du RSUE peut être écourté si le Conseil en décide ainsi, sur proposition du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité (HR).

2. Aux fins du mandat du RSUE, le Sahel est défini comme comprenant l'objectif principal de la stratégie de l'Union européenne pour la sécurité et le développement au Sahel (ci-après dénommée «stratégie»), à savoir le Burkina Faso, le Tchad, le Mali, la Mauritanie et le Niger. Pour les questions ayant des implications plus vastes au niveau de la région, le RSUE traite avec d'autres pays et avec des entités régionales ou internationales au-delà du Sahel mais aussi de l'Afrique de l'Ouest et du Golfe de Guinée, s'il y a lieu.

3. Compte tenu de la nécessité d'une approche régionale des défis interdépendants auxquels est confrontée la région, le RSUE pour le Sahel travaille en consultation étroite avec les autres RSUE concernés, y compris le RSUE pour la région du Sud de la Méditerranée, le RSUE pour les droits de l'homme et le RSUE auprès de l'Union africaine.

Article 2

Objectifs généraux

1. Le mandat du RSUE est fondé sur les objectifs généraux poursuivis par l'Union à l'égard du Sahel, qui consistent à contribuer activement aux efforts régionaux et internationaux visant à instaurer durablement paix, sécurité et développement dans la région. Le RSUE s'attache en outre à améliorer la qualité, l'intensité et l'incidence de l'action pluridimensionnelle que mène l'Union au Sahel.

2. Le RSUE contribue à élaborer et à mettre en œuvre l'approche de l'Union qui englobe tous les aspects de l'action de l'Union, notamment sur les plans politique, de la sécurité et du développement, y compris la stratégie, et qui coordonne tous les instruments pertinents des actions de l'Union.

3. La priorité est accordée, dans un premier temps, au Mali et à sa stabilisation à long terme ainsi qu'aux dimensions régionales du conflit qui y sévit.

---

[1] Décision 2013/133/PESC du Conseil du 18 mars 2013 portant nomination du représentant spécial de l'Union européenne pour le Sahel (JO L 75 du 19.3.2013, p. 29).

[2] Décision 2014/130/PESC du Conseil du 10 mars 2014 prorogeant le mandat du représentant spécial de l'Union européenne pour le Sahel (JO L 71 du 12.3.2014, p. 14).

4. Pour ce qui est du Mali, les objectifs généraux de l'Union consistent à encourager, grâce à une utilisation coordonnée et effective de tous ses instruments, le retour de ce pays et de sa population sur la voie de la paix, de la réconciliation, de la sécurité et du développement. Il convient également de prêter l'attention requise au Burkina Faso et au Niger, notamment dans la perspective des élections qui se tiendront dans ces pays.

Article 3

Mandat

1. Afin d'atteindre les objectifs généraux de l'Union à l'égard du Sahel, le mandat du RSUE consiste à:

a) contribuer activement à la mise en œuvre, la coordination et la poursuite de l'approche globale de l'Union à l'égard de la crise régionale, sur la base de sa stratégie, en vue d'améliorer la cohérence et l'efficacité globales des activités de l'Union au Sahel, en particulier au Mali;

b) dialoguer avec tous les acteurs de la région, les gouvernements, les autorités régionales, les organisations régionales et internationales, la société civile et la diaspora, en vue de favoriser la réalisation des objectifs de l'Union, et contribuer à une meilleure compréhension du rôle de l'Union au Sahel;

c) représenter l'Union dans les enceintes régionales et internationales compétentes, y compris le groupe de soutien et de suivi sur la situation au Mali, et assurer la visibilité du soutien qu'apporte l'Union à la gestion de la crise et à la prévention des conflits, y compris la mission militaire de l'Union européenne visant à contribuer à la formation des forces armées maliennes (EUTM Mali) et la mission PSDC de l'Union européenne au Niger (EUCAP Sahel Niger);

d) entretenir une coopération étroite avec les Nations unies, en particulier avec le représentant spécial du secrétaire général pour l'Afrique de l'Ouest et le représentant spécial du secrétaire général pour le Mali, l'Union africaine (UA), en particulier le haut représentant de l'UA pour le Mali et le Sahel, la Communauté économique des États de l'Afrique de l'Ouest (Cedeao) et d'autres acteurs nationaux, régionaux et internationaux de premier plan, y compris les autres envoyés spéciaux pour le Sahel ainsi qu'avec les entités pertinentes dans la zone du Maghreb;

e) suivre attentivement les questions relevant de la dimension régionale et transfrontalière de la crise, parmi lesquelles le terrorisme, le crime organisé, le trafic d'armes, le trafic d'êtres humains, le trafic de drogues, les flux de réfugiés et de migrants et les flux financiers correspondants; en étroite coopération avec le coordinateur de l'Union européenne pour la lutte contre le terrorisme, contribuer au développement de la stratégie de l'Union européenne visant à lutter contre le terrorisme;

f) maintenir des contacts politiques réguliers de haut niveau avec les pays de la région touchés par le terrorisme et le crime international afin de mettre en œuvre une approche cohérente et globale et de faire en sorte que l'Union joue un rôle déterminant dans les efforts internationaux de lutte contre le terrorisme et le crime international. Il s'agit pour l'Union d'apporter un soutien actif à la mise en place de capacités régionales dans le secteur de la sécurité et de veiller à ce que les causes profondes du terrorisme et du crime international au Sahel soient abordées de manière appropriée;

g) suivre attentivement les conséquences des crises humanitaires dans la région sur les plans politique et de la sécurité;

h) en ce qui concerne le Mali, contribuer aux efforts déployés aux niveaux régional et international pour faciliter la résolution de la crise au Mali, en particulier un retour complet à la normale sur le plan constitutionnel et à la gouvernance dans tout le territoire et un dialogue national ouvert à tous et crédible conduisant à un règlement politique durable;

i) promouvoir le renforcement des institutions, la réforme du secteur de la sécurité et la consolidation de la paix et la réconciliation à long terme au Mali;

j) contribuer à la mise en œuvre dans la région de la politique de l'Union en matière de droits de l'homme en coopération avec le RSUE pour les droits de l'homme, y compris les orientations de l'Union européenne en matière de droits de l'homme, en particulier les orientations de l'Union européenne sur les enfants face aux conflits armés ainsi que sur les violences contre les femmes et la lutte contre toutes les formes de discrimination à leur encontre, et la politique de l'Union à l'égard des femmes, de la paix et de la sécurité, notamment en suivant et en relatant les développements intervenus ainsi qu'en formulant des recommandations à cet égard, et maintenir des contacts réguliers avec les autorités pertinentes au Mali et dans la région, le bureau du procureur de la Cour pénale internationale, le Haut-Commissariat des Nations unies aux droits de l'homme, les défenseurs des droits de l'homme et les observateurs dans la région;

k) contrôler le respect des résolutions pertinentes du Conseil de sécurité des Nations unies, en particulier les résolutions 2056 (2012), 2071 (2012), 2085 (2012) et 2100 (2013) du Conseil de sécurité des Nations unies, et en rendre compte.

2. Aux fins de l'exécution de son mandat, le RSUE s'emploie notamment à:

a) rendre des avis et présenter des rapports sur la formulation des positions de l'Union dans les enceintes régionales et internationales, le cas échéant, afin d'encourager et de soutenir de manière proactive l'approche globale de l'Union à l'égard de la crise au Sahel;

b) garder une vue d'ensemble de toutes les activités de l'Union et coopérer étroitement avec les délégations de l'Union concernées.

Article 4

Exécution du mandat

1. Le RSUE est responsable de l'exécution de son mandat et agit sous l'autorité du HR.

2. Le comité politique et de sécurité (COPS) maintient un lien privilégié avec le RSUE et constitue le principal point de contact de ce dernier avec le Conseil. Le COPS fournit des orientations stratégiques et politiques au RSUE dans le cadre de son mandat, sans préjudice des responsabilités du HR.

3. Le RSUE travaille en coordination étroite avec le Service européen pour l'action extérieure (SEAE) et ses départements pertinents, en particulier le coordinateur pour le Sahel.

Article 5

Financement

1. Le montant de référence financière destiné à couvrir les dépenses liées au mandat du RSUE pendant la période allant du 1er mars 2015 au 31 octobre 2015 est de 900 000 EUR.

2. Les dépenses sont gérées conformément aux procédures et règles applicables au budget général de l'Union.

3. La gestion des dépenses fait l'objet d'un contrat entre le RSUE et la Commission. Le RSUE répond de toutes les dépenses devant la Commission.

Article 6

Constitution et composition de l'équipe

1. Dans les limites de son mandat et des moyens financiers y afférents mis à disposition, le RSUE est responsable de la constitution de son équipe. Celle-ci dispose des compétences spécifiques requises par le mandat en ce qui concerne certaines questions de politique et de sécurité. Le RSUE informe rapidement le Conseil et la Commission de la composition de son équipe.

2. Les États membres, les institutions de l'Union et le SEAE peuvent proposer le détachement d'agents appelés à travailler avec le RSUE. Les rémunérations du personnel détaché auprès du RSUE sont prises en charge par l'État membre concerné, l'institution de l'Union concernée ou le SEAE. Les experts détachés par les États membres auprès des institutions de l'Union ou du SEAE peuvent également être affectés auprès du RSUE. Le personnel international sous contrat doit avoir la nationalité d'un État membre.

3. L'ensemble du personnel détaché reste sous l'autorité administrative de l'État membre d'origine, de l'institution de l'Union qui le détache ou du SEAE et il exerce ses fonctions et agit dans l'intérêt du mandat du RSUE.

4. Le personnel du RSUE est installé au même endroit que les services concernés du SEAE ou que les délégations de l'Union afin d'assurer la cohérence de leurs activités respectives.

Article 7

Privilèges et immunités du RSUE et de son personnel

Les privilèges, immunités et autres garanties nécessaires à l'exécution et au bon déroulement de la mission du RSUE et des membres de son personnel sont convenus d'un commun accord avec les pays hôtes, selon le cas. Les États membres et le SEAE apportent tout le soutien nécessaire à cet effet.

Article 8

Sécurité des informations classifiées de l'Union européenne

Le RSUE et les membres de son équipe respectent les principes et les normes minimales de sécurité définis par la décision 2013/488/UE du Conseil ([1]).

([1]) Décision 2013/488/UE du Conseil du 23 septembre 2013 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 274 du 15.10.2013, p. 1).

Article 9

Accès aux informations et soutien logistique

1. Les États membres, la Commission, le SEAE et le secrétariat général du Conseil veillent à ce que le RSUE puisse accéder à toutes les informations pertinentes.

2. Les délégations de l'Union et/ou les États membres, selon le cas, apportent un soutien logistique dans la région.

Article 10

Sécurité

Conformément à la politique de l'Union concernant la sécurité du personnel déployé à titre opérationnel à l'extérieur de l'Union en vertu du titre V du traité, le RSUE prend toutes les mesures raisonnablement applicables, conformément à son mandat et en fonction de la situation en matière de sécurité sur le territoire relevant de sa compétence, pour assurer la sécurité de l'ensemble du personnel placé sous son autorité directe, en particulier:

a) en établissant un plan de sécurité spécifique, sur la base des orientations du SEAE, prévoyant notamment des mesures de sécurité physiques, organisationnelles et procédurales spécifiques, régissant la gestion des déplacements en toute sécurité du personnel vers la zone géographique et à l'intérieur de celle-ci, ainsi que la gestion des incidents de sécurité, et comprenant un plan pour les situations de crise et un plan d'évacuation pour la mission;

b) en veillant à ce que l'ensemble du personnel déployé en dehors de l'Union soit couvert par une assurance «haut risque» en adéquation avec la situation existant dans la zone géographique;

c) en veillant à ce que tous les membres de l'équipe déployés en dehors de l'Union, y compris le personnel recruté sur place, aient suivi une formation appropriée en matière de sécurité avant ou dès leur arrivée dans la zone géographique, sur la base des niveaux de risque attribués à la zone en question;

d) en veillant à ce que l'ensemble des recommandations formulées d'un commun accord à la suite des évaluations de sécurité effectuées régulièrement soient mises en œuvre et en présentant au Conseil, au HR et à la Commission des rapports écrits sur la mise en œuvre de ces recommandations ainsi que sur d'autres questions relatives à la sécurité dans le cadre du rapport de situation et le rapport sur l'exécution du mandat.

Article 11

Rapports

1. Le RSUE fait rapport régulièrement au HR et au COPS. Si nécessaire, il rend également compte aux groupes de travail du Conseil. Des rapports sont régulièrement diffusés par l'intermédiaire du réseau COREU. Le RSUE peut transmettre des rapports au Conseil des affaires étrangères. Conformément à l'article 36 du traité, le RSUE peut être associé à l'information du Parlement européen.

2. Le RSUE établit des rapports sur la meilleure manière de mener à bien les initiatives de l'Union, telles que la contribution de l'Union aux réformes, y compris les aspects politiques des projets de développement pertinents de l'Union, en coordination avec les délégations de l'Union dans la région.

Article 12

Coordination avec d'autres acteurs de l'Union

1. Dans le cadre de la stratégie, le RSUE contribue à l'unité, à la cohérence et à l'efficacité de l'action politique et diplomatique de l'Union et aide à assurer que tous les instruments de l'Union et toutes les actions des États membres sont utilisés de façon cohérente, en vue d'atteindre les objectifs généraux de l'Union.

2. Les activités du RSUE sont coordonnées avec celles des délégations de l'Union et de la Commission, ainsi qu'avec celles des autres RSUE actifs dans la région. Le RSUE informe régulièrement les missions des États membres et les délégations de l'Union dans la région.

3. Sur le terrain, des contacts étroits sont maintenus avec les chefs des délégations de l'Union et les chefs de mission des États membres. Le RSUE, en étroite coopération avec les délégations concernées de l'Union, formule, au niveau local, des orientations politiques à l'intention des chefs des missions de l'EUCAP Sahel Niger et de l'EUCAP Sahel Mali et du commandant de la mission EUTM Mali. Le RSUE, le commandant de la mission EUTM Mali et le commandant d'opération civile de l'EUCAP Sahel Niger et de l'EUCAP Sahel Mali se consultent en fonction des besoins.

Article 13

Évaluation

La mise en œuvre de la présente décision et sa cohérence avec d'autres contributions de l'Union en faveur de la région font l'objet d'une évaluation régulière. Le RSUE présente au Conseil, au HR et à la Commission, à la fin du mois d'août 2015, un rapport complet sur l'exécution du mandat.

Article 14

Entrée en vigueur

La présente décision entre en vigueur le jour de son adoption.

Elle est applicable à partir du 1er mars 2015.

Fait à Bruxelles, le 16 mars 2015.

Par le Conseil
Le président
F. MOGHERINI

DÉCISION (PESC) 2015/440 DU CONSEIL

du 16 mars 2015

prorogeant le mandat du représentant spécial de l'Union européenne pour la Corne de l'Afrique

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur l'Union européenne, et notamment son article 33 et son article 31, paragraphe 2,

vu la proposition du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité,

considérant ce qui suit:

(1) Le 8 décembre 2011, le Conseil a adopté la décision 2011/819/PESC [1] portant nomination de M. Alexander RONDOS en tant que représentant spécial de l'Union européenne (RSUE) pour la Corne de l'Afrique. Le mandat du RSUE doit expirer le 28 février 2015.

(2) Il y a lieu de proroger le mandat du RSUE jusqu'au 31 octobre 2015.

(3) Le RSUE exécutera son mandat dans le contexte d'une situation susceptible de se détériorer et de compromettre la réalisation des objectifs de l'action extérieure de l'Union énoncés à l'article 21 du traité,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Représentant spécial de l'Union européenne

Le mandat de M. Alexander RONDOS en tant que RSUE pour la Corne de l'Afrique est prorogé jusqu'au 31 octobre 2015. Le Conseil peut décider de mettre fin plus tôt au mandat du RSUE, sur la base d'une évaluation du Comité politique et de sécurité (COPS) et sur proposition du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité (HR).

Aux fins du mandat du RSUE, la Corne de l'Afrique est définie comme étant la région comprenant la République de Djibouti, l'État d'Érythrée, la République démocratique fédérale d'Éthiopie, la République du Kenya, la République fédérale de Somalie, la République du Soudan, la République du Soudan du Sud et la République d'Ouganda. Pour les questions ayant des implications plus vastes au niveau de la région, le RSUE traite avec des pays et entités régionales au-delà de la Corne de l'Afrique, s'il y a lieu.

Article 2

Objectifs généraux

1. Le mandat du RSUE est fondé sur les objectifs généraux poursuivis par l'Union à l'égard de la Corne de l'Afrique, conformément au cadre stratégique adopté le 14 novembre 2011 et aux conclusions du Conseil sur la question, qui consistent à contribuer activement aux efforts régionaux et internationaux visant à instaurer une coexistence pacifique, une paix durable, la sécurité et le développement dans les pays de la région et entre eux. Le RSUE s'attache en outre à améliorer la qualité, l'intensité, l'incidence et la visibilité de l'action pluridimensionnelle que mène l'Union dans la Corne de l'Afrique.

2. Les objectifs généraux sont notamment les suivants:

a) poursuivre la stabilisation de la Somalie, sous l'angle en particulier de la dimension régionale;

b) assurer la coexistence pacifique du Soudan et du Soudan du Sud, ceux-ci constituant deux États viables et prospères, dotés de structures politiques solides et responsables;

c) résoudre les conflits actuels et éviter les conflits potentiels à l'intérieur des pays de la région ou entre eux;

d) soutenir la coopération politique, économique et en matière de sécurité au niveau régional.

[1] Décision 2011/819/PESC du Conseil du 8 décembre 2011 portant nomination du représentant spécial de l'Union européenne pour la Corne de l'Afrique (JO L 327 du 9.12.2011, p. 62).

Article 3

Mandat

1. Afin d'atteindre les objectifs de l'Union à l'égard de la Corne de l'Afrique, le mandat du RSUE consiste:

a) à dialoguer avec toutes les parties prenantes concernées de la région, les gouvernements, les autorités régionales, les organisations internationales et régionales, la société civile et les diasporas, en vue de favoriser la réalisation des objectifs de l'Union, et contribuer à une meilleure compréhension du rôle de l'Union dans la région;

b) à représenter l'Union dans les instances internationales compétentes, le cas échéant, et à assurer la visibilité du soutien qu'apporte l'Union à la gestion des crises et à la prévention et la résolution des conflits;

c) à encourager et à appuyer une coopération politique et en matière de sécurité et une intégration économique effectives dans la région grâce au partenariat qui existe entre l'Union, d'une part, et l'Union africaine (UA) et les organisations régionales, notamment l'Autorité intergouvernementale pour le développement (IGAD), d'autre part;

d) à suivre l'évolution politique dans la région et à contribuer à l'élaboration de la politique de l'Union à l'égard de la région, notamment en ce qui concerne la Somalie, le Soudan, le Soudan du Sud, le différend frontalier entre l'Éthiopie et l'Érythrée et la mise en œuvre de l'accord d'Alger, l'initiative du bassin du Nil et d'autres problèmes qui se posent dans la région et qui ont une incidence sur sa sécurité, sa stabilité et sa prospérité;

e) en ce qui concerne la Somalie, en agissant en étroite coordination avec l'envoyé spécial de l'Union européenne pour la Somalie et les partenaires régionaux et internationaux concernés, y compris le représentant spécial du secrétaire général des Nations unies pour la Somalie et l'UA, à contribuer activement aux actions et initiatives qui sont de nature à consolider la stabilisation et à déboucher sur des arrangements pour la période suivant la transition en Somalie, l'accent étant mis sur la promotion d'une approche internationale coordonnée et cohérente à l'égard de la Somalie, la mise en place de relations de bon voisinage et le soutien au développement du secteur de la sécurité en Somalie, y compris dans le cadre de la mission militaire de l'Union européenne visant à contribuer à la formation des forces de sécurité somaliennes (EUTM Somalia), de la force navale placée sous la direction de l'Union européenne (EUNAVFOR Atalanta), de la mission de l'Union européenne visant au renforcement des capacités maritimes régionales dans la Corne de l'Afrique (EUCAP Nestor) et du soutien constant de l'Union en faveur de la Mission de l'Union africaine en Somalie (AMISOM), en étroite coopération avec les États membres;

f) en ce qui concerne le Soudan et le Soudan du Sud, à contribuer, en agissant en étroite coopération avec les chefs des délégations de l'Union concernés, à la cohérence et à l'efficacité de la politique de l'Union à l'égard du Soudan et du Soudan du Sud et à soutenir leur coexistence pacifique, notamment par la mise en œuvre des accords d'Addis-Abeba et la résolution des questions en suspens suivant l'accord de paix global, y compris Abyei, par la définition de solutions politiques aux conflits en cours, en particulier au Darfour, au Kordofan méridional et au Nil Bleu, par la mise en place d'institutions au Soudan du Sud et par la réconciliation nationale. À cet égard, le RSUE contribue à une approche internationale cohérente, en coopération étroite avec l'UA, en particulier son groupe de mise en œuvre de haut niveau sur le Soudan, les Nations unies et d'autres parties prenantes régionales et internationales de premier plan;

g) à suivre attentivement les défis transfrontières qui touchent la Corne de l'Afrique, y compris le terrorisme, la radicalisation, la sécurité maritime et la piraterie, la criminalité organisée, le trafic d'armes, les flux de réfugiés et de migrants et les conséquences des crises humanitaires sur les plans politique et de la sécurité;

h) à œuvrer en faveur de l'accès de l'aide humanitaire dans l'ensemble de la région;

i) à contribuer à la mise en œuvre de la décision 2011/168/PESC du Conseil [1] et de la politique de l'Union en matière de droits de l'homme, en coopération avec le RSUE pour les droits de l'homme, y compris les orientations de l'Union européenne en matière de droits de l'homme, en particulier les orientations de l'Union européenne sur les enfants face aux conflits armés ainsi que les lignes directrices de l'Union européenne sur les violences contre les femmes et les filles et la lutte contre toutes les formes de discrimination à leur encontre, et de la politique de l'Union concernant la résolution 1325 (2000) du Conseil de sécurité des Nations unies, notamment en suivant et en relatant les évolutions intervenues ainsi qu'en formulant des recommandations à cet égard.

2. Aux fins de l'exécution de son mandat, le RSUE s'emploie notamment:

a) à formuler des avis et à présenter des rapports sur la définition des positions de l'Union dans les enceintes internationales, selon le cas, afin de promouvoir de manière proactive l'approche globale de l'Union à l'égard de la Corne de l'Afrique;

b) à garder une vue d'ensemble de toutes les activités de l'Union.

[1] Décision 2011/168/PESC du Conseil du 21 mars 2011 concernant la Cour pénale internationale et abrogeant la position commune 2003/444/PESC (JO L 76 du 22.3.2011, p. 56).

Article 4

Exécution du mandat

1. Le RSUE est responsable de l'exécution de son mandat et agit sous l'autorité du HR.

2. Le COPS maintient un lien privilégié avec le RSUE et constitue le principal point de contact du RSUE avec le Conseil. Le COPS fournit des orientations stratégiques et politiques au RSUE dans le cadre de son mandat, sans préjudice des compétences du HR.

3. Le RSUE travaille en coordination étroite avec le Service européen pour l'action extérieure (SEAE) et ses services compétents, les délégations de l'Union dans la région et la Commission.

Article 5

Financement

1. Le montant de référence financière destiné à couvrir les dépenses liées au mandat du RSUE pour la période du 1er mars 2015 au 31 octobre 2015 est de 1 770 000 EUR.

2. Les dépenses sont gérées conformément aux procédures et règles applicables au budget général de l'Union.

3. La gestion des dépenses fait l'objet d'un contrat entre le RSUE et la Commission. Le RSUE répond devant la Commission de toutes les dépenses.

Article 6

Constitution et composition de l'équipe

1. Dans les limites de son mandat et des moyens financiers y afférents mis à disposition, le RSUE est responsable de la constitution de son équipe. L'équipe possède les compétences requises en ce qui concerne certaines questions de politique et de sécurité spécifiques, selon les besoins du mandat. Le RSUE informe rapidement et régulièrement le Conseil et la Commission de la composition de son équipe.

2. Les États membres, les institutions de l'Union et le SEAE peuvent proposer le détachement d'agents appelés à travailler avec le RSUE. Les rémunérations de ce personnel détaché sont prises en charge, respectivement, par l'État membre, l'institution de l'Union concernée ou le SEAE. Les experts détachés par les États membres auprès des institutions de l'Union ou du SEAE peuvent également être affectés auprès du RSUE. Le personnel international sous contrat a la nationalité d'un État membre.

3. L'ensemble du personnel détaché reste sous l'autorité administrative de l'État membre qui le détache, de l'institution de l'Union qui le détache ou du SEAE et il exerce ses fonctions et agit dans l'intérêt du mandat du RSUE.

4. Le personnel du RSUE est installé au même endroit que les services concernés du SEAE ou que les délégations de l'Union afin de contribuer à la cohérence de leurs activités respectives.

Article 7

Privilèges et immunités du RSUE et de son personnel

Les privilèges, immunités et autres garanties nécessaires à l'exécution et au bon déroulement de la mission du RSUE et des membres de son personnel sont définis d'un commun accord avec les pays hôtes, selon le cas. Les États membres et le SEAE apportent tout le soutien nécessaire à cet effet.

Article 8

Sécurité des informations classifiées de l'Union européenne

Le RSUE et les membres de son équipe respectent les principes et les normes minimales de sécurité établis par la décision 2013/488/UE du Conseil ([1]).

([1]) Décision 2013/488/UE du Conseil du 23 septembre 2013 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 274 du 15.10.2013, p. 1).

Article 9

Accès aux informations et soutien logistique

1. Les États membres, la Commission, le SEAE et le secrétariat général du Conseil veillent à ce que le RSUE puisse accéder à toutes les informations pertinentes.

2. Les délégations de l'Union dans la région et les États membres, selon le cas, apportent un soutien logistique dans la région.

Article 10

Sécurité

Conformément à la politique de l'Union concernant la sécurité du personnel déployé à titre opérationnel à l'extérieur de l'Union en vertu du titre V du traité, le RSUE prend toutes les mesures raisonnablement applicables, conformément à son mandat et en fonction de la situation en matière de sécurité sur le territoire relevant de sa compétence, pour assurer la sécurité de l'ensemble du personnel placé sous son autorité directe, notamment:

a) en établissant, sur la base des orientations du SEAE, un plan de sécurité spécifique à la mission, prévoyant des mesures de sécurité physique, organisationnelles et procédurales propres à la mission, régissant la gestion des déplacements en toute sécurité du personnel vers la zone de la mission et à l'intérieur de celle-ci, ainsi que la gestion des incidents de sécurité, et comprenant un plan pour les situations de crise et un plan d'évacuation de la mission;

b) en veillant à ce que l'ensemble du personnel déployé en dehors de l'Union soit couvert par une assurance «haut risque» en adéquation avec la situation existant dans la zone de la mission;

c) en veillant à ce que tous les membres de son équipe déployés en dehors de l'Union, y compris le personnel recruté sur place, aient suivi une formation appropriée en matière de sécurité avant ou dès leur arrivée dans la zone de la mission, sur la base des niveaux de risque attribués à la zone en question par le SEAE;

d) en veillant à ce que l'ensemble des recommandations formulées d'un commun accord à la suite des évaluations de sécurité effectuées régulièrement soient mises en œuvre, et en présentant au Conseil, au HR et à la Commission des rapports écrits sur la mise en œuvre de ces recommandations ainsi que sur d'autres questions relatives à la sécurité dans le cadre du rapport de situation et du rapport sur l'exécution du mandat.

Article 11

Rapports

1. Le RSUE fait rapport régulièrement, oralement et par écrit, au HR et au COPS. Si nécessaire, il rend également compte aux groupes de travail du Conseil. Des rapports sont régulièrement diffusés par l'intermédiaire du réseau COREU. Le RSUE peut transmettre des rapports au Conseil des affaires étrangères. Conformément à l'article 36 du traité, le RSUE peut être associé à l'information du Parlement européen.

2. Le RSUE établit des rapports sur la meilleure manière de mener à bien les initiatives de l'Union, telles que la contribution de l'Union aux réformes, y compris les aspects politiques des projets de développement pertinents de l'Union, en coordination avec les délégations de l'Union dans la région.

Article 12

Coordination

1. Le RSUE contribue à l'unité, à la cohérence et à l'efficacité des actions de l'Union et veille à ce que l'ensemble des instruments de l'Union et des actions des États membres soient utilisés de manière cohérente en vue d'atteindre les objectifs généraux de l'Union. Les activités du RSUE sont coordonnées avec celles des délégations de l'Union et de la Commission. Le RSUE informe régulièrement les missions des États membres et les délégations de l'Union dans la région.

2. Sur le terrain, des contacts étroits sont maintenus avec les chefs des délégations de l'Union et les chefs des missions des États membres. Ceux-ci mettent tout en œuvre pour assister le RSUE dans l'exécution de son mandat. Le RSUE, agissant en étroite coordination avec les délégations concernées de l'Union, formule, sur place, des orientations politiques à l'intention du commandant de la force EUNAVFOR Atalanta, du commandant de la mission de l'Union européenne EUTM Somalia et du chef de la mission EUCAP Nestor. Le RSUE, les commandants des opérations de l'Union européenne et le commandant d'opération civile se concertent en fonction des besoins.

3. Le RSUE coopère étroitement avec les autorités des pays concernés, les Nations unies, l'UA, l'IGAD, d'autres acteurs nationaux, régionaux et internationaux, ainsi qu'avec la société civile de la région.

Article 13

Évaluation

La mise en œuvre de la présente décision et sa cohérence avec d'autres contributions de l'Union en faveur de la région font l'objet d'une évaluation régulière. Le RSUE présente au Conseil, au HR et à la Commission un rapport complet sur l'exécution de son mandat d'ici au 31 août 2015.

Article 14

Entrée en vigueur

La présente décision entre en vigueur le jour de son adoption.

Elle est applicable à partir du 1er mars 2015.

Fait à Bruxelles, le 16 mars 2015.

Par le Conseil
Le président
F. MOGHERINI

DÉCISION (PESC) 2015/441 DU CONSEIL

du 16 mars 2015

modifiant et prorogeant la décision 2010/96/PESC relative à une mission militaire de l'Union européenne visant à contribuer à la formation des forces de sécurité somaliennes

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur l'Union européenne, et notamment son article 42, paragraphe 4, et son article 43, paragraphe 2,

vu la proposition du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité,

considérant ce qui suit:

(1) Le 15 février 2010, le Conseil a adopté la décision 2010/96/PESC ([1]). Le mandat de la mission militaire de l'Union se termine le 31 mars 2015.

(2) La conférence de Bruxelles sur la Somalie, qui a eu lieu le 16 septembre 2013, a jeté les bases du Pacte pour la Somalie et a été l'amorce, grâce au groupe de travail «New Deal», d'un mécanisme de coordination et de prise en main par la Somalie.

(3) Lors de la réunion internationale qui s'est tenue le 18 septembre 2014 à Londres, à l'invitation conjointe du Royaume-Uni et de la Somalie, le gouvernement fédéral a exposé la «voie vers le développement» de l'armée nationale somalienne à l'horizon 2019, conçue par le ministère de la défense, ainsi que ses besoins immédiats.

(4) À la suite du réexamen stratégique qui a eu lieu en octobre 2014, le mandat de la mission militaire de l'Union devrait être prorogée jusqu'au 31 décembre 2016.

(5) Conformément à l'article 5 du protocole n° 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'élaboration et à la mise en œuvre des décisions et actions de l'Union qui ont des implications en matière de défense. Le Danemark ne participe pas à la mise en œuvre de la présente décision et ne contribue donc pas au financement de la présente mission.

(6) Il convient de proroger à nouveau le mandat de la mission militaire de l'Union et de l'adapter,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

La décision 2010/96/PESC est modifiée comme suit:

1) À l'article 1er, le paragraphe 2 est remplacé par le texte suivant:

«2. Aux fins de la réalisation des objectifs énoncés au paragraphe 1, la mission militaire de l'Union est déployée en Somalie afin de contribuer au renforcement des institutions dans le secteur de la défense en dispensant des conseils stratégiques et d'apporter un soutien direct à l'armée nationale somalienne grâce à des activités de formation, de conseil et d'encadrement. La mission militaire de l'Union est également prête à fournir, dans les limites de ses moyens et de ses capacités, un appui aux autres acteurs de l'Union dans la mise en œuvre de leurs mandats respectifs dans le domaine de la sécurité et de la défense en Somalie.»

2) L'article 3 est remplacé par le texte suivant:

«*Article 3*

Désignation de l'état-major de la mission

1. L'état-major de la mission est situé en Somalie, à Mogadiscio, à l'aéroport international. Il remplit à la fois les fonctions d'état-major d'opération et d'état-major de force.

2. L'état-major de la mission comprend un bureau de liaison et de soutien à Nairobi et une cellule de soutien à Bruxelles.»

([1]) Décision 2010/96/PESC du Conseil du 15 février 2010 relative à une mission militaire de l'Union européenne visant à contribuer à la formation des forces de sécurité somaliennes (JO L 44 du 19.2.2010, p. 16).

3) À l'article 7, le paragraphe 4 est remplacé par le texte suivant:

«4. La mission militaire de l'Union opère, dans les limites de ses moyens et de ses capacités, en étroite coopération avec les autres acteurs de la communauté internationale présents dans la région, notamment les Nations unies et l'AMISOM, conformément aux exigences convenues du gouvernement fédéral de la Somalie.»

4) À l'article 10, le paragraphe suivant est ajouté:

«5. Le montant de référence financière pour les coûts communs de la mission militaire de l'Union pour la période allant du 1er avril 2015 au 31 décembre 2016 s'élève à 17 507 399 EUR. Le pourcentage de ce montant de référence visé à l'article 25, paragraphe 1, d'ATHENA est fixé à 30 % et le pourcentage de l'engagement visé à l'article 32, paragraphe 3, d'ATHENA est fixé à 90 %.»

5) L'article suivant est inséré:

«*Article 10 ter*

Cellule de projets

1. La mission militaire de l'Union dispose d'une cellule de projets pour recenser et mettre en œuvre les projets qui correspondent aux objectifs de la mission et contribuent à l'exécution du mandat; ces projets seront financés par les États membres ou des États tiers.

2. Sous réserve du paragraphe 3, le commandant de la mission de l'Union est autorisé à recourir à des contributions financières des États membres ou d'États tiers pour la mise en œuvre de projets identifiés comme complétant de manière cohérente d'autres actions de la mission militaire de l'Union. Dans ce cas, le commandant de la mission de l'Union conclut un accord avec ces États, portant notamment sur les procédures particulières de traitement des plaintes émanant de tiers et concernant des dommages résultant d'actes ou d'omissions du commandant de la mission de l'Union dans l'utilisation des fonds fournis par ces États.

En aucun cas les États contributeurs ne peuvent rendre l'Union ou le HR responsable d'actes ou d'omissions du commandant de la mission de l'Union dans l'utilisation des fonds de ces États.

3. Le COPS marque son accord sur l'acceptation d'une contribution financière d'États tiers à la cellule de projets.»

6) L'article 11 est modifié comme suit:

a) au paragraphe 1, la phrase introductive est remplacée par «Le HR est autorisé à communiquer aux États tiers associés à la présente décision, le cas échéant et selon les besoins de la mission, des informations classifiées de l'Union européenne établies aux fins de la mission, conformément à la décision 2013/488/UE du Conseil (*):

(*) Décision 2013/488/UE du Conseil du 23 septembre 2013 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 274 du 15.10.2013, p. 1).»

b) au paragraphes 2 et 3, les termes «décision 2011/292/UE» sont remplacés par les termes «décision 2013/488/UE»;

7) À l'article 12, les paragraphes 2 et 3 sont remplacés par le texte suivant:

«2. Le mandat de la mission militaire de l'Union prend fin le 31 décembre 2016.

3. La présente décision est abrogée à compter de la date de fermeture de l'état-major de la mission de l'Union, du bureau de liaison et de soutien de Nairobi et de la cellule de soutien de Bruxelles, conformément aux plans approuvés pour la fin de la mission militaire de l'Union, et sans préjudice des procédures concernant la vérification et la reddition des comptes de la mission militaire de l'Union, établies dans Athena.»

Article 2

La présente décision entre en vigueur le jour de son adoption.

Elle est applicable à partir du 1er avril 2015.

Fait à Bruxelles, le 16 mars 2015.

Par le Conseil

Le président

F. MOGHERINI

DÉCISION (PESC) 2015/442 DU CONSEIL

du 16 mars 2015

relative au lancement de la mission de conseil militaire PSDC de l'Union européenne en République centrafricaine (EUMAM RCA) et modifiant la décision (PESC) 2015/78

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur l'Union européenne, et notamment son article 42, paragraphe 4, et son article 43, paragraphe 2,

vu la décision (PESC) 2015/78 du Conseil du 19 janvier 2015 relative à une mission de conseil militaire PSDC de l'Union européenne en République centrafricaine (EUMAM RCA) [1], et notamment son article 4,

vu la proposition du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité,

considérant ce qui suit:

(1) Le 19 janvier 2015, le Conseil a adopté la décision (PESC) 2015/78.

(2) Le 9 février 2015, le Conseil a approuvé les règles d'engagement de l'EUMAM RCA.

(3) Le 6 mars 2015, le Conseil a approuvé le plan de mission de l'EUMAM RCA.

(4) Le 11 mars 2015, le Comité politique et de sécurité a accueilli favorablement la lettre du commandant de la mission relative à la recommandation de lancer l'EUMAM RCA et le calendrier envisagé pour la déclaration de la capacité opérationnelle initiale de l'EUMAM RCA,

(5) L'EUMAM RCA devrait être lancée le 16 mars 2015.

(6) Conformément à l'article 5 du protocole n° 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'élaboration et à la mise en œuvre des décisions et actions de l'Union qui ont des implications en matière de défense. En conséquence, le Danemark ne participe pas à la mise en œuvre de la présente décision et ne contribue donc pas au financement de la présente mission,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

La mission de conseil militaire PSDC de l'Union européenne en République centrafricaine (EUMAM RCA) est lancée le 16 mars 2015.

Article 2

Le commandant de la mission de l'Union EUMAM RCA est autorisé à lancer l'exécution de la mission avec effet immédiat.

Article 3

L'article 4, paragraphe 2 de la décision (PESC) 2015/78 est remplacé par le texte suivant:

«2. L'EUMAM RCA est lancée par décision du Conseil à la date recommandée par le commandant de mission, à la suite de l'approbation du plan de mission et, si nécessaire, de règles d'engagement complémentaires.»

[1] JO L 13 du 20.1.2015, p. 8.

Article 4

La présente décision entre en vigueur le jour de son adoption.

Fait à Bruxelles, le 16 mars 2015.

Par le Conseil
Le président
F. MOGHERINI

DÉCISION (UE, Euratom) 2015/443 DE LA COMMISSION

du 13 mars 2015

relative à la sécurité au sein de la Commission

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 249,

vu le traité instituant la Communauté européenne de l'énergie atomique,

vu le protocole n° 7 sur les privilèges et immunités de l'Union européenne annexé aux traités, et notamment son article 18,

considérant ce qui suit:

(1) L'objectif de la sécurité au sein de la Commission est de permettre à la Commission d'exercer ses activités dans un environnement sûr en adoptant une approche cohérente et intégrée en matière de sécurité, qui assure un niveau de protection adéquat pour les personnes, les biens et les informations, proportionnel aux risques identifiés, ainsi qu'une sécurité efficace et bien adaptée.

(2) À l'instar d'autres institutions internationales, la Commission est confrontée à des menaces et des défis majeurs dans le domaine de la sécurité, en particulier en ce qui concerne le terrorisme, les cyberattaques et l'espionnage politique et commercial.

(3) La Commission européenne a signé des accords en matière de sécurité pour ses principaux sites avec les gouvernements belge, luxembourgeois et italien ([1]). Ces textes confirment que la Commission est responsable de sa propre sécurité.

(4) Dans le but d'assurer la sécurité des personnes, des biens et des informations, la Commission peut être amenée à prendre des mesures dans des domaines protégés par des droits fondamentaux inscrits dans la Charte des droits fondamentaux et dans la Convention européenne des droits de l'homme, et tels que reconnus par la Cour de justice de l'Union européenne.

(5) Par conséquent, toute mesure devrait être justifiée par l'importance de l'intérêt qu'elle vise à protéger, être proportionnée et garantir le respect total des droits fondamentaux, notamment le droit à la vie privée et à la protection des données.

(6) Au sein d'un système engagé à respecter l'État de droit et les droits fondamentaux, la Commission doit s'efforcer d'atteindre un niveau adéquat de sécurité pour son personnel, ses biens et ses informations, qui lui permette d'exercer ses activités sans pour autant limiter les droits fondamentaux au-delà du strict nécessaire.

(7) La sécurité au sein de la Commission est fondée sur les principes de légalité, de transparence, de proportionnalité et de responsabilité.

(8) Les membres du personnel mandatés pour prendre des mesures de sécurité ne doivent subir aucun préjudice du fait de leurs actions, sauf s'ils agissent en dehors de leur mandat ou en violation de la loi; à cet égard, la présente décision doit donc être considérée comme une instruction de service au sens du statut.

(9) La Commission prend des initiatives appropriées pour promouvoir et renforcer sa culture de la sécurité, en assurant une sécurité plus efficace, en améliorant sa gouvernance en matière de sécurité, en élargissant et en intensifiant les réseaux et la coopération avec les autorités compétentes à l'échelon international, européen et national, ainsi qu'en améliorant le suivi et le contrôle de la mise en œuvre des mesures de sécurité.

(10) La mise en place du Service européen pour l'action extérieure (SEAE) en tant qu'organe de l'Union fonctionnant de manière autonome a eu un impact significatif sur les intérêts de la Commission en matière de sécurité et requiert donc que des règles et des procédures relatives à la coopération en ce qui concerne la sûreté et la sécurité soient établies entre le SEAE et la Commission, en particulier au regard du respect des responsabilités de la Commission en termes de devoir de diligence à l'égard du personnel de la Commission au sein des délégations de l'Union.

([1]) Voir «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» du 31 décembre 2004, «Accord de sécurité signé entre la Commission et le gouvernement luxembourgeois» du 20 janvier 2007, et «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» du 22 juillet 1959.

(11) La politique de sécurité de la Commission devrait être appliquée d'une manière cohérente par rapport aux processus et procédures internes susceptibles d'impliquer un élément de sécurité. Il s'agit notamment de la gestion de la continuité des opérations, qui vise à préserver les fonctions critiques de la Commission en cas d'interruption des activités, et du système ARGUS pour la coordination de crise multisectorielle.

(12) Nonobstant les mesures déjà en place au moment de l'adoption de la présente décision et notifiées au Contrôleur européen de la protection des données ([1]), toute mesure prise en vertu de la présente décision et impliquant le traitement de données à caractère personnel est soumise aux modalités d'application conformes à l'article 21, qui prévoient des garanties appropriées pour les personnes concernées.

(13) En conséquence, il est nécessaire que la Commission réexamine, mette à jour et consolide la base réglementaire existante en matière de sécurité au sein de la Commission.

(14) Il convient dès lors d'abroger la décision C(94) 2129 de la Commission ([2]),

A ADOPTÉ LA PRÉSENTE DÉCISION:

CHAPITRE 1

DISPOSITIONS GÉNÉRALES

Article premier

Définitions

Aux fins de la présente décision, on entend par:

1) «biens», tous les biens et possessions meubles et immeubles de la Commission;

2) «service de la Commission», l'une des directions générales ou l'un des services de la Commission ou l'un des cabinets des membres de la Commission;

3) «système d'information et de communication» ou «SIC», tout système permettant le traitement d'informations sous forme électronique, avec l'ensemble des moyens nécessaires pour le faire fonctionner, y compris l'infrastructure, l'organisation, le personnel et les ressources d'information;

4) «contrôle des risques», toute mesure de sécurité raisonnablement susceptible d'assurer le contrôle efficace d'un risque de sécurité, par des moyens visant à prévenir, atténuer, éviter ou transférer le risque;

5) «situation de crise», toute circonstance, événement, incident ou urgence (ou une succession ou combinaison de ces facteurs) représentant une menace majeure ou immédiate pour la sécurité de la Commission, quelle qu'en soit l'origine;

6) «donnée», une information revêtant une forme qui lui permet d'être communiquée, enregistrée ou traitée;

7) «membre de la Commission chargé de la sécurité», un membre de la Commission sous l'autorité duquel est placée la direction générale des ressources humaines et de la sécurité;

8) «données à caractère personnel», les données à caractère personnel telles que définies à l'article 2, point a), du règlement (CE) n° 45/2001 du Parlement européen et du Conseil ([3]);

9) «locaux», tous les biens et possessions immeubles et assimilés de la Commission;

10) «prévention du risque», toute mesure de sécurité raisonnablement susceptible d'empêcher, retarder ou faire cesser un risque de sécurité;

11) «risque de sécurité», la combinaison entre le niveau de la menace, le niveau de vulnérabilité et l'impact possible d'un événement;

12) «sécurité au sein de la Commission», la sécurité des personnes, des biens et des informations au sein de la Commission, en particulier l'intégrité physique des personnes et des biens, l'intégrité, la confidentialité et la disponibilité des informations et des systèmes d'information et de communication, ainsi que le fonctionnement sans entrave des activités de la Commission;

([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]) Décision C(94) 2129 de la Commission du 8 septembre 1994 relative aux tâches du bureau de sécurité.

([3]) Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

13) «mesure de sécurité», toute mesure prise conformément à la présente décision aux fins du contrôle des risques de sécurité;

14) «statut», le statut des fonctionnaires de l'Union européenne énoncé dans le règlement (CEE, Euratom, CECA) n° 259/68 du Conseil ([1]) et ses actes modificatifs;

15) «menace pour la sécurité», tout événement ou agent raisonnablement susceptible de nuire à la sécurité s'il ne fait pas l'objet d'une riposte et d'un contrôle;

16) «menace immédiate pour la sécurité», une menace pour la sécurité qui survient sans avertissement préalable ou dans un délai extrêmement bref après un tel avertissement;

17) «menace majeure pour la sécurité», une menace pour la sécurité raisonnablement susceptible de provoquer la mort, des blessures ou des préjudices graves et des dommages importants aux biens, de compromettre des informations très sensibles ou de provoquer l'interruption des systèmes informatiques ou des capacités de fonctionnement essentielles de la Commission;

18) «vulnérabilité», toute faiblesse de quelque nature que ce soit raisonnablement susceptible de nuire à la sécurité de la Commission si une ou plusieurs menaces en tirent parti pour se concrétiser.

Article 2

Objet

1. La présente décision définit les objectifs, les principes de base, l'organisation et les responsabilités en matière de sécurité au sein de la Commission.

2. La présente décision s'applique à tous les services de la Commission et dans l'ensemble des locaux de la Commission. Le personnel de la Commission travaillant dans les délégations de l'Union est soumis aux règles de sécurité applicables au Service européen pour l'action extérieure ([2]).

3. Nonobstant toute indication spécifique concernant des groupes particuliers de personnel, la présente décision s'applique aux membres de la Commission, au personnel de la Commission couvert par le statut et par le régime applicable aux autres agents de l'Union européenne, aux experts nationaux détachés auprès de la Commission (END), aux prestataires de services et à leur personnel, aux stagiaires et à toute personne ayant accès aux bâtiments et autres propriétés de la Commission, ou à des informations gérées par la Commission.

4. Les dispositions de la présente décision s'appliquent sans préjudice des décisions de la Commission 2002/47/CE, CECA, Euratom ([3]) et 2004/563/CE, Euratom ([4]), ainsi que des décisions de la Commission C(2006) 1623 ([5]) et C(2006) 3602 ([6]).

CHAPITRE 2

PRINCIPES

Article 3

Principes relatifs à la sécurité au sein de la Commission

1. Dans le cadre de la mise en œuvre de la présente décision, la Commission se conforme aux traités et notamment à la Charte des droits fondamentaux ainsi qu'au protocole n° 7 sur les privilèges et immunités de l'Union européenne, aux textes visés au considérant 2, à toutes les règles du droit national applicables et aux termes de la présente décision. Si nécessaire, une note de sécurité au sens de l'article 21, paragraphe 2, fournissant des orientations à cet égard, sera publiée.

2. La sécurité au sein de la Commission est fondée sur les principes de légalité, de transparence, de proportionnalité et de responsabilité.

3. Par légalité, on entend la nécessité de maintenir strictement dans le cadre juridique l'exécution de la présente décision, ainsi que la nécessité de se conformer aux exigences légales.

([1]) Règlement (CEE, Euratom, CECA) n° 259/68 du Conseil du 29 février 1968 fixant le statut des fonctionnaires des Communautés européennes ainsi que le régime applicable aux autres agents de ces Communautés, et instituant des mesures particulières temporairement applicables aux fonctionnaires de la Commission (régime applicable aux autres agents) (JO L 56 du 4.3.1968, p. 1).

([2]) Décision de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité 2013/C 190/01 du 19 avril 2013 relative aux règles de sécurité applicables au Service européen pour l'action extérieure (JO C 190 du 29.6.2013, p. 1).

([3]) Décision 2002/47/CE, CECA, Euratom de la Commission du 23 janvier 2002 modifiant son règlement intérieur (JO L 21 du 24.1.2002, p. 23), ajoutant en annexe les dispositions concernant l'administration des documents.

([4]) Décision 2004/563/CE, Euratom de la Commission du 7 juillet 2004 modifiant son règlement intérieur (JO L 251 du 27.7.2004, p. 9), ajoutant en annexe les dispositions concernant les documents électroniques et numérisés.

([5]) Décision C(2006) 1623 de la Commission du 21 avril 2006 établissant une politique harmonisée en matière de santé et de sécurité au travail pour l'ensemble du personnel de la Commission européenne.

([6]) Décision C(2006) 3602 de la Commission du 16 août 2006 relative à la sécurité des systèmes d'information utilisés par les services de la Commission.

4. Toute mesure de sécurité doit être prise ouvertement, sauf si cela est raisonnablement susceptible de nuire à son effet. Les personnes concernées par une mesure de sécurité sont informées au préalable des motifs et de l'impact de la mesure, sauf si la divulgation d'une telle information est raisonnablement susceptible de nuire à l'effet de la mesure. Dans ce cas, la personne concernée par la mesure de sécurité est informée une fois que le risque de nuire à l'effet de la mesure de sécurité est éliminé.

5. Les services de la Commission veillent à ce que les questions de sécurité soient prises en compte dès le début de l'élaboration et de la mise en œuvre des politiques, décisions, programmes, projets et activités de la Commission dont ils ont la charge. Pour ce faire, ils font appel à la direction générale des ressources humaines et de la sécurité de manière générale et au responsable de la sécurité des systèmes d'information de la Commission pour ce qui concerne les systèmes informatiques, et ce dès les premières étapes de préparation.

6. Le cas échéant, la Commission s'efforce de coopérer avec les autorités compétentes de l'État hôte, des autres États membres et des autres institutions, agences ou organes de l'Union européenne, lorsque cela est possible, en tenant compte des mesures prises ou prévues par ces autorités pour lutter contre le risque de sécurité en question.

Article 4

Obligation de conformité

1. La conformité à la présente décision et à ses modalités d'application, ainsi qu'aux mesures de sécurité et aux instructions données par le personnel mandaté, est obligatoire.

2. Le non-respect des règles de sécurité est passible d'une sanction disciplinaire conformément aux traités et au statut, de sanctions contractuelles et/ou de poursuites judiciaires en vertu du droit national.

CHAPITRE 3

ASSURER LA SÉCURITÉ

Article 5

Personnel mandaté

1. Seul le personnel autorisé sur la base d'un mandat nominatif attribué par le directeur général des ressources humaines et de la sécurité, compte tenu de ses obligations actuelles, peut être habilité à prendre une ou plusieurs des mesures suivantes:

1) port d'arme de défense;

2) réalisation des enquêtes de sécurité visées à l'article 13;

3) adoption des mesures de sécurité visées à l'article 12, comme indiqué dans le mandat.

2. La durée des mandats visés au paragraphe 1 n'excède pas la période durant laquelle la personne concernée occupe le poste ou la fonction pour lequel le mandat a été attribué. Les mandats sont attribués conformément aux dispositions applicables définies à l'article 3, paragraphe 1.

3. En ce qui concerne le personnel mandaté, la présente décision constitue une instruction de service au sens de l'article 21 du statut.

Article 6

Dispositions générales concernant les mesures de sécurité

1. Lorsqu'elle prend des mesures de sécurité, la Commission veille notamment, autant qu'il est raisonnablement possible, à:

a) demander uniquement l'aide ou l'assistance de l'État concerné, à condition que cet État soit un État membre de l'Union européenne ou, sinon, un État partie à la Convention européenne des droits de l'homme, ou qu'il garantisse des droits au moins équivalents aux droits garantis par ladite convention;

b) transférer des informations concernant un individu exclusivement à des destinataires, autres que les institutions et organes de l'Union, qui ne sont pas soumis à la législation nationale adoptée en application de la directive 95/46/CE du Parlement européen et du Conseil ([1]), conformément à l'article 9 du règlement (CE) n° 45/2001;

([1]) Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31).

c) lorsqu'un individu représente une menace pour la sécurité, toute mesure de sécurité vise cet individu et ce dernier peut être contraint d'en supporter les coûts. De telles mesures de sécurité peuvent viser d'autres individus uniquement si une menace immédiate ou majeure pour la sécurité doit être contrôlée et que les conditions suivantes sont réunies:

   a) les mesures envisagées à l'égard de l'individu représentant la menace pour la sécurité ne peuvent pas être prises ou ne seront probablement pas efficaces;

   b) la Commission ne peut pas contrôler la menace pour la sécurité par ses propres moyens ou ne peut le faire en temps opportun;

   c) la mesure ne représente pas un danger disproportionné pour l'autre individu et ses droits.

2. La direction de la sécurité de la direction générale des ressources humaines et de la sécurité dresse une liste des mesures de sécurité susceptibles de requérir l'ordonnance d'un juge conformément aux lois et règlements des États membres accueillant les locaux de la Commission.

3. La direction de la sécurité de la direction générale des ressources humaines et de la sécurité peut s'adresser à un contractant pour effectuer des tâches en relation avec la sécurité, sous la direction et la supervision de la direction de la sécurité.

Article 7

Mesures de sécurité concernant les personnes

1. Un niveau de protection adéquat est accordé aux personnes dans les locaux de la Commission, en tenant compte des exigences en matière de sûreté et de sécurité.

2. En cas de risque majeur de sécurité, la direction générale des ressources humaines et de la sécurité fournit une protection rapprochée aux membres de la Commission ou à d'autres membres du personnel lorsqu'une évaluation de la menace indique qu'une telle protection est nécessaire pour assurer leur sécurité.

3. En cas de risque majeur de sécurité, la Commission peut ordonner l'évacuation de ses locaux.

4. Les victimes d'accidents ou d'attaques à l'intérieur des locaux de la Commission bénéficient d'une assistance.

5. Afin de prévenir et contrôler les risques de sécurité, le personnel mandaté peut effectuer une vérification des antécédents des personnes entrant dans le champ d'application de la présente décision, de manière à déterminer si l'octroi à ces personnes de l'accès aux locaux ou à des informations de la Commission représente une menace pour la sécurité. À cette fin, et conformément au règlement (CE) n° 45/2001 ainsi qu'aux dispositions visées à l'article 3, paragraphe 1, le personnel mandaté concerné peut:

a) utiliser toutes les sources d'information dont dispose la Commission, en tenant compte de la fiabilité de la source d'information;

b) accéder au fichier du personnel ou aux données détenues par la Commission concernant les personnes qu'elle emploie ou envisage d'employer, ou pour le personnel des contractants lorsque cela est dûment justifié.

Article 8

Mesures de sécurité concernant la sécurité physique et les biens

1. La sécurité des biens est assurée en appliquant des mesures physiques et techniques de protection appropriées et les procédures correspondantes, ci-après désignées par le terme de «sécurité physique», créant ainsi un système à plusieurs niveaux.

2. Des mesures peuvent être adoptées en vertu du présent article afin de protéger des personnes ou des informations au sein de la Commission, ainsi que pour protéger des biens.

3. Les objectifs de la sécurité physique sont les suivants:

— prévenir les actes de violence à l'égard des membres de la Commission ou de personnes entrant dans le champ d'application de la présente décision,

— prévenir les actes d'espionnage et les écoutes concernant des informations sensibles ou classifiées,

— prévenir le vol, les actes de vandalisme et de sabotage ou d'autres actions violentes visant à détériorer ou détruire les bâtiments et les biens de la Commission,

— permettre les enquêtes et les investigations concernant les incidents de sécurité, notamment par des vérifications des registres de contrôle des entrées et sorties, de la vidéosurveillance (télévision en circuit fermé), des enregistrements d'appels téléphoniques et autres données similaires visées ci-après à l'article 22, paragraphe 2, et d'autres sources d'information.

4. La sécurité physique inclut:

— une politique d'accès applicable à toute personne ou tout véhicule demandant l'accès aux locaux de la Commission, y compris les parcs de stationnement,

— un système de contrôle des accès composé de gardiens, d'équipements et mesures techniques, de systèmes d'information ou d'une combinaison de tous ces éléments.

5. Les actions suivantes peuvent être entreprises pour assurer la sécurité physique:

— enregistrement des entrées et des sorties de personnes, véhicules, biens et équipements dans et hors des locaux de la Commission,

— contrôles d'identité dans les locaux,

— inspection des véhicules, biens et équipements par des moyens visuels ou techniques,

— interdiction de l'accès de personnes, véhicules et biens non autorisés aux locaux de la Commission.

Article 9

Mesures de sécurité concernant les informations

1. La sécurité des informations concerne toutes les informations traitées par la Commission.

2. Quelle qu'en soit la forme, la sécurité des informations vise un équilibre entre d'une part les principes de transparence, de proportionnalité, de responsabilité et d'efficacité et d'autre part la nécessité de protéger les informations contre les accès, utilisation, divulgation, modification ou destruction non autorisés.

3. La sécurité des informations vise à protéger la confidentialité, l'intégrité et la disponibilité de ces informations.

4. Par conséquent, des processus de gestion des risques sont utilisés pour classifier les informations et élaborer des mesures, procédures et normes de sécurité proportionnées, y compris des mesures d'atténuation.

5. Ces principes généraux à la base de la sécurité des informations s'appliquent notamment en ce qui concerne:

a) les «informations classifiées de l'Union européenne» (ci-après «ICUE»), à savoir toute information ou tout matériel identifié comme tel par la classification de sécurité de l'Union européenne, dont la divulgation non autorisée pourrait porter atteinte à des degrés divers aux intérêts de l'Union européenne, ou à ceux d'un ou de plusieurs de ses États membres;

b) les «informations sensibles non classifiées», à savoir toute information ou tout matériel que la Commission est tenue de protéger en raison d'obligations légales énoncées dans les traités ou des actes adoptés en application de ces derniers, et/ou en raison de leur sensibilité. Les informations sensibles non classifiées incluent, mais sans s'y limiter, toute information ou tout matériel couvert par l'obligation de secret professionnel, telle que visée à l'article 339 du TFUE, toute information couverte par les intérêts protégés à l'article 4 du règlement (CE) nº 1049/2001 du Parlement européen et du Conseil ([1]), lu conjointement avec la jurisprudence correspondante de la Cour de justice de l'Union européenne, ou les données à caractère personnel entrant dans le champ d'application du règlement (CE) nº 45/2001.

6. Les informations sensibles non classifiées sont soumises à des règles concernant leur gestion et leur conservation. Elles ne sont communiquées qu'aux personnes ayant un «besoin d'en connaître». Si cela est jugé nécessaire pour la protection effective de leur confidentialité, elles sont identifiées au moyen d'un marquage de sécurité, avec des instructions de traitement correspondantes approuvées par le directeur général des ressources humaines et de la sécurité. Lorsqu'elles sont traitées ou conservées dans les systèmes d'information et de communication, ces informations sont également protégées en conformité avec la décision C(2006) 3602, ainsi que ses modalités d'application et les normes correspondantes.

7. Toute personne responsable de la compromission ou de la perte d'ICUE ou d'informations sensibles non classifiées, identifiées comme telles dans les règles concernant leur traitement et leur conservation, est passible de sanctions disciplinaires conformément au statut. De telles sanctions disciplinaires s'appliquent sans préjudice d'autres actions en justice ou procédures pénales intentées par les autorités nationales compétentes des États membres conformément à leurs lois et règlements, et des moyens de recours contractuels.

([1]) Règlement (CE) nº 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (JO L 145 du 31.5.2001, p. 43).

Article 10

Mesures de sécurité concernant les systèmes d'information et de communication

1. L'ensemble des systèmes d'information et de communication (SIC) utilisés par la Commission sont conformes à la politique de sécurité des systèmes d'information de la Commission, telle qu'énoncée dans la décision C(2006) 3602, ses modalités d'application et les normes de sécurité correspondantes.

2. Les services de la Commission qui détiennent, gèrent ou utilisent des CIS ne peuvent autoriser d'autres institutions, agences, organes ou autres organismes de l'Union à accéder à ces systèmes que si ces derniers peuvent fournir une assurance raisonnable que leurs systèmes informatiques sont protégés à un niveau équivalent à la politique de sécurité des systèmes d'information de la Commission, telle qu'énoncée dans la décision C(2006) 3602, ses modalités d'application et les normes de sécurité correspondantes. La Commission assure le suivi du respect de ces dispositions et, en cas de grave manquement ou de persistance du manquement, elle est habilitée à interdire l'accès.

Article 11

Analyse criminalistique concernant la cybersécurité

La direction générale des ressources humaines et de la sécurité est notamment chargée de mener les analyses techniques et criminalistiques en coopération avec les services compétents de la Commission dans le but de contribuer aux enquêtes de sécurité visées à l'article 13, en lien avec le contre-espionnage, les fuites de données, les cyberattaques et la sécurité des systèmes d'information.

Article 12

Mesures de sécurité concernant les personnes et les objets

1. Afin d'assurer la sécurité au sein de la Commission et de prévenir et contrôler les risques, le personnel mandaté conformément à l'article 5 peut, dans le respect des principes énoncés à l'article 3, prendre entre autres une ou plusieurs des mesures de sécurité suivantes:

a) sécurisation des scènes et des preuves, notamment registres de contrôle des entrées et sorties et images de vidéosurveillance, en cas d'incidents ou de comportements susceptibles de donner lieu à des procédures administratives, disciplinaires, civiles ou pénales;

b) mesures limitées concernant des personnes présentant une menace pour la sécurité, notamment l'ordre de quitter les locaux de la Commission, l'escorte de personnes hors des locaux de la Commission, l'interdiction de l'accès aux locaux de la Commission pour une certaine durée, déterminée selon des critères à définir dans les modalités d'application;

c) mesures limitées concernant les objets présentant une menace pour la sécurité, notamment le retrait, la saisie et l'élimination de ces objets;

d) fouille des locaux de la Commission, y compris des bureaux situés dans ces locaux;

e) examen des SIC et des données échangées sur les équipements, téléphones et appareils de télécommunications, des registres, des comptes utilisateurs, etc.;

f) autres mesures de sécurité spécifiques ayant un effet similaire destinées à prévenir ou contrôler des risques de sécurité, notamment dans le contexte des droits de la Commission en tant que bailleur ou en tant qu'employeur conformément au droit national applicable.

2. Dans des circonstances exceptionnelles, les membres du personnel de la direction de la sécurité de la direction générale des ressources humaines et de la sécurité, mandatés conformément à l'article 5, peuvent prendre les éventuelles mesures urgentes qui s'imposent, en stricte conformité avec les principes énoncés à l'article 3. Dès que possible après avoir pris ces mesures, ils informent le directeur de la direction de la sécurité, qui demande le mandat correspondant auprès du directeur général des ressources humaines et de la sécurité, confirmant les mesures prises et autorisant toute action supplémentaire nécessaire; le cas échéant, il prend contact avec les autorités nationales compétentes.

3. Les mesures de sécurité visées dans le présent article sont documentées au moment où elles sont prises ou, en cas de risque immédiat ou de situation de crise, dans un délai raisonnable après avoir été prises. Dans ce dernier cas, la documentation doit également inclure les éléments sur lesquels était basée l'évaluation concernant l'existence d'un risque immédiat ou d'une situation de crise. La documentation peut être concise mais doit être constituée de manière à permettre à la personne faisant l'objet de la mesure d'exercer ses droits de la défense et ses droits à la protection des données à caractère personnel conformément au règlement (CE) n° 45/2001, et à permettre un examen de la légalité de la mesure. Le dossier personnel de la personne concernée ne doit contenir aucune information concernant les mesures de sécurité spécifiques appliquées à un membre du personnel.

4. En prenant les mesures de sécurité visées au point b), la Commission garantit en outre que l'individu concerné se voit offrir la possibilité de contacter un avocat ou une personne de confiance et est informé de son droit de faire appel au contrôleur européen de la protection des données.

Article 13

Enquêtes

1. Sans préjudice de l'article 86 et de l'annexe IX du statut, et de tout accord spécial entre la Commission et le SEAE tel que l'accord spécial signé le 28 mai 2014 entre la direction générale des ressources humaines et de la sécurité de la Commission européenne et le Service européen pour l'action extérieure concernant le devoir de sollicitude à l'égard du personnel de la Commission affecté dans les délégations de l'Union, des enquêtes de sécurité peuvent être menées:

a) en cas d'incidents touchant la sécurité au sein de la Commission, y compris en cas de suspicion d'infractions pénales;

b) en cas de fuite, usage abusif ou compromission potentiels d'informations sensibles non classifiées, d'ICUE ou d'informations classifiées Euratom;

c) dans le contexte du contre-espionnage et de l'antiterrorisme;

d) en cas de cyberincidents graves.

2. La décision de mener une enquête de sécurité est prise par le directeur général des ressources humaines et de la sécurité, qui sera également destinataire du rapport d'enquête.

3. Les enquêtes de sécurité sont menées exclusivement par des membres du personnel habilités de la direction générale des ressources humaines et de la sécurité, dûment mandatés conformément à l'article 5.

4. Le personnel mandaté exerce ses pouvoirs en matière d'enquête de sécurité de manière indépendante, selon les termes de son mandat, et est investi des pouvoirs visés à l'article 12.

5. Le personnel mandaté ayant compétence pour mener des enquêtes de sécurité peut collecter des informations auprès de toutes les sources disponibles en lien avec toute infraction administrative ou pénale commise au sein des locaux de la Commission ou impliquant des personnes visées à l'article 2, paragraphe 3, que ce soit en tant que victime ou en tant qu'auteur de telles infractions.

6. La direction générale des ressources humaines et de la sécurité informe les autorités compétentes de l'État membre hôte ou de tout autre État membre concerné, le cas échéant, en particulier si l'enquête a mis au jour des indices montrant qu'un acte criminel a été perpétré. Dans ce contexte, la direction générale des ressources humaines et de la sécurité peut, si cela est nécessaire ou approprié, apporter un soutien aux autorités de l'État membre hôte ou d'un autre État membre concerné.

7. En cas de cyberincidents graves, la direction générale de l'informatique collabore étroitement avec la direction générale des ressources humaines et de la sécurité pour l'assister sur toutes les questions techniques. La direction générale des ressources humaines et de la sécurité décide, en concertation avec la direction générale de l'informatique, s'il est approprié d'informer les autorités compétentes du pays hôte ou de tout autre État membre concerné. Les services de coordination en cas d'incident de l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union européenne (CERT-UE) seront sollicités en ce qui concerne l'assistance aux autres institutions et agences de l'Union européenne susceptibles d'être affectées.

8. Les enquêtes de sécurité sont documentées.

Article 14

Délimitation des compétences concernant les enquêtes de sécurité et les autres types d'investigations

1. Lorsque la direction de la sécurité de la direction générale des ressources humaines et de la sécurité mène des enquêtes de sécurité visées à l'article 13, et si ces enquêtes entrent dans le champ de compétence de l'Office européen de lutte antifraude (OLAF) ou de l'Office d'investigation et de discipline de la Commission (IDOC), elle se met immédiatement en relation avec ces organismes en vue, notamment, de ne pas compromettre les étapes ultérieures menées par l'OLAF ou l'IDOC. Le cas échéant, la direction de la sécurité de la direction générale des ressources humaines et de la sécurité convie l'OLAF ou l'IDOC à participer à l'enquête.

2. Les enquêtes de sécurité visées à l'article 13 ont lieu sans préjudice des pouvoirs de l'OLAF et de l'IDOC établis dans les règles régissant ces organismes. La direction de la sécurité de la direction générale des ressources humaines et de la sécurité peut être sollicitée pour apporter une assistance technique dans les enquêtes engagées par l'OLAF ou l'IDOC.

3. La direction de la sécurité de la direction générale des ressources humaines et de la sécurité peut être sollicitée pour assister les agents de l'OLAF lorsqu'ils accèdent aux locaux de la Commission conformément à l'article 3, paragraphe 5, et à l'article 4, paragraphe 4, du règlement (UE, Euratom) nº 883/2013 du Parlement européen et du Conseil ([1]), afin de

([1]) Règlement (UE, Euratom) nº 883/2013 du Parlement européen et du Conseil du 11 septembre 2013 relatif aux enquêtes effectuées par l'Office européen de lutte antifraude (OLAF) et abrogeant le règlement (CE) nº 1073/1999 du Parlement européen et du Conseil et le règlement (Euratom) nº 1074/1999 du Conseil (JO L 248 du 18.9.2013, p. 1).

leur faciliter la tâche. La direction de la sécurité informe le secrétaire général et le directeur général de la direction générale des ressources humaines et de la sécurité de ces demandes d'assistance ou, si ces enquêtes sont menées dans des locaux de la Commission occupés par ses membres ou par son secrétaire général, elle en informe le président de la Commission et le commissaire chargé des ressources humaines.

4. Sans préjudice de l'article 22, point a), du statut, si une affaire relève de la compétence à la fois de la direction de la sécurité de la direction générale des ressources humaines et de la sécurité et de l'IDOC, la direction de la sécurité indique le plus tôt possible, dans son rapport au directeur général des ressources humaines conformément à l'article 13, s'il existe des motifs justifiant que l'IDOC soit saisi de l'affaire. Ce stade est considéré comme atteint notamment lorsqu'une menace immédiate pour la sécurité a cessé. Le directeur général des ressources humaines et de la sécurité se prononce sur la question.

5. Si une affaire relève de la compétence à la fois de la direction de la sécurité de la direction générale des ressources humaines et de la sécurité et de l'OLAF, la direction de la sécurité fait immédiatement rapport au directeur général des ressources humaines et de la sécurité et informe le directeur général de l'OLAF le plus tôt possible. Ce stade est considéré comme atteint notamment lorsqu'une menace immédiate pour la sécurité a cessé.

Article 15

Inspections de sécurité

1. La direction générale des ressources humaines et de la sécurité effectue des inspections de sécurité afin de vérifier le respect de la présente décision et de ses modalités d'application par les services de la Commission et les personnes, et de formuler des recommandations si cela est jugé nécessaire.

2. Le cas échéant, la direction générale des ressources humaines et de la sécurité effectue des inspections de sécurité ou des visites d'évaluation ou de suivi de la sécurité afin de vérifier si la sécurité du personnel, des biens et des informations de la Commission placés sous la responsabilité d'autres institutions, agences ou organes de l'Union, d'États membres, de pays tiers ou d'organisations internationales, est correctement assurée conformément à des règles, règlements et normes de sécurité au moins équivalents à ceux de la Commission. Le cas échéant et dans un esprit de bonne coopération entre les administrations, ces inspections de sécurité comprennent également des inspections menées dans le contexte de l'échange d'informations classifiées avec d'autres institutions, organes et agences de l'Union, des États membres, des pays tiers ou des organisations internationales.

3. Le présent article s'applique mutatis mutandis au personnel de la Commission travaillant dans les délégations de l'Union sans préjudice de tout accord spécial entre la Commission et le SEAE tel que l'accord spécial signé le 28 mai 2014 entre la direction générale des ressources humaines et de la sécurité de la Commission européenne et le Service européen pour l'action extérieure concernant le devoir de sollicitude à l'égard du personnel de la Commission affecté dans les délégations de l'Union.

Article 16

États d'alerte et gestion des situations de crise

1. La direction générale des ressources humaines et de la sécurité est chargée de mettre en place les mesures d'état d'alerte appropriées à titre d'anticipation ou de riposte face à des menaces et des incidents affectant la sécurité au sein de la Commission, ainsi que les mesures requises pour gérer les situations de crise.

2. Les mesures d'état d'alerte visées au paragraphe 1 doivent être proportionnelles au niveau de menace pour la sécurité. Les niveaux d'état d'alerte sont définis en étroite coopération avec les services compétents des autres institutions, agences et organes de l'Union et ceux de l'État membre ou des États membres accueillant les locaux de la Commission.

3. La direction générale des ressources humaines et de la sécurité fait office de point de contact pour les états d'alerte et la gestion des situations de crise.

CHAPITRE 4

ORGANISATION

Article 17

Responsabilités générales des services de la Commission

1. Les responsabilités de la Commission visées dans la présente décision sont exercées par la direction générale des ressources humaines et de la sécurité sous l'autorité et la responsabilité du membre de la Commission chargé de la sécurité.

2. Les dispositions spécifiques concernant la cybersécurité sont définies dans la décision C(2006) 3602.

3. Les responsabilités relatives à la mise en œuvre de la présente décision et de ses modalités d'application, ainsi qu'au respect quotidien de celles-ci, peuvent être déléguées à d'autres services de la Commission, dès lors qu'une organisation décentralisée de la sécurité offre un gain d'efficacité ou des économies de temps et de ressources significatifs, par exemple en raison de la localisation géographique des services concernés.

4. Lorsque le paragraphe 3 s'applique, la direction générale des ressources humaines et de la sécurité, et le cas échéant la direction générale de l'informatique, conclut des accords avec les différents services de la Commission en définissant clairement les rôles et les responsabilités concernant la mise en œuvre et le suivi des politiques de sécurité.

Article 18

La direction générale des ressources humaines et de la sécurité

1. La direction générale des ressources humaines et de la sécurité est notamment chargée de:

1) élaborer la politique de sécurité de la Commission, les modalités d'application et les notes de sécurité;

2) réunir des informations pour évaluer les menaces et les risques pour la sécurité et sur toutes les questions susceptibles de concerner la sécurité au sein de la Commission;

3) fournir une contre-surveillance électronique et une protection à tous les sites de la Commission, en tenant dûment compte des évaluations des menaces et des preuves d'activités non autorisées allant contre les intérêts de la Commission;

4) fournir un service d'urgence 24 h/24 et 7 jours/7 pour les services et le personnel de la Commission pour toutes les questions en lien avec la sûreté et la sécurité;

5) mettre en œuvre des mesures de sécurité visant à atténuer les risques de sécurité et à développer et entretenir des SIC adaptés afin de couvrir ses besoins opérationnels, en particulier dans le domaine du contrôle d'accès physique, de la gestion des autorisations de sécurité et du traitement des informations sensibles et classifiées de l'Union européenne;

6) sensibiliser, organiser des exercices et des manœuvres et fournir une formation et des conseils sur toutes les questions en lien avec la sécurité au sein de la Commission, en vue de promouvoir une culture de la sécurité et de créer un groupe de personnes parfaitement formées sur les questions de sécurité.

2. Sans préjudice des compétences et responsabilités d'autres services de la Commission, la direction générale des ressources humaines et de la sécurité assure la liaison externe:

1) avec les organismes chargés de la sécurité des autres institutions, agences et organes de l'Union sur les questions liées à la sécurité des personnes, des biens et des informations au sein de la Commission;

2) avec les services de sécurité, de renseignement et d'évaluation des menaces, notamment les autorités de sécurité nationales, des États membres, des pays tiers et des organisations et organismes internationaux, sur les questions relatives à la sécurité des personnes, des biens et des informations au sein de la Commission;

3) avec les services de police et autres services d'urgence sur toutes les questions de routine et d'urgence concernant la sécurité de la Commission;

4) avec les autorités de sécurité des autres institutions, agences et organes de l'Union, des États membres et des pays tiers dans le domaine de la riposte aux cyberattaques ayant un impact potentiel sur la sécurité au sein de la Commission;

5) concernant la réception, l'évaluation et la diffusion des renseignements relatifs à des menaces représentées par des activités terroristes et d'espionnage affectant la sécurité au sein de la Commission;

6) concernant les questions relatives aux informations classifiées, comme indiqué plus en détail dans la décision de la Commission (UE, Euratom) 2015/444 ([1]).

3. La direction générale des ressources humaines et de la sécurité est responsable de la transmission sécurisée des informations effectuée en vertu du présent article, y compris la transmission de données à caractère personnel.

Article 19

Le groupe d'experts sécurité de la Commission (ComSEG)

Un groupe d'experts sécurité de la Commission est mis en place, avec pour mandat de conseiller la Commission, le cas échéant, sur les questions relatives à sa politique de sécurité interne et plus particulièrement à la protection des informations classifiées de l'Union européenne.

([1]) Décision (UE, Euratom) 2015/444 de la Commission du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (voir page 53 du présent Journal officiel).

Article 20

Responsables locaux de la sécurité (LSO)

1. Chaque service ou cabinet de la Commission nomme un responsable local de la sécurité (LSO), qui fait office de point de contact principal entre le service concerné et la direction générale des ressources humaines et de la sécurité pour toutes les questions en lien avec la sécurité au sein de la Commission. Le cas échéant, un ou plusieurs responsables locaux de la sécurité adjoints peuvent être désignés. Le responsable local de la sécurité est un fonctionnaire ou un agent temporaire.

2. En sa qualité de point de contact principal sur la sécurité au sein de son service ou cabinet de la Commission, le responsable local de la sécurité fait rapport à la direction générale des ressources humaines et de la sécurité et à sa hiérarchie à intervalles réguliers sur les questions de sécurité concernant son service et de façon immédiate sur tout incident de sécurité, notamment lorsque des ICUE ou des informations sensibles non classifiées peuvent avoir été compromises.

3. Pour les questions relatives à la sécurité des systèmes d'information et de communication, le responsable local de la sécurité se met en relation avec le responsable de la sécurité informatique au niveau local (LISO) de son service, dont le rôle et les responsabilités sont définis dans la décision C(2006) 3602.

4. Il participe aux activités de formation et de sensibilisation à la sécurité répondant aux besoins spécifiques du personnel, des contractants et des autres personnes travaillant sous l'autorité du service de la Commission auquel il est rattaché.

5. Le responsable local de la sécurité peut se voir confier des tâches spécifiques en cas de risque de sécurité majeur ou immédiat ou d'urgence à la demande de la direction générale des ressources humaines et de la sécurité. Le directeur général ou le directeur des ressources humaines de la direction générale locale du responsable local de la sécurité est informé de ces tâches spécifiques par la direction générale des ressources humaines et de la sécurité.

6. Les responsabilités du responsable local de la sécurité sont assumées sans préjudice du rôle et des responsabilités assignés aux responsables de la sécurité informatique au niveau local (LISO), aux responsables en matière de santé et de sécurité, aux agents contrôleurs (RCO) et à toute autre fonction impliquant des responsabilités en matière de sécurité ou de sûreté. Le responsable local de la sécurité se met en relation avec eux pour assurer une approche cohérente de la sécurité et un flux d'information efficace sur les questions en lien avec la sécurité au sein de la Commission.

7. Le responsable local de la sécurité a directement accès à son directeur général ou son chef de service tout en informant sa hiérarchie directe. Il détient une autorisation de sécurité pour accéder aux ICUE, au moins jusqu'au niveau SECRET UE.

8. Afin de promouvoir l'échange d'informations et les meilleures pratiques, la direction générale des ressources humaines et de la sécurité organise au moins deux fois par an une conférence des responsables locaux de la sécurité. Les responsables locaux de la sécurité ont l'obligation d'assister à ces conférences.

CHAPITRE 5

MISE EN ŒUVRE

Article 21

Modalités d'application et notes de sécurité

1. Au besoin, l'adoption des modalités d'application de la présente décision fera l'objet d'une décision d'habilitation distincte de la Commission en faveur du membre de la Commission chargé des questions de sécurité, conformément au règlement intérieur.

2. Après avoir été habilité à la suite de la décision de la Commission susvisée, le membre de la Commission chargé des questions de sécurité peut rédiger des notes de sécurité définissant des lignes directrices et des bonnes pratiques en matière de sécurité dans le cadre du champ d'application de la présente décision et de ses modalités d'application.

3. La Commission peut déléguer les tâches mentionnées dans les premier et deuxième paragraphes du présent article au directeur général des ressources humaines et de la sécurité au moyen d'une décision de délégation distincte, conformément au règlement intérieur.

CHAPITRE 6

DISPOSITIONS DIVERSES ET DISPOSITIONS FINALES

Article 22

Traitement des données à caractère personnel

1. La Commission traite les données à caractère personnel requises pour la mise en œuvre de la présente décision conformément au règlement (CE) n° 45/2001.

2. Nonobstant les mesures déjà en place au moment de l'adoption de la présente décision et notifiées au contrôleur européen de la protection des données ([1]), toute mesure prise en vertu de la présente décision et impliquant le traitement de données à caractère personnel, notamment en lien avec les registres des entrées et sorties, enregistrements de vidéosurveillance, enregistrements d'appels téléphoniques aux services de permanence ou aux centres de répartition et données similaires, nécessaires pour des raisons de sécurité ou de riposte à une crise, est soumise aux modalités d'application conformes à l'article 21, qui prévoient des garanties appropriées pour les personnes concernées.

3. Le directeur général de la direction générale des ressources humaines et de la sécurité est responsable de la sécurité de tout traitement de données à caractère personnel effectué dans le contexte de la présente décision.

4. Ces modalités d'application et procédures sont adoptées après consultation du délégué à la protection des données et du contrôleur européen de la protection des données, conformément au règlement (CE) n° 45/2001.

Article 23

Transparence

La présente décision et ses modalités d'application sont portées à l'attention du personnel de la Commission et de toutes les personnes auxquelles elles s'appliquent.

Article 24

Abrogation des décisions précédentes

La décision C(94) 2129 est abrogée.

Article 25

Entrée en vigueur

La présente décision entre en vigueur le jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Fait à Bruxelles, le 13 mars 2015.

Par la Commission
Le président
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.

DÉCISION (UE, Euratom) 2015/444 DE LA COMMISSION

du 13 mars 2015

concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 249,

vu le traité instituant la Communauté européenne de l'énergie atomique, et notamment son article 106,

vu le protocole n° 7 sur les privilèges et immunités de l'Union européenne annexé aux traités, et notamment son article 18,

considérant ce qui suit:

(1) Les dispositions de la Commission en matière de sécurité concernant la protection des informations classifiées de l'Union européenne (ICUE) doivent être révisées et actualisées, en tenant compte des évolutions institutionnelles, organisationnelles, opérationnelles et technologiques.

(2) La Commission européenne a signé des accords en matière de sécurité pour ses principaux sites avec les gouvernements belge, luxembourgeois et italien ([1]).

(3) La Commission, le Conseil et le Service européen pour l'action extérieure sont résolus à appliquer des normes équivalentes de sécurité pour protéger les ICUE.

(4) Il importe d'associer, le cas échéant, le Parlement européen et d'autres institutions, agences, organes ou organismes de l'Union aux principes, aux normes et à la réglementation relatifs à la protection des informations classifiées qui sont nécessaires pour protéger les intérêts de l'Union et de ses États membres.

(5) Les risques pesant sur les ICUE sont gérés dans le cadre d'une procédure. Cette dernière vise à déterminer les risques connus pesant sur la sécurité, à définir des mesures de sécurité permettant de ramener ces risques à un niveau acceptable conformément aux principes de base et aux normes minimales énoncés dans la présente décision et à appliquer ces mesures selon la notion de défense en profondeur. L'efficacité de telles mesures fait l'objet d'une évaluation constante.

(6) Au sein de la Commission, la sécurité physique visant à protéger les informations classifiées correspond à l'application de mesures physiques et techniques de protection pour empêcher l'accès non autorisé aux ICUE.

(7) La gestion des ICUE correspond à l'application de mesures administratives pour contrôler les ICUE tout au long de leur cycle de vie afin de compléter les mesures prévues aux chapitres 2, 3 et 5 de la présente décision et de contribuer ainsi à la dissuasion, à la détection et au retour aux conditions opérationnelles dans le cadre de la compromission ou de la perte délibérée ou accidentelle de telles informations. Ces mesures concernent en particulier la création, la conservation, l'enregistrement, la duplication, la traduction, le déclassement, la déclassification, le transport et la destruction des ICUE et elles complètent les règles générales de la Commission relatives à la gestion des documents [décisions 2002/47/CE, CECA, Euratom ([2]) et 2004/563/CE, Euratom ([3])].

([1]) Voir 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 du 31 décembre 2004, Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois du 20 janvier 2007, et 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 du 22 juillet 1959.

([2]) Décision 2002/47/CE, CECA, Euratom de la Commission du 23 janvier 2002 modifiant son règlement intérieur (JO L 21 du 24.1.2002, p. 23).

([3]) Décision 2004/563/CE, Euratom de la Commission du 7 juillet 2004 modifiant son règlement intérieur (JO L 251 du 27.7.2004, p. 9).

(8) La présente décision est arrêtée sans préjudice des règlements suivants:

a) règlement (Euratom) nº 3 ([1]);

b) règlement (CE) nº 1049/2001 du Parlement européen et du Conseil ([2]);

c) règlement (CE) nº 45/2001 du Parlement européen et du Conseil ([3]);

d) règlement (CEE, Euratom) nº 354/83 du Conseil ([4]),

A ADOPTÉ LA PRÉSENTE DÉCISION:

CHAPITRE PREMIER

PRINCIPES DE BASE ET NORMES MINIMALES

Article premier

Définitions

Aux fins de la présente décision, on entend par:

1) «service de la Commission», l'une des directions générales ou l'un des services de la Commission ou l'un des cabinets des membres de la Commission;

2) «matériel cryptographique», les algorithmes cryptographiques, les modules matériels et logiciels cryptographiques, et les produits comprenant les modalités de mise en œuvre et la documentation y relative, ainsi que les éléments de mise à la clé;

3) «déclassification», la suppression de toute classification de sécurité;

4) «défense en profondeur», l'application d'un éventail de mesures de sécurité organisées en plusieurs niveaux de défense;

5) «document», toute information enregistrée quelles que soient sa forme ou ses caractéristiques physiques;

6) «déclassement», le passage à un niveau de classification de sécurité inférieur;

7) «traitement» d'ICUE, l'ensemble des actions dont les ICUE sont susceptibles de faire l'objet tout au long de leur cycle de vie. Sont ainsi visés leur création, leur enregistrement, leur traitement, leur transport, leur déclassement, leur déclassification et leur destruction. En ce qui concerne les systèmes d'information et de communication (SIC), sont en outre compris leur collecte, leur affichage, leur transmission et leur stockage;

8) «détenteur», une personne dûment autorisée qui, sur la base d'un besoin d'en connaître avéré, est en possession d'un élément d'ICUE et à laquelle il incombe par conséquent d'en assurer la protection;

9) «modalités d'application», tout ensemble de dispositions ou notes de sécurité adoptées conformément au chapitre 5 de la décision de la Commission (UE, Euratom) 2015/443 ([5]);

10) «matériel», tout média, support de données ou élément de machine ou d'équipement, déjà fabriqué ou en cours de fabrication;

11) «autorité d'origine», l'institution, l'organe ou l'agence de l'Union, l'État membre, l'État tiers ou l'organisation internationale sous l'autorité duquel/de laquelle les informations classifiées ont été créées et/ou introduites dans les structures de l'Union;

12) «locaux», tous les biens et possessions immeubles et assimilés de la Commission;

([1]) Règlement (Euratom) nº 3 du 31 juillet 1958 portant application de l'article 24 du traité instituant la Communauté européenne de l'énergie atomique (JO 17 du 6.10.1958, p. 406/58).

([2]) Règlement (CE) nº 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (JO L 145 du 31.5.2001, p. 43).

([3]) Règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

([4]) Règlement (CEE, Euratom) nº 354/83 du Conseil du 1er février 1983 concernant l'ouverture au public des archives historiques de la Communauté économique européenne et de la Communauté européenne de l'énergie atomique (JO L 43 du 15.2.1983, p. 1).

([5]) Décision de la Commission (UE, Euratom) 2015/443 du 13 mars 2015 relative à la sécurité au sein de la Commission (voir page 41 du présent Journal officiel).

13) «procédure de gestion des risques de sécurité», l'ensemble de la procédure consistant à identifier, contrôler et limiter les événements aléatoires susceptibles d'avoir des répercussions sur la sécurité d'une organisation ou de tout système qu'elle utilise. La procédure couvre l'ensemble des activités liées aux risques, y compris l'évaluation, le traitement, l'acceptation et la communication;

14) «statut», le statut des fonctionnaires de l'Union européenne et le régime applicable aux autres agents de l'Union européenne, énoncés dans le règlement (CEE, Euratom, CECA) n° 259/68 du Conseil ([1]);

15) «menace», la cause potentielle d'un incident non souhaité susceptible de porter atteinte à une organisation ou à tout système qu'elle utilise. Les menaces peuvent être accidentelles ou délibérées (malveillantes); elles sont caractérisées par des éléments menaçants, des cibles potentielles et des méthodes d'attaque;

16) «vulnérabilité», toute faiblesse de quelque nature que ce soit dont une ou plusieurs menaces est susceptible de tirer parti pour se concrétiser. La vulnérabilité peut résulter d'une omission ou être liée à un contrôle défaillant en termes de rigueur, d'exhaustivité ou d'homogénéité; elle peut être de nature technique, procédurale, physique, organisationnelle ou opérationnelle.

Article 2

Objet et champ d'application

1. La présente décision définit les principes de base et les normes de sécurité minimales pour la protection des ICUE.

2. La présente décision s'applique à tous les services de la Commission et dans l'ensemble des locaux de la Commission.

3. Nonobstant toute indication spécifique concernant des groupes particuliers de personnel, la présente décision s'applique aux membres de la Commission, au personnel de la Commission couvert par le statut et par le régime applicable aux autres agents de l'Union européenne, aux experts nationaux détachés auprès de la Commission (END), aux prestataires de services et à leur personnel, aux stagiaires et à toute personne ayant accès aux bâtiments et autres propriétés de la Commission, ou à des informations gérées par la Commission.

4. Les dispositions de la présente décision s'appliquent sans préjudice de la décision 2002/47/CE, CECA, Euratom et de la décision 2004/563/CE, Euratom.

Article 3

Définition des ICUE, classifications et marquages de sécurité

1. Par «informations classifiées de l'Union européenne» (ICUE), on entend toute information ou tout matériel identifié comme tel par la classification de sécurité de l'Union européenne, dont la divulgation non autorisée pourrait porter atteinte à des degrés divers aux intérêts de l'Union européenne, ou à ceux d'un ou de plusieurs de ses États membres.

2. Les ICUE relèvent de l'un des niveaux de classification suivants:

a) TRÈS SECRET UE/EU TOP SECRET: informations et matériels dont la divulgation non autorisée pourrait causer un préjudice exceptionnellement grave aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres;

b) SECRET UE/EU SECRET: informations et matériels dont la divulgation non autorisée pourrait nuire gravement aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres;

c) CONFIDENTIEL UE/EU CONFIDENTIAL: informations et matériels dont la divulgation non autorisée pourrait nuire aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres;

d) RESTREINT UE/EU RESTRICTED: informations et matériels dont la divulgation non autorisée pourrait être défavorable aux intérêts de l'Union européenne ou d'un ou de plusieurs de ses États membres.

3. Les ICUE portent un marquage de classification de sécurité conformément au paragraphe 2. Elles peuvent porter des marquages supplémentaires, qui ne sont pas des marquages de classification mais sont destinés à désigner le domaine d'activité auquel elles sont liées, identifier l'autorité d'origine, limiter la diffusion, restreindre l'utilisation ou indiquer la communicabilité.

([1]) Règlement (CEE, Euratom, CECA) n° 259/68 du Conseil, du 29 février 1968, fixant le statut des fonctionnaires des Communautés européennes ainsi que le régime applicable aux autres agents de ces Communautés, et instituant des mesures particulières temporairement applicables aux fonctionnaires de la Commission (régime applicable aux autres agents) (JO L 56 du 4.3.1968, p. 1).

Article 4

Gestion de la classification

1. Chaque membre de la Commission ou service de la Commission veille à ce que les ICUE qu'il crée soient classifiées de manière appropriée, clairement identifiées en tant qu'ICUE, et qu'elles ne conservent leur niveau de classification qu'aussi longtemps que nécessaire.

2. Sans préjudice de l'article 26 ci-après, les ICUE ne sont pas déclassées ni déclassifiées, et aucun des marquages de classification de sécurité visés à l'article 3, paragraphe 2, n'est modifié ni supprimé sans le consentement écrit préalable de l'autorité d'origine.

3. Le cas échéant, des modalités d'application sur le traitement des ICUE, comprenant un guide pratique de la classification, sont adoptées conformément à l'article 60 ci-après.

Article 5

Protection des informations classifiées

1. Les ICUE sont protégées conformément à la présente décision et à ses modalités d'application.

2. Il incombe au détenteur de tout élément d'ICUE de le protéger conformément à la présente décision et à ses modalités d'application, conformément aux dispositions prévues au chapitre 4 ci-après.

3. Lorsque les États membres introduisent des informations classifiées portant un marquage national de classification de sécurité dans les structures ou réseaux de la Commission, cette dernière protège ces informations conformément aux règles applicables aux ICUE de niveau équivalent tel que prévu dans le tableau d'équivalence des classifications de sécurité figurant à l'annexe I.

4. Un ensemble d'ICUE peut justifier un niveau de protection correspondant à une classification plus élevée que celle appliquée à ses différentes composantes.

Article 6

Gestion des risques de sécurité

1. Les mesures de sécurité pour la protection des ICUE tout au long de leur cycle de vie sont proportionnées en particulier à leur classification de sécurité, à la forme sous laquelle se présentent les informations ou les matériels ainsi qu'à leur volume, au lieu et à la construction des établissements où se trouvent des ICUE et à la menace évaluée à l'échelle locale que représentent les activités malveillantes et/ou criminelles, y compris l'espionnage, le sabotage et le terrorisme.

2. Les plans d'urgence tiennent compte de la nécessité de protéger les ICUE en cas d'urgence afin de prévenir l'accès et la divulgation non autorisés ainsi que la perte d'intégrité ou de disponibilité.

3. Les mesures de prévention et de retour aux conditions opérationnelles visant à limiter l'impact de défaillances ou d'incidents graves sur le traitement et le stockage des ICUE sont prévues dans les plans de continuité de l'activité de tous les services.

Article 7

Mise en œuvre de la présente décision

1. Le cas échéant, les modalités d'application en complément ou à l'appui de la présente décision sont adoptées conformément à l'article 60 ci-après.

2. Les services de la Commission prennent toutes les mesures nécessaires dans le cadre leur responsabilité pour veiller à ce que, lors du traitement ou de la conservation des ICUE ou de toute autre information classifiée, la présente décision et les modalités d'application correspondantes soient appliquées.

3. Les mesures de sécurité prises en application de la présente décision sont conformes aux principes en matière de sécurité au sein de la Commission énoncés à l'article 3 de la décision (UE, Euratom) 2015/443.

4. Le directeur général des ressources humaines et de la sécurité met en place l'autorité de sécurité de la Commission au sein de la direction générale des ressources humaines et de la sécurité. L'autorité de sécurité de la Commission assume les responsabilités qui lui sont assignées par la présente décision et ses modalités d'application.

5. Au sein de chaque service de la Commission, le responsable local de la sécurité (LSO), visé à l'article 20 de la décision (UE, Euratom) 2015/443, assume les responsabilités générales suivantes aux fins de la protection des ICUE, conformément à la présente décision, en coopération étroite avec la direction générale des ressources humaines et de la sécurité:

a) gestion des demandes d'autorisations de sécurité pour le personnel;

b) contribution aux réunions de formation et de sensibilisation sur la sécurité;

c) supervision de l'agent contrôleur (RCO) du service;

d) dénonciation des infractions à la sécurité et de la compromission des ICUE;

e) conservation des clés de rechange et du relevé de chaque combinaison;

f) exécution d'autres tâches en relation avec la protection des ICUE ou définies par les modalités d'application.

Article 8

Infractions à la sécurité et compromission des ICUE

1. Une infraction à la sécurité est un acte ou une omission commis par une personne qui est contraire aux règles de sécurité énoncées dans la présente décision et ses modalités d'application.

2. Il y a compromission lorsque, à la suite d'une infraction à la sécurité, des ICUE ont été divulguées en totalité ou en partie à des personnes non autorisées.

3. Toute infraction à la sécurité, réelle ou présumée, est immédiatement signalée à l'autorité de sécurité de la Commission.

4. Lorsqu'il est avéré ou qu'il existe des motifs raisonnables de supposer que des ICUE ont été compromises ou perdues, une enquête de sécurité est menée conformément à l'article 13 de la décision (UE, Euratom) 2015/443.

5. Toutes les mesures appropriées sont prises pour:

a) en informer l'autorité d'origine;

b) faire en sorte qu'une enquête soit menée par des membres du personnel n'étant pas directement concernés par l'infraction afin d'établir les faits;

c) évaluer le préjudice éventuel causé aux intérêts de l'Union ou des États membres;

d) éviter que les faits ne se reproduisent; et

e) informer les autorités compétentes des mesures prises.

6. Toute personne responsable d'une violation des règles de sécurité énoncées dans la présente décision est passible d'une sanction disciplinaire conformément au statut. Toute personne responsable de la compromission ou de la perte d'ICUE est passible de sanctions disciplinaires et/ou peut faire l'objet d'une action en justice conformément aux dispositions législatives et réglementaires applicables.

CHAPITRE 2

MESURES DE SÉCURITÉ CONCERNANT LE PERSONNEL

Article 9

Définitions

Aux fins du présent chapitre, les définitions suivantes sont applicables:

1) Par «autorisation d'accès aux ICUE», on entend une décision de l'autorité de sécurité de la Commission prise en fonction d'une assurance donnée par une autorité compétente d'un État membre attestant qu'un fonctionnaire de la Commission, un autre agent ou un expert national détaché peut, pour autant que son besoin d'en connaître ait été établi et qu'il ait été correctement informé des responsabilités qui lui incombent en la matière, être autorisé à avoir accès aux ICUE jusqu'à un niveau de classification donné (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur) jusqu'à une date donnée; l'individu en question est alors «autorisé sécurité».

2) Par «autorisation de sécurité du personnel», on entend l'application de mesures visant à faire en sorte que l'accès aux ICUE ne soit accordé qu'aux personnes qui ont:

   a) un besoin d'en connaître,

   b) fait l'objet d'une autorisation de sécurité du niveau correspondant, lorsqu'il y a lieu, et

   c) été informées de leurs responsabilités.

3) Par «habilitation de sécurité du personnel» (HSP), on entend une déclaration émanant d'une autorité compétente d'un État membre établie à la suite d'une enquête de sécurité menée par les autorités compétentes d'un État membre et attestant qu'une personne peut, pour autant que son besoin d'en connaître ait été établi et qu'elle ait été correctement informée des responsabilités qui lui incombent en la matière, être autorisée à avoir accès aux ICUE jusqu'à un niveau de classification donné (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur) jusqu'à une date donnée.

4) Par «certificat d'habilitation de sécurité du personnel» (CHSP), on entend un certificat délivré par une autorité compétente attestant qu'une personne détient une habilitation de sécurité valable ou une autorisation de sécurité délivrée par l'autorité de sécurité de la Commission, indiquant le niveau de classification des ICUE auxquelles la personne peut être autorisée à avoir accès (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur), la durée de validité de l'habilitation ou autorisation de sécurité correspondante et la date d'expiration du certificat.

5) Par «enquête de sécurité», on entend les procédures d'enquête menées par l'autorité compétente d'un État membre, dans le respect de ses dispositions législatives et réglementaires nationales, en vue d'obtenir l'assurance qu'il n'existe pas de renseignements défavorables de nature à empêcher une personne d'obtenir une habilitation de sécurité jusqu'à un niveau déterminé (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur).

Article 10

Principes de base

1. Une personne ne peut se voir accorder l'accès à des ICUE qu'après:

(1) que son besoin d'en connaître a été établi;

(2) avoir été informée des règles de sécurité applicables à la protection des ICUE ainsi que des normes et lignes directrices correspondantes en matière de sécurité, et avoir reconnu les responsabilités qui lui incombent en matière de protection de ces informations; et

(3) pour les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, s'être vu accorder une autorisation de sécurité du niveau correspondant ou avoir été dûment autorisée en vertu de ses fonctions conformément aux dispositions législatives et réglementaires nationales.

2. Toutes les personnes qui, en raison de leurs attributions, peuvent avoir besoin d'accéder à des ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur font l'objet d'une autorisation de sécurité du niveau correspondant avant que l'accès à de telles ICUE ne leur soit accordé. La personne concernée consent par écrit à se soumettre à la procédure d'habilitation de sécurité concernant le personnel. Dans le cas contraire, cette personne ne peut être affectée à un poste, une fonction ou une tâche requérant l'accès des informations classifiées de niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur.

3. Les procédures d'habilitation de sécurité concernant le personnel ont pour but de déterminer si une personne, compte tenu de sa loyauté, de son intégrité et de sa fiabilité, peut être autorisée à avoir accès à des ICUE.

4. Il convient d'établir, au moyen d'une enquête de sécurité, la loyauté, l'intégrité et la fiabilité d'une personne aux fins de l'octroi d'une habilitation de sécurité lui permettant d'accéder à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur; cette enquête est menée par les autorités compétentes d'un État membre conformément aux dispositions législatives et réglementaires nationales.

5. L'autorité de sécurité de la Commission assume seule la responsabilité de se mettre en relation avec les autorités nationales de sécurité (ANS) ou d'autres autorités nationales compétentes pour toutes les questions relevant de l'habilitation de sécurité. Tous les contacts entre les services de la Commission et leur personnel d'une part et les ANS ou autres autorités compétentes d'autre part doivent passer par l'autorité de sécurité de la Commission.

Article 11

Procédure d'autorisation de sécurité

1. Il appartient à chaque directeur général ou chef de service au sein de la Commission de répertorier, au sein de son service, les postes nécessitant l'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur pour s'acquitter de leurs tâches et exigeant par conséquent une autorisation de sécurité.

2. Dès lors qu'il a connaissance de la nomination d'une personne à un poste nécessitant l'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, le responsable local de la sécurité (LSO) du service de la Commission concerné informe l'autorité de sécurité de la Commission, qui transmet à cette personne le questionnaire d'habilitation de sécurité délivré par l'ANS de l'État membre dont est ressortissant l'intéressé nommé en tant que membre du personnel des institutions européennes. La personne concernée consent par écrit à se soumettre à la procédure d'habilitation de sécurité et renvoie le questionnaire rempli dans les plus brefs délais à l'autorité de sécurité de la Commission.

3. L'autorité de sécurité de la Commission transmet le questionnaire d'habilitation de sécurité rempli à l'ANS de l'État membre dont est ressortissant l'intéressé nommé en tant que membre du personnel des institutions européennes et demande qu'il soit procédé à une enquête de sécurité pour le niveau de classification des ICUE auxquelles cette personne devra avoir accès.

4. Si des informations utiles à une enquête de sécurité sont portées à la connaissance de l'autorité de sécurité de la Commission concernant une personne ayant demandé une habilitation de sécurité, l'autorité de sécurité de la Commission, agissant conformément à la réglementation applicable, en avertit l'ANS compétente.

5. À l'issue de l'enquête de sécurité, et dès que possible après avoir été informée par l'ANS compétente de son évaluation générale des conclusions de l'enquête en question, l'autorité de sécurité de la Commission:

a) peut accorder à l'intéressé l'autorisation d'accéder à des ICUE jusqu'au niveau de classification correspondant jusqu'à une date qu'elle détermine elle-même, mais n'excédant pas une durée de 5 ans, lorsque les résultats de l'enquête de sécurité permettent d'obtenir l'assurance qu'il n'existe pas de renseignements défavorables de nature à mettre en doute la loyauté, l'intégrité et la fiabilité de l'intéressé;

b) lorsque le résultat de l'enquête de sécurité ne permet pas d'obtenir cette assurance, conformément à la règlementation applicable, informe l'intéressé, qui peut demander à être entendu par l'autorité de sécurité de la Commission; celle-ci peut à son tour demander à l'ANS compétente tout éclaircissement complémentaire qu'elle est en mesure de donner conformément à ses dispositions législatives et réglementaires nationales. En cas de confirmation des résultats de l'enquête, il n'est pas accordé d'autorisation aux fins de l'accès à des ICUE.

6. L'enquête de sécurité et ses résultats obéissent aux dispositions législatives et réglementaires en vigueur dans l'État membre concerné, y compris celles relatives aux recours. Les décisions de l'autorité de sécurité de la Commission sont susceptibles de recours conformément au statut.

7. La Commission acceptera l'autorisation d'accès à des ICUE octroyée par toute autre institution, organe ou agence de l'Union, pour autant qu'elle reste valable. Les autorisations couvriront toute fonction exercée par l'intéressé au sein de la Commission. L'institution, l'organe ou l'agence de l'Union dans lequel la personne prend ses fonctions signalera le changement d'employeur à l'ANS concernée.

8. Si l'intéressé n'entame pas sa période de service dans un délai de douze mois à compter de la notification des conclusions de l'enquête de sécurité à l'autorité de sécurité de la Commission ou si cette période de service connaît une interruption de douze mois au cours de laquelle l'intéressé n'occupe pas de poste au sein de la Commission, d'une autre institution, organe ou agence de l'Union ou d'une administration nationale d'un État membre, l'autorité de sécurité de la Commission en réfère à l'ANS compétente afin que celle-ci confirme que l'habilitation de sécurité reste valable et pertinente.

9. Si des informations sont portées à la connaissance de l'autorité de sécurité de la Commission concernant un risque de sécurité que représente une personne titulaire d'une autorisation de sécurité valide, l'autorité de sécurité, agissant conformément à la réglementation applicable, en avertit l'ANS compétente.

10. Lorsqu'une ANS notifie à l'autorité de sécurité de la Commission que l'assurance visée au paragraphe 5, point a), n'est plus fournie concernant une personne titulaire d'une autorisation valide d'accès à des ICUE, l'autorité de sécurité de la Commission peut demander à l'ANS concernée tout éclaircissement qu'elle est en mesure de donner dans le respect de ses dispositions législatives et réglementaires nationales. Si les informations défavorables sont confirmées par l'ANS compétente, l'autorisation de sécurité est retirée et la personne concernée n'est plus autorisée à avoir accès aux ICUE, ni à des postes où un tel accès est possible et où elle pourrait nuire à la sécurité.

11. Toute décision de retirer ou suspendre une autorisation d'accès à des ICUE à une personne entrant dans le champ d'application de la présente décision et, s'il y a lieu, les raisons la justifiant sont communiquées à la personne concernée, qui peut demander à être entendue par l'autorité de sécurité de la Commission. Les informations communiquées par une ANS sont soumises aux dispositions législatives et réglementaires en vigueur dans l'État membre concerné. Les décisions prises dans ce contexte par l'autorité de sécurité de la Commission sont susceptibles de recours conformément au statut.

12. Les services de la Commission veillent à ce que les experts nationaux détachés auprès d'eux pour occuper un poste nécessitant une autorisation de sécurité pour accéder à des ICUE présentent, avant de prendre leurs fonctions, une HSP ou un certificat d'habilitation de sécurité du personnel (CHSP) valable, conformément aux dispositions législatives et réglementaires nationales, à l'autorité de sécurité de la Commission qui, sur cette base, délivre une autorisation de sécurité pour l'accès aux ICUE jusqu'au niveau équivalent à celui indiqué dans l'habilitation de sécurité nationale, avec une validité maximale couvrant la durée de leur mission.

Accès à des ICUE pour les personnes dûment autorisées en vertu de leurs fonctions

13. Les membres de la Commission, qui ont accès aux ICUE en vertu de leurs fonctions conformément au traité, sont informés de leurs obligations en matière de sécurité en ce qui concerne la protection des ICUE.

Registres des habilitations de sécurité et des autorisations de sécurité

14. L'autorité de sécurité de la Commission tient des registres des habilitations de sécurité et des autorisations accordées aux fins de l'accès à des ICUE, conformément à la présente décision. Ces registres contiennent au minimum le niveau de classification des ICUE auxquelles l'intéressé peut se voir accorder l'accès, la date à laquelle l'habilitation de sécurité a été délivrée et sa durée de validité.

15. L'autorité de sécurité de la Commission peut délivrer un CHSP précisant le niveau de classification des ICUE auxquelles l'intéressé peut se voir accorder l'accès (CONFIDENTIEL UE/EU CONFIDENTIAL ou un niveau supérieur), la durée de validité de l'autorisation d'accès à des ICUE correspondante et la date d'expiration du certificat proprement dit.

Renouvellement des autorisations de sécurité

16. Après la première délivrance d'une autorisation de sécurité et pour autant que l'intéressé ait accompli une période de service ininterrompue auprès de la Commission européenne ou d'une autre institution, organe ou agence de l'Union et qu'il ait toujours besoin d'avoir accès aux ICUE, l'autorisation de sécurité pour l'accès aux ICUE est réexaminée en vue de son renouvellement, généralement tous les cinq ans à compter de la date de notification des conclusions de la dernière enquête de sécurité sur laquelle elle était fondée.

17. L'autorité de sécurité de la Commission peut prolonger la validité de l'autorisation de sécurité existante pour une période de douze mois au maximum, pour autant que l'ANS compétente ou une autre autorité nationale compétente n'ait reçu aucun renseignement défavorable dans un délai de deux mois à compter de la date de transmission de la demande de renouvellement et du questionnaire d'habilitation de sécurité correspondant. Si, à la fin de cette période de douze mois, l'ANS compétente ou une autre autorité nationale compétente n'a pas notifié son avis à l'autorité de sécurité de la Commission, l'intéressé est affecté à des fonctions qui ne nécessitent pas d'autorisation de sécurité.

Article 12

Réunions d'information sur les autorisations de sécurité

1. Après avoir participé à la réunion d'information sur les autorisations de sécurité organisée par l'autorité de sécurité de la Commission, toutes les personnes auxquelles a été délivrée une autorisation de sécurité reconnaissent par écrit qu'elles sont conscientes de leurs obligations en matière de protection des ICUE et des conséquences qui pourraient résulter si des ICUE devaient être compromises. L'autorité de sécurité de la Commission tient un registre de ces déclarations écrites.

2. Toutes les personnes autorisées à avoir accès aux ICUE ou tenues de les traiter sont averties dans un premier temps et périodiquement informées par la suite des menaces pesant sur la sécurité, et elles doivent rendre compte immédiatement à l'autorité de sécurité de la Commission de toute démarche ou activité qu'elles jugent suspecte ou inhabituelle.

3. Toutes les personnes qui cessent d'exercer des fonctions nécessitant un accès aux ICUE sont informées, et le cas échéant reconnaissent par écrit, qu'elles ont l'obligation de continuer à protéger les ICUE.

Article 13

Autorisations de sécurité temporaires

1. Dans des circonstances exceptionnelles, lorsque cela est dûment justifié dans l'intérêt du service et en attendant l'achèvement de l'enquête de sécurité complète, l'autorité de sécurité de la Commission peut, après avoir consulté l'ANS de l'État membre dont l'intéressé est ressortissant et sous réserve des résultats des vérifications préliminaires effectuées pour s'assurer de l'absence d'informations défavorables pertinentes, accorder à titre temporaire l'autorisation d'accéder à des ICUE pour une fonction déterminée, sans préjudice des dispositions concernant le renouvellement des habilitations de sécurité. Ces autorisations temporaires d'accès aux ICUE sont valables pour une période non renouvelable ne dépassant pas six mois et ne donnent pas accès aux informations classifiées TRÈS SECRET UE/EU TOP SECRET.

2. Après avoir été informées conformément à l'article 12, paragraphe 1, toutes les personnes auxquelles a été délivrée une autorisation temporaire reconnaissent par écrit qu'elles sont conscientes de leurs obligations en matière de protection des ICUE et des conséquences qui pourraient résulter si des ICUE devaient être compromises. L'autorité de sécurité de la Commission tient un registre de ces déclarations écrites.

Article 14

Participation à des réunions classifiées organisées par la Commission

1. Les services de la Commission chargés d'organisation des réunions lors desquelles des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont traitées informent, par l'intermédiaire de leur responsable local de la sécurité ou de l'organisateur de la réunion, l'autorité de sécurité de la Commission suffisamment à l'avance des dates, heures, lieux et participants à ces réunions.

2. Sous réserve des dispositions de l'article 11, paragraphe 13, les personnes désignées pour participer à des réunions organisées par la Commission lors desquelles des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont traitées, ne peuvent le faire qu'après confirmation de leur situation au regard de l'habilitation ou de l'autorisation de sécurité. L'accès à ces réunions classifiées est refusé aux personnes pour lesquelles l'autorité de sécurité de la Commission n'a vu aucun CHSP ni autre preuve d'habilitation de sécurité, ainsi qu'aux participants de la Commission qui ne détiennent pas d'autorisation de sécurité.

3. Avant d'organiser une réunion classifiée, l'organisateur responsable de la réunion ou le responsable local de la sécurité du service de la Commission organisateur de la réunion demande aux participants extérieurs de fournir à l'autorité de sécurité de la Commission un CHSP ou une autre preuve d'habilitation de sécurité. L'autorité de sécurité de la Commission informe le responsable local de la sécurité ou l'organisateur de la réunion de tout CHSP ou autre preuve de HSP qu'elle reçoit. Le cas échéant, il peut être fait usage d'une liste de noms récapitulative mentionnant les preuves d'habilitation de sécurité voulues.

4. Lorsque l'autorité de sécurité de la Commission est informée par les autorités compétentes qu'une HSP a été retirée à une personne dont les fonctions requièrent la participation à des réunions organisées par la Commission, l'autorité de sécurité de la Commission en informe le responsable local de la sécurité du service de la Commission chargé d'organiser la réunion.

Article 15

Accès potentiel aux ICUE

Les courriers, les gardes et les escortes doivent disposer d'une autorisation de sécurité du niveau correspondant ou faire l'objet d'une enquête appropriée conformément aux dispositions législatives et réglementaires nationales, et être informés des procédures de sécurité applicables à la protection des ICUE ainsi que des obligations qui leur incombent en matière de protection des informations de cette nature qui leur sont confiées.

CHAPITRE 3

MESURES DE SÉCURITÉ PHYSIQUE VISANT À PROTÉGER LES INFORMATIONS CLASSIFIÉES

Article 16

Principes de base

1. Les mesures de sécurité physique sont destinées à faire obstacle à toute intrusion par la ruse ou par la force, à avoir un effet dissuasif, à empêcher et détecter les actes non autorisés et permettre d'établir une distinction entre les membres du personnel au regard de l'accès aux ICUE conformément au principe du besoin d'en connaître. Ces mesures sont déterminées sur la base d'une procédure de gestion des risques, conformément à la présente décision et à ses modalités d'application.

2. Plus précisément, les mesures de sécurité physique sont destinées à prévenir l'accès non autorisé aux ICUE en:

a) garantissant que les ICUE sont correctement traitées et stockées;

b) permettant d'établir une distinction entre les membres du personnel au regard de l'accès aux ICUE sur la base de leur besoin d'en connaître et, le cas échéant, de leur autorisation de sécurité;

c) ayant un effet dissuasif, en empêchant et en détectant les actes non autorisés; et

d) en empêchant ou en retardant toute intrusion par la ruse ou par la force.

3. Les mesures physiques de sécurité sont mises en place pour tous les locaux, bâtiments, bureaux, salles et autres zones dans lesquels des ICUE sont traitées ou stockées, y compris les zones où se trouvent les systèmes d'information et de communication visés au chapitre 5.

4. Des zones où sont stockées des ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont créées en tant que zones sécurisées conformément au présent chapitre et agréées par l'autorité d'homologation de sécurité de la Commission.

5. Seuls des équipements ou des dispositifs agréés par l'autorité de sécurité de la Commission sont utilisés pour protéger les ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur.

Article 17

Règles et mesures en matière de sécurité physique

1. Les mesures de sécurité physique sont choisies en fonction d'une évaluation de la menace réalisée par l'autorité de sécurité de la Commission, le cas échéant en concertation avec d'autres services de la Commission, d'autres institutions, agences ou organes de l'Union et/ou les autorités compétentes des États membres. La Commission applique une procédure de gestion du risque pour protéger les ICUE dans ses locaux afin de garantir un niveau de protection physique qui soit proportionné au risque évalué. La procédure de gestion des risques tient compte de tous les facteurs pertinents, et notamment:

a) du niveau de classification des ICUE;

b) de la forme et du volume des ICUE, sachant que l'application de mesures de protection plus strictes pourrait être requise pour des volumes importants ou en cas de compilation d'ICUE;

c) de l'environnement et de la structure des bâtiments ou des zones où se trouvent des ICUE; et

d) de l'évaluation de la menace que constituent les services de renseignement prenant pour cible l'Union, ses institutions, organes ou agences ou les États membres, ainsi que les actes de sabotage, le terrorisme et les activités subversives ou les autres activités criminelles.

2. En appliquant la notion de défense en profondeur, l'autorité de sécurité de la Commission détermine la bonne combinaison de mesures de sécurité physique qu'il convient de mettre en œuvre. À cet effet, l'autorité de sécurité de la Commission élabore des normes et des critères minimaux établis dans les modalités d'application.

3. L'autorité de sécurité de la Commission est autorisée à mener des fouilles aux entrées et aux sorties afin d'avoir un effet dissuasif quant à l'introduction non autorisée de matériel dans des locaux ou des bâtiments ou au retrait non autorisé de toute ICUE des lieux précités.

4. Lorsque des ICUE risquent d'être vues, même accidentellement, les services de la Commission concernés prennent les mesures appropriées, définies par l'autorité de sécurité de la Commission, pour parer à ce risque.

5. Pour les nouveaux établissements, les règles en matière de sécurité physique et leurs spécifications fonctionnelles doivent être définies avec le consentement de l'autorité de sécurité de la Commission lors de la planification et de la conception des établissements. Pour les établissements existants, les règles en matière de sécurité physique doivent être appliquées conformément aux normes et critères minimaux définis dans les modalités d'application.

Article 18

Équipement destiné à la protection physique des ICUE

1. Deux types de zones physiquement protégées sont créés en vue de la protection physique des ICUE:

a) les zones administratives; et

b) les zones sécurisées (dont les zones sécurisées du point de vue technique).

2. Il appartient à l'autorité d'homologation de sécurité de la Commission d'établir qu'une zone répond aux conditions requises pour être désignée comme zone administrative, zone sécurisée ou zone sécurisée du point de vue technique.

3. Pour les zones administratives:

a) un périmètre défini est établi de façon visible afin de permettre le contrôle des personnes et, dans la mesure du possible, des véhicules;

b) ne peuvent y pénétrer sans escorte que les personnes dûment autorisées par l'autorité de sécurité de la Commission ou toute autre autorité compétente; et

c) toutes les autres personnes sont escortées en permanence ou font l'objet de contrôles équivalents.

4. Pour les zones sécurisées:

a) un périmètre défini et protégé est établi de façon visible et toutes les entrées et sorties sont contrôlées par un système de laissez-passer ou d'identification individuelle;

b) ne peuvent y pénétrer sans escorte que les personnes habilitées et expressément autorisées à y entrer sur la base de leur besoin d'en connaître; et

c) toutes les autres personnes sont escortées en permanence ou font l'objet de contrôles équivalents.

5. Lorsque le fait de pénétrer dans une zone sécurisée équivaut en pratique à un accès direct aux informations classifiées qu'elle renferme, les règles supplémentaires suivantes sont d'application:

a) le niveau de classification le plus élevé qui s'applique aux informations conservées habituellement dans la zone doit être clairement indiqué;

b) tous les visiteurs doivent disposer d'une autorisation spécifique pour pénétrer dans la zone, sont escortés en permanence et disposent de l'habilitation de sécurité correspondante, sauf si des mesures sont prises pour empêcher l'accès aux ICUE.

6. Les zones sécurisées qui sont protégées contre les écoutes sont qualifiées de zones sécurisées du point de vue technique. Les règles supplémentaires suivantes sont applicables:

a) ces zones sont équipées d'un système de détection des intrusions (SDI), verrouillées lorsqu'elles ne sont pas occupées et gardées lorsqu'elles sont occupées. Toutes les clés sont gérées conformément à l'article 20;

b) toutes les personnes et tous les matériels entrant dans ces zones sont contrôlés;

c) ces zones doivent faire l'objet, à intervalles réguliers, d'inspections physiques et/ou techniques par l'autorité de sécurité de la Commission. Ces inspections doivent également être effectuées après une entrée non autorisée, réelle ou présumée; et

d) ces zones ne sont pas équipées de lignes de communication, de téléphones ou d'autres dispositifs de communication ou matériels électriques ou électroniques qui ne sont pas autorisés.

7. Nonobstant le paragraphe 6, point d), avant d'être utilisé dans des zones dans lesquelles sont organisées des réunions ou sont exécutées des tâches mettant en jeu des informations classifiées SECRET UE/EU SECRET et d'un niveau de classification supérieur, et lorsque la menace pesant sur des ICUE est jugée élevée, tout dispositif de communication et tout matériel électrique ou électronique est d'abord examiné par l'autorité de sécurité de la Commission pour vérifier qu'aucune information intelligible ne peut être transmise par inadvertance ou de manière illicite par ces équipements en dehors du périmètre de la zone sécurisée.

8. Les zones sécurisées qui ne sont pas occupées vingt-quatre heures sur vingt-quatre par le personnel de service sont, au besoin, inspectées après les heures normales de travail et à intervalles aléatoires en dehors de ces heures, sauf si un SDI a été installé.

9. Des zones sécurisées et des zones sécurisées du point de vue technique peuvent être temporairement établies dans une zone administrative en vue de la tenue d'une réunion classifiée ou à toute autre fin similaire.

10. Le responsable local de la sécurité du service de la Commission concerné établit des procédures d'exploitation de sécurité (SecOP) pour chaque zone sécurisée dont il a la charge, qui précisent, conformément aux dispositions de la présente décision et de ses modalités d'application:

a) le niveau de classification des ICUE traitées ou stockées dans la zone;

b) les mesures de surveillance et de protection qu'il convient de mettre en place;

c) les personnes autorisées à pénétrer dans la zone sans escorte en raison de leur besoin d'en connaître et en fonction de leur autorisation de sécurité;

d) le cas échéant, les procédures applicables aux escortes ou à la protection des ICUE lorsque d'autres personnes sont autorisées à pénétrer dans la zone;

e) les autres mesures et procédures applicables.

11. Les chambres fortes sont installées dans des zones sécurisées. Les murs, les planchers, les plafonds, les fenêtres et les portes verrouillables sont approuvés par l'autorité de sécurité de la Commission et offrent une protection équivalente à celle d'un meuble de sécurité approuvé pour le stockage d'ICUE du même niveau de classification.

Article 19

Mesures de protection physiques applicables au traitement et au stockage des ICUE

1. Les ICUE RESTREINT UE/EU RESTRICTED peuvent être traitées:

a) dans une zone sécurisée;

b) dans une zone administrative à condition que les personnes non autorisées ne puissent avoir accès aux ICUE; ou

c) en dehors d'une zone sécurisée ou d'une zone administrative à condition que le détenteur les transporte conformément à l'article 31 et se soit engagé à se conformer aux mesures compensatoires prévues dans les modalités d'application pour empêcher que des personnes non autorisées aient accès aux ICUE.

2. Les ICUE RESTREINT UE/EU RESTRICTED sont stockées dans un meuble de bureau adapté et fermé dans une zone administrative ou dans une zone sécurisée. Ces informations peuvent être temporairement stockées en dehors d'une zone administrative ou d'une zone sécurisée à condition que le détenteur se soit engagé à se conformer aux mesures compensatoires prévues dans les modalités d'application.

3. Les ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET peuvent être traitées:

a) dans une zone sécurisée;

b) dans une zone administrative à condition que les personnes non autorisées ne puissent avoir accès aux ICUE; ou

c) en dehors d'une zone sécurisée ou d'une zone administrative à condition que le détenteur:

   i) se soit engagé à se conformer aux mesures compensatoires prévues dans les modalités d'application pour empêcher que des personnes non autorisées aient accès aux ICUE;

   ii) exerce en personne un contrôle permanent sur les ICUE; et

   iii) si les documents sont sous forme papier, qu'il en ait informé le bureau d'ordre compétent.

4. Les ICUE classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET sont stockées dans une zone sécurisée, dans un meuble de sécurité ou une chambre forte.

5. Les ICUE classifiées TRÈS SECRET UE/EU TOP SECRET sont traitées dans une zone sécurisée, mise en place et entretenue par l'autorité de sécurité de la Commission, et agréée à ce niveau de classification par l'autorité d'homologation de sécurité de la Commission.

6. Les ICUE classifiées TRÈS SECRET UE/EU TOP SECRET sont stockées dans une zone sécurisée, agréée à ce niveau de classification par l'autorité d'homologation de sécurité de la Commission, selon l'une des modalités suivantes:

a) dans un meuble de sécurité conformément aux dispositions de l'article 18, moyennant un ou plusieurs des contrôles supplémentaires suivants:

   (1) protection ou vérification en permanence par un membre habilité du personnel de sécurité ou du personnel de service;

   (2) un système de détection des intrusions approuvé auquel on associe du personnel de sécurité prêt à intervenir en cas d'incident;

   ou

b) dans une chambre forte équipée d'un système de détection des intrusions à laquelle on associe du personnel de sécurité prêt à intervenir en cas d'incident.

Article 20

Contrôle des clés et combinaisons utilisées pour la protection des ICUE

1. Des procédures de gestion des clés et des combinaisons pour les bureaux, les salles, les chambres fortes et les meubles de sécurité sont définies dans les modalités d'application conformément à l'article 60 ci-après. Ces procédures sont destinées à empêcher un accès non autorisé.

2. Les combinaisons doivent être mémorisées par le plus petit nombre possible de personnes qui ont besoin de les connaître. Les combinaisons des meubles de sécurité et des chambres fortes servant au stockage d'ICUE doivent être changées:

a) à la réception d'un nouveau meuble;

b) lors de tout changement du personnel connaissant la combinaison;

c) en cas de compromission, réelle ou présumée;

d) lorsqu'une serrure a fait l'objet d'un entretien ou d'une réparation; et

e) au moins tous les douze mois.

CHAPITRE 4

GESTION DES INFORMATIONS CLASSIFIÉES DE L'UNION EUROPÉENNE

Article 21

Principes de base

1. Tous les documents d'ICUE doivent être gérés conformément à la politique de la Commission en matière de gestion des documents et doivent donc être répertoriés, enregistrés, conservés puis éliminés, soumis à un échantillonnage ou transférés aux archives historiques conformément à la liste commune de conservation des dossiers au niveau de la Commission européenne.

2. Les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont enregistrées à des fins de sécurité avant leur diffusion et lors de leur réception. Les informations classifiées TRÈS SECRET UE/EU TOP SECRET sont enregistrées dans des bureaux d'ordre désignés.

3. Un système de bureaux d'ordre pour les ICUE est mis en place au sein de la Commission conformément aux dispositions de l'article 27.

4. Les services et les locaux de la Commission dans lesquels les ICUE sont traitées ou stockées font l'objet d'une inspection régulière par l'autorité de sécurité de la Commission.

5. En dehors des zones physiquement protégées, les ICUE sont transmises entre les services et les locaux selon les modalités suivantes:

a) en règle générale, les ICUE sont transmises par voie électronique protégée par des produits cryptographiques agréés conformément au chapitre 5;

b) si la voie visée au point a) n'est pas utilisée, les ICUE sont transportées:

   i) soit sur des supports électroniques (par exemple clé USB, CD, disque dur) protégés par des produits cryptographiques agréés conformément au chapitre 5;

   ii) soit, dans tous les autres cas, de la manière prescrite dans les modalités d'application.

Article 22

Classifications et marquages

1. Les informations sont classifiées dans les cas où elles doivent être protégées compte tenu de leur confidentialité, conformément à l'article 3, paragraphe 1.

2. L'autorité d'origine des ICUE est chargée de déterminer le niveau de classification de sécurité, conformément aux modalités d'application, normes et lignes directrices applicables en matière de classification, et de la diffusion initiale des informations.

3. Le niveau de classification des ICUE est fixé conformément à l'article 3, paragraphe 2, et aux modalités d'application correspondantes.

4. La classification de sécurité est clairement et correctement indiquée, indépendamment de la forme sous laquelle se présentent les ICUE: format papier, forme orale, électronique ou autre.

5. Les différentes parties d'un document donné (pages, paragraphes, sections, annexes, appendices et pièces jointes) peuvent nécessiter une classification différente et doivent alors porter le marquage afférent, y compris lorsqu'elles sont stockées sous forme électronique.

6. Le niveau général de classification d'un document ou d'un dossier est au moins aussi élevé que celui de sa partie portant la classification la plus élevée. Lorsqu'il rassemble des informations provenant de plusieurs sources, le document final est examiné pour en fixer le niveau général de classification de sécurité car il peut requérir un niveau de classification supérieur à celui de chacune des parties qui le composent.

7. Dans la mesure du possible, les documents dont toutes les parties n'ont pas le même niveau de classification sont structurés de manière que les parties ayant des niveaux de classification différents puissent au besoin être aisément identifiées et séparées des autres.

8. Les lettres ou notes d'envoi accompagnant des pièces jointes portent le plus haut niveau de classification attribué à ces dernières. L'autorité d'origine indique clairement leur niveau de classification lorsqu'elles sont séparées de leurs pièces jointes, au moyen d'un marquage approprié, par exemple:

CONFIDENTIEL UE/EU CONFIDENTIAL

Sans pièce(s) jointe(s) RESTREINT UE/EU RESTRICTED

Article 23

Marquages

Outre l'un des marquages de classification de sécurité prévus à l'article 3, paragraphe 2, les ICUE peuvent porter des marquages complémentaires, tels que:

a) un identifiant désignant l'autorité d'origine;

b) des marquages restrictifs, des mots-codes ou des acronymes utilisés pour préciser le domaine d'activité sur lequel porte le document ou pour indiquer une diffusion particulière en fonction du besoin d'en connaître ou des restrictions d'utilisation;

c) des marquages relatifs à la communicabilité;

d) le cas échéant, la date ou l'événement particulier à partir desquels elles peuvent être déclassées ou déclassifiées.

Article 24

Abréviations indiquant la classification

1. Des abréviations uniformisées indiquant la classification peuvent être utilisées pour préciser le niveau de classification des différents paragraphes d'un texte. Les abréviations ne remplacent pas la mention de la classification en toutes lettres.

2. Les abréviations uniformisées ci-après peuvent être utilisées dans les documents classifiés de l'Union européenne pour indiquer le niveau de classification de sections ou blocs de texte de moins d'une page:

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

Article 25

Création d'ICUE

1. Lors de la création de documents classifiés de l'Union européenne:

a) sur chaque page figure un marquage indiquant clairement le niveau de classification;

b) chaque page est numérotée;

c) le document porte un numéro d'enregistrement et un sujet qui n'est pas lui-même une information classifiée, sauf s'il s'est vu apposer un marquage à ce titre;

d) le document est daté;

e) les documents classifiés SECRET UE/EU SECRET ou d'un niveau de classification supérieur portent un numéro d'exemplaire sur chaque page dès lors qu'ils doivent être diffusés en plusieurs exemplaires.

2. Lorsqu'il n'est pas possible d'appliquer le paragraphe 1 à des ICUE, d'autres mesures appropriées sont prises conformément aux modalités d'application.

Article 26

Déclassement et déclassification des ICUE

1. Au moment de la création du document classifié, l'autorité d'origine indique, si possible, si les ICUE qui y figurent peuvent ou non être déclassées ou déclassifiées à une date donnée ou après un événement spécifique.

2. Chaque service de la Commission réexamine régulièrement les ICUE dont il est l'autorité d'origine pour déterminer si leur niveau de classification est toujours d'application. Un système pour réexaminer au moins une fois tous les cinq ans le niveau de classification des ICUE enregistrées dont la Commission est l'auteur est instauré conformément aux modalités d'application. Un tel réexamen n'est pas nécessaire lorsque l'autorité d'origine a indiqué dès le départ que les informations seraient automatiquement déclassées ou déclassifiées et que celles-ci se sont vu apposer les marquages correspondants.

3. Les informations classifiées RESTREINT UE/EU RESTRICTED dont la Commission est l'auteur sont considérées comme étant automatiquement déclassifiées à l'issue d'une période de trente ans, conformément au règlement (CEE, Euratom) nº 354/83 du Conseil modifié par le règlement (CE, Euratom) nº 1700/2003 du Conseil ([1]).

Article 27

Bureaux d'ordre pour les ICUE au sein de la Commission

1. Sans préjudice de l'article 52, paragraphe 5 ci-après, dans chaque service de la Commission où des ICUE de niveau CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET sont traitées ou stockées, on détermine un bureau d'ordre local compétent chargé de veiller à ce que les ICUE soient traitées conformément à la présente décision.

2. Le bureau d'ordre géré par le secrétariat général représente le bureau d'ordre central pour les ICUE. Il constitue:

— le bureau d'ordre local pour le secrétariat général de la Commission;

— le bureau d'ordre pour les cabinets privés des membres de la Commission, sauf s'ils disposent d'un bureau d'ordre local désigné pour les ICUE;

— le bureau d'ordre pour les directions générales ou les services qui n'ont pas de bureau d'ordre local pour les ICUE;

— le principal point d'entrée et de sortie pour toutes les informations classifiées RESTREINT UE/EU RESTRICTED et d'un niveau de classification supérieur jusqu'à SECRET UE/EU SECRET inclus, échangées entre la Commission et ses services et des pays tiers et organisations internationales, ainsi que, si des dispositions spécifiques le prévoient, pour d'autres institutions, agences et organes de l'Union européenne.

3. Au sein de la Commission, un bureau d'ordre est désigné par l'autorité de sécurité de la Commission pour faire fonction d'autorité centrale de réception et de diffusion des informations classifiées TRÈS SECRET UE/EU TOP SECRET. S'il y a lieu, les bureaux d'ordre subordonnés peuvent être désignés pour traiter ces informations à des fins d'enregistrement.

4. Ces bureaux d'ordre subordonnés ne peuvent transmettre de documents TRÈS SECRET UE/EU TOP SECRET directement à d'autres bureaux d'ordre subordonnés rattachés au même bureau d'ordre TRÈS SECRET UE/EU TOP SECRET central sans l'autorisation expresse et écrite de ce dernier, ni à des bureaux d'ordre extérieurs.

5. Les bureaux d'ordre pour les ICUE sont conçus comme des zones sécurisées telles que définies au chapitre 3 et agréées par l'autorité d'homologation de sécurité de la Commission (AHS).

Article 28

Agent contrôleur

1. Chaque bureau d'ordre pour les ICUE est géré par un agent contrôleur (RCO).

2. L'agent contrôleur dispose d'une habilitation de sécurité appropriée.

3. L'agent contrôleur est placé sous la supervision du responsable local de la sécurité au sein du service de la Commission pour ce qui concerne l'application des dispositions relatives à la manipulation des ICUE et la mise en œuvre des règles, normes et lignes directrices correspondantes en matière de sécurité.

4. Dans le cadre de ses responsabilités de gestion du bureau d'ordre pour les ICUE auquel il est affecté, l'agent contrôleur exécute les tâches générales suivantes conformément à la présente décision et aux modalités d'application, normes et lignes directrices correspondantes:

— gestion des opérations relatives à l'enregistrement, la conservation, la reproduction, la traduction, la transmission, l'expédition et la destruction des ICUE ou leur transfert au service des archives historiques;

— vérification périodique de la nécessité de maintenir la classification de ces informations;

— exécution de toute autre tâche en relation avec la protection des ICUE définie dans les modalités d'application.

Article 29

Enregistrement des ICUE à des fins de sécurité

1. Aux fins de la présente décision, on entend par enregistrement à des fins de sécurité (ci-après dénommé «enregistrement») l'application de procédures permettant de garder la trace du cycle de vie des ICUE, y compris de leur diffusion.

([1]) Règlement (CE, Euratom) nº 1700/2003 du Conseil du 22 septembre 2003 modifiant le règlement (CEE, Euratom) nº 354/83 concernant l'ouverture au public des archives historiques de la Communauté économique européenne et de la Communauté européenne de l'énergie atomique (JO L 243 du 27.9.2003, p. 1).

2. Tout élément d'information ou matériel classifié CONFIDENTIEL UE/EU CONFIDENTIAL et d'un niveau de classification supérieur est enregistré par un bureau d'ordre déterminé à chaque fois qu'il est réceptionné ou expédié par une entité structurée.

3. Lorsque les ICUE sont traitées ou stockées à l'aide d'un système d'information et de communication (SIC), les procédures d'enregistrement peuvent être mises en œuvre au moyen de processus intervenant au sein du SIC même.

4. Les modalités d'application contiennent des dispositions plus détaillées concernant l'enregistrement des ICUE à des fins de sécurité.

Article 30

Duplication et traduction des documents classifiés de l'Union européenne

1. Les documents classifiés TRÈS SECRET UE/EU TOP SECRET ne doivent pas être dupliqués ou traduits sans le consentement écrit préalable de l'autorité d'origine.

2. Lorsque l'autorité d'origine de documents classifiés SECRET UE/EU SECRET et d'un niveau de classification inférieur n'a pas imposé de restrictions à leur duplication ou à leur traduction, lesdits documents peuvent être dupliqués ou traduits sur instruction du détenteur.

3. Les mesures de sécurité applicables au document original le sont aussi à ses copies et à ses traductions.

Article 31

Transport des ICUE

1. Les ICUE sont transportées de manière à les protéger contre toute divulgation non autorisée durant le transport.

2. Le transport des ICUE est soumis à des mesures de protection:

— en adéquation avec le niveau de classification des ICUE transportées;

— adaptées aux conditions spécifiques de leur transport, notamment selon que les ICUE sont transportées:

  — à l'intérieur d'un même bâtiment de la Commission ou d'un groupe autonome de bâtiments de la Commission,

  — entre des bâtiments de la Commission situés dans un même État membre,

  — à l'intérieur de l'Union,

  — de l'Union vers le territoire d'un État tiers; et

  — adaptées à la nature et la forme des ICUE concernées.

3. Ces mesures de protection sont indiquées en détail dans les modalités d'application ou, dans le cas de projets et programmes visés à l'article 42, en tant que partie intégrante des instructions de sécurité relatives à un programme ou un projet (ISP).

4. Les modalités d'application ou les ISP incluent des dispositions en rapport avec le niveau de classification des ICUE concernant:

— le mode de transport, à savoir transport par porteur, courrier diplomatique ou militaire, services postaux ou services de courrier commercial;

— l'emballage des ICUE;

— les contre-mesures techniques pour les ICUE transportées sur support électronique;

— toute autre mesure de nature procédurale, physique ou électronique;

— les procédures d'enregistrement;

— l'emploi de personnel disposant d'autorisations de sécurité.

5. Lorsque les ICUE sont transportées par des supports électroniques, et nonobstant l'article 21, paragraphe 5, les mesures de protection énoncées dans les modalités d'application correspondantes peuvent être complétées par des contre-mesures techniques appropriées approuvées par l'autorité de sécurité de la Commission, de façon à réduire au minimum le risque de perte ou de compromission.

Article 32

Destruction des ICUE

1. Les documents classifiés de l'Union européenne qui ne sont plus nécessaires peuvent être détruits, compte tenu des règlements relatifs aux archives et des règles et règlements de la Commission relatifs à la gestion et à l'archivage des documents, en particulier la liste commune de conservation des dossiers au niveau de la Commission européenne.

2. Les ICUE de niveau CONFIDENTIEL UE/EU CONFIDENTIAL et d'un niveau de classification supérieur sont détruites par l'agent contrôleur du bureau d'ordre compétent sur instruction du détenteur ou d'une autorité compétente. L'agent contrôleur actualise en conséquence les cahiers d'enregistrement et les autres informations relatives aux enregistrements.

3. La destruction de documents classifiés SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET est effectuée par l'agent contrôleur en présence d'un témoin justifiant de l'habilitation de sécurité correspondant au moins au niveau de classification du document à détruire.

4. L'agent du bureau d'ordre et le témoin, lorsque la présence de ce dernier est requise, signent un procès-verbal de destruction qui est rempli dans le bureau d'ordre. L'agent contrôleur du bureau d'ordre compétent conserve les procès-verbaux de destruction des documents TRÈS SECRET UE/EU TOP SECRET pendant dix ans au minimum, et ceux des documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET pendant cinq ans au minimum.

5. Les documents classifiés, y compris ceux dont la classification est RESTREINT UE/EU RESTRICTED, sont détruits par des méthodes définies dans les modalités d'application et répondant aux normes UE applicables ou à des normes équivalentes.

6. La destruction des supports de données informatiques utilisés pour les ICUE s'effectue conformément aux procédures définies dans les modalités d'application.

Article 33

Destruction des ICUE en cas d'urgence

1. Les services de la Commission qui détiennent des ICUE établissent des plans tenant compte des conditions locales pour assurer la sauvegarde en temps de crise des matériels classifiés de l'Union européenne, y compris si nécessaire des plans de destruction et d'évacuation en cas d'urgence. Ils émettent les consignes qu'ils jugent appropriées pour éviter que des ICUE ne tombent entre les mains de personnes non autorisées.

2. Les dispositions prises pour la sauvegarde et/ou la destruction en temps de crise des matériels CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET ne doivent en aucun cas nuire à la sauvegarde ni à la destruction des matériels TRÈS SECRET UE/EU TOP SECRET, et notamment des matériels de chiffrement, dont la prise en charge doit avoir la priorité sur toutes les autres tâches.

3. En cas d'urgence, s'il existe un risque imminent de divulgation non autorisée, les ICUE sont détruites par le détenteur de manière à ce qu'elles ne puissent pas être reconstituées en tout ou en partie. L'autorité d'origine et le bureau d'ordre d'origine sont informés de la destruction en urgence d'ICUE enregistrées.

4. Les modalités d'application contiennent des dispositions plus détaillées concernant la destruction des ICUE.

CHAPITRE 5

PROTECTION DES INFORMATIONS CLASSIFIÉES DE L'UNION EUROPÉENNE DANS LES SYSTÈMES D'INFORMATION ET DE COMMUNICATION (SIC)

Article 34

Principes d'assurance de l'information

1. Par «assurance de l'information (AI) dans le domaine des systèmes d'information et de communication», on entend la certitude que ces systèmes protégeront les informations qu'ils traitent et fonctionneront comme ils le doivent, quand ils le doivent, sous le contrôle d'utilisateurs légitimes.

2. Une assurance de l'information efficace garantit des niveaux appropriés de:

Authenticité: garantie que l'information est véridique et émane de sources dignes de foi;

Disponibilité: caractéristique de l'information selon laquelle elle est accessible et utilisable, à la demande d'une entité autorisée;

Confidentialité: propriété selon laquelle les informations ne sont pas divulguées à des personnes ou à des entités non autorisées et l'accès à ces informations n'est pas accordé à des processus non autorisés;

Intégrité: propriété consistant à préserver l'exactitude et le caractère complet des informations et éléments;

Non-répudiation: la possibilité de prouver qu'une action ou un événement a eu lieu, de sorte qu'il ne peut être contesté par la suite.

3. L'AI est fondée sur un processus de gestion des risques.

Article 35

Définitions

Aux fins du présent chapitre, les définitions suivantes sont applicables:

a) par «homologation», on entend l'agrément formel d'un système d'information et de communication par l'autorité d'homologation de sécurité (AHS) autorisant son emploi pour traiter des ICUE dans son environnement opérationnel, après la validation formelle du plan de sécurité et la mise en œuvre adéquate de celui-ci;

b) par «processus d'homologation», on entend les étapes et tâches requises avant d'obtenir l'agrément de l'autorité d'homologation de sécurité. Ces étapes et tâches sont définies dans une norme de processus d'homologation;

c) on entend par «système d'information et de communication» (SIC) tout système permettant le traitement d'informations sous forme électronique. Un système d'information et de communication comprend l'ensemble des moyens nécessaires pour le faire fonctionner, y compris l'infrastructure, l'organisation, le personnel et les ressources d'information;

d) on entend par «risque résiduel» le risque qui subsiste après que des mesures de sécurité ont été mises en œuvre, étant entendu qu'il est impossible de contrer toutes les menaces et d'éliminer toutes les vulnérabilités;

e) on entend par «risque» la possibilité qu'une menace donnée se concrétise en tirant parti des vulnérabilités internes et externes d'une organisation ou d'un des systèmes qu'elle utilise et cause ainsi un préjudice à l'organisation ou à ses ressources matérielles ou immatérielles. Il se mesure en tenant compte à la fois de la probabilité de voir se concrétiser des menaces et de l'impact de celles-ci;

f) l'«acceptation des risques» consiste à décider d'accepter qu'un risque résiduel subsiste au terme du traitement des risques;

g) l'«évaluation des risques» consiste à déterminer les menaces et les vulnérabilités et à procéder à l'analyse des risques correspondants, c'est-à-dire à examiner leur probabilité et leur impact;

h) la «communication des risques» consiste à sensibiliser la communauté des utilisateurs du SIC aux risques, à informer les autorités d'homologation de ces risques et à faire rapport à leur sujet aux autorités responsables de l'exploitation;

i) le «traitement des risques» consiste à atténuer, à éliminer, à réduire (par un ensemble approprié de mesures sur le plan technique, physique ou au niveau de l'organisation ou des procédures), à transférer ou à surveiller les risques.

Article 36

SIC traitant des ICUE

1. Les SIC traitent des ICUE dans le respect de la notion d'AI.

2. Pour les SIC traitant des ICUE, le respect de la politique de sécurité des systèmes d'information de la Commission, telle qu'énoncée dans la décision C(2006)3602 ([1]) de la Commission, implique:

a) l'application de la méthode «planifier-déployer-contrôler-agir» pour la mise en œuvre de la politique de sécurité des systèmes d'information tout au long du cycle de vie du système d'information;

b) la détermination des besoins de sécurité au moyen d'une évaluation d'impact sur l'activité;

c) la réalisation d'une classification formelle des éléments pour le système d'information et les données qu'il contient;

([1]) C(2006) 3602 du 16 août 2006 relative à la sécurité des systèmes d'information utilisés par les services de la Commission.

d) la mise en œuvre de toutes les mesures de sécurité obligatoires définies par la politique de sécurité des systèmes d'information;

e) l'application d'un processus de gestion des risques, composé des étapes suivantes: identification des menaces et des vulnérabilités, évaluation des risques, traitement des risques, acceptation des risques et communication des risques;

f) la définition d'un plan de sécurité, incluant la politique de sécurité et les procédures d'exploitation de sécurité, ainsi que sa mise en œuvre, sa vérification et sa révision.

3. L'ensemble du personnel participant à l'élaboration, au développement, aux essais, au fonctionnement, à la gestion ou à l'utilisation des SIC traitant des ICUE notifie à l'AHS toutes les faiblesses en matière de sécurité, les incidents, les infractions à la sécurité ou les compromissions potentiels susceptibles d'avoir un impact sur la protection du SIC et/ou des ICUE qu'il contient.

4. Lorsque la protection des ICUE est assurée par des produits cryptographiques, ces produits doivent être approuvés comme suit:

a) la préférence est donnée aux produits agréés par le Conseil ou par le secrétaire général du Conseil en sa qualité d'autorité d'agrément cryptographique du Conseil, sur recommandation du groupe d'experts sécurité de la Commission;

b) lorsque des motifs opérationnels particuliers le justifient, l'autorité d'agrément cryptographique de la Commission (AAC) peut, sur recommandation du groupe d'experts sécurité de la Commission, ne pas respecter les exigences prévues au point a) et délivrer un agrément à titre provisoire pour une période spécifique.

5. Lors de la transmission, du traitement et du stockage des ICUE par voie électronique, des produits cryptographiques qui ont fait l'objet d'un agrément sont utilisés. Nonobstant cette exigence, des procédures spécifiques peuvent être appliquées en cas d'urgence ou dans le cadre de configurations techniques spécifiques après agrément de l'AAC.

6. Des mesures de sécurité sont mises en œuvre afin de protéger les SIC traitant des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur contre la compromission de ces informations par des émissions électromagnétiques non intentionnelles («mesures de sécurité TEMPEST»). Ces mesures de sécurité sont proportionnées au risque d'exploitation et au niveau de classification des informations.

7. L'autorité de sécurité de la Commission exerce les fonctions suivantes:

— autorité chargée de l'AI (AAI);

— autorité d'homologation de sécurité (AHS);

— autorité TEMPEST (AT);

— autorité d'agrément cryptographique (AAC);

— autorité chargée de la distribution cryptographique (ADC).

8. Pour chaque système, l'autorité de sécurité de la Commission désigne une autorité opérationnelle chargée de l'AI.

9. Les responsabilités des fonctions décrites aux paragraphes 7 et 8 seront définies dans les modalités d'application.

Article 37

Homologation des SIC traitant des ICUE

1. Tous les SIC traitant des ICUE font l'objet d'un processus d'homologation basé sur les principes d'AI, dont le niveau de détail doit être proportionné au niveau de protection requis.

2. Le processus d'homologation inclut la validation formelle par l'AHS de la Commission du plan de sécurité pour le SIC concerné, afin d'obtenir l'assurance que:

a) le processus de gestion des risques visé à l'article 36, paragraphe 2, a été correctement mis en œuvre;

b) le détenteur du système a accepté le risque résiduel en connaissance de cause; et

c) un niveau suffisant de protection du SIC et des ICUE qu'il traite a été atteint conformément à la présente décision.

3. L'AHS de la Commission délivre une déclaration d'homologation qui détermine le niveau maximal de classification des ICUE qui peuvent être traitées dans un SIC ainsi que les modalités et les conditions de fonctionnement correspondantes. Cette disposition s'applique sans préjudice des missions du conseil d'homologation de sécurité défini à l'article 11 du règlement (UE) nº 512/2014 du Parlement européen et du Conseil [1].

4. Un comité conjoint d'homologation de sécurité (CHS) est chargé de l'homologation des SIC de la Commission qui impliquent plusieurs parties. Ce comité est composé d'un représentant de l'AHS de chaque partie concernée et présidé par un représentant de l'AHS de la Commission.

5. Le processus d'homologation consiste en une série de tâches exécutées par les parties concernées. La responsabilité de la préparation des dossiers d'homologation et de la documentation incombe entièrement au détenteur du SIC.

6. L'homologation relève de la responsabilité de l'AHS de la Commission qui, à tout moment au cours du cycle de vie du SIC, est habilitée à:

a) exiger qu'un processus d'homologation soit appliqué;

b) procéder à un audit ou une inspection du SIC;

c) si les conditions de fonctionnement ne sont plus satisfaites, exiger l'élaboration et la mise en œuvre effective d'un plan d'amélioration de la sécurité selon un calendrier bien défini, en retirant éventuellement l'autorisation d'utiliser le SIC jusqu'à ce que les conditions de son fonctionnement soient à nouveau satisfaites.

7. Le processus d'homologation est établi dans une norme sur le processus d'homologation applicable aux SIC traitant des ICUE, adoptée conformément à l'article 10, paragraphe 3, de la décision C(2006) 3602.

Article 38

Situations d'urgence

1. Nonobstant les dispositions du présent chapitre, les procédures spécifiques décrites ci-après peuvent être appliquées dans les situations d'urgence, telles que les crises, les conflits ou les guerres, imminentes ou effectives, ou dans des circonstances opérationnelles exceptionnelles.

2. Sous réserve du consentement de l'autorité compétente, les ICUE peuvent être transmises au moyen de produits cryptographiques agréés pour un niveau de classification inférieur ou sans faire l'objet d'un chiffrement dans le cas où tout retard causerait un préjudice indéniablement plus important que celui qui découlerait de la divulgation du matériel classifié et dans les conditions suivantes:

a) l'expéditeur et le destinataire ne possèdent pas le dispositif de chiffrement nécessaire; et

b) le matériel classifié ne peut être communiqué en temps voulu par aucun autre moyen.

3. Les informations classifiées transmises dans les conditions visées au paragraphe 1 ne portent aucun marquage ni indication qui les distinguerait d'informations non classifiées ou pouvant être protégées à l'aide d'un produit cryptographique disponible. Leur destinataire est informé, sans délai et par d'autres moyens, du niveau de classification.

4. Un rapport est adressé par la suite à l'autorité compétente et au groupe d'experts sécurité de la Commission.

CHAPITRE 6

SÉCURITÉ INDUSTRIELLE

Article 39

Principes de base

1. Par «sécurité industrielle», on entend l'application de mesures visant à assurer la protection des ICUE

a) dans le cadre de contrats classifiés, par:

   i) des candidats ou des soumissionnaires tout au long de la durée de la procédure d'appel d'offres et de passation de marché,

   ii) des contractants ou des sous-traitants tout au long du cycle de vie des contrats classifiés;

[1] Règlement (CE) nº 512/2014 du Parlement européen et du Conseil du 16 avril 2014 modifiant le règlement (UE) nº 912/2010 établissant l'Agence du GNSS européen (JO L 150 du 20.5.2014, p. 72).

b) dans le cadre de conventions de subvention classifiées, par:

i) des candidats durant les procédures d'octroi de subventions;

ii) des bénéficiaires tout au long du cycle de vie des conventions de subvention classifiées.

2. De tels contrats ou conventions de subvention ne doivent pas concerner des informations classifiées TRÈS SECRET UE/EU TOP SECRET.

3. Sauf mention contraire, les dispositions du présent chapitre visant des contrats classifiés ou des contractants s'appliquent également aux contrats de sous-traitance classifiés et aux sous-traitants.

Article 40

Définitions

Aux fins du présent chapitre, on entend par:

a) «contrat classifié», un contrat-cadre ou un contrat, tel que défini dans le règlement (CE, Euratom) nº 1605/2002 ([1]), conclu par la Commission ou l'un de ses services avec un contractant en vue de la fourniture de biens meubles ou immeubles, de la réalisation de travaux ou de la prestation de services, dont l'exécution requiert ou implique la création, le traitement ou le stockage d'ICUE;

b) «contrat de sous-traitance classifié», un contrat conclu par un contractant de la Commission ou de l'un de ses services avec un autre contractant (c'est-à-dire le sous-traitant) en vue de la fourniture de biens meubles ou immeubles, de la réalisation de travaux ou de la prestation de services, dont l'exécution nécessite ou implique la création, le traitement ou le stockage d'ICUE;

c) «convention de subvention classifiée», une convention aux termes de laquelle la Commission octroie une subvention, telle que définie dans la première partie, titre VI, du règlement (CE, Euratom) nº 1605/2002, et dont l'exécution nécessite ou implique la création, le traitement ou le stockage d'ICUE;

d) «autorité de sécurité désignée (ASD)», l'autorité responsable devant l'autorité nationale de sécurité (ANS) d'un État membre qui est chargée de communiquer à des entités industrielles ou autres la politique nationale dans tous les domaines relevant de la sécurité industrielle et de fournir des orientations et une aide pour sa mise en œuvre. Les fonctions de l'ASD peuvent être exercées par l'ANS ou par toute autre autorité compétente.

Article 41

Procédure applicable aux contrats et conventions de subvention classifiés

1. En tant qu'autorité contractante, chaque service de la Commission veille à ce que les normes minimales de sécurité industrielle prévues dans le présent chapitre soient mentionnées ou intégrées dans le contrat et respectées lors de l'octroi de contrats ou conventions de subvention classifiés.

2. Aux fins du paragraphe 1, les services compétents au sein de la Commission demandent l'avis de la direction générale des ressources humaines et de la sécurité, en particulier la direction de la sécurité, et veillent à ce que les contrats et contrats de sous-traitance types et les conventions de subvention types incluent des dispositions reflétant les principes de base et les normes minimales de protection des ICUE que doivent respecter les contractants et les sous-traitants, de même que les bénéficiaires des conventions de subvention.

3. La Commission collabore étroitement avec l'ANS, l'ASD ou toute autre autorité compétente des États membres concernés.

4. Lorsqu'une autorité contractante envisage de lancer une procédure visant à conclure un contrat classifié ou une convention de subvention classifiée, elle demande l'avis de l'autorité de sécurité de la Commission sur les questions concernant la classification et les éléments de la procédure à tous les stades de celle-ci.

5. Les modèles pour les contrats et contrats de sous-traitance classifiés, les conventions de subvention classifiées, les avis de marché, les documents d'orientation concernant les conditions dans lesquelles des habilitations de sécurité d'établissement (HSE) sont requises, les instructions de sécurité relatives à un programme/un projet (ISP), les annexes de sécurité (AS), les visites, la transmission et le transport d'ICUE dans le cadre de contrats ou de conventions de subvention classifiés, sont établis dans les modalités d'application sur la sécurité industrielle, après consultation du groupe d'experts sécurité de la Commission.

([1]) Règlement (CE, Euratom) nº 1605/2002 du Conseil du 25 juin 2002 portant règlement financier applicable au budget général des Communautés européennes (JO L 248 du 16.9.2002, p. 1).

6. La Commission peut conclure des contrats ou des conventions de subvention classifiés destinés à confier à des opérateurs économiques immatriculés dans un État membre ou dans un État tiers ayant conclu un accord ou un arrangement administratif en vertu du chapitre 7 de la présente décision, des tâches qui impliquent ou nécessitent l'accès, le traitement ou le stockage d'ICUE.

Article 42

Aspects liés à la sécurité dans un contrat classifié ou une convention de subvention classifiée

1. Les contrats classifiés ou les conventions de subvention classifiées incluent les aspects suivants liés à la sécurité:

Instructions de sécurité relatives à un programme/un projet

a) Par «instructions de sécurité relatives à un programme/un projet» (ISP), on entend une liste des procédures de sécurité appliquées à un programme ou à un projet spécifique en vue d'uniformiser ces procédures. Elles peuvent être revues tout au long de la durée du programme ou du projet.

b) La direction générale des ressources humaines et de la sécurité élabore des ISP génériques; les services de la Commission chargés des programmes ou des projets impliquant le traitement ou le stockage d'ICUE peuvent élaborer, le cas échéant, des ISP spécifiques basées sur les ISP génériques.

c) Des ISP spécifiques sont élaborées en particulier pour les programmes et les projets caractérisés par l'importance de leur portée, leur échelle ou leur complexité, ou par la multitude et/ou la diversité des contractants, bénéficiaires et autres partenaires et acteurs impliqués, par exemple en ce qui concerne leur statut juridique. Les ISP spécifiques sont élaborées par le ou les services de la Commission gérant le programme ou le projet, en coopération étroite avec la direction générale des ressources humaines et de la sécurité.

d) La direction générale des ressources humaines et de la sécurité soumet les ISP génériques et spécifiques pour avis au groupe d'experts sécurité de la Commission.

Annexe de sécurité

a) Par «annexe de sécurité» (AS), on entend un ensemble de conditions contractuelles spéciales, établi par l'autorité contractante, qui fait partie intégrante de tout contrat classifié impliquant l'accès à des ICUE ou la création de telles informations, dans lequel sont définis les conditions de sécurité ou les éléments du contrat qui doivent être protégés pour des raisons de sécurité.

b) Les impératifs de sécurité propres à un contrat sont exposés dans une AS. Le cas échéant, l'AS contient le guide de la classification de sécurité (GCS) et fait partie intégrante du contrat ou du contrat de sous-traitance classifié ou de la convention de subvention classifiée.

c) L'AS contient les dispositions imposant au contractant ou au bénéficiaire de respecter les normes minimales énoncées dans la présente décision. L'autorité contractante s'assure que l'AS indique que le non-respect de ces normes minimales peut constituer un motif suffisant de résiliation du contrat ou de la convention de subvention.

2. Les ISP et les AS incluent un GCS en tant qu'élément de sécurité obligatoire:

a) par «guide de la classification de sécurité» (GCS), on entend un document qui décrit les éléments d'un programme, projet, contrat ou convention de subvention qui sont classifiés, et précise les niveaux de classification de sécurité applicables. Le GCS peut être étoffé tout au long de la durée du programme, projet, contrat ou convention de subvention et les éléments d'information peuvent être reclassifiés ou déclassés; lorsqu'il existe, le GCS fait partie de l'AS.

b) Avant de lancer un appel d'offres en vue de l'attribution d'un contrat classifié ou d'attribuer un tel contrat, le service de la Commission, en sa qualité d'autorité contractante, détermine la classification de sécurité de toute information devant être fournie aux candidats, soumissionnaires ou contractants, ainsi que la classification de sécurité de toute information devant être créée par le contractant. Dans cette perspective, il élabore un GCS qui sera utilisé aux fins de l'exécution du contrat, conformément à la présente décision et à ses modalités d'application, après consultation de l'autorité de sécurité de la Commission.

c) Les principes ci-après sont appliqués pour déterminer le niveau de classification de sécurité des différents éléments d'un contrat classifié:

i) dans le cadre de l'élaboration d'un GCS, le service de la Commission, en tant qu'autorité contractante, tient compte de tous les aspects pertinents en matière de sécurité, y compris de la classification de sécurité attribuée aux informations fournies et dont l'utilisation aux fins du contrat a été approuvée par l'autorité d'origine desdites informations;

ii) le niveau général de classification du contrat ne peut pas être inférieur à la classification la plus élevée de l'un de ses éléments; et

iii) le cas échéant, l'autorité contractante se met en rapport, par l'intermédiaire de l'autorité de sécurité de la Commission, avec les ANS, les ASD ou toute autre autorité de sécurité compétente des États membres dans l'éventualité d'une modification touchant au niveau de classification des informations créées par les contractants ou fournies à ceux-ci dans le cadre de l'exécution d'un contrat et lors de toute modification ultérieure du GCS.

Article 43

Accès aux ICUE pour le personnel des contractants et des bénéficiaires

L'autorité contractante ou qui octroie la subvention veille à ce que le contrat classifié ou la convention de subvention classifiée renferme des dispositions indiquant que le personnel d'un contractant, sous-traitant ou bénéficiaire qui, aux fins de l'exécution du contrat, contrat de sous-traitance ou convention de subvention classifié(e), requiert l'accès à des ICUE, peut se voir accorder un tel accès uniquement si les conditions suivantes sont remplies:

a) s'être vu accorder une autorisation de sécurité du niveau correspondant ou avoir été dûment autorisé en fonction de son besoin d'en connaître;

b) avoir été informé des règles de sécurité applicables à la protection des ICUE et avoir reconnu les responsabilités qui lui incombent en matière de protection de ces informations;

c) avoir reçu une habilitation de sécurité du niveau correspondant pour les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET par l'ANS, l'ASD ou toute autre autorité compétente respective.

Article 44

Habilitation de sécurité d'établissement

1. Par «habilitation de sécurité d'établissement» (HSE), on entend une décision administrative prise par une ANS, une ASD ou toute autre autorité de sécurité compétente selon laquelle, du point de vue de la sécurité, un établissement peut assurer un niveau suffisant de protection pour les ICUE d'un niveau de classification de sécurité déterminé.

2. Une HSE est délivrée par l'ANS, l'ASD ou toute autre autorité de sécurité compétente d'un État membre afin d'indiquer, conformément aux dispositions législatives et réglementaires nationales, qu'un opérateur économique est en mesure, au sein de ses établissements, de garantir aux ICUE la protection adaptée au niveau de classification approprié (CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET). Cette HSE est présentée à l'autorité de sécurité de la Commission qui la transmet au service de la Commission agissant en qualité d'autorité contractante ou octroyant la subvention, avant qu'un candidat, soumissionnaire ou contractant, ou demandeur ou bénéficiaire d'une subvention, puisse recevoir des ICUE ou avoir accès à des ICUE.

3. S'il y a lieu, l'autorité contractante avertit, par l'intermédiaire de l'autorité de sécurité de la Commission, l'ANS, l'ASD ou toute autre autorité de sécurité compétente concernée qu'une HSE est nécessaire pour l'exécution du contrat. Une HSE ou une HSP est requise lorsque des ICUE classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET doivent être fournies dans le cadre de la procédure de passation de marché ou d'octroi de subvention.

4. L'autorité contractante ou qui octroie la subvention n'attribue pas de contrat classifié ou de convention de subvention classifiée au soumissionnaire ou participant sélectionné tant que l'ANS, l'ASD ou toute autre autorité de sécurité compétente de l'État membre dans lequel le contractant ou le soumissionnaire concerné est immatriculé, ne lui a pas confirmé qu'une HSE appropriée a été délivrée.

5. Lorsque l'autorité de sécurité de la Commission a été avertie par l'ANS, l'ASD ou toute autre autorité de sécurité compétente ayant délivré une HSE, de modifications apportées à ladite HSE, elle informe le service de la Commission agissant en qualité d'autorité contractante ou qui octroie la subvention. Dans le cadre d'un contrat de sous-traitance, l'ANS, l'ASD ou toute autre autorité de sécurité compétente en est informée.

6. Pour l'autorité contractante ou qui octroie la subvention, le retrait d'une HSE par l'ANS, l'ASD ou toute autre autorité de sécurité compétente concernée constitue un motif suffisant pour résilier un contrat classifié ou exclure un candidat, soumissionnaire ou demandeur de la procédure d'appel d'offres. Une disposition est incluse à cet effet dans les contrats types et les conventions de subvention types à élaborer.

Article 45

Dispositions applicables aux contrats et conventions de subvention classifiés

1. Lorsque des ICUE sont communiquées à un candidat, soumissionnaire ou demandeur durant la procédure de passation de marché, l'appel d'offres ou l'appel de propositions contient une disposition obligeant le candidat, le soumissionnaire ou le demandeur qui ne présente pas d'offre ou de proposition ou qui n'est pas sélectionné à restituer tous les documents classifiés dans un délai spécifié.

2. L'autorité contractante ou qui octroie la subvention informe, par l'intermédiaire de l'autorité de sécurité de la Commission, l'ANS, l'ASD ou toute autre autorité de sécurité compétente qu'un contrat classifié ou une convention de subvention classifiée a été attribué, et lui communique les données correspondantes, notamment le nom du ou des contractants ou bénéficiaires, la durée du contrat et le niveau maximal de classification.

3. Lorsqu'il est mis fin à un tel contrat ou convention de subvention, l'autorité contractante ou qui octroie la subvention avertit rapidement, par l'intermédiaire de l'autorité de sécurité de la Commission, l'ANS, l'ASD ou toute autre autorité de sécurité compétente de l'État membre dans lequel le contractant ou le bénéficiaire de la subvention est immatriculé.

4. En principe, le contractant ou le bénéficiaire de la subvention est tenu de restituer à l'autorité contractante ou qui octroie la subvention les ICUE en sa possession, dès que le contrat classifié ou la convention de subvention classifiée arrive à expiration ou que la participation d'un bénéficiaire de la subvention arrive à son terme.

5. Des dispositions spéciales concernant l'élimination d'ICUE durant l'exécution du contrat classifié ou de la convention de subvention classifiée ou à son expiration figurent dans l'AS.

6. Lorsque le contractant ou le bénéficiaire de la subvention est autorisé à conserver des ICUE après l'expiration d'un contrat classifié ou d'une convention de subvention classifiée, les normes minimales figurant dans la présente décision demeurent d'application et la confidentialité des ICUE est protégée par le contractant ou le bénéficiaire de la subvention.

Article 46

Dispositions spécifiques applicables aux contrats classifiés

1. Les conditions pertinentes pour la protection des ICUE dans lesquelles le contractant peut sous-traiter des activités sont définies dans l'appel d'offres et le contrat classifié.

2. Un contractant doit obtenir l'autorisation de l'autorité contractante avant de pouvoir sous-traiter des éléments d'un contrat classifié. Aucun contrat de sous-traitance impliquant l'accès à des ICUE ne peut être attribué à des sous-traitants immatriculés dans un pays tiers, sauf s'il existe un cadre règlementaire en matière de sécurité des informations tel qu'il est prévu au chapitre 7.

3. Il incombe au contractant de veiller à ce que toutes les activités de sous-traitance soient réalisées en conformité avec les normes minimales définies dans la présente décision et de s'abstenir de fournir des ICUE à un sous-traitant sans l'autorisation écrite préalable de l'autorité contractante.

4. En ce qui concerne les ICUE créées ou traitées par le contractant, la Commission est considérée comme l'autorité d'origine et les droits qui incombent à l'autorité d'origine sont exercés par l'autorité contractante.

Article 47

Visites liées à des contrats classifiés

1. Lorsque des membres du personnel de la Commission, des contractants ou des bénéficiaires de subvention doivent avoir accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET dans leurs locaux respectifs aux fins de l'exécution d'un contrat classifié ou d'une convention de subvention classifiée, les visites sont organisées en liaison avec les ANS, les ASD ou toute autre autorité de sécurité compétente concernée. L'autorité de sécurité de la Commission est informée de ces visites. Toutefois, dans le cadre de programmes ou projets spécifiques, les ANS, les ASD ou toute autre autorité de sécurité compétente peuvent également convenir d'une procédure selon laquelle ces visites peuvent être organisées directement.

2. Tous les visiteurs sont en possession d'une habilitation de sécurité adéquate et jouissent d'un accès aux ICUE liées au contrat classifié sur la base du principe du besoin d'en connaître.

3. Les visiteurs se voient uniquement accorder l'accès aux ICUE liées à l'objectif de la visite.

4. Les modalités d'application contiennent des dispositions plus détaillées.

5. Le respect des dispositions concernant les visites liées à des contrats classifiés définies dans la présente décision et dans les modalités d'application visées au paragraphe 4 est obligatoire.

Article 48

Transmission et transport d'ICUE en relation avec des contrats classifiés ou des conventions de subvention classifiées

1. En ce qui concerne la transmission des ICUE par voie électronique, les dispositions pertinentes du chapitre 5 de la présente décision s'appliquent.

2. En ce qui concerne le transport d'ICUE, les dispositions pertinentes du chapitre 4 de la présente décision et de ses modalités d'application s'appliquent, conformément aux dispositions législatives et réglementaires nationales.

3. En ce qui concerne le transport de matériel classifié en tant que fret, les principes ci-après s'appliquent pour déterminer les mesures de sécurité à mettre en œuvre:

a) la sécurité est assurée à tous les stades pendant le transport, du point d'origine jusqu'à la destination finale;

b) le degré de protection accordé à un envoi est déterminé en fonction du niveau de classification le plus élevé du matériel qu'il contient;

c) avant tout transfert transfrontalier de matériel classifié CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, un plan de transport est établi par l'expéditeur et approuvé par l'ANS, l'ASD ou toute autre autorité de sécurité compétente concernée;

d) les trajets sont directs dans la mesure du possible, et aussi rapides que les circonstances le permettent;

e) chaque fois que cela est possible, les itinéraires ne devraient passer que par des États membres. Les itinéraires passant par des États autres que les États membres ne devraient être suivis qu'à condition d'avoir été autorisés par l'ANS, l'ASD ou toute autre autorité de sécurité compétente des États de l'expéditeur et du destinataire.

Article 49

Transfert d'ICUE aux contractants ou bénéficiaires de subvention établis dans des États tiers

Les ICUE sont transférées aux contractants ou bénéficiaires de subvention établis dans des États tiers conformément aux mesures de sécurité convenues entre l'autorité de sécurité de la Commission, le service de la Commission, en sa qualité d'autorité contractante ou octroyant la subvention, et l'ANS, l'ASD ou toute autre autorité de sécurité compétente de l'État tiers concerné dans lequel le contractant ou le bénéficiaire de la subvention est immatriculé.

Article 50

Traitement d'informations classifiées RESTREINT UE/EU RESTRICTED dans le cadre de contrats classifiés ou de conventions de subvention classifiées

1. La protection des informations classifiées RESTREINT UE/EU RESTRICTED traitées ou stockées dans le cadre de contrats classifiés ou de conventions de subvention classifiées est fondée sur les principes de proportionnalité et de rentabilité.

2. Aucune HSE ni HSP n'est requise dans le cadre de contrats classifiés ou de conventions de subvention classifiées impliquant le traitement d'informations classifiées au niveau RESTREINT UE/EU RESTRICTED.

3. Lorsqu'un contrat ou une convention de subvention prévoit le traitement d'informations classifiées RESTREINT UE/EU RESTRICTED dans un SIC exploité par un contractant ou un bénéficiaire de subvention, l'autorité contractante ou octroyant la subvention veille, après avoir consulté l'autorité de sécurité de la Commission, à ce que les exigences techniques et administratives à remplir concernant l'homologation du SIC soient précisées dans le contrat ou la convention de subvention; ces exigences sont proportionnées au risque évalué, compte tenu de tous les facteurs pertinents. La portée de l'homologation dudit SIC est décidée d'un commun accord par l'autorité de sécurité de la Commission et l'ANS ou ASD compétente.

CHAPITRE 7

ÉCHANGE D'INFORMATIONS CLASSIFIÉES AVEC D'AUTRES INSTITUTIONS, AGENCES, ORGANES ET ORGANISMES DE L'UNION, AVEC DES ÉTATS MEMBRES ET AVEC DES ÉTATS TIERS ET DES ORGANISATIONS INTERNATIONALES

Article 51

Principes de base

1. Dans le cas où la Commission ou l'un de ses services établit qu'il est nécessaire d'échanger des ICUE avec une autre institution, agence, organe ou organisme de l'Union, ou avec un État tiers ou une organisation internationale, les mesures nécessaires sont prises afin d'instituer un cadre juridique ou administratif approprié à cette fin, pouvant comprendre des accords sur la sécurité des informations ou des arrangements administratifs conclus conformément aux dispositions réglementaires applicables.

2. Sans préjudice de l'article 57, les ICUE sont échangées avec une autre institution, agence, organe ou organisme de l'Union, ou avec un État tiers ou une organisation internationale, uniquement si un tel cadre juridique ou administratif approprié est mis en place et qu'il existe des garanties suffisantes indiquant que l'institution, agence, organe ou organisme de l'Union ou l'État tiers ou l'organisation internationale en question applique des principes de base et des normes minimales équivalents pour la protection des informations classifiées.

Article 52

Échange d'ICUE avec d'autres institutions, agences, organes et organismes de l'Union

1. Avant de conclure un arrangement administratif pour l'échange d'ICUE avec une autre institution, agence, organe ou organisme de l'Union, la Commission s'assure que celle-ci ou celui-ci:

a) dispose d'un cadre réglementaire pour la protection des ICUE établissant des principes de base et des normes minimales équivalents à ceux énoncés dans la présente décision et ses modalités d'application;

b) applique des normes de sécurité et des lignes directrices concernant la sécurité du personnel, la sécurité physique, la gestion des ICUE et la sécurité des systèmes d'information et de communication (SIC) garantissant un niveau de protection des ICUE équivalent à celui appliqué au sein de la Commission;

c) marque les informations classifiées qu'il ou elle crée comme ICUE.

2. En étroite coopération avec les autres services compétents de la Commission, la direction générale des ressources humaines et de la sécurité est le service chef de file au sein de la Commission pour la conclusion d'arrangements administratifs pour l'échange d'ICUE avec d'autres institutions, agences, organes ou organismes de l'Union.

3. Les arrangements administratifs prennent, en règle générale, la forme d'un échange de lettres, signées par le directeur général des ressources humaines et de la sécurité au nom de la Commission.

4. Avant de conclure un arrangement administratif sur l'échange d'ICUE, l'autorité de sécurité de la Commission effectue une visite d'évaluation visant à évaluer le cadre réglementaire pour la protection des ICUE et s'assurer de l'efficacité des mesures mises en œuvre pour protéger les ICUE. L'arrangement administratif prend effet et les ICUE sont échangées uniquement si le résultat de cette visite d'évaluation est satisfaisant et que les recommandations émises à la suite de la visite sont respectées. Des visites de suivi régulières sont effectuées afin de vérifier que l'arrangement administratif est respecté et que les mesures de sécurité mises en place continuent de répondre aux principes de base et normes minimales convenus.

5. Au sein de la Commission, le bureau d'ordre géré par le secrétariat général représente, en règle générale, le principal point d'entrée et de sortie des échanges d'informations classifiées avec d'autres institutions, agences, organes et organismes de l'Union. Toutefois, si pour des raisons de sécurité, d'organisation ou de fonctionnement, cela s'avère plus approprié pour protéger les ICUE, des bureaux d'ordre locaux sont établis au sein des services de la Commission conformément à la présente décision et à ses modalités d'application; ces bureaux servent de point d'entrée et de sortie pour les informations classifiées concernant des sujets relevant de la compétence des services de la Commission concernés.

6. Le groupe d'experts sécurité de la Commission est informé du processus de conclusion d'arrangements administratifs conformément au paragraphe 2.

Article 53

Échange d'ICUE avec les États membres

1. Des ICUE peuvent être échangées avec les États membres et leur être communiquées à condition qu'ils protègent ces informations classifiées conformément aux exigences applicables aux informations classifiées portant un marquage national de classification de sécurité de niveau équivalent, tel que prévu dans le tableau d'équivalence des classifications de sécurité figurant à l'annexe I.

2. Lorsque les États membres introduisent des informations classifiées portant un marquage national de classification de sécurité dans les structures ou réseaux de l'Union européenne, la Commission protège ces informations conformément aux règles applicables aux ICUE de niveau équivalent tel que prévu dans le tableau d'équivalence des classifications de sécurité figurant à l'annexe I.

Article 54

Échange d'ICUE avec des États tiers et des organisations internationales

1. Lorsque la Commission établit qu'il existe un besoin durable d'échanger des informations classifiées avec des États tiers ou des organisations internationales, les mesures nécessaires sont prises pour instituer un cadre juridique ou administratif approprié à cette fin, pouvant comprendre de accords sur la sécurité des informations ou des arrangements administratifs conclus conformément aux dispositions réglementaires applicables.

2. Les accords sur la sécurité des informations ou les arrangements administratifs visés au paragraphe 1 contiennent des dispositions pour garantir que, lorsque des États tiers ou des organisations internationales reçoivent des ICUE, ces informations bénéficient d'une protection conforme à leur niveau de classification et à des normes minimales équivalentes à celles prévues dans la présente décision.

3. La Commission peut conclure des arrangements administratifs, conformément à l'article 56, lorsque le niveau de classification des ICUE n'est en règle générale pas supérieur à RESTREINT UE/EU RESTRICTED.

4. Les arrangements administratifs pour l'échange d'informations classifiées visés au paragraphe 3 contiennent des dispositions pour garantir que, lorsque des États tiers ou des organisations internationales reçoivent des ICUE, ces informations bénéficient d'une protection conforme à leur niveau de classification et à des normes minimales équivalentes à celles prévues dans la présente décision. Le groupe d'experts sécurité de la Commission est consulté sur la conclusion d'accords sur la sécurité des informations ou d'arrangements administratifs.

5. La décision de communiquer des ICUE émanant de la Commission à un État tiers ou à une organisation internationale est prise par le service de la Commission, en tant qu'autorité d'origine des ICUE concernées au sein de la Commission, au cas par cas, en fonction de la nature et du contenu de ces informations, du besoin d'en connaître du destinataire et d'une appréciation des avantages que l'Union peut en retirer. Si l'autorité d'origine des informations classifiées à communiquer, ou des sources qu'elles peuvent contenir, n'est pas la Commission, le service de la Commission qui détient ces informations classifiées demande au préalable le consentement écrit de l'autorité d'origine. Au cas où l'autorité d'origine ne peut être identifiée, le service de la Commission qui détient ces informations classifiées assume cette responsabilité en lieu et place de l'autorité d'origine après avoir consulté le groupe d'experts sécurité de la Commission.

Article 55

Accords sur la sécurité des informations

1. Les accords sur la sécurité des informations avec des États tiers ou des organisations internationales sont conclus conformément à l'article 218 du TFUE.

2. Les accords sur la sécurité des informations:

a) fixent les principes de base et les normes minimales régissant l'échange d'informations classifiées entre l'Union et un État tiers ou une organisation internationale;

b) prévoient des modalités techniques d'application qui doivent être arrêtées d'un commun accord entre les autorités de sécurité compétentes des institutions et organes de l'Union concernés et l'autorité de sécurité compétente de l'État tiers ou de l'organisation internationale concerné(e). Ces modalités tiennent compte du niveau de protection offert par les règlements, les structures et les procédures de sécurité en vigueur au sein de l'État tiers ou de l'organisation internationale concerné(e);

c) prévoient que, préalablement à l'échange d'informations classifiées au titre de l'accord, il a été vérifié que la partie destinataire est apte à protéger et sauvegarder de manière appropriée les informations classifiées qui lui sont transmises.

3. Lorsque la nécessité d'échanger des informations classifiées est établie conformément à l'article 51, paragraphe 1, la Commission consulte le Service européen pour l'action extérieure, le secrétariat général du Conseil et d'autres institutions et organes de l'Union, le cas échéant, afin de déterminer s'il y a lieu de soumettre une recommandation conformément à l'article 218, paragraphe 3, du TFUE.

4. Les ICUE ne font l'objet d'aucun échange par voie électronique, sauf disposition expresse de l'accord sur la sécurité des informations ou des modalités techniques d'application.

5. Au sein de la Commission, le bureau d'ordre géré par le secrétariat général représente, en règle générale, le principal point d'entrée et de sortie des échanges d'informations classifiées avec des États tiers et des organisations internationales. Toutefois, si pour des raisons de sécurité, d'organisation ou de fonctionnement, cela s'avère plus approprié pour protéger les ICUE, des bureaux d'ordre locaux sont établis au sein des services de la Commission conformément à la présente décision et à ses modalités d'application; ces bureaux servent de point d'entrée et de sortie pour les informations classifiées concernant des sujets relevant de la compétence des services de la Commission concernés.

6. Afin d'évaluer l'efficacité des règlements, structures et procédures de sécurité en vigueur dans l'État tiers ou l'organisation internationale concerné(e), la Commission participe à des visites d'évaluation en collaboration avec d'autres institutions, agences ou organes de l'Union, d'un commun accord avec l'État tiers ou l'organisation internationale concerné(e). Ces visites d'évaluation ont pour finalité d'évaluer:

a) le cadre réglementaire applicable à la protection des informations classifiées;

b) tous les aspects spécifiques de la politique de sécurité et du mode d'organisation de la sécurité dans l'État tiers ou l'organisation internationale susceptibles d'avoir une incidence sur le niveau des informations classifiées qui peuvent être échangées;

c) les mesures et les procédures de sécurité effectivement en place; et

d) les procédures d'habilitation de sécurité pour le niveau de classification des ICUE à communiquer.

Article 56

Arrangements administratifs

1. Lorsqu'il existe un besoin durable, dans le contexte d'un cadre politique ou juridique de l'Union, d'échanger avec un État tiers ou une organisation internationale des informations dont le niveau de classification n'est en principe pas supérieur à RESTREINT UE/EU RESTRICTED, et que l'autorité de sécurité de la Commission, après avoir consulté le groupe d'experts sécurité de la Commission, a établi, notamment, que la partie en question ne dispose pas d'un système de sécurité suffisamment développé lui permettant de conclure un accord sur la sécurité des informations, la Commission peut décider de conclure un arrangement administratif avec les autorités compétentes de l'État tiers ou de l'organisation internationale concerné(e).

2. Ces arrangements administratifs prennent, en règle générale, la forme d'un échange de lettres.

3. Une visite d'évaluation est réalisée préalablement à la conclusion de l'arrangement. Le groupe d'experts sécurité de la Commission est informé du résultat de la visite d'évaluation. Si des raisons exceptionnelles justifient l'échange urgent d'informations classifiées, les ICUE peuvent être communiquées à condition que tout soit mis en œuvre pour effectuer dès que possible une visite d'évaluation.

4. Les ICUE ne font l'objet d'aucun échange par voie électronique, sauf disposition expresse de l'arrangement administratif.

Article 57

Communication ad hoc exceptionnelle d'ICUE

1. S'il n'existe aucun accord sur la sécurité des informations ni arrangement administratif, et si la Commission ou l'un de ses services décide qu'il est nécessaire, à titre exceptionnel dans le contexte d'un cadre politique ou juridique de l'Union, de communiquer des ICUE à un État tiers ou à une organisation internationale, l'autorité de sécurité de la Commission vérifie, dans la mesure du possible, auprès des autorités de sécurité de l'État tiers ou de l'organisation internationale concerné(e) que son règlement, ses structures et ses procédures de sécurité permettent de garantir que les ICUE qui lui seront communiquées bénéficieront d'une protection conforme à des normes qui ne sont pas moins strictes que celles prévues dans la présente décision.

2. La décision de communiquer des ICUE à l'État tiers ou à l'organisation internationale concerné(e) est prise, après consultation du groupe d'experts sécurité de la Commission, par la Commission sur la base d'une proposition du membre de la Commission chargé des questions de sécurité.

3. Lorsqu'une décision de communiquer des ICUE a été prise par la Commission et sous réserve du consentement de l'autorité d'origine, y compris des auteurs des sources qu'elles peuvent contenir, le service de la Commission compétent transmet les informations concernées, qui portent un marquage relatif à la communicabilité indiquant l'État tiers ou l'organisation internationale auquel elles ont été communiquées. Avant la communication effective ou au moment de celle-ci, la tierce partie concernée s'engage par écrit à protéger les ICUE qui lui sont transmises conformément aux principes de base et aux normes minimales prévus dans la présente décision.

CHAPITRE 8

DISPOSITIONS FINALES

Article 58

Remplacement de la décision précédente

La présente décision abroge et remplace la décision 2001/844/CE, CECA, Euratom de la Commission [1].

Article 59

Informations classifiées créées avant l'entrée en vigueur de la présente décision

1. Toutes les ICUE portant un marquage en application de la décision 2001/844/CE, CECA, Euratom continuent d'être protégées conformément aux dispositions pertinentes de la présente décision.

2. Toutes les informations classifiées détenues par la Commission à la date d'entrée en vigueur de la décision 2001/844/CE, CECA, Euratom, à l'exception des informations classifiées Euratom:

a) lorsqu'elles ont été créées par la Commission, restent considérées comme reclassifiées par défaut dans la catégorie RESTREINT UE, à moins que leur auteur n'ait décidé de leur attribuer une autre classification au plus tard le 31 janvier 2002 et n'en ait informé tous les destinataires du document concerné;

b) lorsqu'elles ont été créées par des personnes extérieures à la Commission, sont maintenues dans leur classification originelle et donc traitées comme des ICUE du même niveau, à moins que l'auteur n'accepte de les déclassifier ou de les déclasser.

Article 60

Modalités d'application et notes de sécurité

1. Au besoin, l'adoption des modalités d'application de la présente décision feront l'objet d'une décision d'habilitation distincte de la Commission en faveur du membre de la Commission chargé des questions de sécurité, conformément au règlement intérieur.

2. Après avoir été habilité à la suite de la décision de la Commission susvisée, le membre de la Commission chargé des questions de sécurité peut rédiger des notes de sécurité définissant des lignes directrices et des bonnes pratiques en matière de sécurité dans le cadre du champ d'application de la présente décision et de ses modalités d'application.

3. La Commission peut déléguer les tâches mentionnées dans les premier et deuxième paragraphes du présent article au directeur général des ressources humaines et de la sécurité au moyen d'une décision de délégation distincte, conformément au règlement intérieur.

Article 61

Entrée en vigueur

La présente décision entre en vigueur le jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Fait à Bruxelles, le 13 mars 2015.

Par la Commission

Le président

Jean-Claude JUNCKER

[1] Décision 2001/844/CE, CECA, Euratom de la Commission du 29 novembre 2001 modifiant son règlement intérieur (JO L 317 du 3.12.2001, p. 1).

ANNEXE I

ÉQUIVALENCE DES CLASSIFICATIONS DE SÉCURITÉ

UE	TRÈS 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
Belgique	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)	Note [1] ci-dessous
Bulgarie	Строго секретно	Секретно	Поверително	За служебно ползване
République tchèque	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danemark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Allemagne	Streng geheim	Geheim	VS [2] — Vertraulich	VS — Nur für den Dienstgebrauch
Estonie	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irlande	Top Secret	Secret	Confidential	Restricted
Grèce	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Espagne	Secreto	Reservado	Confidencial	Difusión Limitada
France	Très Secret Défense	Secret Défense	Confidentiel Défense	Note [3] ci-dessous
Croatie	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italie	Segretissimo	Segreto	Riservatissimo	Riservato
Chypre	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Lettonie	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lituanie	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembourg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hongrie	«Szigorúan titkos!»	«Titkos!»	«Bizalmas!»	«Korlátozott terjesztésű!»
Malte	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Pays-Bas	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Autriche	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Pologne	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Roumanie	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovénie	Strogo tajno	Tajno	Zaupno	Interno
Slovaquie	Prísne tajné	Tajné	Dôverné	Vyhradené
Finlande	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Suède ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Royaume-Uni	UK TOP SECRET	UK SECRET	Pas d'équivalence ([5])	UK OFFICIAL — SENSITIVE

([1]) La classification «Diffusion restreinte/Beperkte Verspreiding» n'est pas une classification de sécurité en Belgique. La Belgique traite et protège les informations RESTREINT UE/EU RESTRICTED d'une manière qui n'est pas moins stricte que les normes et procédures décrites dans le règlement de sécurité du Conseil de l'Union européenne.

([2]) Allemagne: VS = Verschlusssache.

([3]) La France n'utilise pas la catégorie de classification «RESTREINT» dans son système national. Elle traite et protège les informations RESTREINT UE/EU RESTRICTED d'une manière qui n'est pas moins stricte que les normes et procédures décrites dans le règlement de sécurité du Conseil de l'Union européenne.

([4]) Suède: les marquages de classification de sécurité de la première ligne sont utilisés par les autorités chargées de la défense et les marquages de la deuxième ligne par les autres autorités.

([5]) Le Royaume-Uni traite et protège les ICUE marquées CONFIDENTIEL UE/EU CONFIDENTIAL conformément aux exigences de sécurité relatives à la protection des informations classifiées UK SECRET.

ANNEXE II

LISTE DES ABRÉVIATIONS

Acronyme	Signification
AC	Autorité Crypto
AAC	Autorité d'agrément cryptographique
CCTV	Closed Circuit Television — système de télévision en circuit fermé (vidéosurveillance)
ADC	Autorité de distribution cryptographique
SIC	Systèmes d'information et de communication traitant des ICUE
ASD	Autorité de sécurité désignée
ICUE	Informations classifiées de l'Union européenne
HSE	Habilitation de sécurité d'établissement
AI	Assurance de l'information
AAI	Autorité chargée de l'assurance de l'information
SDI	Système de détection des intrusions
TI	Technologies de l'information
LSO	Responsable local de la sécurité
ANS	Autorité nationale de sécurité
HSP	Habilitation de sécurité du personnel
CHSP	Certificat d'habilitation de sécurité du personnel
ISP	Instructions de sécurité relatives à un programme/un projet
RCO	Agent contrôleur
AHS	Autorité d'homologation de sécurité
AS	Annexe de sécurité
GCS	Guide de la classification de sécurité
SecOP	Procédures d'exploitation de sécurité
AT	Autorité TEMPEST
TFUE	Traité sur le fonctionnement de l'Union européenne

ANNEXE III

LISTE DES AUTORITÉS NATIONALES DE SÉCURITÉ

BELGIQUE

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles
Téléphone secrétariat: +32 25014542
Fax +32 25014596
E-mail: nvo-ans@diplobel.fed.be

BULGARIE

State Commission on Information Security
90 Cherkovna Str.
1505 Sofia
Téléphone +359 29333600
Fax +359 29873750
E-mail: dksi@government.bg
Site web: www.dksi.bg

RÉPUBLIQUE TCHÈQUE

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Téléphone +420 257283335
Fax +420 257283110
E-mail: czech.nsa@nbu.cz
Site web: www.nbu.cz

DANEMARK

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Téléphone +45 33148888
Fax +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Téléphone +45 33325566
Fax +45 33931320

ALLEMAGNE

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin
Téléphone +49 30186810
Fax +49 30186811441
E-mail: oesIII3@bmi.bund.de

ESTONIE

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn
Téléphone +372 717 0019, +372 7170117
Fax +372 7170213
E-mail: nsa@mod.gov.ee

GRÈCE

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

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos — Athens
Téléphone +30 2106572045
+ 30 2106572009
Fax +30 2106536279, +30 2106577612

ESPAGNE

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid
Téléphone +34 913725000
Fax +34 913725808
E-mail: nsa-sp@areatec.com

FRANCE

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
Téléphone +33 171758177
Fax + 33 171758200

CROATIE

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Croatia
Téléphone +385 14681222
Fax + 385 14686049
Site web: www.uvns.hr

IRLANDE

National Security Authority
Department of Foreign Affairs
76 — 78 Harcourt Street
Dublin 2
Téléphone +353 14780822
Fax +353 14082959

ITALIE

Presidenza del Consiglio dei Ministri
D.I.S. — U.C.Se.
Via di Santa Susanna, 15
00187 Roma
Téléphone +39 0661174266
Fax +39 064885273

CHYPRE

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

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia
Téléphone +357 22807569, +357 22807643,
+357 22807764
Fax +357 22302351
E-mail: cynsa@mod.gov.cy

LETTONIE

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV-1001 Riga
Téléphone +371 67025418
Fax +371 67025454
E-mail: ndi@sab.gov.lv

LITUANIE

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lituania National Security Authority)
Gedimino 40/1
LT-01110 Vilnius
Téléphone +370 706 66701, +370 706 66702
Fax +370 706 66700
E-mail: nsa@vsd.lt

LUXEMBOURG

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg
Téléphone +352 24782210 central
+ 352 24782253 direct
Fax +352 24782243

HONGRIE

Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Téléphone +36 (1) 7952303
Fax +36 (1) 7950344

Adresse postale:
H-1357 Budapest, PO Box 2
E-mail: nbf@nbf.hu
Site web: www.nbf.hu

MALTE

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Téléphone +356 21249844
Fax +356 25695321

PAYS-BAS

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Téléphone +31 703204400
Fax +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag
Téléphone +31 703187060
Fax +31 703187522

AUTRICHE

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien
Téléphone +43 1531152594
Fax +43 1531152615
E-mail: ISK@bka.gv.at

POLOGNE

Agencja Bezpieczeństwa Wewnętrznego — ABW
(Internal Security Agency)
2A Rakowiecka St.
00-993 Warszawa
Téléphone +48 22 58 57 944
Fax +48 22 58 57 443
E-mail: nsa@abw.gov.pl
Site web: www.abw.gov.pl

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Téléphone +351 213031710
Fax +351 213031711

ROUMANIE

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA — ORNISS National Registry Office for Classified Information)
4 Mures Street
012275 Bucharest
Téléphone +40 212245830
Fax +40 212240714
E-mail: nsa.romania@nsa.ro
Site web: www.orniss.ro

SLOVÉNIE

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Téléphone +386 14781390
Fax +386 14781399
E-mail: gp.uvtp@gov.si

SLOVAQUIE

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava
Téléphone +421 268692314
Fax +421 263824005
Site web: www.nbusr.sk

FINLANDE

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Téléphone 16055890
Fax +358 916055140
E-mail: NSA@formin.fi

SUÈDE

Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
S-103 39 Stockholm
Téléphone +46 84051000
Fax +46 87231176
E-mail: ud-nsa@foreign.ministry.se

ROYAUME-UNI

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Téléphone 1: +44 2072765649
Téléphone 2: +44 2072765497
Fax +44 2072765651
E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk

ISSN 1977-0693 (édition électronique)
ISSN 1725-2563 (édition papier)

Office des publications de l'Union européenne
2985 Luxembourg
LUXEMBOURG

FR