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