II

(Actes non législatifs)

DÉCISIONS

DÉCISION DU CONSEIL

du 31 mars 2011

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

(2011/292/UE)

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 240, paragraphe 3,

vu la décision 2009/937/UE du Conseil du 1er décembre 2009 portant adoption de son règlement intérieur [1], et notamment son article 24,

considérant ce qui suit:

(1) Afin de développer les activités du Conseil dans tous les domaines qui requièrent le traitement d'informations classifiées, il convient de mettre en place un système de sécurité global aux fins de la protection des informations classifiées couvrant le Conseil, son secrétariat général et les États membres.

(2) La présente décision devrait s'appliquer lorsque le Conseil, ses instances préparatoires et son secrétariat général (SGC) traitent des informations classifiées de l'UE (ICUE).

(3) Conformément aux dispositions législatives et réglementaires nationales et dans la mesure requise pour le fonctionnement du Conseil, les États membres devraient respecter la présente décision lorsque leurs autorités compétentes, leur personnel ou leurs contractants traitent des ICUE, afin que chacun puisse avoir la certitude qu'un niveau équivalent de protection est assuré pour les ICUE.

(4) Le Conseil et la Commission sont résolus à appliquer des normes équivalentes de sécurité pour protéger les ICUE.

(5) Le Conseil souligne qu'il importe d'associer, le cas échéant, le Parlement européen et d'autres institutions, agences, organes ou organismes de l'UE 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.

(6) Les agences et les organes de l'UE créés en vertu du titre V, chapitre 2, du traité sur l'Union européenne, Europol et Eurojust appliquent, dans le cadre de leur organisation interne, les principes de base et les normes minimales énoncés dans la présente décision aux fins de la protection des ICUE, comme le prévoient leurs actes fondateurs respectifs.

(7) Les règles de sécurité adoptées par le Conseil aux fins de la protection des ICUE sont appliquées dans le cadre des opérations de gestion de crise mises en place en vertu du titre V, chapitre 2, du traité sur l'Union européenne et par leur personnel.

(8) Les représentants spéciaux de l'UE et les membres de leurs équipes appliquent les règles de sécurité adoptées par le Conseil aux fins de la protection des ICUE.

(9) La présente décision est arrêtée sans préjudice des articles 15 et 16 du traité sur le fonctionnement de l'Union européenne, ni des instruments les mettant en œuvre.

(10) La présente décision est arrêtée sans préjudice des pratiques en vigueur au sein des États membres en matière d'information de leurs parlements nationaux sur les activités de l'Union,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Objectif, champ d'application et définitions

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

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

2. Ces principes de base et normes minimales s'appliquent au Conseil et au SGC et sont respectés par les États membres, conformément à leurs dispositions législatives et réglementaires nationales, afin que chacun puisse avoir la certitude qu'un niveau équivalent de protection est assuré pour les ICUE.

3. Aux fins de la présente décision, les définitions figurant à l'appendice A s'appliquent.

Article 2

Définition des ICUE, classifications et marquages de sécurité

1. Par «informations classifiées de l'UE» (ICUE), on entend toute information ou tout matériel identifié comme tel par une classification de sécurité de l'UE, 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 pour désigner le domaine d'activité auquel elles sont liées, identifier l'autorité d'origine, limiter la diffusion, restreindre l'utilisation ou indiquer la communicabilité.

Article 3

Gestion de la classification

1. Les autorités compétentes veillent à ce que les ICUE soient classifiées de manière appropriée, clairement identifiées en tant qu'informations classifiées, et qu'elles ne conservent leur niveau de classification qu'aussi longtemps que nécessaire.

2. Les ICUE ne sont pas déclassées ni déclassifiées, et aucun des marquages visés à l'article 2, paragraphe 3, n'est modifié ni supprimé sans le consentement écrit préalable de l'autorité d'origine.

3. Le Conseil approuve une politique de sécurité sur la création d'ICUE, qui comprend un guide pratique de la classification.

Article 4

Protection des informations classifiées

1. Les ICUE sont protégées conformément à la présente décision.

2. Il incombe au détenteur de tout élément d'ICUE de le protéger conformément à la présente décision.

3. 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, le Conseil et le SGC protègent 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'appendice B.

4. Les grandes quantités ou la compilation d'ICUE peuvent justifier un niveau de protection correspondant à une classification plus élevée.

Article 5

Gestion des risques de sécurité

1. 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, telle que définie à l'appendice A. L'efficacité de telles mesures fait l'objet d'une évaluation constante.

2. 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.

3. 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.

4. 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.

Article 6

Mise en œuvre de la présente décision

1. Le cas échéant, le Conseil approuve, sur recommandation du comité de sécurité, les politiques de sécurité énonçant les mesures destinées à mettre en œuvre la présente décision.

2. Le comité de sécurité peut arrêter à son niveau des lignes directrices en matière de sécurité en complément ou à l'appui de la présente décision et de toute politique de sécurité approuvée par le Conseil.

Article 7

Mesures de sécurité concernant le personnel

1. La sécurité du personnel passe par l'application de mesures visant à faire en sorte que l'accès aux ICUE ne soit accordé qu'aux personnes qui ont:

— un besoin d'en connaître,

— fait l'objet d'une habilitation de sécurité du niveau correspondant, lorsqu'il y a lieu, et

— été informées de leurs responsabilités.

2. 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.

3. Toutes les personnes au sein du SGC 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 habilitation de sécurité du niveau correspondant avant que l'accès à de telles ICUE leur soit accordé. La procédure d'habilitation de sécurité concernant le personnel pour les fonctionnaires et autres agents du SGC est présentée à l'annexe I.

4. Le personnel des États membres visé à l'article 14, paragraphe 3, qui, en raison de ses attributions, peut avoir besoin d'accéder à des ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur fait l'objet d'une habilitation de sécurité du niveau correspondant ou est dûment autorisé en vertu de ses fonctions, conformément aux dispositions législatives et réglementaires nationales, avant que l'accès à de telles ICUE ne lui soit accordé.

5. Avant de se voir accorder l'accès à des ICUE et à intervalles réguliers par la suite, toutes les personnes concernées sont informées des responsabilités qui leur incombent en matière de protection des ICUE conformément à la présente décision et reconnaissent ces responsabilités.

6. Les modalités d'application du présent article figurent à l'annexe I.

Article 8

Sécurité physique

1. Par «sécurité physique», on entend l'application de mesures physiques et techniques de protection pour empêcher l'accès non autorisé aux ICUE.

2. 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.

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 définis à l'article 10, paragraphe 2.

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 à l'annexe II et agréées par l'autorité de sécurité compétente.

5. Seuls des équipements ou des dispositifs agréés sont utilisés pour protéger les ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur.

6. Les modalités d'application du présent article figurent à l'annexe II.

Article 9

Gestion des informations classifiées

1. Par «gestion des informations classifiées», on entend l'application de mesures administratives pour contrôler les ICUE tout au long de leur cycle de vie afin de compléter les mesures prévues aux articles 7, 8 et 10 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, l'enregistrement, la duplication, la traduction, le transport et la destruction des ICUE.

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 autorités compétentes au sein du SGC et des États membres établissent un bureau d'ordre à cette fin. Les informations classifiées TRÈS SECRET UE/EU TOP SECRET sont enregistrées dans des bureaux d'ordre désignés.

3. Les services et les locaux dans lesquels les ICUE sont traitées ou stockées font l'objet d'une inspection régulière par l'autorité de sécurité compétente.

4. 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 à l'article 10, paragraphe 6;

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 à l'article 10, paragraphe 6;

ii) soit, dans tous les autres cas, de la manière prescrite par l'autorité de sécurité compétente conformément aux mesures de protection pertinentes prévues à l'annexe III.

5. Les modalités d'application du présent article figurent à l'annexe III.

Article 10

Protection des ICUE traitées dans les systèmes de communication et d'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. Une AI efficace garantit des niveaux appropriés de confidentialité, d'intégrité, de disponibilité, de non-répudiation et d'authenticité. L'AI est fondée sur un processus de gestion des risques.

2. On entend par «système d'information et de communication» 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. La présente décision s'applique aux systèmes d'information et de communication traitant des ICUE (SIC).

3. Les SIC traitent des ICUE dans le respect de la notion d'AI.

4. Tous les SIC font l'objet d'un processus d'homologation. L'homologation vise à obtenir l'assurance que toutes les mesures de sécurité appropriées ont été mises en œuvre et que les ICUE et les SIC font l'objet d'un niveau suffisant de protection conformément à la présente décision. La déclaration d'homologation détermine le niveau maximal de classification des informations qui peuvent être traitées dans un SIC ainsi que les modalités et les conditions correspondantes.

5. Les SIC traitant des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et d'un niveau de classification supérieur sont protégés de telle manière que les informations ne peuvent pas être compromises par des émissions électromagnétiques non intentionnelles («mesures de sécurité Tempest»).

6. Lorsque la protection des ICUE est assurée par des produits cryptographiques, ces produits doivent être approuvés comme suit:

a) la confidentialité des informations classifiées SECRET UE/EU SECRET et d'un niveau de classification supérieur est protégée par des produits cryptographiques agréés par le Conseil en tant qu'autorité d'agrément cryptographique (AAC), sur recommandation du comité de sécurité;

b) la confidentialité des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou RESTREINT UE/EU RESTRICTED est protégée par des produits cryptographiques agréés par le secrétaire général du Conseil (ci-après dénommé «le secrétaire général») en tant qu'AAC, sur recommandation du comité de sécurité.

Nonobstant le point b), au sein des systèmes nationaux des États membres, la confidentialité des ICUE classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou RESTREINT UE/EU RESTRICTED peut être protégée par des produits cryptographiques agréés par l'AAC d'un État membre.

7. Lors de la transmission 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 comme le prévoit l'annexe IV.

8. Les autorités compétentes du SGC et des États membres créent respectivement les fonctions suivantes en matière d'AI:

a) une autorité chargée de l'AI (AAI);

b) une autorité Tempest (AT);

c) une autorité d'agrément cryptographique (AAC);

d) une autorité chargée de la distribution cryptographique (ADC).

9. Pour chaque système, les autorités compétentes du SGC et des États membres créent respectivement:

a) une autorité d'homologation de sécurité (AHS);

b) une autorité opérationnelle chargée de l'AI.

10. Les modalités d'application du présent article figurent à l'annexe IV.

Article 11

Sécurité industrielle

1. Par «sécurité industrielle», on entend l'application de mesures visant à assurer la protection des ICUE par des contractants ou des sous-traitants dans le cadre de négociations précontractuelles et tout au long du cycle de vie des contrats classifiés. De tels contrats ne doivent pas concerner l'accès à des informations classifiées TRÈS SECRET UE/EU TOP SECRET.

2. Le SGC peut, par voie contractuelle, confier à des entités industrielles ou autres immatriculées dans un État membre ou dans un pays tiers ayant conclu un accord ou un arrangement administratif en vertu de l'article 12, paragraphe 2, point a) ou b), des tâches qui impliquent ou nécessitent l'accès, le traitement ou le stockage d'ICUE ou la communication de telles informations.

3. En tant qu'autorité contractante, le SGC veille à ce que les normes minimales de sécurité industrielle prévues dans la présente décision et mentionnées dans le contrat soient respectées lors de l'octroi de contrats classifiés à des entités industrielles ou autres.

4. L'autorité nationale de sécurité (ANS), l'autorité de sécurité désignée (ASD) ou toute autre autorité compétente de chaque État membre veille, autant que le permettent les dispositions législatives et réglementaires nationales, à ce que les contractants et les sous-traitants immatriculés sur le territoire dudit État prennent toutes les mesures appropriées pour protéger les ICUE dans le cadre de négociations précontractuelles et lors de l'exécution d'un contrat classifié.

5. L'ANS, l'ASD ou toute autre autorité compétente de chaque État membre veille, conformément aux dispositions législatives et réglementaires nationales, à ce que les contractants et les sous-traitants immatriculés sur le territoire dudit État, qui participent à des contrats classifiés ou à des contrats de sous-traitance nécessitant l'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET au sein de leurs établissements, soient en possession, lors de l'exécution desdits contrats ou durant la phase précontractuelle, d'une habilitation nationale de sécurité d'établissement (HSE) du niveau de classification correspondant.

6. Lorsque les membres du personnel d'un contractant ou d'un sous-traitant doivent, en raison de leurs fonctions aux fins de l'exécution d'un contrat classifié, accéder à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, l'ANS/ASD ou toute autre autorité de sécurité compétente leur délivre une habilitation de sécurité du personnel (HSP), conformément aux dispositions législatives ou réglementaires nationales et dans le respect des normes minimales de sécurité définies à l'annexe I.

7. Les modalités d'application du présent article figurent à l'annexe V.

Article 12

Échange d'informations classifiées avec des pays tiers et des organisations internationales

1. Dans le cas où le Conseil établit qu'il est nécessaire d'échanger des ICUE avec un pays tiers ou une organisation internationale, un cadre approprié est mis en place à cette fin.

2. Afin d'établir un tel cadre et de définir des règles réciproques relatives à la protection des informations classifiées échangées,

a) le Conseil conclut des accords sur les procédures de sécurité concernant l'échange et la protection des informations classifiées (ci-après dénommés «accords sur la sécurité des informations»); ou

b) le secrétaire général peut conclure des arrangements administratifs, conformément au paragraphe 17 de l'annexe VI, lorsque le niveau de classification des ICUE à communiquer n'est en règle générale pas supérieur à RESTREINT UE/EU RESTRICTED.

3. Les accords sur la sécurité des informations ou les arrangements administratifs visés au paragraphe 2 contiennent des dispositions pour garantir que, lorsque des pays 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 qui ne sont pas moins strictes que celles prévues dans la présente décision.

4. La décision de communiquer des ICUE émanant du Conseil à un pays tiers ou à une organisation internationale est prise par le Conseil, 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'UE peut en retirer. Si l'autorité d'origine des informations classifiées à communiquer n'est pas le Conseil, le SGC lui demande au préalable son consentement écrit. Au cas où l'auteur ne peut être identifié, le Conseil assume cette responsabilité en lieu et place de l'auteur.

5. Des visites d'évaluation sont organisées pour s'assurer de l'efficacité des mesures de sécurité mises en place dans un pays tiers ou une organisation internationale pour la protection des ICUE fournies ou échangées.

6. Les modalités d'application du présent article figurent à l'annexe VI.

Article 13

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.

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 compétente.

4. Lorsqu'il est avéré ou qu'il existe des motifs raisonnables de supposer que des ICUE ont été compromises ou perdues, l'autorité de sécurité compétente prend toutes les mesures appropriées conformément aux dispositions législatives et réglementaires applicables 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'UE ou des États membres;

d) éviter que les faits ne se reproduisent; et

e) informer les autorités compétentes des mesures prises.

5. Toute personne responsable d'une violation des règles de sécurité énoncées dans la présente décision est passible d'une sanction disciplinaire conformément aux dispositions législatives et réglementaires applicables. 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.

Article 14

Responsabilité de la mise en œuvre

1. Le Conseil prend toutes les mesures nécessaires pour assurer la cohérence globale de l'application de la présente décision.

2. Le secrétaire général prend toutes les mesures nécessaires pour faire en sorte que, lors du traitement ou du stockage des ICUE ou de toute autre information classifiée, la présente décision soit appliquée dans les locaux utilisés par le Conseil et au sein du SGC, y compris dans ses bureaux de liaison situés dans des pays tiers, par les fonctionnaires et autres agents du SGC, le personnel détaché auprès du SGC et les contractants du SGC.

3. Les États membres prennent toutes les mesures appropriées, conformément à leurs dispositions législatives et réglementaires nationales respectives, pour faire en sorte que, lors du traitement ou du stockage des ICUE, la présente décision soit respectée par:

a) le personnel des représentations permanentes des États membres auprès de l'Union européenne ainsi que par les délégués nationaux assistant à des sessions du Conseil ou des réunions de ses instances préparatoires, ou participant à d'autres activités du Conseil;

b) les autres membres du personnel des administrations nationales des États membres, y compris le personnel détaché auprès de ces administrations, qu'ils soient en poste sur le territoire des États membres ou à l'étranger;

c) les autres personnes dans les États membres dûment autorisées, en raison de leurs fonctions, à avoir accès aux ICUE; et

d) les contractants des États membres, qu'ils soient sur le territoire des États membres ou à l'étranger.

Article 15

Organisation de la sécurité au sein du Conseil

1. Dans le cadre du rôle qui lui incombe et qui consiste à assurer la cohérence globale de l'application de la présente décision, le Conseil approuve:

a) les accords visés à l'article 12, paragraphe 2, point a);

b) les décisions autorisant la communication d'ICUE à des pays tiers et des organisations internationales;

c) un programme annuel d'inspection proposé par le secrétaire général et recommandé par le comité de sécurité pour inspecter les services et les locaux des États membres et des agences et organes de l'UE créés en vertu du titre V, chapitre 2, du traité sur l'Union européenne, ainsi que d'Europol et d'Eurojust, et effectuer des visites d'évaluation dans des pays tiers et des organisations internationales afin de s'assurer de l'efficacité des mesures mises en œuvre pour la protection des ICUE; et

d) les politiques de sécurité prévues à l'article 6, paragraphe 1.

2. Le secrétaire général est l'autorité de sécurité du SGC. En cette qualité, le secrétaire général:

a) applique la politique de sécurité du Conseil et la réexamine périodiquement;

b) assure, avec les ANS des États membres, la coordination de toutes les questions de sécurité relatives à la protection des informations classifiées présentant un intérêt pour les activités du Conseil;

c) accorde les HSP de l'UE aux fonctionnaires et autres agents du SGC conformément à l'article 7, paragraphe 3, avant que l'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur leur soit accordé;

d) le cas échéant, fait enquêter sur toute compromission ou perte réelle ou présumée d'informations classifiées détenues par le Conseil ou provenant de ce dernier et demande aux autorités de sécurité compétentes de participer à de telles enquêtes;

e) procède à des inspections périodiques des dispositions de sécurité destinées à assurer la protection des informations classifiées sur les locaux du SGC;

f) procède à des inspections périodiques des dispositions de sécurité destinées à assurer la protection des ICUE dans les agences et les organes de l'UE créés en vertu du titre V, chapitre 2, du traité sur l'Union européenne, au sein d'Europol et d'Eurojust ainsi que dans le cadre des opérations de gestion de crise mises en place en vertu du titre V, chapitre 2, du traité sur l'Union européenne et auprès des représentants spéciaux de l'UE (RSUE) et des membres de leurs équipes;

g) procède, en collaboration et en accord avec l'ANS concernée, à des inspections périodiques des dispositions de sécurité destinées à assurer la protection des ICUE dans les services et les locaux des États membres;

h) assure la coordination des mesures de sécurité avec les autorités compétentes des États membres qui sont responsables de la protection des informations classifiées et, le cas échéant, des pays tiers ou des organisations internationales, y compris en ce qui concerne la nature des menaces pesant sur la sécurité des ICUE et les moyens de les protéger;

i) conclut les arrangements administratifs visés à l'article 12, paragraphe 2, point b); et

j) procède à des visites d'évaluation initiales et périodiques dans des pays tiers ou des organisations internationales afin de s'assurer de l'efficacité des mesures mises en œuvre pour la protection des ICUE qui leur ont été fournies ou ont été échangées avec eux.

Le bureau de sécurité du SGC est à la disposition du secrétaire général pour l'aider à s'acquitter de ces responsabilités.

3. Aux fins de la mise en œuvre de l'article 14, paragraphe 3, il conviendrait que les États membres:

a) désignent une ANS responsable des dispositions de sécurité destinées à assurer la protection des ICUE afin que:

i) les ICUE détenues par tout service, organisme ou agence national, public ou privé, sur le territoire national ou à l'étranger soient protégées conformément à la présente décision;

ii) les dispositions de sécurité destinées à assurer la protection des ICUE soient périodiquement inspectées;

iii) toutes les personnes employées dans une administration nationale ou par un contractant et susceptibles d'avoir accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur détiennent une habilitation de sécurité correspondante ou soient dûment autorisées en vertu de leurs fonctions conformément aux dispositions législatives et réglementaires nationales;

iv) des programmes de sécurité soient mis au point en tant que de besoin de telle sorte que le risque de compromission ou de perte d'ICUE soit réduit au minimum;

v) les questions de sécurité liées à la protection des ICUE fassent l'objet d'une coordination avec les autres autorités nationales compétentes, y compris celles visées dans la présente décision; et

vi) des réponses soient apportées aux demandes d'habilitation de sécurité appropriées émanant des agences et des organes de l'UE créés en vertu du titre V, chapitre 2, du traité sur l'Union européenne, d'Europol, d'Eurojust ainsi que des opérations de gestion de crise mises en place en vertu du titre V, chapitre 2, du traité sur l'Union européenne ou des RSUE et de leurs équipes.

Les ANS figurent sur la liste de l'appendice C;

b) veillent à ce que leurs autorités compétentes communiquent à leur gouvernement et, par l'intermédiaire de ces derniers au Conseil, des informations sur la nature des menaces qui pèsent sur la sécurité des ICUE et des conseils sur les moyens de s'en protéger.

Article 16

comité de sécurité

1. Un comité de sécurité est créé par la présente décision. Il examine et évalue toute question de sécurité relevant du champ d'application de la présente décision, et transmet des recommandations au Conseil, le cas échéant.

2. Le comité de sécurité est composé de représentants des ANS des États membres, un représentant de la Commission et du Service européen pour l'action extérieure assistant à ses réunions. Il est présidé par le secrétaire général ou par son délégué désigné. Il se réunit sur instruction du Conseil ou à la demande du secrétaire général ou d'une ANS.

Des représentants des agences et des organes de l'UE créés en vertu du titre V, chapitre 2, du traité sur l'Union européenne, ainsi que d'Europol et d'Eurojust, peuvent être invités à assister à ses réunions lorsque les questions traitées les concernent.

3. Le comité de sécurité organise ses activités de manière à être en mesure de formuler des recommandations sur des aspects spécifiques de la sécurité. Il met en place une sous-division spécialisée dans les questions concernant l'assurance de l'information et d'autres sous-divisions spécialisées si nécessaire. Il établit le mandat de ces sous-divisions spécialisées et reçoit leurs rapports d'activités comprenant, le cas échéant, des recommandations, quelles qu'elles soient, destinées au Conseil.

Article 17

Remplacement de la décision précédente

1. La présente décision abroge et remplace la décision 2001/264/CE du Conseil du 19 mars 2001 adoptant le règlement de sécurité du Conseil [1].

2. Toutes les ICUE portant un marquage en application de la décision 2001/264/CE continuent d'être protégées conformément aux dispositions pertinentes de cette décision.

Article 18

Entrée en vigueur

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

Fait à Bruxelles, le 31 mars 2011.

Par le Conseil

Le président

VÖLNER P.

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

ANNEXES

ANNEXE I

Mesures de sécurité concernant le personnel

ANNEXE II

Sécurité physique

ANNEXE III

Gestion des informations classifiées

ANNEXE IV

Protection des ICUE traitées dans les SIC

ANNEXE V

Sécurité industrielle

ANNEXE VI

Échange d'informations classifiées avec des pays tiers et des organisations internationales

ANNEXE I

MESURES DE SÉCURITÉ CONCERNANT LE PERSONNEL

I. INTRODUCTION

1. La présente annexe énonce les modalités d'application de l'article 7. Elle prévoit notamment les critères permettant 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, ainsi que les procédures d'enquête et administratives à suivre à cet effet.

2. Dans l'ensemble de la présente annexe, sauf dans les cas où il est nécessaire de faire une distinction, on entend par «habilitation de sécurité du personnel» une habilitation nationale de sécurité du personnel (HSP nationale) et/ou une habilitation de sécurité du personnel de l'UE (HSP de l'UE) telles que définies à l'appendice A.

II. AUTORISER L'ACCÈS AUX ICUE

3. Une personne ne peut être autorisée à avoir accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur qu'après:

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

   b) s'être vu accorder une HSP du niveau correspondant ou avoir été dûment autorisée en vertu de ses fonctions conformément aux dispositions législatives et réglementaires nationales; et

   c) avoir été informée des règles et procédures de sécurité applicables à la protection des ICUE et avoir reconnu les responsabilités qui lui incombent en matière de protection de ces informations.

4. Il appartient à chacun des États membres et au SGC de répertorier, au sein de leurs structures, les postes nécessitant l'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur et exigeant par conséquent une HSP du niveau correspondant.

III. RÈGLES EN MATIÈRE D'HABILITATION DE SÉCURITÉ DU PERSONNEL

5. Après réception d'une demande dûment autorisée, les ANS ou les autres autorités nationales compétentes sont chargées de veiller à la réalisation des enquêtes de sécurité relatives aux ressortissants de leur pays qui doivent accéder à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur. Les normes d'enquête doivent être conformes aux dispositions législatives et réglementaires nationales.

6. Si la personne concernée réside sur le territoire d'un autre État membre ou d'un État tiers, les autorités nationales compétentes sollicitent une aide auprès de l'autorité compétente de l'État de résidence conformément aux dispositions législatives et réglementaires nationales. Les États membres se prêtent assistance pour effectuer les enquêtes de sécurité, conformément aux dispositions législatives et réglementaires nationales.

7. Lorsque les dispositions législatives et réglementaires nationales le permettent, les ANS ou les autres autorités nationales compétentes peuvent effectuer les enquêtes relatives aux non-ressortissants qui doivent accéder à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur. Les normes d'enquête doivent être conformes aux dispositions législatives et réglementaires nationales.

Critères à retenir dans le cadre des enquêtes de sécurité

8. 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 HSP lui permettant d'accéder à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur. L'autorité nationale compétente effectue une appréciation générale sur la base des conclusions de l'enquête. À lui seul, un élément défavorable ne constitue pas nécessairement un motif de refus d'une HSP. Parmi les principaux critères à retenir à cet effet, il conviendrait de déterminer, dans la mesure où les dispositions législatives et réglementaires nationales le permettent, si l'intéressé:

   a) a commis ou a tenté de commettre un acte d'espionnage, de terrorisme, de sabotage, de trahison ou de sédition, seul ou en association avec d'autres, s'est rendu complice d'un tel acte ou a incité une autre personne à le commettre;

   b) est ou a été lié à des espions, des terroristes, des saboteurs ou des personnes que l'on peut raisonnablement soupçonner de l'être, ou à des représentants d'organisations ou d'États étrangers, notamment des services de renseignement étrangers, qui sont susceptibles de menacer la sécurité de l'UE et/ou des États membres, à moins que ce lien ait été autorisé dans le cadre d'une mission officielle;

c) est ou a été membre d'une organisation qui, par des moyens violents ou subversifs ou par d'autres moyens illégaux, cherche, entre autres, à renverser le gouvernement d'un État membre, à modifier l'ordre constitutionnel d'un État membre ou à provoquer un changement de régime ou de politique dans un État membre;

d) est ou a été sympathisant d'une organisation décrite au point c), est ou a été lié de près à des membres d'une telle organisation;

e) a délibérément dissimulé, altéré ou falsifié des informations importantes, notamment du point de vue de la sécurité, ou a délibérément menti en remplissant un questionnaire de sécurité ou lors d'un entretien de sécurité;

f) a été reconnu coupable d'une ou de plusieurs infractions pénales;

g) a des antécédents de dépendance à l'alcool, d'usage de drogues illicites et/ou d'abus de drogues licites;

h) a ou a eu des comportements de nature à entraîner un risque de vulnérabilité au chantage ou à des pressions;

i) a fait preuve, en acte ou en parole, d'un manque d'honnêteté, de loyauté ou de fiabilité, ou s'est montré indigne de confiance;

j) s'est livré à des violations graves ou répétées du règlement de sécurité, a cherché ou a réussi à mener des activités non autorisées concernant les systèmes d'information et de communication;

k) est susceptible de faire l'objet de pressions (par exemple, en raison de la possession d'une ou plusieurs nationalités d'États non membres de l'UE ou par l'intermédiaire de parents ou de proches qui pourraient être vulnérables face à des services de renseignement étrangers, des groupes terroristes ou d'autres organisations ou personnes se livrant à des activités subversives, dont les visées peuvent menacer les intérêts de l'UE et/ou des États membres dans le domaine de la sécurité).

9. Les antécédents financiers et médicaux de la personne concernée peuvent également être pris en considération, le cas échéant et dans le respect des dispositions législatives et réglementaires nationales, au cours de l'enquête de sécurité.

10. La personnalité, la conduite et la situation du conjoint, du cohabitant ou d'un membre de la famille proche peuvent également être pris en considération, le cas échéant et dans le respect des dispositions législatives et réglementaires nationales, au cours de l'enquête de sécurité.

Règles en matière d'enquête applicables à l'accès aux ICUE

Première délivrance d'une HSP

11. La première HSP donnant accès aux informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET se fonde sur une enquête de sécurité portant sur les cinq dernières années au moins, ou sur la période comprise entre l'âge de 18 ans et la date de l'enquête, la période la plus courte étant retenue; cette enquête comprend les éléments suivants:

a) un questionnaire national de sécurité concernant le personnel, correspondant au niveau de classification des ICUE auxquelles l'intéressé pourrait avoir à accéder, est rempli, puis transmis à l'autorité de sécurité compétente;

b) vérification de l'identité/de la citoyenneté/de la nationalité: la date et le lieu de naissance de l'intéressé ainsi que son identité doivent être vérifiés. Sa citoyenneté et/ou sa nationalité, passées et présentes, doivent être établies; ce processus vise notamment à déterminer s'il est susceptible de céder à des pressions d'origine étrangère, par exemple en raison de son lieu de résidence antérieur ou de contacts passés; et

c) vérification des antécédents aux niveaux national et local: il convient de procéder à des vérifications dans les fichiers de la sûreté et les casiers judiciaires, lorsque ces derniers existent, et/ou dans d'autres registres analogues des administrations ou de la police. Il convient de vérifier les fichiers des services répressifs dans le ressort desquels la personne a résidé ou a travaillé.

12. La première HSP donnant accès aux informations TRÈS SECRET UE/EU TOP SECRET se fonde sur une enquête de sécurité portant sur les dix dernières années au moins, ou sur la période comprise entre l'âge de 18 ans et la date de l'enquête, la période la plus courte étant retenue. Si des entretiens ont lieu conformément au point e), les enquêtes portent sur les sept dernières années au moins, ou sur la période comprise entre l'âge de 18 ans et la date de l'enquête, la période la plus courte étant retenue. Outre les critères indiqués au paragraphe 8 ci-dessus, les éléments ci-après font l'objet d'une enquête, dans la mesure où les dispositions législatives et réglementaires nationales le permettent, avant l'octroi d'une HSP de niveau TRÈS SECRET UE/EU TOP SECRET; ils peuvent aussi faire l'objet d'une enquête avant l'octroi d'une HSP de niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, dans les cas où les dispositions législatives et réglementaires nationales l'exigent:

a) situation financière: il y a lieu de rechercher des informations sur la situation financière de l'intéressé pour déterminer si, en raison de graves difficultés financières, il est susceptible de céder à des pressions étrangères ou nationales, ou pour mettre en lumière un éventuel enrichissement inexpliqué;

b) éducation: il y a lieu, afin de pouvoir vérifier le parcours éducatif de l'intéressé, de rechercher des informations dans les écoles, universités et autres établissements d'enseignement fréquentés par l'intéressé depuis l'âge de 18 ans ou pendant une période jugée appropriée par l'autorité menant l'enquête;

c) emploi: il y a lieu de rechercher des informations relatives à la situation actuelle et passée en matière d'emploi, en se reportant à des sources telles que les attestations de travail, les rapports sur le rendement ou l'efficacité, les employeurs ou les supérieurs hiérarchiques;

d) service militaire: le cas échéant, vérification des états de service de l'intéressé et du type de dispense obtenu; et

e) entretiens: lorsque la législation nationale le prévoit et l'autorise, un ou des entretiens sont menés avec la personne concernée. Des entretiens sont également menés avec d'autres personnes qui sont en mesure de porter un jugement objectif sur les antécédents, les activités, la loyauté, l'intégrité et la fiabilité de l'intéressé. Lorsque dans le cadre de la pratique nationale, on demande à la personne qui fait l'objet de l'enquête de mentionner des personnes de référence, celles-ci doivent être interrogées, sauf si des raisons valables s'y opposent.

13. Le cas échéant et conformément aux dispositions législatives et réglementaires nationales, des recherches complémentaires peuvent être menées pour exploiter toutes les informations pertinentes dont on dispose sur l'intéressé et pour corroborer des informations défavorables ou les infirmer.

Renouvellement d'une HSP

14. Après la première délivrance d'une HSP et pour autant que l'intéressé ait accompli une période de service ininterrompue auprès d'une administration nationale ou du SGC et qu'il ait toujours besoin d'avoir accès aux ICUE, l'HSP est réexaminée en vue de son renouvellement dans un délai ne dépassant pas cinq ans pour une habilitation TRÈS SECRET UE/EU TOP SECRET et dix ans pour une habilitation SECRET UE/EU SECRET ou CONFIDENTIEL UE/EU CONFIDENTIAL avec effet à compter de la date de notification des conclusions de la dernière enquête de sécurité sur laquelle elle était fondée. Toutes les enquêtes de sécurité à effectuer en vue du renouvellement d'une HSP couvrent la période écoulée depuis la dernière enquête.

15. En vue du renouvellement d'une HSP, les éléments énoncés aux paragraphes 11 et 12 font l'objet d'une enquête.

16. Les demandes de renouvellement sont présentées en temps voulu, compte tenu du délai nécessaire pour réaliser les enquêtes de sécurité. Néanmoins, lorsque l'ANS concernée ou une autre autorité nationale compétente a reçu la demande de renouvellement en question et le questionnaire de sécurité correspondant avant l'expiration d'une HSP et que l'enquête de sécurité nécessaire n'est pas achevée, l'autorité nationale compétente peut, lorsque les dispositions législatives et réglementaires nationales le permettent, proroger la validité de l'HSP existante pour une durée de douze mois au maximum. Si, à la fin de cette période de douze mois, l'enquête de sécurité n'est toujours pas achevée, l'intéressé est affecté à des fonctions qui ne nécessitent pas une HSP.

Procédures appliquées au sein du SGC en matière d'HSP

17. En ce qui concerne les fonctionnaires et autres agents du SGC, l'autorité de sécurité du SGC transmet le questionnaire de sécurité rempli à l'ANS de l'État membre dont l'intéressé est ressortissant et demande qu'il soit procédé à une enquête de sécurité pour le niveau de classification des ICUE auxquelles l'intéressé devra avoir accès.

18. Si des informations utiles à une enquête de sécurité sont portées à la connaissance du SGC concernant une personne ayant demandé une HSP de l'UE, le SGC, agissant conformément à la réglementation applicable, en avertit l'ANS compétente.

19. À l'issue de l'enquête de sécurité, l'ANS compétente notifie à l'autorité de sécurité du SGC les conclusions de l'enquête en question, à l'aide du modèle-type prévu par le comité de sécurité pour la correspondance.

a) Lorsque, à l'issue de l'enquête de sécurité, on obtient 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, l'autorité investie du pouvoir de nomination (AIPN) du SGC peut accorder une HSP de l'UE à l'intéressé et l'autoriser à accéder à des ICUE du niveau de classification correspondant jusqu'à une date déterminée.

b) Lorsque, à l'issue de l'enquête de sécurité, on n'obtient pas cette assurance, l'AIPN du SGC en informe l'intéressé, qui peut demander à être entendu par l'AIPN. Celle-ci peut 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, l'HSP de l'UE n'est pas accordée.

20. 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'AIPN du SGC sont susceptibles de recours conformément au statut des fonctionnaires de l'Union européenne et au régime applicable aux autres agents de l'Union européenne, fixés dans le règlement (CEE, Euratom, CECA) n° 259/68 [1] (ci-après dénommés «statut et régime applicable»).

21. L'assurance sur laquelle une HSP de l'UE se fonde, pour autant qu'elle reste valable, couvre toute fonction exercée par l'intéressé au sein du SGC ou de la Commission.

22. 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'AIPN du SGC 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 du SGC ou d'une administration nationale d'un État membre, les conclusions précitées sont soumises à l'ANS compétente afin que celle-ci confirme qu'elles restent valables et pertinentes.

23. Si des informations sont portées à la connaissance du SGC concernant un risque de sécurité que représente une personne titulaire d'une HSP de l'UE valide, le SGC, agissant conformément à la réglementation applicable, en avertit l'ANS compétente. Lorsqu'une ANS notifie au SGC que l'assurance visée au paragraphe 19, point a), n'est plus fournie concernant une personne titulaire d'HSP de l'UE valide, l'AIPN du SGC 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, l'HSP de l'UE 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.

24. Toute décision de retirer une HSP de l'UE à un fonctionnaire ou à un autre agent du SGC et, s'il y a lieu, les raisons la justifiant sont communiquées à la personne concernée, qui peut demander à être entendue par l'AIPN. Les informations communiquées par une ANS sont soumises aux dispositions législatives et réglementaires en vigueur dans l'État membre concerné, y compris celles relatives aux recours. Les décisions de l'AIPN du SGC sont susceptibles de recours conformément au statut et au régime applicable.

25. Les experts nationaux détachés auprès du SGC pour occuper un poste nécessitant une HSP de l'UE doivent présenter à l'autorité de sécurité du SGC avant de prendre leurs fonctions une HSP nationale valable leur donnant accès aux ICUE.

Registres des HSP

26. Chaque État membre et le SGC tiennent respectivement des registres des HSP nationales et des HSP de l'UE accordées aux fins d'accès à des ICUE. Ces registres contiennent au minimum le niveau de classification des ICUE auxquelles l'intéressé peut se voir accorder l'accès (CONFIDENTIEL UE/EU CONFIDENTIAL ou un niveau supérieur), la date à laquelle l'HSP a été délivrée et sa durée de validité.

27. L'autorité de sécurité compétente peut délivrer un certificat d'habilitation de sécurité du personnel (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'HSP nationale donnant accès aux ICUE ou de l'HSP de l'UE correspondante et la date d'expiration du certificat proprement dit.

Exemptions de l'obligation d'HSP

28. L'accès aux ICUE dont bénéficient les personnes dans les États membres qui sont dûment autorisées en raison de leurs fonctions est déterminé conformément aux dispositions législatives et réglementaires nationales; ces personnes sont informées des obligations qui leur incombent en matière de sécurité en ce qui concerne la protection des ICUE.

IV. FORMATION ET SENSIBILISATION À LA SÉCURITÉ

29. Toutes les personnes qui se sont vu délivrer une HSP doivent reconnaître 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. Le cas échéant, les États membres et le SGC tiennent un registre de ces déclarations écrites.

30. 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 aux autorités de sécurité compétentes de toute démarche ou activité qu'elles jugent suspecte ou inhabituelle.

31. 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.

[1] JO L 56 du 4.3.1968, p. 1.

V. CIRCONSTANCES EXCEPTIONNELLES

32. Lorsque les dispositions législatives et réglementaires nationales le permettent, une HSP délivrée par une autorité nationale compétente d'un État membre aux fins d'accès à des informations nationales classifiées peut, pendant une période temporaire dans l'attente de la délivrance d'une HSP nationale aux fins d'accès à des ICUE, permettre à des fonctionnaires nationaux d'accéder à des ICUE jusqu'au niveau équivalent indiqué dans le tableau d'équivalence figurant à l'appendice B, dans les cas où un tel accès temporaire est requis dans l'intérêt de l'UE. Lorsque les dispositions législatives et réglementaires nationales ne permettent pas un tel accès temporaire à des ICUE, les ANS en informent le comité de sécurité.

33. En cas d'urgence, lorsque cela est dûment justifié dans l'intérêt du service et en attendant l'achèvement de l'enquête de sécurité complète, l'AIPN du SGC 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, accorder à titre temporaire aux fonctionnaires et autres agents du SGC l'autorisation d'accéder à des ICUE pour une fonction déterminée. Ces autorisations temporaires sont valables pour une période ne dépassant pas six mois et ne donnent pas accès aux informations classifiées TRÈS SECRET UE/EU TOP SECRET. 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. Le SGC tient un registre de ces déclarations écrites.

34. Lorsqu'une personne doit être affectée à un poste requérant une HSP dont le niveau dépasse d'un niveau celui qu'elle possède, l'affectation peut être décidée à titre provisoire, pour autant que les conditions suivantes soient réunies:

a) l'accès aux ICUE d'un niveau supérieur répond à une nécessité impérieuse qui doit être justifiée par écrit par le supérieur hiérarchique de la personne concernée;

b) l'accès doit être limité à des éléments particuliers des ICUE et servir aux attributions;

c) la personne détient une HSP nationale ou de l'UE valable;

d) des démarches ont été entreprises en vue d'obtenir une autorisation pour le niveau d'accès nécessaire pour le poste;

e) des contrôles satisfaisants ont été effectués par l'autorité compétente permettant d'établir l'absence de violations graves ou répétées du règlement de sécurité par la personne concernée;

f) l'affectation de la personne est approuvée par l'autorité compétente; et

g) une trace de l'accès exceptionnel, y compris une description des informations auxquelles accès a été donné, doit être conservée par le bureau d'ordre ou le bureau d'ordre subordonné compétent.

35. La procédure décrite ci-dessus est utilisée pour un accès ponctuel à des ICUE dont la classification dépasse d'un niveau le niveau d'habilitation de la personne concernée. Il ne convient pas de recourir de manière répétée à cette procédure.

36. Dans des circonstances très exceptionnelles, c'est-à-dire en cas de missions dans un environnement hostile ou au cours de périodes de tension internationale croissante lorsque des mesures d'urgence l'exigent, plus particulièrement afin de sauver des vies, les États membres et le secrétaire général peuvent accorder, si possible par écrit, un accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET à des personnes qui ne détiennent pas l'HSP requise, à condition que l'accès accordé soit absolument indispensable et qu'il n'y ait pas de raison de douter de la loyauté, de l'intégrité et de la fiabilité de la personne concernée. Une trace de l'autorisation précisant les informations pour lesquelles l'accès a été approuvé doit être conservée.

37. Pour les informations classifiées TRÈS SECRET UE/EU TOP SECRET, un tel accès d'urgence est limité aux ressortissants d'États membres de l'UE s'étant vu octroyer l'accès soit à des informations dont le niveau de classification national équivaut à TRÈS SECRET UE/EU TOP SECRET soit à des informations classifiées SECRET UE/EU SECRET.

38. Le comité de sécurité est informé des cas où il est recouru à la procédure décrite aux paragraphes 36 et 37.

39. Lorsque les dispositions législatives et réglementaires d'un État membre édictent des règles plus strictes en matière d'autorisations temporaires, d'affectations provisoires ou d'accès ponctuel ou d'urgence des personnes concernées à des informations classifiées, les procédures prévues dans la présente section ne sont appliquées que dans les limites éventuellement imposées par les dispositions législatives et réglementaires nationales en vigueur.

40. Chaque année, le comité de sécurité reçoit un rapport sur le recours aux procédures énoncées dans la présente section.

VI. PARTICIPATION AUX SESSIONS ET RÉUNIONS DANS LE CADRE DU CONSEIL

41. Sous réserve du paragraphe 28, les personnes désignées pour participer à des sessions du Conseil ou à des réunions d'instances préparatoires du Conseil au sein 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 la situation de l'intéressé au regard de l'HSP. Pour les délégués, un CHSP ou une autre preuve d'HSP doit être transmis au bureau de sécurité du SGC par les autorités compétentes ou, à titre exceptionnel, présenté par le délégué concerné. Le cas échéant, il peut être fait usage d'une liste de noms récapitulative mentionnant les preuves d'habilitation voulues.

42. Lorsqu'une HSP nationale, accordée à des fins d'accès à des ICUE, est, pour des raisons de sécurité, retirée à une personne dont les fonctions requièrent la participation à des sessions du Conseil ou à des réunions d'instances préparatoires du Conseil, l'autorité compétente en informe le SGC.

VII. ACCÈS POTENTIEL AUX ICUE

43. Lorsqu'une personne doit être employée dans une fonction susceptible de lui donner un accès potentiel à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau supérieur, elle doit être dûment habilitée ou escortée en permanence.

44. Les courriers, les gardes et les escortes doivent disposer d'une habilitation 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.

ANNEXE II

SÉCURITÉ PHYSIQUE

I. INTRODUCTION

1. La présente annexe énonce les modalités d'application de l'article 8. Elle prévoit les règles minimales de protection physique des locaux, bâtiments, bureaux, salles et autres zones où des ICUE sont traitées et stockées, y compris des zones où se trouvent des SIC.

2. 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 habilitation 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.

II. RÈGLES ET MESURES EN MATIÈRE DE SÉCURITÉ PHYSIQUE

3. Les mesures de sécurité physique sont choisies en fonction d'une évaluation de la menace réalisée par les autorités compétentes. Il convient que tant le SGC que les États membres appliquent une procédure de gestion du risque pour protéger les ICUE dans leurs 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'UE ou des États membres, ainsi que les actes de sabotage, le terrorisme et les activités subversives ou les autres activités criminelles.

4. En appliquant la notion de défense en profondeur, l'autorité de sécurité compétente détermine la bonne combinaison de mesures de sécurité physique qu'il convient de mettre en œuvre. Il peut s'agir d'une ou de plusieurs des mesures suivantes:

   a) barrière périmétrique: une barrière physique qui défend les limites d'une zone devant être protégée;

   b) système de détection des intrusions (SDI): un tel système peut être utilisé pour améliorer le niveau de sécurité d'une barrière périmétrique ou dans des salles et des bâtiments pour remplacer le personnel de sécurité ou l'aider dans sa tâche;

   c) contrôle des accès: il peut être exercé sur un site, un ou plusieurs bâtiments d'un site ou des zones ou salles à l'intérieur d'un bâtiment. Ce contrôle peut être exercé par des moyens électroniques ou électromécaniques, par un membre du personnel de sécurité et/ou un réceptionniste, ou par tout autre moyen physique;

   d) personnel de sécurité: un personnel de sécurité formé, supervisé et, au besoin, dûment habilité peut être employé, notamment, pour dissuader des personnes de planifier des intrusions clandestines;

   e) système de télévision en circuit fermé (CCTV): un tel système peut être utilisé par le personnel de sécurité pour effectuer des vérifications en cas d'incident ou de déclenchement de l'alarme des SDI sur des sites étendus ou des enceintes;

   f) éclairage de sécurité: un tel éclairage peut être utilisé pour dissuader un intrus potentiel ainsi que pour fournir la lumière nécessaire à une surveillance efficace, soit directement par le personnel de sécurité soit indirectement par l'intermédiaire d'un système de CCTV; et

   g) toute autre mesure physique appropriée destinée à avoir un effet dissuasif quant à l'accès non autorisé ou à détecter un tel accès, ou à prévenir la perte ou la détérioration d'ICUE.

5. L'autorité compétente peut être 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.

6. Lorsque des ICUE risquent d'être vues, même accidentellement, des mesures appropriées sont prises pour parer à ce risque.

7. Pour les nouveaux établissements, les règles en matière de sécurité physique et leurs spécifications fonctionnelles doivent être définies lors de la planification et de la conception des établissements. Pour les établissements existants, les règles en matière de sécurité physique doivent être appliquées dans toute la mesure du possible.

III. ÉQUIPEMENT DESTINÉ À LA PROTECTION PHYSIQUE DES ICUE

8. Lors de l'achat de l'équipement destiné à la protection physique des ICUE (comme des meubles de sécurité, des déchiqueteuses, des serrures de porte, des systèmes électroniques de contrôle des accès, des SDI, des systèmes d'alarme), l'autorité de sécurité compétente veille à ce que cet équipement réponde aux normes techniques et aux conditions minimales agréées.

9. Les spécifications techniques de l'équipement devant servir à la protection physique des ICUE sont définies dans des lignes directrices en matière de sécurité, qu'il appartient au comité de sécurité d'approuver.

10. Les systèmes de sécurité sont périodiquement inspectés et l'équipement est entretenu à intervalles réguliers. L'entretien prend en compte les résultats des inspections afin de garantir un fonctionnement optimal continu de l'équipement.

11. Il convient de réévaluer à chaque inspection l'efficacité des différentes mesures de sécurité et du système de sécurité dans son ensemble.

IV. ZONES PHYSIQUEMENT PROTÉGÉES

12. Deux types de zones physiquement protégées, ou leurs équivalents au niveau national, 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).

    Dans la présente décision, toutes les références aux zones administratives et aux zones sécurisées, y compris les zones sécurisées du point de vue technique, s'entendent comme visant également les zones équivalentes au niveau national.

13. Il appartient à l'autorité de sécurité compétente 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.

14. 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 compétente; et

    c) toutes les autres personnes sont escortées en permanence ou font l'objet de contrôles équivalents.

15. 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;

    c) toutes les autres personnes sont escortées en permanence ou font l'objet de contrôles équivalents.

16. 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.

17. 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 de SDI, verrouillées lorsqu'elles ne sont pas occupées et gardées lorsqu'elles sont occupées. Toutes les clés sont contrôlées conformément à la section VI;

    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 selon les exigences de l'autorité de sécurité compétente. 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.

18. Nonobstant le paragraphe 17, 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 compétente 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.

19. 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.

20. 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.

21. Des procédures d'exploitation de sécurité sont arrêtées pour chacune des zones sécurisées et précisent:

    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 en raison de leur besoin d'en connaître et en fonction de leur habilitation;

    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.

22. 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 compétente et offrent une protection équivalente à celle d'un meuble de sécurité approuvé pour le stockage d'ICUE du même niveau de classification.

V. MESURES DE PROTECTION PHYSIQUES APPLICABLES AU TRAITEMENT ET AU STOCKAGE DES ICUE

23. Les ICUE classifiées 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 aux dispositions de l'annexe III, paragraphes 28 à 40, et se soit engagé à se conformer aux mesures compensatoires prévues dans les instructions de sécurité émises par l'autorité de sécurité compétente pour empêcher que des personnes non autorisées aient accès aux ICUE.

24. Les ICUE classifiées 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 sécurisée ou d'une zone administrative à condition que le détenteur se soit engagé à se conformer aux mesures compensatoires prévues dans les instructions de sécurité émises par l'autorité de sécurité compétente.

25. Les ICUE classifiées 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) transporte les ICUE conformément aux dispositions de l'annexe III, paragraphes 28 à 40;

        ii) se soit engagé à se conformer aux mesures compensatoires prévues dans les instructions de sécurité émises par l'autorité de sécurité compétente pour empêcher que des personnes non autorisées aient accès aux ICUE;

        iii) exerce en personne un contrôle permanent sur les ICUE; et

        iv) si les documents sont sous forme papier, qu'il en ait informé le bureau d'ordre compétent.

26. 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.

27. Les ICUE classifiées TRÈS SECRET UE/EU TOP SECRET sont traitées dans une zone sécurisée.

28. Les ICUE classifiées TRÈS SECRET UE/EU TOP SECRET sont stockées dans une zone sécurisée, selon l'une des modalités suivantes:

    a) dans un meuble de sécurité conformément au paragraphe 8, moyennant un ou plusieurs des contrôles supplémentaires suivants:

        i) protection ou vérification en permanence par un membre habilité du personnel de sécurité ou du personnel de service;

        ii) 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.

29. Les règles régissant le transport des ICUE en dehors des zones physiquement protégées figurent à l'annexe III.

VI. CONTRÔLE DES CLÉS ET COMBINAISONS UTILISÉES POUR LA PROTECTION DES ICUE

30. L'autorité de sécurité compétente définit les procédures de gestion des clés et des combinaisons pour les bureaux, les salles, les chambres fortes et les meubles de sécurité. Ces procédures protègent d'un accès non autorisé.

31. 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) lors de tout changement du personnel connaissant la combinaison;

    b) en cas de compromission, réelle ou présumée;

    c) lorsqu'une serrure a fait l'objet d'un entretien ou d'une réparation; et

    d) au moins tous les douze mois.

ANNEXE III

GESTION DES INFORMATIONS CLASSIFIÉES

I. INTRODUCTION

1. La présente annexe énonce les modalités d'application de l'article 9. Elle prévoit les mesures administratives visant à contrôler les ICUE tout au long de leur cycle de vie en vue de contribuer 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.

II. GESTION DE LA CLASSIFICATION

Classifications et marquages

2. Les informations sont classifiées dans les cas où elles doivent être protégées compte tenu de leur confidentialité.

3. L'autorité d'origine des ICUE est chargée de déterminer le niveau de classification de sécurité, conformément aux lignes directrices applicables en matière de classification, et de la diffusion initiale des informations.

4. Le niveau de classification des ICUE est fixé conformément à l'article 2, paragraphe 2, et en se reportant à la politique de sécurité qui doit être approuvée conformément à l'article 3, paragraphe 3.

5. 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.

6. 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.

7. 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.

8. Dans la mesure du possible, les documents dont toutes les parties n'ont pas le même niveau de classification sont structurés de manière à ce que les parties ayant des niveaux de classification différents puissent au besoin être aisément identifiées et séparées des autres.

9. 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

Marquages

10. Outre l'un des marquages de classification de sécurité prévus à l'article 2, 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.

Abréviations indiquant la classification

11. 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.

12. Les abréviations uniformisées ci-après peuvent être utilisées dans les documents classifiés de l'UE 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

Création d'ICUE

13. Lors de la création de documents classifiés de l'UE:

a) sur chaque page figure un marquage indiquant clairement le niveau de classification;

b) chaque page est numérotée;

c) le document porte un numéro de référence 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.

14. Lorsqu'il n'est pas possible d'appliquer le paragraphe 13 à des ICUE, d'autres mesures appropriées sont prises conformément aux lignes directrices en matière de sécurité qui doivent être arrêtées en vertu de l'article 6, paragraphe 2.

Déclassement et déclassification des ICUE

15. Au moment de la création du document classifié, l'autorité d'origine indique, si possible et notamment en ce qui concerne les informations classifiées RESTREINT UE/EU RESTRICTED, si les ICUE qui y figurent peuvent ou non être déclassées ou déclassifiées à une date donnée ou après un événement spécifique.

16. Le SGC réexamine régulièrement les ICUE en sa possession pour déterminer si leur niveau de classification est toujours d'application. Le SGC instaure un système pour réexaminer le niveau de classification des ICUE enregistrées dont il est l'auteur, au moins une fois tous les cinq ans. 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.

III. ENREGISTREMENT DES ICUE À DES FINS DE SÉCURITÉ

17. Pour chacune des entités structurées qui existent au sein du SGC et des administrations nationales des États membres et dans lesquelles des ICUE sont traitées, on détermine un bureau d'ordre compétent chargé de veiller à ce que les ICUE soient traitées conformément à la présente décision. Les bureaux d'ordre sont conçus comme des zones sécurisées telles que définies à l'annexe II.

18. 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 d'un matériel, y compris de sa diffusion et de sa destruction.

19. Tout 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 parvient à une entité structurée ou qu'il en sort.

20. Le bureau d'ordre central du SGC garde une trace de toutes les informations classifiées communiquées par le Conseil et le SGC à des États tiers et à des organisations internationales, ainsi que de toutes les informations classifiées reçues d'États tiers ou d'organisations internationales.

21. Dans le cas d'un SIC, les procédures d'enregistrement peuvent être mises en œuvre au moyen de processus intervenant au sein du SIC même.

22. Le Conseil approuve une politique de sécurité sur l'enregistrement des ICUE à des fins de sécurité.

Bureaux d'ordre TRÈS SECRET UE/EU TOP SECRET

23. Un bureau d'ordre est désigné dans les États membres et au SGC 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.

24. Ces bureaux d'ordre subordonnés ne peuvent transmettre de documents TRES SECRET UE/EU TOP SECRET directement à d'autres bureaux d'ordre subordonnés rattachés au même bureau d'ordre TRES SECRET UE/EU TOP SECRET central sans l'autorisation expresse et écrite de ce dernier ni à des bureaux d'ordre extérieurs.

IV. DUPLICATION ET TRADUCTION DES DOCUMENTS CLASSIFIÉS DE L'UE

25. 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.

26. 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.

27. Les mesures de sécurité applicables au document original le sont aussi à ses copies et à ses traductions.

V. TRANSPORT DES ICUE

28. Le transport des ICUE est soumis aux mesures de protection énoncées aux paragraphes 30 à 40. Lorsque les ICUE sont transportées par des supports électroniques, et nonobstant l'article 9, paragraphe 4, les mesures de protection énoncées ci-après peuvent être complétées par des contre-mesures techniques appropriées prescrites par l'autorité de sécurité compétente, de façon à réduire au minimum le risque de perte ou de compromission.

29. Les autorités de sécurité compétentes au sein du SGC et dans les États membres donnent des instructions sur le transport des ICUE conformément à la présente décision.

À l'intérieur d'un même bâtiment ou d'un groupe autonome de bâtiments

30. Les ICUE transportées à l'intérieur d'un même bâtiment ou d'un groupe autonome de bâtiments sont dissimulées en vue de prévenir l'observation de leur contenu.

31. À l'intérieur d'un même bâtiment ou d'un groupe autonome de bâtiments, les informations classifiées TRÈS SECRET UE/EU TOP SECRET sont transportées dans une enveloppe sécurisée avec pour seule mention le nom du destinataire.

À l'intérieur de l'UE

32. Les ICUE transportées entre des bâtiments ou des locaux à l'intérieur de l'UE sont emballées de manière à être protégées de toute divulgation non autorisée.

33. Le transport d'informations classifiées jusqu'au niveau SECRET UE/EU SECRET à l'intérieur de l'UE s'effectue par l'un des moyens suivants:

a) le courrier militaire, gouvernemental ou diplomatique, selon le cas;

b) le transport par porteur, à condition:

i) que le porteur ne se sépare pas des ICUE, à moins que leur stockage ne soit assuré conformément aux règles énoncées à l'annexe II;

ii) que les ICUE ne soient pas déballées pendant le transport ni lues dans des lieux publics;

iii) que la personne soit informée des responsabilités qui lui incombent en matière de sécurité;

iv) que la personne soit, si nécessaire, munie d'un certificat de courrier.

c) les services postaux ou les services de courrier commercial, à condition:

i) qu'ils soient agréés par l'ANS compétente conformément aux dispositions législatives et réglementaires nationales;

ii) qu'ils appliquent les mesures de protection appropriées conformément aux exigences minimales qui seront prévues dans les lignes directrices en matière de sécurité arrêtées en vertu de l'article 6, paragraphe 2.

En cas de transport d'un État membre vers un autre État membre, les dispositions du point c) sont limitées aux informations classifiées jusqu'au niveau CONFIDENTIEL UE/EU CONFIDENTIAL.

34. Le matériel classifié CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET (par exemple, équipement ou machine) qui ne peut être transporté par les moyens visés au paragraphe 33 est transporté en tant que fret par des sociétés de transport commercial conformément à l'annexe V.

35. Le transport des informations classifiées TRÈS SECRET UE/EU TOP SECRET, entre des bâtiments ou des locaux à l'intérieur de l'UE, s'effectue par courrier militaire, gouvernemental ou diplomatique, selon le cas.

De l'UE vers le territoire d'un pays tiers

36. Les ICUE transportées de l'UE vers le territoire d'un pays tiers sont emballées de manière à être protégées de toute divulgation non autorisée.

37. Le transport des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET de l'UE vers le territoire d'un pays tiers s'effectue par l'un des moyens suivants:

a) le courrier militaire ou diplomatique;

b) le transport par porteur, à condition:

i) que le paquet porte un sceau officiel ou soit emballé de manière à indiquer qu'il s'agit d'un envoi officiel ne devant pas être soumis à contrôle douanier ou de sécurité;

ii) que la personne soit munie d'un certificat de courrier identifiant le paquet et l'autorisant à le transporter;

iii) que le porteur ne se sépare pas des ICUE, à moins que leur stockage ne soit assuré conformément aux règles énoncées à l'annexe II;

iv) que les ICUE ne soit pas déballées pendant le transport ni lues dans des lieux publics; et

v) que la personne soit informée des responsabilités qui lui incombent en matière de sécurité.

38. Le transport des informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET communiquées par l'UE à un pays tiers ou à une organisation internationale est conforme aux dispositions applicables au titre d'un accord sur la sécurité des informations ou d'un arrangement administratif conclu en vertu de l'article 12, paragraphe 2, point a) ou b).

39. Les informations classifiées RESTREINT UE/EU RESTRICTED peuvent aussi être transportées par des services postaux ou par des services de courrier commercial.

40. Le transport des informations classifiées TRÈS SECRET UE/EU TOP SECRET, de l'UE vers le territoire d'un pays tiers, s'effectue par courrier militaire ou diplomatique.

VI. DESTRUCTION DES ICUE

41. Les documents classifiés de l'UE qui ne sont plus nécessaires peuvent être détruits, sans préjudice de la réglementation applicable en matière d'archivage.

42. Les documents faisant l'objet d'un enregistrement en application de l'article 9, paragraphe 2, de la présente décision sont détruits par le bureau d'ordre compétent sur instruction du détenteur ou d'une autorité compétente. Les cahiers d'enregistrement et les autres informations relatives aux enregistrements sont actualisés en conséquence.

43. La destruction de documents classifiés SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET est effectuée en présence d'un témoin justifiant de l'habilitation de sécurité correspondant au moins au niveau de classification du document à détruire.

44. 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. Le bureau d'ordre 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.

45. Les documents classifiés, y compris ceux dont la classification est RESTREINT UE/EU RESTRICTED, sont détruits par des méthodes répondant aux normes UE applicables ou à des normes équivalentes, ou homologuées par les États membres conformément aux normes techniques nationales, pour empêcher leur reconstitution totale ou partielle.

46. La destruction des supports de données informatiques utilisés pour des ICUE s'effectue conformément à l'annexe IV, paragraphe 36.

VII. INSPECTIONS ET VISITES D'ÉVALUATION

47. Le terme «inspection» utilisé ci-après désigne:

a) toute inspection visée à l'article 9, paragraphe 3, et à l'article 15, paragraphe 2, points e), f) et g); ou

b) toute visite d'évaluation visée à l'article 12, paragraphe 5,

ayant pour but d'évaluer l'efficacité des mesures mises en œuvre pour protéger les ICUE.

48. Les inspections sont notamment menées aux fins suivantes:

a) veiller à ce que les normes minimales requises fixées dans la présente décision en matière de protection des ICUE soient respectées;

b) mettre l'accent sur l'importance de la sécurité et d'une gestion efficace des risques au sein des entités inspectées;

c) recommander des contre-mesures pour atténuer l'impact particulier de la perte de confidentialité, d'intégrité ou de disponibilité des informations classifiées; et

d) renforcer les programmes mis en place par les autorités de sécurité en matière de formation et de sensibilisation à la sécurité.

49. Avant la fin de chaque année civile, le Conseil adopte le programme d'inspection prévu à l'article 15, paragraphe 1, point c), pour l'année suivante. Les dates exactes de chaque inspection sont fixées en accord avec l'agence ou l'organe de l'UE, l'État membre, le pays tiers ou l'organisation internationale concerné(e).

Conduite des inspections

50. Les inspections sont effectuées en vue de contrôler les prescriptions, les réglementations et les procédures applicables dans l'entité inspectée et de vérifier que les pratiques en vigueur au sein de l'entité satisfont aux principes de base et aux normes minimales fixés par la présente décision et par les dispositions qui régissent l'échange d'informations classifiées avec cette entité.

51. Les inspections se déroulent en deux phases. Avant l'inspection proprement dite, une réunion préparatoire est organisée, si nécessaire, avec l'entité concernée. À l'issue de cette réunion préparatoire, l'équipe d'inspection établit, de concert avec ladite entité, un programme d'inspection détaillé couvrant tous les secteurs de la sécurité. L'équipe d'inspection a accès à tous les lieux, notamment aux bureaux d'ordre et aux points de présence SIC, où sont traitées des ICUE.

52. Les inspections effectuées dans les administrations nationales des États membres sont réalisées sous la responsabilité d'une équipe d'inspection commune SGC/Commission en totale coopération avec les responsables de l'entité inspectée.

53. Les inspections effectuées dans des pays tiers et dans les organisations internationales sont réalisées sous la responsabilité d'une équipe d'inspection commune SGC/Commission en totale coopération avec les responsables du pays tiers ou de l'organisation internationale faisant l'objet de l'inspection.

54. Les inspections d'agences et d'organes de l'UE créés en vertu du titre V, chapitre 2, du traité sur l'Union européenne, ainsi que celles d'Europol et d'Eurojust, sont menées par le bureau de sécurité du SGC avec l'aide de spécialistes de l'ANS dans le ressort de laquelle se situe l'agence ou l'organe. La direction de la sécurité de la Commission européenne (DSCE) peut être associée dans les cas où elle échange régulièrement des ICUE avec l'agence ou l'organe en question.

55. Dans le cadre des inspections des agences et organes de l'UE créés en vertu du titre V, chapitre 2, du traité sur l'Union européenne, ainsi que de celles d'Europol et d'Eurojust, des pays tiers et des organisations internationales, le concours et l'assistance des experts des ANS sont sollicités conformément à des modalités à définir par le comité de sécurité.

Rapports d'inspection

56. À l'issue de l'inspection, les principales conclusions et recommandations sont présentées à l'entité inspectée. Un rapport d'inspection est ensuite établi sous la responsabilité de l'autorité de sécurité du SGC (bureau de sécurité). Lorsque des mesures correctives et des recommandations ont été proposées, le rapport doit contenir suffisamment d'éléments précis pour étayer les conclusions dégagées. Le rapport d'inspection est transmis à l'autorité compétente de l'entité inspectée.

57. En ce qui concerne les inspections effectuées dans les administrations nationales des États membres:

a) le projet de rapport d'inspection est transmis à l'ANS concernée afin de vérifier qu'il ne contient pas d'erreur de fait et qu'aucune information d'un niveau de classification supérieur à RESTREINT UE/EU RESTRICTED n'y figure;

b) sauf si l'ANS de l'État membre en question demande de surseoir à une diffusion générale, les rapports d'inspection sont diffusés à l'ensemble des membres du comité de sécurité ainsi qu'à la DSCE; le rapport est classifié RESTREINT UE/EU RESTRICTED;

Un rapport périodique est établi sous la responsabilité de l'autorité de sécurité du SGC (bureau de sécurité) pour souligner les enseignements qui ont été tirés des inspections effectuées dans les États membres au cours d'une période précise et est examiné par le comité de sécurité.

58. En ce qui concerne les visites d'évaluation dans les pays tiers et les organisations internationales, le rapport est diffusé au comité de sécurité ainsi qu'à la DSCE. Le rapport reçoit, au minimum, la classification RESTREINT UE/EU RESTRICTED. Toute mesure corrective est vérifiée lors d'une visite de suivi et signalée au comité de sécurité.

59. En ce qui concerne les inspections d'agences et d'organes de l'UE créés en vertu du titre V, chapitre 2, du traité sur l'Union européenne, ainsi que celles d'Europol et d'Eurojust, les rapports d'inspection sont diffusés aux membres du comité de sécurité et à la DSCE. Le projet de rapport d'inspection est transmis à l'agence ou à l'organe concerné(e) afin de vérifier qu'il ne contient pas d'erreur de fait et qu'aucune information d'un niveau de classification supérieur à RESTREINT UE/EU RESTRICTED n'y figure. Toute mesure corrective est vérifiée lors d'une visite de suivi et signalée au comité de sécurité.

60. L'autorité de sécurité du SGC procède régulièrement à des inspections des entités structurées du SGC aux fins prévues au paragraphe 48.

Liste de contrôle en matière d'inspection

61. L'autorité de sécurité du SGC (bureau de sécurité) établit et met à jour une liste de contrôle des éléments à vérifier au cours d'une inspection. Cette liste de contrôle est transmise au comité de sécurité.

62. Les informations nécessaires pour compléter la liste de contrôle sont obtenues, notamment au cours de l'inspection, auprès des services chargés de la gestion de la sécurité de l'entité faisant l'objet de l'inspection. Sitôt complétée avec les réponses détaillées obtenues, la liste de contrôle est classifiée en accord avec l'entité inspectée. Elle ne fait pas partie du rapport d'inspection.

ANNEXE IV

PROTECTION DES ICUE TRAITÉES DANS LES SIC

I. INTRODUCTION

1. La présente annexe énonce les modalités d'application de l'article 10.

2. Les propriétés et les notions d'AI figurant ci-après sont essentielles pour la sécurité et l'exécution correcte des opérations dans le cadre d'un SIC.

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.

II. PRINCIPES D'ASSURANCE DE L'INFORMATION

3. Les dispositions énoncées ci-après constituent les éléments fondamentaux permettant de garantir la sécurité de tout SIC traitant des ICUE. Les modalités précises de mise en œuvre de ces dispositions sont définies dans les politiques et les lignes directrices en matière de sécurité d'AI.

Gestion des risques de sécurité

4. La gestion des risques de sécurité fait partie intégrante de la définition, de l'élaboration, de l'exploitation et de la maintenance d'un SIC. La gestion des risques (évaluation, traitement, acceptation et communication) est mise en œuvre conjointement, dans le cadre d'un processus itératif, par les représentants des détenteurs de systèmes, les autorités responsables du projet, les autorités chargées de l'exploitation et les autorités d'homologation de sécurité selon une procédure d'évaluation des risques ayant fait ses preuves, transparente et pouvant être parfaitement comprise. Le domaine d'application du SIC et ses ressources sont clairement définis dès le début du processus de gestion des risques.

5. Les autorités compétentes examinent les menaces potentielles qui pèsent sur le SIC, tiennent à jour les évaluations des menaces et veillent à leur exactitude afin que celles-ci rendent compte de l'environnement opérationnel du moment. Elles actualisent en permanence leurs connaissances relatives aux questions de vulnérabilité et revoient régulièrement l'évaluation de la vulnérabilité afin de suivre l'évolution de la technologie de l'information.

6. Le traitement des risques de sécurité vise à appliquer un ensemble de mesures de sécurité offrant un équilibre satisfaisant entre les besoins des utilisateurs, les coûts et le risque de sécurité résiduel.

7. Les exigences spécifiques, l'étendue et le niveau de détail fixés par l'AHS compétente aux fins de l'homologation d'un SIC sont proportionnés au risque évalué, compte tenu de tous les facteurs pertinents, y compris le niveau de classification des ICUE qui sont traitées dans le SIC. Dans le cadre de l'homologation, le risque résiduel fait l'objet d'un énoncé formel et est accepté par une autorité responsable.

Sécurité du SIC tout au long de son cycle de vie

8. Assurer la sécurité d'un SIC tout au long de son cycle de vie, de son lancement à son retrait, est une obligation.

9. Le rôle de chaque acteur d'un SIC et les interactions entre ces acteurs, en termes de sécurité du système, doivent être clairement déterminés pour chaque phase du cycle de vie.

10. Tout SIC, y compris les mesures de sécurité techniques et non techniques dont il fait l'objet, est soumis à des essais de sécurité au cours du processus d'homologation afin de s'assurer que le niveau d'assurance requis est atteint et de vérifier qu'il est correctement mis en œuvre, intégré et configuré.

11. Des évaluations, inspections et examens de sécurité sont réalisés à intervalles réguliers durant la phase opérationnelle ainsi que dans le cadre de la maintenance d'un SIC, de même qu'en toute circonstance exceptionnelle.

12. Les documents relatifs à la sécurité d'un SIC évoluent tout au long du cycle de vie de celui-ci, évolution qui s'inscrit pleinement dans le cadre du processus de gestion du changement et de la configuration.

Meilleures pratiques

13. Le SGC et les États membres travaillent de concert à l'élaboration des meilleures pratiques destinées à protéger les ICUE traitées par un SIC. Les lignes directrices concernant les meilleures pratiques énoncent des mesures visant à assurer la sécurité du SIC sur le plan technique et physique ainsi qu'au niveau de l'organisation et des procédures et dont l'efficacité pour lutter contre certaines menaces et vulnérabilités a été démontrée.

14. Il convient, aux fins de la protection des ICUE traitées par un SIC, de mettre à profit les enseignements tirés par les entités travaillant dans le domaine de l'AI, que ce soit au sein ou en dehors de l'UE.

15. La diffusion et la mise en œuvre ultérieure des meilleures pratiques contribuent à atteindre un niveau équivalent d'assurance dans l'ensemble des SIC traitant des ICUE et exploités par le SGC et les États membres.

Défense en profondeur

16. Afin d'atténuer les risques qui pèsent sur un SIC, un éventail de mesures de sécurité techniques et non techniques organisées en plusieurs niveaux de défense doit être mis en œuvre. Ces niveaux sont notamment les suivants:

a) *la dissuasion:* mesures de sécurité visant à dissuader un éventuel adversaire de projeter une attaque du SIC;

b) *la prévention:* mesures de sécurité visant à empêcher ou à stopper une attaque du SIC;

c) *la détection:* mesures de sécurité visant à déceler une attaque du SIC en train de se produire;

d) *la résilience:* mesures de sécurité visant à faire en sorte que l'attaque n'ait un impact que sur un nombre aussi faible que possible d'informations ou de ressources du SIC et à prévenir d'autres dommages; et

e) *le retour aux conditions opérationnelles:* mesures de sécurité visant à rétablir la sécurité du SIC.

La rigueur de ces mesures de sécurité est déterminée sur la base d'une évaluation des risques.

17. Les autorités compétentes s'assurent qu'elles sont en mesure de faire face aux incidents dont l'ampleur dépasse les limites de l'organisation ou du pays touché, afin de coordonner les réactions et d'échanger des informations sur ces incidents et l'ensemble des risques qui en découlent (capacités de réaction en cas d'urgence informatique).

Principes du minimalisme et du moindre privilège

18. Seuls sont mis en œuvre les fonctions, dispositifs et services indispensables pour répondre aux exigences opérationnelles.

19. Les utilisateurs d'un SIC et les processus automatisés se voient uniquement accorder les droits d'accès, les privilèges ou les autorisations requises pour mener à bien leur tâche, afin de limiter tout dommage résultant d'accidents, d'erreurs ou d'utilisations non autorisées des ressources du SIC.

20. Les procédures d'enregistrement mises en œuvre par un SIC, le cas échéant, sont vérifiées dans le cadre du processus d'homologation.

Sensibilisation à l'assurance de l'information

21. La sensibilisation aux risques et aux mesures de sécurité disponibles constitue la première ligne de défense destinée à assurer la sécurité des SIC. En particulier, tout le personnel intervenant dans le cycle de vie d'un SIC, y compris les utilisateurs, doit bien comprendre:

a) que les défaillances en matière de sécurité peuvent porter gravement atteinte aux SIC;

b) le préjudice potentiel que peuvent causer à autrui l'interconnectivité et l'interdépendance; et

c) la responsabilité et l'obligation de rendre des comptes qui lui incombent concernant la sécurité du SIC, selon les fonctions qui sont les siennes dans le cadre des systèmes et processus.

22. Afin que les responsabilités en matière de sécurité soient bien comprises, une formation et une sensibilisation à l'AI sont obligatoires pour tout le personnel concerné, y compris les cadres supérieurs et les utilisateurs du SIC.

Évaluation et approbation des produits de sécurité informatique

23. Le niveau de confiance requis dans les mesures de sécurité, défini comme un niveau d'assurance, est déterminé à l'issue du processus de gestion des risques et conformément aux politiques et lignes directrices applicables en matière de sécurité.

24. Le niveau d'assurance fait l'objet d'une vérification au moyen de procédés et de méthodes reconnus à l'échelon international ou agréés au niveau national. Il s'agit principalement d'évaluations, de contrôles et d'audits.

25. Les produits cryptographiques destinés à protéger les ICUE sont évalués et agréés par une AAC nationale d'un État membre.

26. Avant d'être recommandés au Conseil ou au secrétaire général pour agrément, en application de l'article 10, paragraphe 6, ces produits cryptographiques doivent avoir satisfait à une évaluation par seconde partie réalisée par une autorité dûment qualifiée (AQUA) d'un État membre n'intervenant pas dans la conception ni dans la fabrication de l'équipement concerné. L'ampleur de l'évaluation par seconde partie nécessaire dépend du niveau de classification maximal envisagé des ICUE que ces produits doivent protéger. Le Conseil approuve une politique de sécurité concernant l'évaluation et l'agrément de produits cryptographiques.

27. Lorsque des motifs opérationnels particuliers le justifient, le Conseil ou le secrétaire général, selon le cas, peut, sur recommandation du comité de sécurité, ne pas respecter les exigences prévues aux paragraphes 25 et 26 et délivrer un agrément à titre provisoire pour une période spécifique, en application de la procédure énoncée à l'article 10, paragraphe 6.

28. L'AQUA est une AAC d'un État membre qui a été agréée, sur la base de critères définis par le Conseil, pour procéder à la deuxième évaluation des produits cryptographiques destinés à protéger les ICUE.

29. Le Conseil approuve une politique de sécurité concernant la qualification et l'approbation des produits de sécurité informatique non cryptographiques.

Transmission à l'intérieur de zones sécurisées

30. Nonobstant les dispositions de la présente décision, lorsque la transmission d'ICUE s'effectue uniquement à l'intérieur de zones sécurisées, une diffusion non chiffrée ou d'un niveau de chiffrement inférieur peut être envisagée compte tenu des résultats d'un processus de gestion des risques et avec l'accord de l'AHS.

Interconnexion sécurisée des SIC

31. Aux fins de la présente décision, on entend par «interconnexion» la connexion directe d'au moins deux systèmes informatiques permettant à ceux-ci d'échanger des données et d'autres ressources en matière d'information (communication, par exemple) de façon unidirectionnelle ou multidirectionnelle.

32. Un SIC doit de prime abord considérer tout système informatique interconnecté comme n'étant pas fiable et mettre en œuvre des mesures de protection destinées à contrôler les échanges d'informations classifiées.

33. Lorsqu'un SIC est interconnecté avec un autre système électronique, les conditions de base suivantes doivent être réunies:

    a) les conditions opérationnelles ou d'activités pour ces interconnexions sont définies et approuvées par les autorités compétentes;

    b) l'interconnexion est soumise à un processus de gestion des risques et d'homologation et est approuvée par les AHS compétentes; et

    c) des services de protection en bordure (SPB) sont mis en place à la périphérie de tout SIC.

34. Il ne peut y avoir aucune interconnexion entre un SIC homologué et un réseau non protégé ou public, sauf lorsque le SIC comporte un système de protection en bordure homologué installé à cette fin entre le SIC et le réseau non protégé ou public. Les mesures de sécurité applicables à une telle interconnexion sont examinées par l'autorité chargée de l'assurance de l'information compétente et approuvées par l'AHS compétente.

    Lorsque le réseau public ou non protégé sert uniquement à des fins de transmission et que les données sont chiffrées au moyen d'un produit cryptographique agréé conformément à l'article 10, une telle connexion n'est pas considérée comme une interconnexion.

35. Un SIC homologué pour traiter des informations TRÈS SECRET UE/EU TOP SECRET ne peut pas être interconnecté directement ou en cascade à un réseau non protégé ou public.

Supports de données informatiques

36. Les supports de données informatiques sont détruits conformément aux procédures approuvées par l'autorité de sécurité compétente.

37. Les supports de données informatiques sont réutilisés, déclassés ou déclassifiés conformément à une politique de sécurité arrêtée en vertu de l'article 6, paragraphe 1.

Situations d'urgence

38. Nonobstant les dispositions de la présente décision, 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.

39. 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 ou ne possèdent aucun dispositif de chiffrement; et

b) le matériel classifié ne peut être communiqué en temps voulu par aucun autre moyen.

40. Les informations classifiées transmises dans les conditions visées au paragraphe 38 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.

41. Lorsque des informations sont transmises en application du paragraphe 38, un rapport est par la suite adressé à ce sujet à l'autorité compétente et au comité de sécurité.

III. AUTORITÉS COMPÉTENTES EN MATIÈRE D'ASSURANCE DE L'INFORMATION

42. Les États membres et le SGC instituent les autorités compétentes en matière d'AI ci-après. Ces autorités ne doivent pas nécessairement être dotées d'entités structurées distinctes. Elles sont investies de mandats distincts. Cependant, ces autorités et leurs responsabilités connexes peuvent être associées ou intégrées dans la même entité structurée ou se partager entre différentes entités structurées, à condition que l'on veille à éviter au niveau interne tout conflit d'intérêt et tout chevauchement des tâches.

Autorité chargée de l'assurance de l'information

43. L'AAI s'acquitte des tâches suivantes:

a) définir les politiques et les lignes directrices de sécurité en matière d'AI et en surveiller l'efficacité et la pertinence;

b) conserver et gérer les données techniques relatives aux produits cryptographiques;

c) veiller à ce que les mesures en matière d'AI sélectionnées aux fins de la protection des ICUE soient conformes aux orientations régissant leur éligibilité et leur sélection;

d) veiller à ce que les produits cryptographiques soient sélectionnés conformément aux orientations régissant leur éligibilité et leur sélection;

e) coordonner la formation et la sensibilisation à l'AI;

f) mener des consultations avec le fournisseur du système, les intervenants en matière de sécurité et les représentants des utilisateurs au sujet des politiques et des lignes directrices de sécurité en matière d'AI; et

g) veiller à ce que les sous-divisions spécialisées du comité de sécurité disposent, de par leur composition, des compétences requises en matière d'AI.

Autorité Tempest

44. L'autorité Tempest (AT) est chargée de veiller à la conformité des SIC aux stratégies et lignes directrices Tempest. Elle approuve les contre-mesures Tempest pour les installations et les produits destinés à protéger des ICUE jusqu'à un certain niveau de classification dans leur environnement opérationnel.

Autorité d'agrément cryptographique

45. L'autorité d'agrément cryptographique (AAC) est chargée de veiller à ce que les produits cryptographiques soient conformes aux politiques respectives des différents États membres et du Conseil en matière cryptographique. Elle agrée les produits cryptographiques pour la protection d'ICUE jusqu'à un certain niveau de classification dans leur environnement opérationnel. S'agissant des États membres, l'AAC est en outre chargée de l'évaluation des produits cryptographiques.

Autorité de distribution cryptographique

46. L'autorité de distribution cryptographique (ADC) s'acquitte des tâches suivantes:

a) gérer le matériel cryptographique de l'UE et en rendre compte;

b) veiller à ce que les procédures et les circuits appropriés soient mis en place pour rendre compte de tout le matériel cryptographique de l'UE et en assurer la manutention, le stockage et la distribution en toute sécurité; et

c) assurer le transfert et la reprise du matériel cryptographique de l'UE auprès des personnes ou des services utilisateurs.

Autorité d'homologation de sécurité

47. L'autorité d'homologation de sécurité de chaque système s'acquitte des tâches suivantes:

a) veiller à ce que les SIC soient conformes aux politiques et lignes directrices de sécurité pertinentes, délivrer une déclaration d'homologation pour les SIC en vue du traitement des ICUE jusqu'à un certain niveau de classification dans leur environnement opérationnel et indiquant les conditions et modalités de l'homologation ainsi que les critères dont l'existence justifie une nouvelle homologation;

b) mettre en place un processus d'homologation de sécurité conforme aux politiques pertinentes et indiquant clairement les conditions d'homologation que doivent remplir les SIC relevant de sa responsabilité;

c) définir une stratégie d'homologation de sécurité qui indique le niveau de précision du processus d'homologation en fonction du niveau d'assurance requis;

d) étudier et approuver les documents se rapportant à la sécurité, y compris en ce qui concerne la gestion des risques et les énoncés des risques résiduels, les énoncés des impératifs de sécurité propres à un système (ci-après dénommés «SSRS»), les documents concernant la vérification de la mise en œuvre des mesures de sécurité et les procédures d'exploitation de sécurité (ci-après dénommées «SecOP»), et veiller à ce qu'ils soient conformes aux politiques et aux règles du Conseil en matière de sécurité;

e) vérifier la mise en œuvre des mesures de sécurité en rapport avec les SIC en effectuant elle-même ou en finançant des évaluations, des inspections ou des réexamens en la matière;

f) définir les exigences en matière de sécurité (par exemple les niveaux d'habilitation de sécurité du personnel) applicables aux postes sensibles dans le cadre d'un SIC;

g) accepter la sélection des produits cryptographiques et Tempest ayant fait l'objet d'une approbation qui sont utilisés pour assurer la sécurité d'un SIC;

h) approuver, le cas échéant dans le cadre d'une approbation conjointe, l'interconnexion d'un SIC à d'autres SIC; et

i) mener des consultations avec le fournisseur du système, les intervenants en matière de sécurité et les représentants des utilisateurs au sujet de la gestion des risques de sécurité, et notamment du risque résiduel, et des conditions et modalités de la déclaration d'homologation.

48. L'AHS du SGC est chargée de l'homologation de tous les SIC exploités dans le cadre de la compétence du SGC.

49. L'AHS compétente d'un État membre est chargée de l'homologation des SIC et des éléments des SIC exploités dans le cadre de la compétence d'un État membre.

50. Un comité conjoint d'homologation de sécurité (CHS) est chargé de l'homologation des SIC qui sont du ressort aussi bien de l'AHS du SGC que des AHS des États membres. Ce comité est composé d'un représentant de l'AHS de chaque État membre, un représentant de l'AHS de la Commission assistant à ses réunions. Les autres entités disposant de nœuds de connexion avec un SIC sont invitées à assister aux réunions lorsque celles-ci portent sur le système considéré.

Le CHS est présidé par un représentant de l'AHS du SGC. Il statue par consensus entre les représentants des AHS des institutions, des États membres et des autres entités disposant de nœuds de connexion avec le SIC considéré. Le CHS rend compte à intervalles réguliers de ses activités au comité de sécurité et notifie à celui-ci toute déclaration d'homologation.

Autorité opérationnelle chargée de l'assurance de l'information

51. L'autorité opérationnelle chargée de l'AI pour chaque système s'acquitte des tâches suivantes:

a) élaborer des documents relatifs à la sécurité de chaque système conformes à la politique et aux lignes directrices en matière de sécurité, et notamment les SSRS, y compris en ce qui concerne le risque résiduel, les SecOP et le volet cryptographique du processus d'homologation des SIC;

b) participer à la sélection et à la mise à l'essai des mesures, dispositifs et logiciels de sécurité technique propres à un système, superviser leur mise en œuvre et s'assurer qu'ils sont installés, configurés et entretenus de manière sûre conformément aux documents de sécurité pertinents;

c) participer à la sélection des mesures et des dispositifs de sécurité Tempest lorsque les SSRS le prévoient, et veiller à ce qu'ils soient installés et entretenus de manière sûre en coopération avec l'AT;

d) assurer le suivi de la mise en œuvre et de l'application des SecOP et, s'il y a lieu, déléguer les responsabilités opérationnelles de sécurité au détenteur du système;

e) gérer et utiliser les produits cryptographiques, assurer la protection des éléments chiffrés et contrôlés et, au besoin, assurer la production de variables cryptographiques;

f) procéder au réexamen et à des analyses de sécurité et à des tests, notamment afin d'établir les rapports nécessaires sur les risques encourus, comme l'exige l'AHS;

g) dispenser une formation sur l'AI propre à chaque SIC;

h) mettre en œuvre et gérer des mesures de sécurité propres à chaque SIC.

ANNEXE V

SÉCURITÉ INDUSTRIELLE

I. INTRODUCTION

1. La présente annexe énonce les modalités d'application de l'article 11. Elle prévoit des mesures de sécurité générales applicables aux entités industrielles ou autres dans le cadre de négociations précontractuelles et tout au long du cycle de vie des contrats classifiés attribués par le SGC.

2. Le Conseil approuve une politique de sécurité industrielle indiquant en particulier les modalités précises en ce qui concerne les HSE, les annexes de sécurité (AS), les visites, la transmission et le transport des ICUE.

II. ASPECTS LIÉS À LA SÉCURITÉ DANS UN CONTRAT CLASSIFIÉ

Guide de la classification de sécurité (GCS)

3. Avant de lancer un appel d'offres en vue de l'attribution d'un contrat classifié ou d'attribuer un tel contrat, le SGC, en sa qualité d'autorité contractante, détermine la classification de sécurité de toute information devant être fournie aux soumissionnaires et aux contractants, ainsi que la classification de sécurité de toute information devant être créée pour le contractant. Dans cette perspective, le SGC élabore un guide de la classification de sécurité (GCS), qui sera utilisé aux fins de l'exécution du contrat.

4. Les principes ci-après sont appliqués pour déterminer le niveau de classification de sécurité des différents éléments d'un contrat classifié:

   a) dans le cadre de l'élaboration d'un GCS, le SGC 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;

   b) 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

   c) le cas échéant, le SGC se met en rapport avec les ANS/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.

Annexe de sécurité (AS)

5. Les impératifs de sécurité propres à un contrat sont exposés dans une AS. Le cas échéant, l'AS contient le GCS et fait partie intégrante du contrat ou du contrat de sous-traitance classifié.

6. L'AS contient les dispositions imposant au contractant et/ou au sous-traitant de respecter les normes minimales énoncées dans la présente décision. Le non-respect de ces normes minimales peut constituer un motif suffisant de résiliation du contrat.

Instructions de sécurité relatives à un programme/un projet (ISP)

7. En fonction de la portée des programmes ou des projets impliquant l'accès à des ICUE ou leur traitement ou stockage, l'autorité contractante chargée de gérer le projet ou le programme considéré peut élaborer des instructions de sécurité relatives à un programme/un projet (ISP). Les ISP doivent être approuvées par les ANS/ASD ou toute autre autorité de sécurité compétente des États membres associées au programme/projet et peuvent contenir d'autres exigences en matière de sécurité.

III. HABILITATION DE SÉCURITÉ D'ÉTABLISSEMENT (HSE)

8. Une HSE est délivrée par l'ANS/ASD ou toute autre autorité de sécurité compétente d'un État membre afin d'indiquer, conformément aux dispositions législatives et réglementaires nationales, que l'entité industrielle ou autre 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). La HSE est communiquée au SGC, en sa qualité d'autorité contractante, avant que le contractant ou le sous-traitant ou un contractant ou un sous-traitant potentiel ne se voie communiquer des ICUE ou accorder un accès aux ICUE.

9. Lorsqu'elle délivre une HSE, l'ANS/ASD compétente veille au minimum à:

   a) évaluer l'intégrité de l'entité industrielle ou autre;

   b) évaluer les éléments relatifs à la propriété et au contrôle de l'entité ainsi que toute possibilité d'influence indue pouvant être considérés comme constituant un risque de sécurité;

c) vérifier que l'entité industrielle ou toute autre entité a mis en place un système de sécurité dans ses établissements, qui comporte toutes les mesures de sécurité appropriées pour protéger des informations ou du matériel classifiés CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET conformément aux prescriptions de la présente décision;

d) vérifier que le statut en matière de sécurité des directeurs, des propriétaires et des employés qui doivent avoir accès à du matériel classifié CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET a été établi conformément aux prescriptions de la présente décision;

e) vérifier que l'entité industrielle ou toute autre entité a nommé un officier de sécurité d'établissement qui est responsable vis-à-vis de sa direction du respect des obligations en matière de sécurité au sein de l'entité.

10. S'il y a lieu, le SGC, en sa qualité d'autorité contractante, avertit l'ANS/ASD ou toute autre autorité de sécurité compétente qu'une HSE est nécessaire dans la phase précontractuelle ou pour l'exécution du contrat. Une HSE ou une HSP est requise dans la phase précontractuelle lorsque des ICUE classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET doivent être fournies dans la phase de soumission des offres.

11. L'autorité contractante n'attribue pas de contrat classifié au soumissionnaire sélectionné tant que l'ANS/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.

12. L'ANS/ASD ou toute autre autorité de sécurité compétente ayant délivré une HSE notifie au SGC, en sa qualité d'autorité contractante, les modifications éventuellement apportées à ladite HSE. Dans le cadre d'un contrat de sous-traitance, l'ANS/ASD ou toute autre autorité de sécurité compétente en est informée.

13. Le retrait d'une HSE par l'ANS/ASD concernée ou toute autre autorité de sécurité compétente constitue pour le SGC, en sa qualité d'autorité contractante, un motif suffisant pour résilier un contrat classifié ou exclure un soumissionnaire de la procédure d'appel d'offres.

IV. CONTRATS ET CONTRATS DE SOUS-TRAITANCE CLASSIFIÉS

14. Lorsque des ICUE sont communiquées à un soumissionnaire durant la phase précontractuelle, l'appel d'offres contient une disposition prévoyant que le soumissionnaire qui ne présente pas d'offre ou qui n'est pas sélectionné sera tenu de restituer tous les documents classifiés dans un délai spécifié.

15. Une fois qu'un contrat ou un contrat de sous-traitance classifié a été attribué, le SGC, en sa qualité d'autorité contractante, notifie les dispositions en matière de sécurité que comporte le contrat classifié à l'ANS/ASD ou à toute autre autorité de sécurité compétente dont relève le contractant ou le sous-traitant.

16. Lorsqu'il est mis fin à un tel contrat, le SGC, en sa qualité d'autorité contractante, (et/ou l'ANS/ASD ou toute autre autorité de sécurité compétente, selon qu'il conviendra, dans le cas d'un contrat de sous-traitance) avertit immédiatement l'ANS/ASD ou toute autre autorité de sécurité compétente de l'État membre dans lequel le contractant ou le sous-traitant est immatriculé.

17. En principe, le contractant ou le sous-traitant est tenu de restituer à l'autorité contractante les ICUE en sa possession, dès que le contrat ou le contrat de sous-traitance classifié arrive à expiration.

18. Des dispositions spéciales concernant l'élimination d'ICUE durant l'exécution du contrat ou à son expiration figurent dans l'AS.

19. Lorsque le contractant ou le sous-traitant est autorisé à conserver des ICUE après l'expiration d'un contrat, les normes minimales figurant dans la présente demeurent d'application et la confidentialité des ICUE est protégée par le contractant ou le sous-traitant.

20. Les conditions dans lesquelles le contractant peut sous-traiter des activités sont définies dans l'appel d'offres et le contrat.

21. Un contractant doit obtenir l'autorisation du SGC, en sa qualité d'autorité contractante, avant de pouvoir sous-traiter des éléments d'un contrat classifié. Aucun contrat de sous-traitance ne peut être attribué à des entités industrielles ou autres immatriculées dans un État non membre de l'Union européenne n'ayant pas conclu avec l'UE un accord sur la sécurité des informations.

22. 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.

23. En ce qui concerne les ICUE créées ou traitées par le contractant ou le sous-traitant, les droits qui incombent à l'autorité d'origine sont exercés par l'autorité contractante.

V. VISITES LIÉES À DES CONTRATS CLASSIFIÉS

24. Lorsque le SGC, les contractants ou les sous-traitants 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, les visites sont organisées en liaison avec les ANS/ASD ou toute autre autorité de sécurité compétente concernée. Toutefois, dans le cadre de projets spécifiques, les ANS/ASD peuvent également convenir d'une procédure selon laquelle ces visites peuvent être organisées directement.

25. Tous les visiteurs sont en possession d'une HSP adéquate et jouissent d'un accès aux ICUE liées au contrat attribué par le SGC sur la base du principe du besoin d'en connaître.

26. Les visiteurs se voient uniquement accorder l'accès aux ICUE liées à l'objectif de la visite.

VI. TRANSMISSION ET TRANSPORT DES ICUE

27. En ce qui concerne la transmission des ICUE par voie électronique, les dispositions pertinentes de l'article 10 et de l'annexe IV s'appliquent.

28. En ce qui concerne le transport d'ICUE, les dispositions pertinentes de l'annexe III s'appliquent, conformément aux dispositions législatives et réglementaires nationales.

29. 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) une HSE du niveau approprié est obtenue pour les sociétés assurant le transport. En pareil cas, le personnel manipulant l'envoi fait l'objet d'une habilitation de sécurité conformément à l'annexe I;

d) 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 les ANS/ASD ou toute autre autorité de sécurité compétente concernées;

e) les trajets sont directs dans la mesure du possible, et aussi rapides que les circonstances le permettent;

f) 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/ASD ou toute autre autorité de sécurité compétente des États de l'expéditeur et du destinataire.

VII. TRANSFERT D'ICUE AUX CONTRACTANTS ÉTABLIS DANS DES PAYS TIERS

30. Les ICUE sont transférées aux contractants et sous-traitants établis dans des pays tiers conformément aux mesures de sécurité convenues entre le SGC, en sa qualité d'autorité contractante, et l'ANS/ASD du pays tiers concerné dans lequel le contractant est immatriculé.

VIII. TRAITEMENT ET CONSERVATION D'INFORMATIONS CLASSIFIÉES RESTREINT UE/EU RESTRICTED

31. En liaison, s'il y a lieu, avec l'ANS/ASD de l'État membre, le SGC, en sa qualité d'autorité contractante, est habilité à effectuer des visites dans les établissements des contractants/sous-traitants, en vertu de dispositions contractuelles, afin de vérifier que les mesures de sécurité adaptées pour la protection des ICUE de niveau RESTREINT UE/EU RESTRICTED ont été mises en place, comme l'exige le contrat.

32. Dans la mesure où cela est nécessaire en vertu des dispositions légales et réglementaires nationales, les ANS/ASD, ou toute autre autorité de sécurité compétente, doivent être informées par le SGC, en sa qualité d'autorité contractante, des contrats ou des contrats de sous-traitance contenant des informations classifiées RESTREINT UE/EU RESTRICTED.

33. Les contractants ou sous-traitants et leur personnel ne sont pas tenus d'être en possession d'une HSE ou d'une HSP pour les contrats attribués par le SGC et comportant des informations classifiées RESTREINT UE/EU RESTRICTED.

34. Le SGC, en sa qualité d'autorité contractante, examine les réponses aux appels d'offres portant sur des contrats nécessitant l'accès à des informations classifiées RESTREINT UE/EU RESTRICTED, nonobstant les exigences en matière d'HSE ou d'HSP pouvant être prévues par les dispositions législatives et réglementaires nationales.

35. Les conditions régissant la sous-traitance d'activités par un contractant sont conformes au paragraphe 21.

36. Lorsqu'un contrat prévoit le traitement d'informations classifiées RESTREINT UE/EU RESTRICTED dans un SIC exploité par un contractant, le SGC, en sa qualité d'autorité contractante, veille à ce que les exigences techniques et administratives à remplir concernant l'homologation du SIC soient précisées dans le contrat ou tout contrat de sous-traitance; 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 contractante et l'ANS/ASD compétente.

ANNEXE VI

ÉCHANGE D'INFORMATIONS CLASSIFIÉES AVEC DES PAYS TIERS ET DES ORGANISATIONS INTERNATIONALES

I. INTRODUCTION

1. La présente annexe énonce les modalités d'application de l'article 12.

II. CADRES RÉGISSANT L'ÉCHANGE D'INFORMATIONS CLASSIFIÉES

2. Lorsque le Conseil décide qu'il existe un besoin durable d'échanger des informations classifiées,

— un accord sur la sécurité des informations est conclu, ou

— un arrangement administratif est conclu,

conformément à l'article 12, paragraphe 2, et aux sections III et IV et en vertu d'une recommandation du comité de sécurité.

3. Lorsque des ICUE créées aux fins d'une opération PSDC doivent être communiquées à des pays tiers ou à des organisations internationales participant à cette opération, et lorsqu'aucun des cadres prévus au paragraphe 2 n'existe, l'échange d'ICUE avec le pays tiers ou l'organisation internationale contributeur est régi, conformément à la section V ci-dessous, par:

— un accord-cadre de participation,

— un accord de participation ad hoc, ou

— à défaut d'un des accords susmentionnés, un arrangement administratif ad hoc.

4. À défaut d'un des cadres mentionnés aux paragraphes 2 et 3, et lorsque décision est prise de communiquer des ICUE à un pays tiers ou à une organisation internationale sur une base exceptionnelle ad hoc dans le respect des dispositions prévues dans la section VI, il est demandé au pays tiers ou à l'organisation internationale concerné(e) de donner par écrit des assurances garantissant que toute ICUE qui lui est communiquée bénéficie d'une protection conforme aux principes de base et aux normes minimales énoncés dans la présente décision.

III. ACCORDS SUR LA SÉCURITÉ DES INFORMATIONS

5. Les accords sur la sécurité des informations fixent les principes de base et les normes minimales régissant l'échange d'informations classifiées entre l'UE et un pays tiers ou une organisation internationale.

6. Les accords sur la sécurité des informations prévoient des modalités techniques d'application qui doivent être arrêtées d'un commun accord entre le bureau de sécurité du SGC, la DSCE et l'autorité de sécurité compétente du pays 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 du pays tiers ou de l'organisation internationale concerné(e). Elles sont approuvées par le comité de sécurité.

7. 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.

8. Les accords sur la sécurité des informations prévoient que, préalablement à l'échange d'informations classifiées au titre de l'accord, le bureau de sécurité du SGC et la DSCE doivent s'accorder à estimer que la partie destinataire est apte à protéger et sauvegarder de manière appropriée les informations qui lui sont transmises.

9. Lorsque le Conseil conclut un accord de sécurité des informations avec un tiers, un bureau d'ordre est désigné au sein de chaque partie comme principal point d'entrée et de sortie des échanges d'informations classifiées.

10. Afin d'évaluer l'efficacité des règlements, structures et procédures de sécurité en vigueur dans le pays tiers ou l'organisation internationale concerné(e), des visites d'évaluation sont menées par le bureau de sécurité du SGC en collaboration avec la DSCE, d'un commun accord avec le pays tiers ou l'organisation internationale concerné(e). Ces visites d'évaluation sont menées conformément aux dispositions pertinentes de l'annexe III et 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 le pays 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.

11. L'équipe chargée de mener la visite d'évaluation au nom de l'UE détermine si les règles et procédures de sécurité mises en œuvre dans le pays tiers ou l'organisation internationale concerné(e) sont adaptées pour garantir la protection des ICUE au niveau requis.

12. Les conclusions de ces visites sont consignées dans un rapport, sur la base duquel le comité de sécurité fixe le niveau maximal de classification des ICUE qui peuvent être communiquées sur support papier et le cas échéant par voie électronique avec la tierce partie concernée, ainsi que toute condition particulière régissant l'échange d'informations avec celle-ci.

13. Tout est mis en œuvre pour qu'une visite complète d'évaluation de la sécurité soit menée dans le pays tiers ou l'organisation internationale concerné(e) avant l'approbation par le comité de sécurité des modalités d'application, afin d'établir la nature et l'efficacité du système de sécurité en place. Toutefois, lorsque cela n'est pas possible, le bureau de sécurité du SGC remet au comité de sécurité un rapport le plus complet qui soit, fondé sur les informations dont il dispose, qui contient des informations sur le règlement de sécurité applicable et le mode d'organisation de la sécurité dans le pays tiers ou l'organisation internationale concerné(e).

14. Le comité de sécurité peut décider que, dans l'attente de l'examen des conclusions d'une visite d'évaluation, aucune ICUE ne peut être communiquée, ou que de telles informations ne peuvent être communiquées que jusqu'à un niveau déterminé de classification, au pays tiers ou à l'organisation internationale concerné(e); il peut également assortir cette communication d'autres conditions particulières. Le bureau de sécurité du SGC en informe le pays tiers ou l'organisation internationale concerné(e).

15. D'un commun accord avec le pays tiers ou l'organisation internationale concerné(e), le bureau de sécurité du SGC effectue, à intervalles réguliers, des visites de suivi de l'évaluation, afin de s'assurer que les dispositifs en place continuent de satisfaire aux normes minimales qui ont été arrêtées.

16. Lorsque l'accord sur la sécurité des informations est en vigueur et que des informations classifiées sont échangées avec le pays tiers ou l'organisation internationale concerné(e), le comité de sécurité peut décider de modifier le niveau maximal de classification des ICUE pouvant être échangées au format papier ou par voie électronique, en particulier à la lumière de toute visite de suivi de l'évaluation.

IV. ARRANGEMENTS ADMINISTRATIFS

17. Lorsqu'il existe un besoin durable d'échanger, avec un pays 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 le comité de sécurité a établi 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, le secrétaire général peut, sous réserve de l'approbation du Conseil, conclure un arrangement administratif avec les autorités compétentes du pays tiers ou de l'organisation internationale concerné(e).

18. Si, pour des raisons opérationnelles urgentes, un cadre doit être mis en place rapidement pour échanger des informations classifiées, le Conseil peut décider exceptionnellement qu'un arrangement administratif soit conclu pour échanger des informations dont le niveau de classification est supérieur à RESTREINT UE/EU RESTRICTED.

19. Les arrangements administratifs prennent, en règle générale, la forme d'un échange de lettres.

20. Une visite d'évaluation telle que visée au paragraphe 10 est réalisée, et le rapport y relatif est transmis au comité de sécurité, qui doit le juger satisfaisant, avant que des ICUE soient effectivement transmises au pays tiers ou à l'organisation internationale concerné(e). Cependant, si des raisons exceptionnelles, portées à la connaissance du Conseil, 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.

21. Les ICUE ne font l'objet d'aucun échange par voie électronique, sauf disposition expresse de l'arrangement administratif.

V. ÉCHANGE D'INFORMATIONS CLASSIFIÉES DANS LE CADRE D'OPÉRATIONS PSDC

22. Les accords-cadres de participation régissent la participation des pays tiers ou des organisations internationales aux opérations PSDC. Ces accords contiennent des dispositions relatives à la communication des ICUE créées aux fins des opérations PSDC aux pays tiers ou aux organisations internationales contributeurs. Le niveau maximal de classification des ICUE qui peuvent être échangées est RESTREINT UE/EU RESTRICTED pour les opérations PSDC civiles et CONFIDENTIEL UE/EU CONFIDENTIAL pour les opérations PSDC militaires, sauf disposition contraire prévue dans la décision établissant chaque opération PSDC.

23. Les accords de participation ad hoc conclus pour une opération PSDC particulière comprennent des dispositions relatives à la communication des ICUE créées aux fins de ladite opération au pays tiers ou à l'organisation internationale contributeurs. Le niveau maximal de classification des ICUE qui peuvent être échangées est RESTREINT UE/EU RESTRICTED pour les opérations PSDC civiles et CONFIDENTIEL UE/EU CONFIDENTIAL pour les opérations PSDC militaires, sauf disposition contraire prévue dans la décision établissant chaque opération PSDC.

24. Les arrangements administratifs ad hoc concernant la participation d'un pays tiers ou d'une organisation internationale à une opération PSDC particulière peuvent porter, entre autres, sur la communication des ICUE créées aux fins de l'opération à ce pays tiers ou à cette organisation internationale. Ces arrangements administratifs ad hoc sont conclus conformément aux procédures prévues aux paragraphes 17 et 18 de la section IV. Le niveau maximal de classification des ICUE qui peuvent être échangées est RESTREINT UE/EU RESTRICTED pour les opérations PSDC civiles et CONFIDENTIEL UE/EU CONFIDENTIAL pour les opérations PSDC militaires, sauf disposition contraire prévue dans la décision établissant chaque opération PSDC.

25. Aucune modalité d'application ou visite d'évaluation n'est requise préalablement à la mise en œuvre des dispositions relatives à la communication d'ICUE au titre des paragraphes 22, 23 et 24.

26. Si l'État hôte sur le territoire duquel une opération PSDC est menée n'a pas conclu d'accord sur la sécurité des informations ou d'arrangement administratif avec l'UE pour échanger des informations classifiées, un arrangement administratif ad hoc peut être mis en place en cas de besoin opérationnel spécifique et immédiat. Cette possibilité est prévue dans la décision établissant l'opération PSDC. Seules peuvent être communiquées dans de telles circonstances les ICUE créées aux fins de l'opération PSDC dont le niveau de classification n'est pas supérieur à RESTREINT UE/EU RESTRICTED. Dans le cadre d'un tel arrangement administratif ad hoc, l'État hôte s'engage à protéger les ICUE conformément à des normes minimales qui ne sont pas moins strictes que celles prévues dans la présente décision.

27. Les dispositions relatives aux informations classifiées devant figurer dans les accords-cadres de participation, les accords de participation ad hoc et les arrangements administratifs ad hoc visés aux paragraphes 22 à 24 prévoient que le pays tiers ou l'organisation internationale concerné(e) veille à ce que son personnel détaché dans le cadre de toute opération protège les ICUE conformément au règlement de sécurité du Conseil, ainsi qu'aux autres instructions formulées par les autorités compétentes, y compris la chaîne de commandement de l'opération.

28. Si un accord sur la sécurité des informations est conclu ultérieurement entre l'UE et un pays tiers ou une organisation internationale contributeur, l'accord sur la sécurité des informations se substitue à tout accord-cadre de participation, accord de participation ad hoc ou arrangement administratif ad hoc pour ce qui concerne l'échange et le traitement des ICUE.

29. Aucun échange d'ICUE par voie électronique n'est autorisé au titre d'un accord-cadre de participation, d'un accord de participation ad hoc ou d'un arrangement administratif ad hoc conclu avec un pays tiers ou une organisation internationale, sauf disposition expresse de l'accord ou l'arrangement en question.

30. Les ICUE créées aux fins d'une opération PSDC peuvent être divulguées au personnel détaché par des pays tiers ou des organisations internationales dans le cadre de cette opération, conformément aux dispositions des paragraphes 22 à 29. Lorsque l'accès aux ICUE est autorisé dans les locaux ou via le SIC d'une opération PSDC, il convient d'appliquer des mesures (y compris l'enregistrement des ICUE divulguées) permettant d'atténuer le risque de perte ou de compromission. Ces mesures sont définies dans les documents de planification ou de mission pertinents.

VI. COMMUNICATION AD HOC EXCEPTIONNELLE D'ICUE

31. Si aucun cadre n'existe conformément aux sections III à V, et si le Conseil ou l'une de ses instances préparatoires décide qu'il est nécessaire, à titre exceptionnel, de communiquer des ICUE à un pays tiers ou à une organisation internationale, le SGC:

a) vérifie, dans la mesure du possible, auprès des autorités de sécurité du pays 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;

b) invite le comité de sécurité à formuler, sur la base des informations disponibles, une recommandation concernant la confiance qui peut être accordée au règlement, aux structures et aux procédures de sécurité en vigueur dans le pays tiers ou l'organisation internationale auquel les ICUE doivent être communiquées.

32. Si le comité de sécurité émet une recommandation favorable à la communication des ICUE, la question est soumise au Comité des représentants permanents (Coreper), qui statue sur leur communication.

33. Si le comité de sécurité émet une recommandation défavorable quant à la communication des ICUE:

a) pour les questions relatives à la PESC/PSDC, le comité politique et de sécurité débat de la question et formule une recommandation en vue d'une décision du Coreper;

b) pour toutes les autres questions, le Coreper examine la question et prend une décision.

34. Lorsque cela est jugé nécessaire, et sous réserve du consentement préalable écrit de l'autorité d'origine, le Coreper peut décider que les informations classifiées ne peuvent être communiquées qu'en partie ou qu'après avoir été déclassées ou déclassifiées, ou que les informations à communiquer seront préparées sans indiquer de référence à l'origine ou au niveau initial de classification de l'UE.

35. Lorsqu'une décision de communiquer des ICUE a été prise, le SGC transmet le document concerné, qui porte un marquage relatif à la communicabilité indiquant le pays tiers ou l'organisation internationale auquel ce document a été communiqué. 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.

VII. AUTORISATION DE COMMUNIQUER DES ICUE À DES PAYS TIERS OU À DES ORGANISATIONS INTERNATIONALES

36. Lorsqu'il existe, conformément au paragraphe 2, un cadre pour l'échange d'informations classifiées avec un pays tiers ou une organisation internationale, le Conseil prend la décision d'autoriser le secrétaire général à communiquer des ICUE au pays tiers ou à l'organisation internationale concerné(e), dans le respect du principe du consentement de l'autorité d'origine.

37. Lorsqu'il existe, conformément au paragraphe 3, un cadre pour l'échange d'informations classifiées avec un pays tiers ou une organisation internationale, le secrétaire général est autorisé à communiquer des ICUE, conformément à la décision établissant l'opération PSDC et au principe du consentement de l'autorité d'origine.

38. Le secrétaire général peut déléguer ce pouvoir à de hauts fonctionnaires du SGC ou à d'autres personnes placées sous son autorité.

Appendices

Appendice A

DÉFINITIONS

Aux fins de la présente décision, on entend par:

«annexe de sécurité (AS)», 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;

«assurance de l'information», voir l'article 10, paragraphe 1;

«autorité d'origine», l'institution, l'agence ou l'organe de l'UE, l'État membre, le pays 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'UE;

«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;

«certificat d'habilitation de sécurité du personnel (CHSP)», un certificat délivré par une autorité compétente attestant qu'une personne a obtenu une habilitation de sécurité et détient une HSP nationale ou de l'UE valable, et 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'HSP correspondante et la date d'expiration du certificat;

«contractant», une personne physique ou morale dotée de la capacité juridique de conclure des contrats;

«contrat classifié», un contrat conclu par le SGC avec un contractant en vue de la fourniture de biens, de la réalisation de travaux ou de la prestation de services, dont l'exécution requiert ou implique l'accès à des ICUE ou la création de telles informations;

«contrat de sous-traitance classifié», un contrat conclu par un contractant du SGC avec un autre contractant (c'est-à-dire le sous-traitant) en vue de la fourniture de biens, de la réalisation de travaux ou de la prestation de services, dont l'exécution requiert ou implique l'accès à des ICUE ou la création de telles informations;

«cycle de vie d'un SIC», la durée totale d'existence d'un SIC, laquelle comprend le lancement, la conception, la planification, l'analyse des besoins, l'élaboration, le développement, la mise à l'essai, la mise en œuvre, l'exploitation, la maintenance et le démantèlement;

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

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

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

«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;

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

«enquête de sécurité», 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 HSP nationale ou de l'UE lui permettant d'avoir accès à des ICUE jusqu'à un niveau déterminé (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur);

«enregistrement», voir annexe III, paragraphe 18;

«entité industrielle ou autre», une entité s'occupant de la fourniture de biens, de la réalisation de travaux ou de la prestation de services; il peut s'agir d'une entité industrielle, commerciale ou scientifique, ou d'une entité de service, de recherche, d'enseignement ou de développement ou d'une personne exerçant une activité indépendante;

«gestion des informations classifiées», voir article 9, paragraphe 1;

«guide de la classification de sécurité (GCS)», un document qui décrit les éléments d'un programme ou d'un contrat 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 ou du contrat et les éléments d'information peuvent être reclassifiés ou déclassés; lorsqu'il existe, le GCS fait partie de l'AS;

«habilitation de sécurité d'établissement (HSE)», une décision administrative prise par une ANS ou une ASD 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 et selon laquelle le personnel de l'établissement qui doit accéder à des ICUE possède une habilitation de sécurité appropriée et a été informé des conditions de sécurité requises pour accéder à des ICUE et les protéger;

«habilitation de sécurité du personnel (HSP)», l'une des habilitations suivantes ou les deux:

— «habilitation de sécurité du personnel de l'UE (HSP de l'UE) donnant accès aux ICUE», une autorisation émanant de l'autorité investie du pouvoir de nomination du SGC conformément à la présente décision 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, 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; la personne ainsi décrite est «habilitée»,

— «habilitation nationale de sécurité du personnel (HSP nationale) donnant accès aux ICUE», 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, 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; la personne ainsi décrite est «habilitée»;

«homologation», la procédure conduisant à une déclaration formelle de l'autorité d'homologation de sécurité (AHS) indiquant qu'un système est agréé pour fonctionner à un niveau de classification déterminé, selon un mode d'exploitation de sécurité spécifique dans son environnement opérationnel et à un niveau de risque acceptable, pour autant qu'un ensemble approuvé de mesures de sécurité ait été mis en place sur le plan technique et physique, ainsi qu'au niveau de l'organisation et des procédures;

«informations classifiées de l'UE» (ICUE), voir article 2, paragraphe 1;

«instructions de sécurité relatives à un programme/un projet (ISP)», 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;

«interconnexion», voir annexe IV, paragraphe 31;

«matériel», tout document ou élément de machine ou d'équipement, déjà fabriqué ou en cours de fabrication;

«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;

«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;

«mesures de sécurité concernant le personnel», voir article 7, paragraphe 1;

«mode d'exploitation de sécurité», la définition des conditions d'exploitation d'un SIC, compte tenu de la classification des informations traitées et des niveaux d'habilitation, des autorisations formelles d'accès et du besoin d'en connaître de ses utilisateurs. Il existe quatre modes d'exploitation pour le traitement ou la transmission d'informations classifiées: le mode exclusif, le mode dominant, le mode par cloisonnement et le mode multiniveau; on entend par:

— «mode exclusif», un mode d'exploitation selon lequel toutes les personnes ayant accès au SIC sont habilitées au plus haut niveau de classification des informations traitées au sein du SIC, et ont un besoin commun d'en connaître pour toutes les informations traitées au sein du SIC,

— «mode dominant», un mode d'exploitation dans lequel toutes les personnes ayant accès au SIC sont habilitées au plus haut niveau de classification des informations au sein du SIC, mais n'ont pas toutes un besoin commun d'en connaître pour les informations traitées au sein du SIC; une personne seule peut autoriser l'accès à l'information,

— «mode par cloisonnement», un mode d'exploitation dans lequel toutes les personnes ayant accès au SIC sont habilitées au plus haut niveau de classification des informations traitées au sein du SIC, mais ne bénéficient pas toutes d'une autorisation formelle d'accéder à toutes les informations traitées au sein du SIC; une telle autorisation formelle suppose que le contrôle d'accès fasse l'objet d'une gestion centrale formelle par opposition au pouvoir détenu par une personne seule d'accorder l'accès,

— «mode multiniveau», un mode d'exploitation dans lequel les personnes ayant accès au SIC ne sont pas toutes habilitées au plus haut niveau de classification des informations traitées au sein du SIC, et n'ont pas toutes un besoin commun d'en connaître pour les informations traitées au sein du SIC;

«opération PSDC», une opération militaire ou civile de gestion de crise mise en place en vertu du titre V, chapitre 2, du traité sur l'Union européenne;

«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;

«ressource», tout ce qui présente de l'utilité pour une organisation, ses activités et la continuité de celles-ci, y compris les ressources en matière d'information dont l'organisation a besoin pour s'acquitter de sa mission;

«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.

— L'«acceptation des risques» consiste à décider d'accepter qu'un risque résiduel subsiste au terme du traitement des risques.

— 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.

— 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.

— 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;

«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;

«sécurité industrielle», voir article 11, paragraphe 1;

«sécurité physique», voir article 8, paragraphe 1;

«système d'information et de communication (SIC)», voir article 10, paragraphe 2;

«Tempest», l'analyse, l'étude et le contrôle des émissions électromagnétiques susceptibles de compromettre les informations, ainsi que les mesures destinées à les éliminer;

«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 traitement, leur transport, leur déclassement, leur déclassification et leur destruction. En ce qui concerne les SIC, sont en outre compris leur collecte, leur affichage, leur transmission et leur stockage;

«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.

Appendice B

ÉQUIVALENCE DES CLASSIFICATIONS DE SÉCURITÉ

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU 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
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
Roumanie	Strict secret de importanţă deosebită	Strict secret	Secret	Secret de serviciu

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Slovénie	Strogo tajno	Tajno	Zaupno	Interno
Slovaquie	Přísně 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	Top Secret	Secret	Confidential	Restricted

([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.

Appendice C

LISTE DES AUTORITÉS NATIONALES DE SÉCURITÉ (ANS)

BELGIQUE
Autorité nationale de sécurité
SPF Affaires étrangères, commerce extérieur et coopération au développement
Rue des Petits Carmes 15
1000 Bruxelles

Téléphone secrétariat: +32 25014542
Télécopieur: +32 25014596
Adresse électronique: nvo-ans@diplobel.fed.be

DANEMARK
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg

Téléphone: +45 33148888
Télécopieur: +45 33430190

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

Téléphone: +45 33325566
Télécopieur: +45 33931320

BULGARIE
State Commission on Information Security
90 Cherkovna Str.
1505 Sofia

Téléphone: +359 29215911
Télécopieur: +359 29873750
Adresse électronique: dksi@government.bg
Site web: www.dksi.bg

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

Téléphone: +49 30186810
Télécopieur: +49 30186811441
Adresse électronique: oesIII3@bmi.bund.de

RÉPUBLIQUE TCHÈQUE
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56

Téléphone: +420 257283335
Télécopieur: +420 257283110
Adresse électronique: czech.nsa@nbu.cz
Site web: www.nbu.cz

ESTONIE
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn, Estonia

Téléphone: +372 7170113, +372 7170117
Télécopieur: +372 7170213
Adresse électronique: nsa@kmin.ee

IRLANDE
National Security Authority
Department of Foreign Affairs
76 - 78 Harcourt Street
Dublin 2 Irlande

Téléphone: +353 14780822
Télécopieur: +353 14082959

ESPAGNE
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid

Téléphone: +34 913725000
Télécopieur: +34 913725808
Adresse électronique: nsa-sp@areatec.com

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

Τηλέφωνα: +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
STG 1020 Holargos – Athens

Téléphone: +30 2106572045
+30 2106572009
Télécopieur: +30 2106536279
+30 2106577612

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
Télécopieur: +33 171758200

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

Téléphone: +39 0661174266
Télécopieur: +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
Télécopieur: +357 22302351
Adresse électronique: cynsa@mod.gov.cy

LUXEMBOURG
Autorité nationale de sécurité
Boîte postale 2379
1023 Luxembourg

Téléphone: +352 24782210 central,
+352 24782253 direct
Télécopieur: +352 24782243

HONGRIE
Nemzeti Biztonsági Felügyelet
(National Security Authority)
P.O. Box 2
1357 Budapest

Téléphone: +361 3469652
Télécopieur: +361 3469658
Adresse électronique: nbf@nbf.hu
Site web: www.nbf.hu

MALTE
Ministry of Justice and Home Affairs
P.O. Box 146
Valletta

Téléphone: +356 21249844
Télécopieur: +356 25695321

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

Téléphone: +371 67025418
Télécopieur: +371 67025454
Adresse électronique: ndi@sab.gov.lv

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

Téléphone: +370 52663201,
+370 52663202
Télécopieur: +370 52663200
Adresse électronique: nsa@vsd.lt

PAYS-BAS
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag

Téléphone: +31 703204400
Télécopieur: +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag

Téléphone: +31 703187060
Télécopieur: +31 703187522

AUTRICHE
Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien

Téléphone: +43 1531152594
Télécopieur: +43 1531152615
Adresse électronique: ISK@bka.gv.at

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

Téléphone: +48 225857360
Télécopieur: +48 225858509
Adresse électronique: nsa@abw.gov.pl
Site web: www.abw.gov.pl

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

Téléphone: +48 226841247
Télécopieur: +48 226841076
Adresse électronique: skw@skw.gov.pl

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
Télécopieur: +40 212240714
Adresse électronique: nsa.romania@nsa.ro
Site web: www.orniss.ro

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

Téléphone: +351 213031710
Télécopieur: +351 213031711

SLOVÉNIE
Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
SI-1000 Ljubljana

Téléphone: +386 14781390
Télécopieur: +386 14781399

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

Téléphone: +421 268692314
Télécopieur: +421 263824005
Site web: www.nbusr.sk

SUÈDE
Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
SE-103 39 Stockholm

Téléphone: +46 84051000
Télécopieur: +46 87231176
Adresse électronique: ud-nsa@foreign.ministry.se

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

Téléphone 1: +358 916056487
Téléphone 2: +358 916056484
Fax: +358 916055140
Adresse électronique: NSA@formin.fi

ROYAUME-UNI
UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS

Téléphone 1: +44 2072765649
Téléphone 2: +44 2072765497
Télécopieur: +44 2072765651
Adresse électronique: UK-NSA@cabinet-office.x.gsi.gov.uk

Appendice D

LISTE DES ABRÉVIATIONS

Acronyme	Signification
AAC	Autorité d'agrément cryptographique
AAI	Autorité chargée de l'assurance de l'information
ADC	Autorité de distribution cryptographique
AHS	Autorité d'homologation de sécurité
AI	Assurance de l'information
ANS	Autorité nationale de sécurité
AQUA	Autorité dûment qualifiée
AS	Annexes de sécurité
ASD	Autorité de sécurité désignée
AT	Autorité Tempest
CCTV	Closed Circuit Television – système de télévision en circuit fermé
CHS	Comité d'homologation de sécurité
CHSP	Certificat d'habilitation de sécurité du personnel
Coreper	Comité des représentants permanents
DSCE	Direction de la sécurité de la Commission européenne
GCS	Guide de la classification de sécurité
HSE	Habilitation de sécurité d'établissement
HSP	Habilitation de sécurité du personnel
ICUE	Informations classifiées de l'UE
ISP	Instructions de sécurité relatives à un programme/un projet
PESC	Politique étrangère et de sécurité commune
PSDC	Politique de sécurité et de défense commune
RSUE	Représentant spécial de l'UE
SDI	Système de détection des intrusions
SecOP	Security Operating Procedures – procédures d'exploitation de sécurité
SGC	Secrétariat général du Conseil
SIC	Systèmes d'information et de communication traitant des ICUE
SPB	Services de protection en bordure
SSRS	System-Specific Security Requirement Statement – énoncés des impératifs de sécurité propres à un système