ISSN 1977-0936

Journal officiel de l'Union européenne

C 190

Édition de langue française

Communications et informations

56e année

29 juin 2013

Numéro d'information | Sommaire | Page

IV *Informations*

INFORMATIONS PROVENANT DES INSTITUTIONS, ORGANES ET ORGANISMES DE L'UNION EUROPÉENNE

Service européen pour l'action extérieure

2013/C 190/01 Décision de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité du 19 avril 2013 relative aux règles de sécurité applicables au Service européen pour l'action extérieure 1

INFORMATIONS PROVENANT DES ÉTATS MEMBRES

2013/C 190/02 Renseignements communiqués par les États membres sur les aides d'État accordées conformément au règlement (CE) nº 800/2008 de la Commission déclarant certaines catégories d'aide compatibles avec le marché commun en application des articles 87 et 88 du traité (règlement général d'exemption par catégorie) [1] 47

2013/C 190/03 Renseignements communiqués par les États membres sur les aides d'État accordées conformément au règlement (CE) nº 1857/2006 de la Commission concernant l'application des articles 87 et 88 du traité aux aides d'État accordées aux petites et moyennes entreprises actives dans la production de produits agricoles et modifiant le règlement (CE) nº 70/2001 62

2013/C 190/04 Renseignements communiqués par les États membres sur les aides d'État accordées conformément au règlement (CE) nº 800/2008 de la Commission déclarant certaines catégories d'aide compatibles avec le marché commun en application des articles 87 et 88 du traité (règlement général d'exemption par catégorie) [1] 65

FR

Prix: 4 EUR

[1] Texte présentant de l'intérêt pour l'EEE

(suite au verso)

V *Avis*

PROCÉDURES RELATIVES À LA MISE EN ŒUVRE DE LA POLITIQUE DE CONCURRENCE

Commission européenne

2013/C 190/05 Aide d'État — République Hellénique — Aide d'État n° SA.31155 (2013/C) (ex 2013/NN) (ex 2010/N) — Aide d'État en faveur d'Hellenic Postbank S.A. consistant en la création et la capitalisation de la banque-relais «New Hellenic Postbank S.A.» — Invitation à présenter des observations conformément à l'article 108, paragraphe 2, du TFUE [1] 70

FR

[1] Texte présentant de l'intérêt pour l'EEE

IV

(Informations)

INFORMATIONS PROVENANT DES INSTITUTIONS, ORGANES ET ORGANISMES DE L'UNION EUROPÉENNE

SERVICE EUROPÉEN POUR L'ACTION EXTÉRIEURE

DÉCISION DE LA HAUTE REPRÉSENTANTE DE L'UNION POUR LES AFFAIRES ÉTRANGÈRES ET LA POLITIQUE DE SÉCURITÉ

du 19 avril 2013

relative aux règles de sécurité applicables au Service européen pour l'action extérieure

(2013/C 190/01)

LA HAUTE REPRÉSENTANTE DE L'UNION POUR LES AFFAIRES ÉTRANGÈRE ET LA POLITIQUE DE SÉCURITÉ,

vu la décision 2010/427/UE du Conseil du 26 juillet 2010 fixant l'organisation et le fonctionnement du service européen pour l'action extérieure [1] (ci-après le «SEAE»),

vu les recommandations du comité visé à l'article 9, paragraphe 6, de la décision de la haute représentante du 15 juin 2011 relative aux règles de sécurité applicables au service européen pour l'action extérieure [2],

vu l'avis du comité visé à l'article 10, paragraphe 1, de la décision 2010/427/UE du Conseil du 26 juillet 2010 fixant l'organisation et le fonctionnement du SEAE,

considérant ce qui suit:

(1) En tant qu'organe de l'Union européenne fonctionnant de manière autonome, le SEAE devrait être doté de règles de sécurité, telles que visées à l'article 10, paragraphe 1, de la décision 2010/427/UE du Conseil;

(2) La haute représentante de l'Union pour les affaires étrangères et la politique de sécurité (ci-après la «haute représentante» ou «HR») doit fixer pour le SEAE des règles de sécurité englobant tous les aspects de la sécurité pour ce qui est du fonctionnement du SEAE, afin que ce dernier soit en mesure de gérer efficacement les risques menaçant son personnel, ses biens matériels, les informations qu'il détient et ses visiteurs et de s'acquitter des responsabilités qui lui incombent en ce qui concerne l'obligation de vigilance à cet égard;

(3) Il convient, en particulier, de garantir au personnel du SEAE, à ses biens matériels, y compris les systèmes d'information et de communication qu'il possède, aux informations qu'il détient et à ses visiteurs un niveau de protection conforme aux meilleures pratiques en usage au Conseil, à la Commission européenne, dans les États membres et, s'il y a lieu, dans les organisations internationales.

(4) Les règles de sécurité applicables au SEAE devraient contribuer à la mise en place d'un cadre général complet et plus cohérent au sein de l'Union européenne pour ce qui est de la protection des informations classifiées de l'UE (ci-après les «ICUE»), en s'appuyant sur les règles de sécurité du Conseil de l'Union européenne (ci-après le «Conseil») et sur les dispositions de la Commission européenne en matière de sécurité, tout en veillant à maintenir la plus grande cohérence possible avec ces règles et dispositions;

(5) Le SEAE, le Conseil et la Commission sont résolus à appliquer des normes équivalentes de sécurité pour protéger les ICUE;

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

(7) Il importe de fixer l'organisation de la sécurité dans le SEAE et l'allocation des tâches relatives à la sécurité au sein des structures du SEAE;

[1] JO L 201 du 3.8.2010, p. 30.
[2] JO C 304 du 15.10.2011, p. 5.

(8) La haute représentante doit s'appuyer, en fonction des besoins, sur les compétences techniques existant en la matière dans les États membres, au Secrétariat général du Conseil et à la Commission européenne;

(9) La haute représentante doit prendre toutes les mesures qui s'imposent pour appliquer ces règles avec l'appui des États membres, du Secrétariat général du Conseil et de la Commission européenne,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Objet et champ d'application

La présente décision arrête les règles de sécurité applicables au service européen pour l'action extérieure (ci-après les «règles de sécurité applicables au SEAE»).

Conformément à l'article 10, paragraphe 1, de la décision 2010/427/UE du Conseil du 26 juillet 2010 fixant l'organisation et le fonctionnement du service européen pour l'action extérieure, elle s'applique au personnel du SEAE et à tous les membres du personnel des délégations de l'Union, indépendamment de leur statut administratif ou origine, et instaure le cadre réglementaire général en vue de gérer efficacement les risques pesant sur le personnel relevant de la responsabilité du SEAE tel que visé à l'article 2, les locaux du SEAE, ses biens matériels, les informations qu'il détient et ses visiteurs.

Article 2

Définitions

Aux fins de la présente décision, on entend par:

a) «Membres du personnel du SEAE», on entend les fonctionnaires et autres agents du SEAE, y compris le personnel des services diplomatiques des États membres nommés comme agents temporaires, les experts nationaux détachés, tels que définis à l'article 6 de la décision 2010/427/UE du Conseil du 26 juillet 2010 fixant l'organisation et le fonctionnement du service européen pour l'action extérieure.

b) «Membres du personnel placés sous la responsabilité du SEAE», on entend les membres du personnel du SEAE et tous les membres du personnel des délégations de l'Union, indépendamment de leur statut administratif ou origine, ainsi que, aux fins de la présente décision, la haute représentante et, le cas échéant, d'autres membres du personnel résidant au siège du SEAE.

c) «Personnes à charge», on entend les membres de la famille du personnel placé sous la responsabilité du SEAE dans les délégations de l'Union, qui composent leur propre ménage tel qu'il a été notifié au ministère des affaires étrangères de l'État d'accueil.

d) «Locaux du SEAE», on entend tous les établissements du SEAE, y compris les bâtiments, bureaux, salles et autres espaces, ainsi que les lieux hébergeant des systèmes d'information et de communication (dont les équipements de traitement des ICUE), où le SEAE exerce des activités permanentes ou temporaires.

e) «Intérêts du SEAE à protéger», on entend les membres du personnel placés sous la responsabilité du SEAE, les locaux, les personnes à charge, les biens matériels, y compris les systèmes d'information et de communication, les informations et les visiteurs du SEAE.

f) «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.

D'autres définitions figurent dans les annexes pertinentes et à l'appendice A.

Article 3

Devoir de diligence

1. Les règles de sécurité applicables au SEAE ont pour but de lui permettre d'assumer ses responsabilités au regard du devoir de diligence.

2. Le devoir de diligence incombant au SEAE comprend la saine diligence consistant à prendre toutes les mesures raisonnables pour mettre en œuvre les mesures de sécurité visant à empêcher tout préjudice raisonnablement prévisible aux intérêts du SEAE à protéger.

Il comprend à la fois un volet sécurité et un volet sûreté, y compris les éléments de ce type résultant des situations d'urgence ou crises, de quelque nature que ce soit.

3. Compte tenu du devoir de diligence incombant aux États membres, aux institutions ou organes de l'UE et à d'autres parties dont le personnel travaille dans des délégations de l'Union et/ou dans les locaux de délégations de l'Union, ou du devoir de diligence incombant au SEAE lorsque des délégations de l'Union sont hébergées dans les locaux d'autres parties susmentionnées, le SEAE conclut, avec chacune des entités susmentionnées, des arrangements administratifs traitant des rôles et responsabilités, tâches et mécanismes de coopération respectifs.

Article 4

Sécurité physique et sécurité des infrastructures

1. Le SEAE met en place toutes les mesures de sécurité physique appropriées (permanentes ou temporaires), y compris les dispositions de contrôle d'accès, pour l'ensemble des locaux du SEAE, aux fins de la préservation des intérêts du SEAE à protéger. De telles mesures entrent en ligne de compte lors de la conception et de la planification de nouveaux locaux ou avant la location à bail de locaux existants.

2. Dans les pays tiers, le SEAE prend également toute mesure supplémentaire qu'il juge adéquate pour garantir la sécurité physique, qu'elle soit permanente ou temporaire, aux fins de la protection des intérêts qui le nécessitent.

À cette fin, des obligations ou restrictions spéciales peuvent être imposées aux membres du personnel placés sous la responsabilité du SEAE et aux personnes à charge, pour des raisons de sécurité, pendant une période donnée et dans des domaines précis.

3. Les mesures visées aux paragraphes 1 et 2 doivent être proportionnées au risque évalué.

Article 5

Protection des informations classifiées

1. La protection des ICUE est régie par les exigences formulées dans la présente décision, et notamment dans l'annexe A. Le détenteur de toute ICUE est tenu de la protéger en conséquence.

2. Le SEAE veille à ce que seules les personnes réunissant les conditions exposées à l'article 5 de l'annexe A aient accès aux informations classifiées.

3. Les conditions auxquelles les agents locaux peuvent avoir accès aux ICUE sont également fixées par la haute représentante, conformément aux règles de protection des ICUE établies à l'annexe A de la présente décision.

4. La direction de la sécurité du SEAE gère une base de données concernant l'habilitation de sécurité de tous les membres du personnel placés sous la responsabilité du SEAE et de ses contractants.

5. Lorsque les États membres introduisent des informations classifiées portant un marquage national de classification de sécurité dans les structures ou réseaux du SEAE, ce dernier protège ces informations conformément aux règles applicables aux ICUE de niveau équivalent, ainsi que prévu dans les règles applicables conformément à l'annexe A de la présente décision.

6. Les zones du SEAE où sont stockées des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, ou équivalent, sont créées en tant que zones sécurisées conformément aux règles applicables en vertu de l'annexe A de la présente décision, et doivent être approuvées par l'autorité de sécurité du SEAE.

7. Les procédures d'habilitation à l'exécution de tâches incombant à la haute représentante dans le cadre d'accords ou d'arrangements administratifs concernant l'échange d'ICUE avec des pays tiers ou des organisations internationales sont décrites aux annexes A et A VI de la présente décision.

Article 6

Incidents et urgences en matière de sécurité

1. Afin de garantir une réponse opportune et efficace aux incidents en matière de sécurité, le SEAE établit une procédure de signalement de tels incidents et urgences, qui soit opérationnelle 24 heures sur 24, sept jours sur sept, et couvre tout type d'incident en matière de sécurité ou de menace pour les intérêts du SEAE à protéger (par exemple accidents, conflits, actes malveillants, actes criminels, enlèvements et prises d'otages, urgences médicales, incidents au niveau des systèmes d'information et de communication, cyberattaques, etc.).

2. Des lignes d'urgence sont établies entre le siège du SEAE, les délégations de l'Union, le Conseil, la Commission, les représentants spéciaux de l'UE et les États membres, afin de les aider à gérer les incidents sur le plan de la sécurité impliquant du personnel et leurs conséquences, y compris la planification des mesures d'urgence.

3. Cette gestion des incidents de sécurité inclut, entre autres:

— des procédures de soutien efficace au processus décisionnel en cas d'incident de sécurité impliquant du personnel, y compris des décisions liées à l'extraction ou à la suspension d'une mission; et

— une politique et des procédures de récupération du personnel, par exemple en cas de disparitions ou en cas d'enlèvements ou de prises d'otages, en tenant compte des responsabilités particulières des États membres, des institutions de l'UE et du SEAE à cet égard. La nécessité de disposer de capacités spécifiques, dans le cadre de la gestion de telles opérations sur ce point, est prise en considération eu égard aux ressources que les États membres pourraient fournir.

4. Le SEAE met en place des arrangements administratifs en matière de signalement de tout incident de sécurité survenant dans les délégations de l'Union. Les États membres, la Commission, tout autre autorité pertinente, ainsi que les comités de sécurité concernés sont informés, le cas échéant.

5. Les procédures de gestion des incidents devraient être mises à l'épreuve et réexaminées régulièrement.

Article 7

Sécurité des systèmes d'information et de communication

1. Le SEAE protège les informations traitées dans les systèmes d'information et de communication (ci-après «SIC») contre les menaces pesant sur leur confidentialité, leur intégrité, leur disponibilité, leur authenticité et leur non-répudiation.

2. L'autorité de sécurité du SEAE, telle que définie à l'article 12, section I, paragraphe 1, approuve des règles, une politique de sécurité et un programme de sécurité pour la protection de tous les SIC détenus ou exploités par le SEAE.

3. Les règles, la politique et le programme sont conformes à ceux du Conseil et de la Commission et, le cas échéant, avec les politiques de sécurité appliquées par les États membres, et leur mise en œuvre est étroitement coordonnée avec ces derniers.

4. Tous les SIC traitant des informations classifiées font l'objet d'un processus d'homologation. Le SEAE applique un système de gestion de l'homologation de sécurité en concertation avec le Secrétariat général du Conseil et la Commission européenne.

5. Lorsque la protection des ICUE traitées par le SEAE est assurée par des produits cryptographiques, ces produits doivent être agréés par l'autorité d'agrément cryptographique du SEAE, sur recommandation du comité de sécurité du Conseil.

6. L'autorité de sécurité du SEAE met en place, selon les besoins, les autorités chargées de l'assurance de l'information, comme suit:

a) une autorité chargée de l'assurance de l'information;

b) une autorité TEMPEST;

c) une autorité d'agrément cryptographique;

d) une autorité de distribution cryptographique.

7. Pour chaque système, l'autorité de sécurité du SEAE crée les autorités suivantes:

a) une autorité d'homologation de sécurité;

b) b) une autorité opérationnelle chargée de l'assurance de l'information.

8. Les dispositions d'application du présent article concernant la protection des ICUE sont exposées aux annexes A et A IV.

Article 8

Infractions à la sécurité et compromission des informations classifiées

1. Une infraction à la sécurité résulte d'un acte ou d'une omission commis par une personne qui est contraire aux règles de sécurité énoncées dans la présente décision et/ou aux politiques ou lignes directrices en matière de sécurité énonçant les éventuelles mesures nécessaires à sa mise en œuvre, telles qu'approuvées conformément à l'article 20, paragraphe 1.

2. Une compromission d'informations classifiées consiste en une divulgation totale ou partielle desdites informations à des personnes ou entités non autorisées.

3. Toute infraction à la sécurité, réelle ou présumée, et toute compromission d'informations classifiées, réelle ou présumée, sont immédiatement signalées à la direction de la sécurité du SEAE, qui prend les mesures appropriées, telles qu'énoncées à l'annexe A.

4. Toute personne coupable d'une infraction aux règles de sécurité établies dans la présente décision, ou d'une compromission d'informations classifiées, est passible d'une sanction disciplinaire et/ou juridique, conformément aux dispositions législatives et réglementaires applicables, telles qu'énoncées à l'article 11, paragraphe 3, de l'annexe A.

Article 9

Enquêtes sur les incidents de sécurité, infractions et/ou compromissions et actions correctives

1. La direction de la sécurité du SEAE, assistée d'experts d'États membres et/ou d'autres institutions de l'Union, le cas échéant, et moyennant l'autorisation du directeur opérationnel, si besoin est:

a) mène des enquêtes ou procède à des vérifications, le cas échéant:

i) lorsqu'il est notoire ou lorsque des motifs raisonnables laissent penser que des informations classifiées pertinentes pour le SEAE ont été compromises ou perdues;

ii) à chaque infraction aux règles de sécurité ou autre incident de sécurité ou menace pour les intérêts du SEAE à protéger, qu'ils soient réels ou présumés;

b) met en œuvre toute action corrective nécessaire résultant d'enquêtes, lorsqu'il y a lieu.

2. Les enquêteurs ont accès à toutes les informations nécessaires à la conduite de telles enquêtes et bénéficient de toute l'aide de l'ensemble des services du SEAE sur ce point.

Les enquêteurs peuvent entreprendre des actions adéquates pour préserver les preuves réunies d'une manière proportionnée à la gravité du cas examiné.

3. Lorsque l'accès aux informations a trait à des données à caractère personnel, y compris celles contenues dans les systèmes d'information et de communication, un tel accès respectera les dispositions du règlement (CE) n° 45/2001.

4. En cas de nécessité d'établir une base de données d'investigation qui contiendra des données à caractère personnel, le Contrôleur européen de la protection des données (CEPD) en est informé conformément au règlement précité.

Article 10

Gestion des risques de sécurité

1. Afin de déterminer ses besoins en matière de sécurité, le SEAE élabore une méthode globale d'évaluation des risques pour la sécurité, en étroite coopération avec la direction de la sécurité de la Commission et, le cas échéant, avec le bureau de sécurité du Secrétariat général du Conseil.

2. Les risques pesant sur les intérêts du SEAE à protéger 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 et à appliquer ces mesures selon le principe de défense en profondeur. L'efficacité de telles mesures et le niveau de risque font l'objet d'une évaluation constante.

3. Les rôles, responsabilités et tâches fixés dans la présente décision sont sans préjudice de la responsabilité qui incombe à chaque membre du personnel placé sous la responsabilité du SEAE; plus particulièrement, les membres du personnel de l'UE en mission dans des pays tiers doivent faire preuve de bon sens et de discernement pour ce qui a trait à leur propre sécurité, et respecter toutes les dispositions législatives et réglementaires, procédures et consignes de sécurité applicables.

4. Le SEAE prend toutes les mesures raisonnables pour garantir la sécurité de ses intérêts qui doivent être protégés et pour éviter tout dommage raisonnablement prévisible s'y rapportant.

5. Les mesures de sécurité applicables au SEAE visant à protéger les 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, notamment celle évaluée à l'échelle locale, que représentent les activités malveillantes et/ou criminelles, y compris l'espionnage, le sabotage et le terrorisme.

Article 11

Sensibilisation et formation en matière de sécurité

1. L'autorité de sécurité du SEAE veille à l'élaboration et à la mise en œuvre de programmes de sensibilisation et de formation en matière de sécurité au sein du SEAE et fait en sorte que les membres du personnel placés sous la responsabilité du SEAE et, s'il y a lieu, les personnes à leur charge, bénéficient des actions de formation et de sensibilisation nécessaires et proportionnées aux risques inhérents à leur lieu de résidence.

2. Avant de se voir accorder l'accès à des ICUE et à intervalles réguliers par la suite, le personnel est informé des responsabilités qui lui incombent en matière de protection des ICUE, conformément aux règles applicables en vertu de l'article 5, et reconnaît ces responsabilités.

Article 12

Organisation de la sécurité au sein du SEAE

Section 1.

Dispositions générales

1. Le directeur opérationnel (DO) est l'autorité du SEAE compétente en matière de sécurité. En cette qualité, le DO veille:

a) à ce que les mesures de sécurité fassent l'objet, si nécessaire, d'une coordination avec les autorités compétentes des États membres, le secrétariat général du Conseil, la Commission européenne et, s'il y a lieu, les pays tiers ou organisations internationales sur toutes les questions de sécurité présentant un intérêt pour les activités du SEAE, notamment en ce qui concerne la nature des menaces qui pèsent sur les intérêts du SEAE à protéger et les moyens pour ce faire;

b) à ce que les aspects liés à la sécurité soient pleinement pris en compte dès le départ pour l'ensemble des activités du SEAE;

c) à ce que seules les personnes réunissant les conditions exposées à l'article 5 de l'annexe A aient accès aux informations classifiées;

d) à ce que soit établi un système d'enregistrement qui garantisse que les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur soient traitées conformément à la présente décision au sein du SEAE, ainsi qu'au sein des États membres de l'UE, des institutions, organes et organismes de l'Union ou d'autres destinataires autorisés si elles leur ont été communiquées. Un registre distinct est tenu pour toutes les ICUE communiquées par le SEAE à des pays tiers et des organisations internationales, et pour toutes les informations classifiées communiquées par des pays tiers ou des organisations internationales;

e) à ce que les inspections de sécurité visées à l'article 15 soient réalisées;

f) à ce que des enquêtes soient menées sur toute infraction à la sécurité, réelle ou présumée, ainsi que sur toute compromission ou perte - réelle ou présumée - d'informations classifiées détenues par le SEAE ou provenant de ce dernier, et à ce qu'il soit demandé aux autorités de sécurité compétentes de participer à de telles enquêtes;

g) à ce que des mécanismes et des plans adéquats de gestion des incidents et de leurs conséquences soient mis en place, de manière à réagir rapidement et efficacement en cas d'incidents de sécurité;

h) à ce que des mesures appropriées soient prises en cas de non-respect de la présente décision;

i) à ce que des mesures physiques et organisationnelles appropriées soient mises en place pour protéger les intérêts du SEAE qui doivent l'être.

À cet égard, le DO prend les mesures suivantes en concertation avec le secrétaire général exécutif:

— fixe la catégorie de sécurité des délégations, en concertation avec la Commission;

— décide, après consultation de la HR, de l'évacuation, ou non, du personnel des délégations si la sécurité l'exige;

— décide des mesures à appliquer pour la protection des personnes à charge, compte tenu, le cas échéant, des arrangements convenus avec les institutions de l'Union visés à l'article 3, paragraphe 3;

— approuve la politique de communication cryptographique, en particulier le programme d'installation de produits et du mécanisme cryptographiques.

2. Dans ses tâches, le DO est assisté du directeur général responsable de l'administration et des finances, du chef de la direction de la sécurité du SEAE et, le cas échéant, du directeur exécutif responsable du département Réponse aux crises et coordination opérationnelle.

3. Le DO, en sa qualité d'autorité de sécurité du SEAE, peut déléguer des tâches dans ce domaine, le cas échéant.

4. Chaque chef de département/division est tenu de mettre en œuvre les règles de protection des ICUE au sein de son département ou de sa division.

Tout en conservant les responsabilités mentionnées ci-dessus, chaque chef de département/division désigne des membres du personnel pour assurer les fonctions de coordinateur de la sécurité du département/de la division, dont les ressources seront proportionnées au volume d'ICUE traitées par ce département/cette division.

Les coordinateurs de la sécurité du département assistent et soutiennent, le cas échéant, leur chef de département/division dans l'exécution des tâches liées à la sécurité, telles que:

a) l'élaboration de toute exigence de sécurité supplémentaire adaptée aux besoins spécifiques du département/de la division;

b) l'établissement de comptes rendus périodiques sur la sécurité à l'intention des membres de leur département/division;

c) la prise de mesures visant à faire respecter le principe du «besoin d'en connaître» dans leur département/division;

d) la tenue à jour d'une liste de codes et de clés sûrs;

e) le maintien de procédures et de mesures de sécurité;

f) le signalement de toute infraction aux règles de sécurité et/ou de toute compromission d'ICUE tant au directeur qu'à la direction de la sécurité;

g) le débriefing aux membres du personnel qui cessent de travailler pour le SEAE;

h) la fourniture de rapports réguliers, via leur hiérarchie, sur les questions de sécurité du département/de la division;

i) la mise en rapport avec la direction de la sécurité du SEAE sur des questions de sécurité.

Toute activité ou question susceptible d'avoir un impact sur la sécurité est notifiée à la direction de la sécurité du SEAE en temps utile

5. Chaque chef de délégation de l'Union est responsable de la mise en œuvre de l'ensemble des mesures relatives à la sécurité de la délégation de l'Union.

Section 2.

La direction de la sécurité du SEAE

1. Le SEAE dispose d'une direction de la sécurité. Celle-ci doit:

a) gérer, coordonner, superviser et/ou mettre en œuvre toutes les mesures de sécurité dans tous les locaux relevant de la responsabilité du SEAE, au siège, à l'intérieur de l'UE et dans les pays tiers;

b) assurer la cohérence avec la présente décision et avec les modalités d'application de toute activité qui pourrait avoir un impact sur la préservation des intérêts du SEAE à protéger;

c) assurer les fonctions de conseiller principal de la HR, du secrétaire général exécutif et du DO pour toutes les questions liées à la sécurité;

d) se faire assister par les services compétents des États membres, conformément à l'article 10, paragraphe 3, de la décision 2010/427/UE du Conseil fixant l'organisation et le fonctionnement du SEAE;

e) soutenir les activités de l'autorité d'homologation de sécurité du SEAE en effectuant des évaluations de la sécurité physique de l'environnement général de sécurité (EGS) / environnement local de sécurité (ELS) des systèmes d'information et de communication traitant des ICUE, ainsi que des locaux autorisés à traiter et à stocker des ICUE.

2. Le chef de la direction de la sécurité du SEAE est chargé:

a) de garantir la protection générale des intérêts du SEAE à protéger;

b) de rédiger, de revoir et de mettre à jour les règles de sécurité, ainsi que de coordonner les mesures de sécurité avec les autorités nationales compétentes et, le cas échéant, les autorités compétentes de pays tiers et d'organisations internationales liées à l'UE par des accords et/ou des arrangements de sécurité;

c) d'appuyer les procédures du comité de sécurité du SEAE, tel qu'établi à l'article 14, paragraphe 1, de la présente décision;

d) de se mettre en rapport avec tous partenaires ou autorités autres que ceux mentionnés au point b) ci-dessus pour les questions de sécurité, le cas échéant;

e) d'établir des priorités et de soumettre des propositions en vue de la gestion du budget consacré à la sécurité au siège et dans les délégations de l'Union.

3. Le chef de la direction de la sécurité du SEAE est chargé:

a) de garantir l'enregistrement des infractions et compromissions en matière de sécurité, le lancement et la conduite d'enquêtes dans de tels cas, lorsque c'est nécessaire;

b) de se réunir régulièrement, à chaque fois que c'est nécessaire, avec le directeur de la sécurité du Secrétariat général du Conseil et avec le directeur de la direction de la sécurité de la Commission pour discuter de thèmes d'intérêt commun.

4. La direction de la sécurité du SEAE noue des contacts et entretient une coopération étroite avec:

— les départements responsables de la sécurité au sein des ministères nationaux des affaires étrangères;

— les autorités nationales de sécurité (ANS) et/ou les autres autorités compétentes en matière de sécurité dans les États membres afin d'obtenir leur aide quant aux informations dont elle a besoin pour évaluer les dangers et menaces qui peuvent peser sur le SEAE, son personnel, ses activités, ses biens et ses ressources, ainsi que ses informations classifiées dans les lieux où se déroulent normalement ses travaux;

— les autorités de sécurité compétentes des États membres ou des pays d'accueil sur le territoire desquels le SEAE peut exercer ses activités, concernant toute question relative à la protection des membres de son personnel, de ses activités, de ses biens et ressources, ainsi que de ses informations classifiées quand ils se trouvent sur leur territoire;

— le bureau de sécurité du Secrétariat général du Conseil et la direction de la sécurité de la direction générale des ressources humaines et de la sécurité de la Commission et, le cas échéant, les services chargés de la sécurité des autres institutions, organes et organismes de l'UE;

— les services de sécurité de pays tiers ou d'organisations internationales, aux fins de toute coordination utile, et

— les ANS des États membres, concernant toute question relative à la protection des ICUE.

Section 3.

Délégations de l'Union

1. Chaque chef de délégation de l'Union est responsable de la mise en œuvre et de la gestion, au niveau local, de toutes les mesures relatives à la préservation des intérêts du SEAE à protéger dans les locaux de la délégation concernée et relevant de sa compétence.

Il prend, en concertation avec les autorités compétentes de l'État d'accueil si nécessaire, toutes les mesures pouvant être raisonnablement mises en œuvre afin de garantir la mise en place, à cette fin, de mesures physiques et organisationnelles adéquates.

Le chef de délégation établit les procédures de sécurité concernant la protection des personnes à charge, telles que définies à l'article 2, point c), compte tenu, le cas échéant, de tout arrangement administratif visé à l'article 3, paragraphe 3. Le chef de délégation rend compte, sur base annuelle, de toutes les questions de sécurité relevant de sa compétence au chef de la direction de la sécurité du SEAE.

Il est assisté dans sa mission par la direction de la sécurité du SEAE, par le personnel du SEAE au sein de la délégation exerçant des tâches et fonctions ayant trait à la sécurité et par le personnel de sécurité en poste, si nécessaire.

2. Le chef de délégation prend en outre les mesures suivantes:

— il établit des plans de sécurité et d'urgence détaillés pour la délégation, sur la base de procédures opérationnelles standard générales;

— il s'occupe d'un système opérationnel 24 heures sur 24 de gestion des incidents de sécurité et des urgences relevant du champ d'intervention de la délégation;

— il veille à ce que tous les membres du personnel travaillant pour la délégation soient assurés conformément aux conditions en la matière;

— il veille à ce que le thème de la sécurité soit intégré à la formation d'entrée en service que les délégations de l'Union dispensent à tous les membres du personnel avant et au moment de les accueillir; et

— il s'assure de la bonne mise en œuvre des recommandations émises après les évaluations de la sécurité et transmet des rapports écrits à intervalles réguliers au sujet de leur mise en œuvre et d'autres questions de sécurité à l'autorité de sécurité du SEAE.

3. Tout en demeurant responsable et en devant continuer de rendre compte de la préservation de la gestion de la sécurité ainsi que de l'obligation qui lui incombe de garantir la résilience organisationnelle, le chef de délégation peut déléguer l'exécution de ses tâches en matière de sécurité au coordinateur de la sécurité de la délégation (CSD), à savoir soit le chef adjoint de la délégation ou, si personne n'est désigné, quiconque à même d'assurer cette fonction.

Plus particulièrement, les responsabilités suivantes peuvent être confiées au CSD:

— se mettre en rapport, pour les questions de sécurité, avec les autorités compétentes du pays d'accueil et les homologues indiqués au sein des ambassades et des missions diplomatiques des États membres;

— mettre en œuvre des procédures adéquates de gestion de la sécurité en rapport avec les intérêts du SEAE à protéger, y compris la protection des ICUE;

— mettre les membres du personnel au courant des règles de sécurité auxquelles ils doivent se soumettre, ainsi que des risques particuliers dans le pays d'accueil;

— soumettre des demandes à la direction de la sécurité du SEAE concernant les positions nécessitant une habilitation de sécurité du personnel (HSP), et

— tenir le chef de délégation, le responsable régional de la sécurité (RSO) et la direction de la sécurité du SEAE constamment informés des incidents ou nouveaux éléments en la matière ayant un impact sur la préservation des intérêts du SEAE à protéger.

4. Le chef de délégation peut déléguer des tâches de sécurité à caractère administratif ou technique au chef d'administration et à d'autres membres du personnel de la délégation.

5. La délégation de l'Union est assistée d'un responsable régional de la sécurité (RSO). Dans les délégations, les RSO endossent les rôles, définis ci-dessous, dans chacun de leurs domaines de compétences géographiques respectifs.

Dans certaines circonstances, lorsque les conditions de sécurité du moment l'exigent, un RSO précis peut être assigné à résider à temps plein dans une délégation donnée.

Un RSO peut être muté dans une zone ne relevant pas de son domaine de compétence actuel, y compris au siège à Bruxelles, voire devoir accepter un poste résidentiel en fonction de la situation d'un pays en matière de sécurité, et en fonction des exigences de la direction de la sécurité du SEAE.

6. Les RSO sont placés sous le contrôle hiérarchique direct de la direction de la sécurité du SEAE, mais sous le contrôle fonctionnel et administratif direct du chef de délégation concerné. Ils assistent le chef de délégation et les membres du personnel de la délégation dans l'organisation et la mise en œuvre de toutes les mesures physiques, organisationnelles et procédurales liées à la sécurité de l'ensemble des membres du personnel de la délégation, indépendamment de leur origine administrative.

7. Les RSO prodiguent conseil et soutien au chef de délégation et au personnel de délégation. Lorsqu'il y a lieu, en particulier lorsqu'un RSO est assigné à résider à temps plein dans la délégation, il ou elle peut aider la délégation de l'Union dans la gestion et la mise en œuvre de la sécurité, y compris dans la préparation de contrats de sécurité, la gestion d'homologations et d'habilitations.

Article 13

Opérations PSDC et représentants spéciaux de l'UE

La direction de la sécurité du SEAE aide et conseille le directeur de la direction «Gestion des crises et planification» (CMPD), le directeur général de l'État-major de l'UE (EMUE), le commandant d'opérations civiles de la Capacité civile de planification et de conduite (CPCC), ainsi que les commandants d'opérations militaires pour ce qui est du volet «sécurité» des opérations de PSDC, et les représentants spéciaux de l'UE en ce qui concerne le volet «sécurité» de leur mandat, complémentaires aux dispositions spécifiques prévues en la matière dans les politiques pertinentes adoptées par le Conseil.

Article 14

Le comité de sécurité du SEAE

1. Un comité de sécurité est créé par la présente décision.

Il est présidé par le DO ou par son délégué désigné et se réunit sur instruction du président ou à la demande de l'un de ses membres. La direction de la sécurité du SEAE assiste le président dans ses fonctions et soutient administrativement, si nécessaire, les délibérations du comité.

2. Le comité de sécurité du SEAE est composé de représentants:

— de chaque État membre;

— du bureau de sécurité du Secrétariat général du Conseil;

— de la direction de la sécurité de la direction générale des ressources humaines et de la sécurité de la Commission européenne.

Une délégation nationale près le comité de sécurité du SEAE peut être composée de membres:

— de l'autorité nationale de sécurité et/ou de l'autorité de sécurité désignée,

— des départements responsables de la sécurité au sein des ministères nationaux des affaires étrangères.

3. Les représentants du comité peuvent être accompagnés et conseillés par des experts selon ce qu'ils jugent nécessaire. Des représentants d'autres institutions, organes ou organismes de l'UE peuvent être invités à y prendre part lorsque des points pertinents pour leur sécurité sont abordés.

4. Sans préjudice du paragraphe 5 ci-dessous, le comité de sécurité du SEAE assiste le SEAE, par voie de consultation, pour toutes les questions de sécurité pertinentes pour les activités du SEAE, le siège et les délégations de l'Union.

Plus particulièrement, et sans préjudice du paragraphe 5 ci-dessous, le comite de sécurité du SEAE:

a) doit être consulté au sujet:

— des politiques, lignes directrices et concepts de sécurité, ainsi que tout autre document de méthodologie concernant la sécurité, notamment en ce qui concerne la protection d'informations classifiées et les mesures à prendre lorsque les membres du personnel du SEAE ne se conforment pas aux règles de sécurité;

— des aspects techniques de sécurité susceptibles d'influencer la décision de la HR de soumettre une recommandation au Conseil en vue de l'ouverture de négociations concernant les accords sur la sécurité des informations visés à l'article 10, paragraphe 1, point a), de l'annexe A;

— de toute modification de la présente décision;

b) peut être consulté ou informé, le cas échéant, au sujet de questions liées à la sécurité de membres du personnel ou de biens au siège du SEAE et dans les délégations de l'Union, sans préjudice de l'article 3, paragraphe 3;

c) doit être informé de toute compromission ou perte d'ICUE se produisant au sein du SEAE.

5. Toute modification des règles relatives à la protection des ICUE contenues dans la présente décision et son annexe A requiert l'avis unanimement favorable des États membres représentés au sein du comité de sécurité du SEAE. Un tel avis unanimement favorable est également requis avant:

— l'ouverture de négociations portant sur les arrangements administratifs visés à l'article 10, paragraphe 1, point b), de l'annexe A;

— la communication d'informations classifiées dans les circonstances exceptionnelles visées aux paragraphes 9, 11 et 12 de l'annexe A VI;

— d'endosser la responsabilité en tant qu'autorité d'origine des informations dans les circonstances visées à l'article 10, paragraphe 4, in fine, de l'annexe A.

Un avis unanimement favorable est obtenu lorsque les délégations des États membres ne formulent aucune objection pendant les délibérations du comité.

6. Le comité de sécurité du SEAE tient pleinement compte des politiques et lignes directrices de sécurité en vigueur au sein du Conseil et de la Commission.

7. Le comité de sécurité du SEAE reçoit la liste des inspections annuelles du SEAE et les rapports d'inspection, dès qu'ils sont finalisés.

8. Organisation des réunions:

— Le comité de sécurité du SEAE se réunit au moins deux fois par an. Des réunions supplémentaires, à part entière ou au format de sécurité ANS/ASD ou MFA, peuvent être convoquées par le président ou organisées à la demande des membres du comité.

— Le comité de sécurité du SEAE organise ses activités de manière à être en mesure de formuler des recommandations sur des aspects spécifiques de la sécurité. Il peut créer d'autres sous-divisions spécialisées, si nécessaire. Il établit le mandat de ces sous-divisions spécialisées et reçoit leurs rapports d'activités.

— La direction de la sécurité du SEAE est chargée de préparer les points de discussion. Le président établit l'ordre du jour provisoire de chaque réunion. Les membres du comité peuvent proposer d'autres points à examiner.

Article 15

Inspections de sécurité

1. L'autorité de sécurité du SEAE veille à ce que les inspections de sécurité soient réalisées, sur une base régulière, au sein du siège du SEAE et des délégations de l'Union afin de vérifier si les mesures de sécurité sont adéquates et si elles sont conformes à la présente décision. La direction de la sécurité du SEAE peut, le cas échéant, désigner des experts qui apporteront leur contribution en participant aux inspections de sécurité dans les organes et organismes de l'Union visés au titre V, chapitre 2, du traité sur l'Union européenne.

2. Les inspections de sécurité du SEAE sont menées sous l'autorité de la direction de la sécurité du SEAE et, le cas échéant, avec le soutien d'experts en sécurité représentant d'autres institutions de l'Union ou États membres, en particulier dans le cadre des arrangements visés à l'article 3, paragraphe 3.

3. Le SEAE peut s'appuyer, si nécessaire, sur les compétences techniques existant en la matière dans les États membres, au Secrétariat général du Conseil et à la Commission européenne.

En cas de besoin, les experts en sécurité compétents basés dans les missions d'États membres dans des pays tiers et/ou des représentants des services de sécurité diplomatiques des États membres peuvent être invités à participer à l'inspection de sécurité au sein de la délégation de l'Union.

4. Les dispositions d'application du présent article concernant la protection des ICUE sont exposées à l'annexe A III.

Article 16

Visites d'évaluation

Des visites d'évaluation sont organisées afin de s'assurer de l'efficacité des mesures de sécurité en place dans un pays tiers ou une organisation internationale pour ce qui est de la protection des ICUE échangées en vertu d'un arrangement administratif tel que visé à l'article 10, paragraphe 1, point b), de l'annexe A.

La direction de la sécurité du SEAE peut demander à des experts d'apporter leur contribution en participant aux visites d'évaluation organisées dans des pays tiers ou des organisations internationales avec lesquels l'UE a conclu un accord sur la sécurité des informations tel que visé à l'article 10, paragraphe 1, point a), de l'annexe A.

Article 17

Planification de la continuité des activités

La direction de la sécurité du SEAE assiste le DO dans la gestion des aspects des processus opérationnels du SEAE se rapportant à la sécurité, dans le cadre de la planification globale de la continuité des activités du SEAE.

Article 18

Consignes en matière de voyages à l'intention des participants à des missions en dehors de l'UE

La direction de la sécurité du SEAE veille à la disponibilité de consignes en matière de voyages à l'intention des membres du personnel placés sous la responsabilité du SEAE amenés à participer à des missions en dehors de l'UE, en exploitant les ressources de tous les services pertinents du SEAE, notamment la salle de veille de l'UE, le centre de situation conjoint de l'Union européenne, les départements géographiques et les délégations de l'Union.

La direction de la sécurité du SEAE fournit sur demande, en puisant dans les ressources susmentionnées, des consignes spécifiques en matière de voyages concernant les missions de membres du personnel placés sous la responsabilité du SEAE dans des pays tiers présentant un niveau de risque élevé ou accru.

Article 19

Santé et sécurité

Les règles de sécurité du SEAE complètent les règles du SEAE en matière de protection de la santé et de la sécurité, telles qu'adoptées par la haute représentante.

Article 20

Mise en œuvre et réexamen

1. L'autorité de sécurité du SEAE approuve, après avoir consulté, le cas échéant, le comité de sécurité du SEAE, les politiques ou lignes directrices de sécurité fixant les mesures nécessaires à la mise en œuvre de ces règles au sein du SEAE et met en place les capacités nécessaires couvrant tous les aspects de la sécurité, en coopération étroite avec les autorités de sécurité compétentes des États membres et avec le concours des services concernés des institutions de l'Union.

2. Conformément à l'article 4, paragraphe 5, de la décision 2010/427/UE du Conseil du 26 juillet 2010 fixant l'organisation et le fonctionnement du service européen pour l'action extérieure, des arrangements transitoires peuvent être conclus, si besoin est, au moyen d'accords de niveau de service avec les services compétents du Secrétariat général du Conseil et de la Commission.

3. La HR veille à ce que la présente décision soit appliquée avec cohérence et réexamine périodiquement ces règles de sécurité.

4. Les règles de sécurité du SEAE doivent être mises en œuvre en étroite coopération avec les autorités de sécurité compétentes des États membres, avec le bureau de sécurité du Secrétariat général du Conseil et avec la direction de la sécurité de la direction générale des ressources humaines et de la sécurité de la Commission.

5. Le SEAE veille à ce que tous les aspects du processus de sécurité soient pris en considération dans le système du SEAE de réaction en cas de crise.

6. Le DO, en tant qu'autorité de sécurité, et le chef de la direction de la sécurité du SEAE garantissent la mise en œuvre de la présente décision.

Article 21

Remplacement des décisions précédentes

1. La présente décision abroge et remplace la décision de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité du 15 juin 2011 relative aux règles de sécurité applicables au service européen pour l'action extérieure ([1]).

2. La présente décision abroge la décision de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité du 23 février 2011 relative à la désignation et aux tâches de l'autorité de sécurité déléguée du service européen pour l'action extérieure.

Article 22

Dispositions finales

La présente décision entre en vigueur le jour de sa signature.

Elle est publiée au *Journal officiel de l'Union européenne*.

Les autorités compétentes du SEAE informent dûment et en temps utile tous les membres du personnel concernés par la présente décision et ses annexes au sujet de son contenu, de son entrée en vigueur et toute modification qui lui est apportée ultérieurement.

Fait à Bruxelles, le 19 avril 2013.

La haute représentante

C. ASHTON

([1]) JO C 304 du 15.10.2011, p. 5.

ANNEXE A

PRINCIPES ET NORMES DE PROTECTION DES ICUE

Article premier

Objectif, champ d'application et définitions

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

2. Ces principes de base et normes minimales s'appliquent au SEAE et aux membres du personnel placés sous sa responsabilité, tels que visés et définis, respectivement, aux articles 1er et 2 de la présente décision.

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) TRES 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. Le SEAE veille 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. L'autorité de sécurité du SEAE approuve, après avoir consulté le comité de sécurité du SEAE conformément à l'article 14, paragraphe 5, de la présente décision, une politique de sécurité relative à la création d'ICUE comprenant un guide de classification pratique.

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 du SEAE, ce dernier protège ces informations conformément aux règles applicables aux ICUE de niveau équivalent tel que prévu dans le tableau d'équivalence des classifications de sécurité figurant à l'appendice B de la décision 2011/292/UE du Conseil du 31 mars 2011 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'UE.

Le SEAE établit des procédures adéquates afin de tenir des registres précis de l'autorité d'origine

— des informations classifiées que le SEAE reçoit; et

— des sources incluses dans les informations classifiées émanant du SEAE.

Le comité de sécurité du SEAE est informé de ces procédures.

4. Les grandes quantités ou la compilation d'ICUE peuvent justifier un niveau de protection correspondant à une classification plus élevée que celle des éléments qui les composent.

Article 5

Sécurité du personnel amené à traiter des informations classifiées de l'UE

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;

— en ce qui concerne l'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, ont fait l'objet d'une habilitation de sécurité du niveau correspondant, ou ont été dûment autorisées en vertu de leurs fonctions conformément aux dispositions législatives et réglementaires nationales; et

— été informées de leurs responsabilités.

2. Les procédures d'habilitation de sécurité concernant le personnel (HSP) 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. Avant de se voir accorder l'accès à des ICUE et à intervalles réguliers par la suite, toutes les personnes concernées sont informées par écrit des responsabilités qui leur incombent en matière de protection des ICUE conformément à la présente décision et reconnaissent ces responsabilités par écrit.

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

Article 6

Sécurité physique des informations classifiées de l'UE

1. Par «sécurité physique», on entend l'application de mesures physiques et techniques de protection pour dissuader 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 8, 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 A II et agréées par l'autorité de sécurité du SEAE.

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 A II.

Article 7

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 5, 6 et 8 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, le traitement, le stockage 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 SEAE établissent un bureau d'ordre à cette fin. Les informations classifiées TRES 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 du SEAE.

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 7, paragraphe 5, de la présente décision et à des procédures d'exploitation de sécurité (SecOPs) clairement définies;

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 7, paragraphe 5, de la présente décision; soit

   ii) dans tous les autres cas, de la manière prescrite par l'autorité de sécurité du SEAE conformément aux mesures de protection pertinentes prévues à l'annexe A III, section V.

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

Article 8

Protection d'ICUE traitées dans des systèmes d'information et de communication

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» (SIC) tout système permettant le traitement d'informations sous forme électronique. Un système d'information et de communication comprend l'ensemble des moyens nécessaires pour le faire fonctionner, y compris l'infrastructure, l'organisation, le personnel et les ressources d'information. La présente annexe s'applique à tout SIC du SEAE traitant des ICUE.

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

4. Tous les SIC traitant des ICUE 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 sont agréés conformément à l'article 7, paragraphe 5, de la présente décision.

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 A IV.

8. En vertu de l'article 7, paragraphe 6, de la présente décision, les autorités d'AI suivantes sont établies selon les besoins:

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. En vertu de l'article 7, paragraphe 7, de la présente décision, sont créées, pour chaque système:

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 A IV.

Article 9

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 manière générale, de tels contrats ne doivent pas concerner l'accès à des informations classifiées TRES SECRET UE/EU TOP SECRET.

2. Le SEAE 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 sur la sécurité des informations ou un arrangement administratif en vertu de l'article 10, paragraphe 1, de l'annexe A, des tâches qui impliquent ou nécessitent l'accès, le traitement ou le stockage d'ICUE.

3. En tant qu'autorité contractante, le SEAE 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. Il garantit le respect de telles normes minimales via l'ANS/ASD concernée.

4. Les contractants et les sous-traitants immatriculés sur le territoire d'un État membre, qui participent à des contrats classifiés ou à des contrats de sous-traitance nécessitant le traitement et le stockage d'informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET au sein de leurs établissements, sont 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 délivrée par l'ANS, l'ASD ou toute autre autorité de sécurité compétente dudit État membre.

5. 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'autorité nationale de sécurité (ANS), l'autorité de sécurité désignée (ASD) ou toute autre autorité de sécurité compétente leur délivre une HSP, conformément aux dispositions législatives ou réglementaires nationales et dans le respect des normes minimales définies à l'annexe A I.

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

Article 10

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

1. Le SEAE ne peut échanger des ICUE avec un pays tiers ou une organisation internationale que dans les cas suivants:

a) un accord sur la sécurité des informations conclu entre l'UE et ce pays tiers ou cette organisation internationale conformément à l'article 37 du TUE et à l'article 218 du TFUE est en vigueur; ou

b) un arrangement administratif, conclu conformément à la procédure énoncée à l'article 14, paragraphe 5, de la présente décision, entre la HR et les autorités de sécurité compétentes de ce pays tiers ou de cette organisation internationale aux fins de l'échange d'informations dont le niveau de classification n'est en principe pas supérieur à RESTREINT UE/EU RESTRICTED, a pris effet; ou

c) un accord-cadre de participation ou un accord de participation ad hoc, conclu en vertu de l'article 37 du traité sur l'Union européenne et de l'article 218 du traité sur le fonctionnement de l'Union européenne, entre l'UE et ce pays tiers dans le cadre d'une opération PESD de gestion de crise est applicable,

et les conditions exposées dans cet instrument sont réunies.

Les exceptions à la règle générale ci-dessus sont précisées à l'annexe A VI, section V.

2. Les arrangements administratifs visés au paragraphe 1, point b), 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.

Les informations échangées sur la base des accords visés au paragraphe 1, point c), sont limités aux informations relatives aux opérations PSDC auxquelles le pays tiers en question participe sur la base de ces accords et conformément à leurs dispositions.

3. Des visites d'évaluation dans des pays tiers ou des organisations internationales, telles que visées à l'article 16 de la présente décision, sont organisées afin de garantir l'efficacité des mesures de sécurité en matière de protection de toute ICUE échangée.

4. La décision de communiquer des ICUE détenues par le SEAE à un pays tiers ou à une organisation internationale est prise 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.

Le SEAE demande le consentement écrit de toute entité ayant fourni des informations classifiées en tant que sources d'ICUE émanant du SEAE afin d'établir l'absence d'objection à leur communication.

Si l'autorité d'origine des informations classifiées à communiquer n'est pas le SEAE, le SEAE demande au préalable le consentement écrit de l'autorité d'origine.

Si, toutefois, le SEAE est dans l'impossibilité de déterminer l'autorité d'origine, l'autorité de sécurité du SEAE endosse la responsabilité de l'autorité d'origine après avoir obtenu l'avis unanimement favorable des États membres représentés au sein du comité de sécurité du SEAE.

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

Article 11

Infractions à la sécurité et compromission d'informations classifiées

1. Toute infraction à la sécurité, réelle ou présumée, et toute compromission d'informations classifiées, réelle ou présumée, sont immédiatement signalées à la direction de la sécurité du SEAE, qui informe, le cas échéant, la direction de la sécurité de la direction générale des ressources humaines et de la sécurité de la Commission, le bureau de sécurité du Secrétariat général du Conseil, le ou les États membres concernés, ou toute autre entité concernée.

2. Lorsqu'il est avéré ou qu'il existe des motifs raisonnables de supposer que des informations classifiées ont été compromises ou perdues, la direction de la sécurité du SEAE en informe la direction de la sécurité de la Commission européenne, le bureau de sécurité du Secrétariat général du Conseil ou l'ANS du ou des États membres concernés, ou toute autre entité concernée, selon le cas, et prend toutes les mesures nécessaires conformément aux dispositions législatives et réglementaires applicables afin:

a) d'évaluer le préjudice éventuel causé aux intérêts de l'UE ou des États membres;

b) d'éviter que les faits ne se reproduisent;

c) de protéger les éléments de preuve;

d) de 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;

e) de notifier aux autorités concernées les effets de l'événement et des mesures prises; et

f) d'informer l'autorité d'origine.

3. Tout membre du personnel sous la responsabilité du SEAE qui enfreint les 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'informations classifiées est passible de sanctions disciplinaires et/ou peut faire l'objet d'une action en justice conformément aux dispositions législatives et réglementaires applicables.

La direction de la sécurité de la direction générale des ressources humaines et de la sécurité de la Commission, le bureau de sécurité du Secrétariat général du Conseil ou l'ANS du ou des États membres concernés, ou toute entité concernée, sont immédiatement et dûment informés.

4. Pendant que l'infraction et/ou la compromission font l'objet d'une enquête, le chef de la direction de la sécurité du SEAE peut suspendre l'accès individuel aux ICUE et aux locaux du SEAE. La direction de la sécurité de la direction générale des ressources humaines et de la sécurité de la Commission, le bureau de sécurité du Secrétariat général du Conseil ou l'ANS du ou des États membres concernés, ou toute entité concernée, sont immédiatement informés de la présente décision.

ANNEXE A I

MESURES DE SÉCURITÉ CONCERNANT LE PERSONNEL

I. INTRODUCTION

1. La présente annexe contient les dispositions d'application de l'article 5 de l'annexe A. Elle prévoit les critères permettant au SEAE 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. L'«habilitation de sécurité du personnel» (HSP) donnant accès aux ICUE est 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».

3. Le «certificat d'habilitation de sécurité du personnel» (CHSP) est un certificat délivré par l'autorité de sécurité du SEAE précisant l'habilitation d'une personne et le niveau de classification des ICUE auxquelles l'intéressé peut se voir accorder l'accès, la date de validité de la HSP concernée et la date d'expiration du certificat lui-même.

4. L'«autorisation d'accès aux ICUE» est une autorisation que prend l'autorité de sécurité du SEAE en conformité avec la présente décision après qu'une HSP a été délivrée par les autorités compétentes d'un État membre, 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».

II. AUTORISER L'ACCÈS AUX ICUE

5. L'accès à des informations classifiées RESTREINT UE/EU RESTRICTED ne nécessite pas d'habilitation de sécurité et est accordé après:

   a) établissement du lien statutaire ou contractuel de la personne concernée avec le SEAE,

   b) détermination du besoin d'en connaître de la personne,

   c) notification des règles et procédures de sécurité applicables à la protection des ICUE et reconnaissance écrite des responsabilités qui lui incombent en matière de protection de ces informations conformément à la présente décision.

6. 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 par écrit les responsabilités qui lui incombent en matière de protection de ces informations.

7. Le SEAE répertorie, au sein de ses 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, conformément à l'article 4 ci-dessus.

8. Les membres du personnel du SEAE déclarent s'ils possèdent la nationalité de plusieurs pays.

Procédures de demande d'HSP au sein du SEAE

9. En ce qui concerne les membres du personnel du SEAE, l'AIPN du SEAE transmet le questionnaire de sécurité du personnel 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.

10. Lorsqu'une personne possède la nationalité de plusieurs pays, la demande d'enquête de sécurité est adressée à l'ANS du pays dont la personne recrutée est ressortissante.

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

12. À l'issue de l'enquête de sécurité, l'ANS compétente notifie à la direction de la sécurité du SEAE les conclusions de l'enquête en question.

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 de sécurité du SEAE peut accorder à l'intéressé une autorisation d'accès à des ICUE du niveau de classification correspondant jusqu'à une date déterminée.

b) Le SEAE prend toutes les mesures qui s'imposent pour veiller à ce que les conditions ou restrictions imposées par l'ANS soient dûment mises en œuvre. L'ANS est informée des résultats.

c) Lorsque, à l'issue de l'enquête de sécurité, on n'obtient pas cette assurance, l'autorité de sécurité du SEAE en informe l'intéressé, qui peut demander à être entendu par l'autorité de sécurité du SEAE. 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'autorisation d'accès aux ICUE n'est pas accordée. Dans ce cas, le SEAE prend toutes les mesures qui s'imposent pour que le demandeur se voie refuser tout accès aux ICUE.

13. L'enquête de sécurité et ses résultats, sur lesquels le SEAE fonde sa décision d'octroi ou de refus d'une autorisation d'accès aux ICUE, obéissent aux dispositions législatives et réglementaires en vigueur dans l'État membre concerné, y compris celles relatives aux recours. Les décisions de l'autorité de sécurité du SEAE 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»).

14. L'assurance sur laquelle une HSP se fonde, pour autant qu'elle reste valable, couvre toute fonction exercée par l'intéressé au sein du SEAE, du Secrétariat général du Conseil ou de la Commission.

15. Si l'intéressé n'entame pas sa période de service dans un délai de douze mois à compter de la notification des conclusions de l'enquête de sécurité à l'autorité de sécurité du SEAE ou si cette période de service connaît une interruption d'au moins douze mois au cours de laquelle l'intéressé n'occupe pas de poste au sein du SEAE, d'autres institutions, organes ou organismes de l'UE, ou d'une administration nationale d'un État membre nécessitant un accès à des informations classifiées, les conclusions précitées sont soumises à l'ANS compétente afin que celle-ci confirme qu'elles restent valables et pertinentes.

16. Si des informations sont portées à la connaissance du SEAE concernant un risque de sécurité que représente une personne titulaire d'une HSP valide, le SEAE, agissant conformément à la réglementation applicable, en avertit l'ANS compétente. Lorsqu'une ANS notifie au SEAE que l'assurance visée au paragraphe 12, point a), est retirée à une personne titulaire d'une autorisation d'accès aux ICUE valide, l'autorité de sécurité du SEAE 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'autorisation susmentionnée 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.

17. Toute décision de retirer une autorisation d'accès aux ICUE à un membre du personnel du SEAE et, s'il y a lieu, les raisons la justifiant sont communiquées à la personne concernée, qui peut demander à être entendue par l'autorité de sécurité du SEAE. 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'autorité de sécurité du SEAE sont susceptibles de recours conformément au statut et au régime applicable.

18. Les experts nationaux détachés auprès du SEAE pour occuper un poste nécessitant un accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur doivent présenter à l'autorité de sécurité du SEAE avant de prendre leurs fonctions une HSP valable leur donnant accès aux ICUE. La procédure susmentionnée est gérée par l'État membre qui détache les experts nationaux.

Registres des HSP

19. Une base de données pour l'état d'habilitation, en matière de sécurité, de tous les membres du personnel placés sous la responsabilité du SEAE et de ses contractants est administrée par le SEAE. Ces registres contiennent le niveau de classification des ICUE auxquelles l'intéressé peut se voir accorder l'accès (CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau supérieur), la date à laquelle l'HSP a été délivrée et sa durée de validité.

20. Des procédures de coordination adéquates sont mises en place avec les États membres et d'autres institutions, organes et organismes de l'UE pour faire en sorte que le SEAE tienne des registres précis et complets concernant l'état de l'habilitation de sécurité de tous les membres du personnel placés sous la responsabilité du SEAE et des effectifs de ses contractants.

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

21. L'autorité de sécurité du SEAE 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 d'un niveau supérieur), la durée de validité de l'HSP et la date d'expiration du certificat proprement dit.

Exemptions de l'obligation d'HSP

22. Les personnes dûment autorisées à accéder aux ICUE de par les fonctions qu'elles exercent, conformément aux dispositions législatives et réglementaires nationales, sont informées, le cas échéant, par la direction de la sécurité du SEAE des obligations qui leur incombent pour la sécurité des ICUE.

III. FORMATION ET SENSIBILISATION À LA SÉCURITÉ

23. Avant d'être autorisées à accéder aux ICUE, toutes les personnes reconnaissent par écrit qu'elles ont bien compris leurs obligations en matière de protection des ICUE et des conséquences qui pourraient résulter si des ICUE devaient être compromises. Le SEAE tient un registre de ces déclarations écrites.

24. 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.

25. Toutes les personnes ayant accès aux ICUE sont constamment soumises aux mesures de sécurité du personnel permanentes (c'est-à-dire assistance) pendant qu'elles traitent des ICUE. La sécurité permanente du personnel incombe:

a) aux personnes autorisées à accéder aux ICUE: les intéressés sont personnellement responsables de leur propre comportement en matière de sécurité et doivent signaler immédiatement aux autorités de sécurité compétentes toute démarche ou activité qu'ils jugent suspecte ou inhabituelle, ainsi que toute modification de leur propre situation personnelle qui pourrait avoir un impact sur leur HSP ou autorisation d'accéder aux ICUE;

b) aux supérieurs hiérarchiques: ils sont tenus de veiller à ce que leur personnel soit bien au courant des mesures de sécurité et des responsabilités quant à la protection des ICUE, de contrôler la conduite des membres du personnel quant à la sécurité et soit de traiter eux-mêmes tout problème de sécurité, soit de relayer aux autorités de sécurité compétentes toute information négative susceptible d'avoir un impact sur l'HSP ou l'autorisation d'accéder aux ICUE des membres de leur personnel;

c) aux intervenants en matière de sécurité de l'organisation de la sécurité du SEAE telle que visée à l'article 12 de la présente décision: ils sont tenus de proposer des mises au point en matière de sécurité afin que les membres du personnel relevant de leur domaine bénéficient d'informations régulières, de promouvoir une culture de sécurité solide dans leur domaine de responsabilité, de mettre en place des mesures de contrôle de la conduite des membres du personnel en matière de sécurité, ainsi que de signaler aux autorités de sécurité compétentes toute information négative qui pourrait avoir un impact sur les HSP de toute personne;

d) au SEAE et aux États membres: ils mettent en place les nécessaires canaux de communication d'informations susceptibles d'avoir un impact sur l'HSP ou autorisation d'accéder aux ICUE de toute personne.

26. 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.

IV. CIRCONSTANCES EXCEPTIONNELLES

27. En cas d'urgence, lorsque cela est dûment justifié dans l'intérêt du SEAE et en attendant l'achèvement de l'enquête de sécurité complète, l'autorité de sécurité du SEAE 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 SEAE l'autorisation d'accéder à des ICUE pour une fonction déterminée. Une enquête de sécurité complète doit être réalisée le plus rapidement possible. Ces autorisations temporaires sont valables pour une période ne dépassant pas six mois et ne donnent pas accès aux informations classifiées TRES SECRET UE/EU TOP SECRET. Toutes les personnes auxquelles a été délivrée une autorisation temporaire reconnaissent par écrit qu'elles ont bien compris leurs obligations en matière de protection des ICUE et les conséquences qui pourraient résulter si des ICUE devaient être compromises. Le SEAE tient un registre de ces déclarations écrites.

28. 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) l'intéressé possède une HSP valide;

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 du SEAE compétente; et

g) l'ANS/ASD compétente qui a délivré l'HSP à l'intéressé a été consultée et aucune objection n'a été formulée;

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

29. 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.

30. 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, la HR, le secrétaire général exécutif et le directeur opérationnel 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.

31. Pour les informations classifiées TRES 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 TRES SECRET UE/EU TOP SECRET soit à des informations classifiées SECRET UE/EU SECRET.

32. Le comité de sécurité du SEAE est informé des cas où il est recouru à la procédure décrite aux paragraphes 29 et 30.

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

V. PARTICIPATION AUX RÉUNIONS AU SIÈGE DU SEAE ET DANS LES DÉLÉGATIONS DE L'UNION

34. Les personnes désignées pour participer à des réunions au siège du SEAE et dans les délégations de l'Union 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 représentants des États membres, les fonctionnaires du SCG et de la Commission, un CHSP ou toute autre preuve d'HSP est transmis par les autorités concernées à la direction de la sécurité du SEAE, au coordinateur de la sécurité de la délégation de l'Union ou, à titre exceptionnel, est présenté par l'intéressé. Le cas échéant, il peut être fait usage d'une liste de noms récapitulative mentionnant les preuves d'habilitation voulues.

35. Lorsqu'une HSP permettant d'accéder à des ICUE est retirée à une personne dont la fonction l'oblige à participer à des réunions au siège du SEAE ou dans une délégation de l'Union auxquelles des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont traitées, le SEAE en est informé par l'autorité compétente.

VI. ACCÈS POTENTIEL AUX ICUE

36. 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.

37. 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 à intervalles réguliers 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 ou auxquelles ils peuvent avoir accès par inadvertance.

ANNEXE A II

SÉCURITÉ PHYSIQUE DES INFORMATIONS CLASSIFIÉES DE L'UE

I. INTRODUCTION

1. La présente annexe contient les dispositions d'application de l'article 6 de l'annexe A. Elle énonce 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 hébergeant 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. Il convient que le SEAE applique une procédure de gestion des risques 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;

   d) des évaluations de la menace de pays tiers telles qu'élaborées par INTCEN sur la base, en particulier, de rapports établis par les délégations de l'Union, et

   e) 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 du SEAE 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 de sécurité du SEAE peut 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 du SEAE 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 du SEAE 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).

13. Il appartient à l'autorité de sécurité du SEAE 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 de sécurité du SEAE; 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 au niveau adéquat 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;

c) les appareils électroniques sont laissés hors de la zone.

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 de la présente annexe;

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 du SEAE. 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 du SEAE 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 du SEAE 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;

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 A III, paragraphes 30 à 42, et se soit engagé à se conformer aux mesures compensatoires prévues dans les instructions de sécurité émises par l'autorité de sécurité du SEAE 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 du SEAE.

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 A III, paragraphes 30 à 42;

        ii) se soit engagé à se conformer aux mesures compensatoires prévues dans les instructions de sécurité émises par l'autorité de sécurité du SEAE 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 TRES SECRET UE/EU TOP SECRET sont traitées dans une zone sécurisée.

28. Les ICUE classifiées TRES SECRET UE/TOP SECRET UE sont stockées dans une zone sécurisée, au siège 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) 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 A III.

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

30. L'autorité de sécurité du SEAE 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) à la réception d'un nouveau meuble;

    b) lors de tout changement du personnel connaissant la combinaison;

    c) en cas de compromission, réelle ou présumée;

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

    e) au moins tous les douze mois.

ANNEXE A III

GESTION DES INFORMATIONS CLASSIFIÉES

I. INTRODUCTION

1. La présente annexe contient les dispositions d'application de l'article 7 de l'annexe A. 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 diffuser les informations.

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

5. Les informations classifiées des États membres échangées avec le SEAE reçoivent le même niveau de protection que les ICUE portant une classification équivalente. Un tableau d'équivalence figure à l'appendice B de la décision 2011/292/UE du Conseil du 31 mars 2011 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'UE.

6. La classification de sécurité et, le cas échéant, la date ou l'événement spécifique après laquelle ou lequel l'ICUE peut être déclassée ou déclassifiée seront indiqués clairement et correctement, que l'ICUE concernée soit au format papier, oral, électronique ou autre.

7. 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.

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. 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.

10. 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

11. Outre l'un des marquages de classification de sécurité prévus à l'article 2, paragraphe 2, de l'annexe A, 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.

12. Lorsqu'a été prise la décision de communiquer des ICUE à un pays tiers ou à une organisation internationale, la direction de la sécurité du SEAE transmet les informations classifiées concernées, qui portent un marquage relatif à la communicabilité indiquant le pays tiers ou l'organisation internationale auquel ce document doit être communiqué.

13. Une liste des marquages autorisés est adoptée par l'autorité de sécurité du SEAE.

Abréviations indiquant la classification

14. 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.

15. 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:

TRES SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Création d'ICUE

16. 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 CONFIDENTIEL UE/EU CONFIDENTIAL 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.

17. Lorsqu'il n'est pas possible d'appliquer le paragraphe 15 à des ICUE, d'autres mesures appropriées sont prises conformément aux lignes directrices en matière de sécurité qui doivent être arrêtées en vertu de la présente décision.

Déclassement et déclassification des ICUE

18. 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.

19. Le SEAE réexamine régulièrement les ICUE en sa possession pour déterminer si leur niveau de classification est toujours d'application. Le SEAE 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 à un moment précis et que celles-ci se sont vu apposer les marquages correspondants.

III. ENREGISTREMENT DES ICUE À DES FINS DE SÉCURITÉ

20. Un bureau d'ordre central est désigné au siège. Pour chacune des entités structurées qui existent au sein du SEAE et dans lesquelles des ICUE sont traitées, on détermine un bureau d'ordre compétent, subordonné au bureau d'ordre central, qui sera 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 A.

Chaque délégation de l'Union instaure son propre bureau d'ordre responsable des ICUE.

L'autorité de sécurité du SEAE désigne un Chief Registry Officer pour ces bureaux d'ordre.

21. Aux fins de la présente décision, on entend par enregistrement à des fins de sécurité (ci-après «enregistrement») l'application de procédures permettant de garder la trace du cycle de vie d'une information, y compris de sa diffusion et de sa destruction. 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. Tout matériel classifié CONFIDENTIEL UE/EU CONFIDENTIAL et d'un niveau de classification supérieur est enregistré à chaque fois qu'il parvient à une entité structurée ou qu'il en sort, délégations de l'Union comprises. Les informations classifiées TRES SECRET UE/EU TOP SECRET sont enregistrées dans des bureaux d'ordre désignés.

23. Le bureau d'ordre central constitue, au siège du SEAE, le principal point d'entrée et de sortie pour les échanges d'informations classifiées avec des pays tiers et des organisations internationales. Il garde une trace de tous ces échanges.

24. La HR approuve une politique de sécurité concernant l'enregistrement des ICUE à des fins de sécurité, conformément à l'article 14 de la présente décision.

Bureaux d'ordre très secret UE/EU top secret

25. Un bureau d'ordre central est désigné au siège du SEAE pour faire fonction d'autorité centrale de réception et de diffusion des informations classifiées TRES 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.

26. Ces bureaux d'ordre subordonnés ne peuvent pas 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

27. Les documents classifiés TRES SECRET UE/EU TOP SECRET ne doivent pas être dupliqués ou traduits sans le consentement écrit préalable de l'autorité d'origine.

28. 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.

29. Les mesures de sécurité applicables au document original le sont aussi à ses copies et à ses traductions. Les copies des informations CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont créées uniquement par le bureau d'ordre (subordonné) compétent au moyen d'un photocopieur sécurisé. Les copies doivent être enregistrées.

V. TRANSPORT DES ICUE

30. Le transport des ICUE est soumis aux mesures de protection énoncées aux paragraphes 31 à 41. Lorsque les ICUE sont transportées par des supports électroniques, et nonobstant l'article 7, paragraphe 4, de l'annexe A, les mesures de protection énoncées ci-après peuvent être complétées par des contre-mesures techniques appropriées prescrites par l'autorité de sécurité du SEAE, de façon à réduire au minimum le risque de perte ou de compromission.

31. L'autorité de sécurité du SEAE émet les instructions relatives au transport des ICUE conformément à la présente décision.

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

32. 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.

33. À l'intérieur d'un bâtiment ou d'un groupe autonome de bâtiments, les informations classifiées TRES SECRET UE/EU TOP SECRET sont transportées par des membres du personnel disposant de l'habilitation de sécurité adéquate, dans une enveloppe sécurisée avec pour seule mention le nom du destinataire.

À l'intérieur de l'UE

34. 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.

35. 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 A II;

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

iii) que la personne soit habilitée au niveau adéquat et ait reçu des instructions quant à ses responsabilités 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 en vertu de l'article 20, paragraphe 1, de la présente décision.

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.

36. 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 34 est transporté en tant que fret par des sociétés de transport commercial conformément à l'annexe A V.

37. Le transport des informations classifiées TRES 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, ou entre des entités de l'UE situées dans des pays tiers

38. Les ICUE transportées de l'UE vers le territoire d'un pays tiers ou entre des entités de l'UE situées dans des pays tiers sont emballées de manière à être protégées de toute divulgation non autorisée.

39. Le transport des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET de l'UE vers le territoire d'un pays tiers et le transport des ICUE d'un niveau de classification allant jusqu'à SECRET UE/EU SECRET entre des entités de l'UE situées dans des pays tiers s'effectuent 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 A II;

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

v) que les personnes soient habilitées au niveau adéquat et aient reçu des instructions quant à leurs responsabilités en matière de sécurité.

40. 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 10, paragraphe 2, de l'annexe A.

41. Les informations classifiées RESTREINT UE/EU RESTRICTED peuvent aussi être transportées de l'UE vers le territoire d'un pays tiers par des services postaux ou par des services de courrier commercial.

42. Le transport des informations classifiées TRES SECRET UE/EU TOP SECRET de l'UE vers le territoire d'un pays tiers ou entre des entités de l'UE situées dans des pays tiers s'effectue par courrier militaire ou diplomatique.

VI. **DESTRUCTION DES ICUE**

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

44. Les documents faisant l'objet d'un enregistrement en application de l'article 7, paragraphe 2, de l'annexe A 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.

45. La destruction de documents classifiés SECRET UE/EU SECRET ou TRES 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.

46. 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 TRES 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.

47. 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.

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

VII. **INSPECTIONS DE SÉCURITÉ**

Inspections de sécurité du SEAE

49. En vertu de l'article 15 de la présente décision, les inspections de sécurité du SEAE englobent:

a) des inspections de sécurité générales, qui ont pour but d'évaluer le niveau de sécurité général du siège du SEAE, des délégations de l'Union et de tous les locaux dépendants ou connexes, en particulier afin d'évaluer l'efficacité des mesures de sécurité mises en œuvre aux fins de la protection des intérêts du SEAE à protéger;

b) des inspections de sécurité des ICUE, qui ont pour but d'évaluer, généralement aux fins d'une homologation, l'efficacité de mesures mises en œuvre aux fins de la protection des ICUE au sein du siège du SEAE et des délégations de l'Union.

Plus particulièrement, les inspections sont notamment menées aux fins suivantes:

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

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

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

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

Conduite des inspections de sécurité du SEAE et comptes rendus y afférents

50. Les inspections de sécurité du SEAE sont conduites par une équipe d'inspection de la direction de la sécurité du SEAE et, si nécessaire, avec l'aide d'experts en sécurité d'autres institutions de l'UE ou États membres.

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.

51. Les inspections de sécurité du SEAE dans les délégations de l'Union peuvent être conduites, si nécessaire, avec l'aide des responsables de la sécurité des ambassades des États membres situées dans les pays tiers.

52. L'autorité de sécurité du SEAE adopte, avant la fin de chaque année civile, le programme d'inspection du SEAE en matière de sécurité pour l'année suivante.

53. Des inspections de sécurité qui ne sont pas prévues au programme susmentionné peuvent, au besoin, être organisées par l'autorité de sécurité du SEAE.

54. À l'issue de l'inspection de sécurité, les principales conclusions et recommandations sont présentées à l'entité inspectée. Un rapport d'inspection est ensuite établi par l'équipe d'inspection. 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 est transmis à l'autorité de sécurité du SEAE et au chef de l'entité inspectée.

Un rapport périodique est établi sous la responsabilité de la direction de la sécurité du SEAE pour souligner les enseignements qui ont été tirés des inspections effectuées au cours d'une période précise et est examiné par le comité de sécurité du SEAE.

Conduite d'inspections de sécurité et comptes rendus y afférents dans les organes et organismes de l'UE établis en vertu du titre V, chapitre 2, du TUE

55. La direction de la sécurité du SEAE peut, le cas échéant, désigner des experts qui apporteront leur contribution via leur participation aux équipes d'inspection conjointes de l'UE dans les organes et organismes de l'Union visés au titre V, chapitre 2, du traité sur l'Union européenne.

Liste de contrôle des inspections de sécurité du SEAE

56. La direction de la sécurité du SEAE établit et met à jour une liste de contrôle des éléments à vérifier au cours d'une inspection de sécurité du SEAE. Cette liste de contrôle est transmise au comité de sécurité du SEAE.

57. 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 A IV

PROTECTION DES ICUE TRAITÉES DANS LES SIC

I. INTRODUCTION

1. La présente annexe énonce les dispositions d'application de l'article 8 de l'annexe A.

2. Les propriétés et les notions d'assurance de l'information (AI) figurant ci-après sont essentielles pour la sécurité et l'exécution correcte des opérations dans le cadre de systèmes d'information et de communication (SIC):

Authenticité:	la garantie que l'information est véridique et émane de sources dignes de foi
Disponibilité:	la caractéristique de l'information selon laquelle elle est accessible et utilisable, à la demande d'une entité autorisée
Confidentialité:	la 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:	la 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 éprouvée, 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 du SEAE 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. La gestion des risques de sécurité vise à appliquer un ensemble de mesures de sécurité offrant un équilibre satisfaisant entre les besoins des utilisateurs et le risque de sécurité résiduel.

7. Les exigences spécifiques, l'étendue et le niveau de détail fixés par l'autorité d'homologation de sécurité (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 concernant les mesures de sécurité mises en œuvre 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.

Bonnes pratiques

13. Le SEAE, le SCG, la Commission 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 les divers SIC traitant des ICUE exploités par le SEAE.

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

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

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

d) *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) *redressement:* mesures de sécurité visant à rétablir la sécurité du SIC.

La rigueur et l'applicabilité de ces mesures de sécurité sont déterminées sur la base d'une évaluation des risques.

17. Les autorités compétentes du SEAE 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 pour répondre aux exigences opérationnelles afin d'éviter tout risque inutile.

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 et à l'organisation dans son ensemble;

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 autorité d'agrément cryptographique (AAC) nationale d'un État membre.

26. Avant d'être recommandés à l'AAC du SEAE pour agrément, en application de l'article 7, paragraphe 5, de la présente décision, 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.

27. Lorsque des motifs opérationnels particuliers le justifient, l'AAC du SEAE, selon le cas, peut, sur recommandation du comité de sécurité du Conseil, 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 l'article 7, paragraphe 5, de la présente décision.

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. La haute représentante 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 (AAI) 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 7, paragraphe 5, de la présente décision, une telle connexion n'est pas considérée comme une interconnexion.

35. Un SIC homologué pour traiter des informations TRES 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 du SEAE.

37. Les supports de données informatiques sont réutilisés, déclassés ou déclassifiés conformément à une politique de sécurité arrêtée en vertu de l'article 7, paragraphe 2, de la présente décision.

Situations d'urgence

38. Nonobstant les dispositions de la présente décision, les procédures spécifiques décrites ci-après peuvent être appliquées, de manière limitée dans le temps, dans les situations d'urgence, telles que les crises, les conflits ou les guerres, imminents ou effectifs, 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 39 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 le paragraphe 39 est invoqué, un rapport est par la suite adressé à la direction de la sécurité du SEAE, qui le communique à son tour au comité de sécurité du SEAE. Ledit rapport contient au moins l'expéditeur, le destinataire et l'autorité d'origine de chaque ICUE.

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

42. Les autorités compétentes en matière d'AI suivantes sont établies au sein du SEAE. 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 (AAI)

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 du SEAE disposent 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 (AAC)

45. L'AAC est chargée de veiller à ce que les produits cryptographiques soient conformes aux politiques respectives en matière cryptographique. Elle agrée les produits cryptographiques pour la protection d'ICUE jusqu'à un certain niveau de classification dans leur environnement opérationnel.

Autorité chargée de la distribution cryptographique (ADC)

46. L'ADC est chargé 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 (AHS)

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 «SSRS»), les documents concernant la vérification de la mise en œuvre des mesures de sécurité et les procédures d'exploitation de sécurité (ci-après «SecOP»), et veiller à ce qu'ils soient conformes aux politiques et aux règles du SEAE 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 SEAE est chargée de l'homologation de tous les SIC exploités dans le cadre de la compétence du SEAE.

Comité d'homologation de sécurité (CHS)

49. 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 SEAE 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 du SCG et 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 SEAE. 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 du SEAE et notifie à celui-ci toute déclaration d'homologation.

Autorité opérationnelle chargée de l'assurance de l'information

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

a) élaborer des documents relatifs à la sécurité conformes à la politique et aux lignes directrices en matière de sécurité, notamment l'énoncé des impératifs de sécurité propres à un système («SSRS»), y compris en ce qui concerne le risque résiduel, les procédures d'exploitation de sécurité («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 A V

SÉCURITÉ INDUSTRIELLE

I. INTRODUCTION

1. La présente annexe contient les modalités d'application de l'article 9 de l'annexe A. Elle prévoit des dispositions de sécurité générales applicables aux entités industrielles ou autres dans le cadre de négociations précontractuelles et tout au long du cycle de vie de contrats classifiés attribués par le SEAE.

2. La haute représentante approuve une politique de sécurité industrielle indiquant en particulier les modalités précises en ce qui concerne les habilitations de sécurité d'établissement («HSE»), les annexes de sécurité («AS»), les visites, la transmission et le transport d'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 SEAE, 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 par le contractant. Dans cette perspective, le SEAE 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 SEAE 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 SEAE 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. La direction de la sécurité du SEAE demande à l'ANS/ASD ou toute autre autorité de sécurité compétente d'un État membre de délivrer une HSE 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). L'accès aux ICUE n'est ni fourni ou accordé à un contractant ou sous-traitant, réel ou potentiel, tant qu'il n'a pas prouvé auprès du SEAE qu'il dispose d'une HSE.

9. S'il y a lieu, le SEAE, 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.

10. Le SEAE, en sa qualité d'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 sous-traitant concerné est immatriculé, ne lui a pas confirmé qu'une HSE appropriée a été délivrée.

11. Le SEAE, en sa qualité d'autorité contractante, demande à l'ANS/ASD ou toute autre autorité de sécurité compétente ayant délivré une HSE de lui notifier toute information défavorable affectant ladite HSE. Dans le cadre d'un contrat de sous-traitance, l'ANS/ASD ou toute autre autorité de sécurité compétente en est informée.

12. Le retrait d'une HSE par l'ANS/ASD concernée ou toute autre autorité de sécurité compétente constitue pour le SEAE, 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. HABILITATIONS DE SÉCURITÉ DU PERSONNEL (HSP) POUR LE PERSONNEL DES CONTRACTANTS

13. Toutes les personnes travaillant pour des contractants ayant besoin d'un accès à des ICUE classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur doivent avoir reçu une habilitation de sécurité adéquate et avoir un besoin d'en connaître pour pouvoir accéder aux informations. Bien qu'une HSP ne soit pas nécessaire pour pouvoir accéder aux ICUE RESTREINT UE/EU RESTRICTED, les personnes concernées devront faire état d'un besoin d'en connaître pour y accéder.

14. Les demandes d'HSP pour les membres du personnel de contractants sont adressées à l'ANS/ASD responsable de l'entité concernée.

15. Le SEAE attire l'attention des contractants souhaitant employer un ressortissant d'un État tiers à un poste nécessitant un accès aux ICUE sur le fait qu'il est de la responsabilité de l'ANS/ASD de l'État membre dans lequel est située et constituée l'entité qui recrute de déterminer si la personne concernée peut accéder à de telles informations, conformément à la présente décision, et de confirmer que l'autorité d'origine doit avoir donné son consentement avant l'octroi de l'accès en question.

V. CONTRATS ET CONTRATS DE SOUS-TRAITANCE CLASSIFIÉS

16. 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.

17. Une fois qu'un contrat ou un contrat de sous-traitance classifié a été attribué, le SEAE, 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.

18. À l'expiration ou à la résiliation d'un tel contrat, le SEAE, 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.

19. 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 ou est résilié.

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

21. Lorsque le contractant ou le sous-traitant est autorisé à conserver des ICUE après l'expiration ou la résiliation 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.

22. Les conditions dans lesquelles le contractant peut sous-traiter des activités sont définies dans l'invitation à soumissionner et le contrat.

23. Un contractant doit obtenir l'autorisation du SEAE, 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.

24. 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.

25. 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.

VI. VISITES LIÉES À DES CONTRATS CLASSIFIÉS

26. Lorsque le SEAE, 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. Et ce sans préjudice du pouvoir des ANS/ASD, dans le cadre de projets spécifiques, de convenir d'une procédure permettant d'organiser directement de telles visites.

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

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

VII. TRANSMISSION ET TRANSPORT DES ICUE

29. En ce qui concerne la transmission des ICUE par voie électronique, les dispositions pertinentes de l'article 8 et de l'annexe A IV s'appliquent.

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

31. 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, s'il implique également le stockage des informations classifiées dans les installations des contractants. Quoi qu'il en soit, le personnel manipulant l'envoi fait l'objet d'une habilitation de sécurité appropriée conformément à l'annexe A 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 le SEAE, le cas échéant en liaison avec les ANS/ASD tant de l'expéditeur que du destinataire ou toute autre autorité de sécurité compétente concernée;

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 le SEAE ou toute autre autorité de sécurité compétente des États de l'expéditeur et du destinataire.

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

32. Les ICUE sont transférées aux contractants et sous-traitants établis dans des pays tiers ayant conclu un accord de sécurité valide avec l'UE conformément aux mesures de sécurité convenues entre le SEAE, en sa qualité d'autorité contractante, et l'ANS/ASD du pays tiers concerné dans lequel le contractant est immatriculé.

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

33. En liaison, s'il y a lieu, avec l'ANS/ASD de l'État membre, le SEAE, 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.

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

35. 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 SEAE qui comportent des informations classifiées RESTREINT UE/EU RESTRICTED.

36. Le SEAE, 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.

37. Les conditions régissant la sous-traitance d'activités par un contractant sont conformes aux paragraphes 22, 23 et 24.

38. Lorsqu'un contrat prévoit le traitement d'informations classifiées RESTREINT UE/EU RESTRICTED dans un SIC exploité par un contractant, le SEAE, 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 A 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 10 de l'annexe A.

II. **CADRES RÉGISSANT L'ÉCHANGE D'INFORMATIONS CLASSIFIÉES**

2. Le SEAE peut échanger des ICUE avec des pays tiers ou des organisations internationales conformément à l'article 10, paragraphe 1, de l'annexe A.

Afin d'aider la HR dans les responsabilités qui lui incombent en vertu de l'article 218 du TFUE:

a) le département géographique ou thématique concerné du SEAE relève, en concertation avec la direction de la sécurité du SEAE, la nécessité de procéder à un échange à long terme d'ICUE avec l'organisation internationale ou le pays tiers concerné, le cas échéant;

b) la direction de la sécurité du SEAE soumet à la HR, après avoir consulté le département géographique concerné du SEAE, les projets de textes à proposer au Conseil, en vertu de l'article 218, paragraphes 3, 5 et 6, du TFUE, le cas échéant;

c) la direction de la sécurité du SEAE soutient la HR dans la conduite de négociations, en coordination avec les services concernés de la Commission et du Secrétariat général du Conseil;

d) pour ce qui est des accords ou des arrangements conclus avec des pays tiers au sujet de leur participation à des opérations PESD de gestion de crise visés à l'article 10, paragraphe 1, point c), de l'annexe A, la direction «Gestion des crises et planification» du SEAE soumet à la HR, après avoir consulté les services concernés du SEAE, les projets de textes à proposer au Conseil en vertu de l'article 218, paragraphes 3, 5 et 6, du TFUE et soutient la HR dans la conduite des négociations en coordination avec les services concernés du SEAE et du Secrétariat général du Conseil, le cas échéant.

3. Dans les cas où les accords sur la sécurité des informations prévoient des modalités techniques d'application à convenir entre la direction de la sécurité du SEAE - en coordination avec la direction de la sécurité de la direction générale des ressources humaines et de la sécurité de la Commission et le bureau de sécurité du Secrétariat général du Conseil – et l'autorité de sécurité compétente de l'État tiers ou de l'organisation internationale en question, de tels arrangements tiennent compte du niveau de protection prévu par les règlements, les structures et les procédures de sécurité en place dans le pays tiers ou l'organisation internationale concerné.

4. Lorsqu'il existe un besoin durable pour le SEAE d'échanger, avec un pays tiers ou une organisation internationale, des informations dont le niveau de classification n'est pas supérieur à RESTREINT UE/EU RESTRICTED, et qu'il a été 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, la HR peut, sous réserve de l'avis unanimement favorable de la direction de la sécurité du SEAE conformément à l'article 14, paragraphe 5, de la présente décision, conclure un arrangement administratif avec les autorités compétentes du pays tiers ou de l'organisation internationale concerné(e).

5. Les ICUE ne font l'objet d'aucun échange par voie électronique avec un pays tiers ou une organisation internationale, sauf disposition expresse de l'accord sur la sécurité des informations ou de l'arrangement administratif.

6. Conformément à un éventuel arrangement administratif sur l'échange d'informations classifiées, le SEAE et le pays tiers ou l'organisation internationale désignent chacun un bureau d'ordre qui fera office de principal point d'entrée et de sortie pour les informations classifiées échangées. Pour le SEAE, il s'agit de son bureau d'ordre central.

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

III **VISITES D'ÉVALUATION**

8. Les visites d'évaluation visées à l'article 16 de la présente décision sont réalisées d'un commun accord avec le pays tiers ou l'organisation internationale concerné(e), et sont axées sur:

a) le cadre réglementaire applicable à la protection des informations classifiées;

b) toute caractéristique spécifique des dispositions législatives et réglementaires, politiques ou procédures en matière de sécurité du pays tiers ou de l'organisation internationale susceptibles d'avoir un impact sur le niveau maximal de classification des ICUE qui peuvent être échangées;

c) les mesures et procédures de sécurité en vigueur pour la protection des informations classifiées; et

d) les procédures d'habilitation de sécurité pour le niveau de classification des ICUE à communiquer.

9. Les ICUE ne font l'objet d'aucun échange avant qu'une visite d'évaluation n'ait été conduite et que le niveau auquel les informations classifiées peuvent être échangées entre les parties n'ait été déterminé, sur la base de l'équivalence du niveau de protection qui leur sera attribué.

Si, dans l'attente d'une telle visite d'évaluation, une raison exceptionnelle ou urgente d'échanger des informations classifiées est portée à la connaissance de la HR, le SEAE:

a) demande tout d'abord le consentement écrit de l'autorité d'origine afin d'établir l'absence d'objection à la communication;

b) s'en réfère à l'autorité de sécurité du SEAE, qui peut décider de communiquer les informations concernées, après obtention de l'avis unanimement favorable des États membres tels que représentés au comité de sécurité du SEAE.

Si, toutefois, le SEAE est dans l'impossibilité de déterminer l'autorité d'origine, l'autorité de sécurité du SEAE endosse la responsabilité de l'autorité d'origine après avoir obtenu l'avis unanimement favorable du comité de sécurité du SEAE.

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

10. En présence d'un accord d'échange d'informations classifiées avec un pays tiers ou une organisation internationale en vertu de l'article 10, paragraphe 1, de l'annexe A, la décision de communiquer des ICUE par le SEAE à un pays tiers ou une organisation internationale est prise par l'autorité de sécurité du SEAE, qui peut déléguer cette autorisation à de hauts fonctionnaires du SEAE ou à d'autres personnes sous son autorité.

11. Si l'autorité d'origine des informations classifiées à communiquer, y compris les autorités d'origine des sources qu'elles peuvent contenir, n'est pas le SEAE, ce dernier demande tout d'abord à l'autorité d'origine de confirmer par écrit qu'elle ne s'oppose pas à la communication des informations en question. Si le SEAE est dans l'impossibilité de déterminer l'autorité d'origine, l'autorité de sécurité du SEAE endosse la responsabilité de l'autorité d'origine après avoir obtenu l'avis unanimement favorable des États membres représentés au sein du comité de sécurité du SEAE.

V. COMMUNICATION AD HOC EXCEPTIONNELLE D'ICUE

12. En l'absence de l'un des cadres visés à l'article 10, paragraphe 1, de l'annexe A, et dans les cas où les intérêts de l'UE ou d'un ou de plusieurs États membres requièrent la communication d'ICUE pour des raisons politiques, opérationnelles ou urgentes, les ICUE peuvent exceptionnellement être communiquées à un pays tiers ou une organisation internationale dès que les mesures suivantes ont été prises.

Après s'être assurée que les conditions énumérées au paragraphe 11 ci-dessus sont réunies, la direction de la sécurité du SEAE:

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 du SEAE à formuler, sur la base des informations disponibles, un avis 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;

c) s'en réfère à l'autorité de sécurité du SEAE, qui peut décider de communiquer les informations concernées, après obtention de l'avis unanimement favorable des États membres tels que représentés au comité de sécurité du SEAE.

13. En l'absence de l'un des cadres visés à l'article 10, paragraphe 1, de l'annexe A, la tierce partie en question s'engage par écrit à protéger adéquatement les ICUE.

APPENDICE A

DÉFINITIONS

Aux fins de la présente décision, on entend par:

«acceptation des risques», la décision d'accepter qu'un risque résiduel subsiste au terme du traitement des risques;

«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 — voir annexe A V, section II;

«assurance de l'information» (AI) dans le domaine des systèmes d'information et de communication, 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 — voir article 8, paragraphe 1, de l'annexe A;

«autorisation d'accès aux ICUE», une autorisation que prend l'autorité de sécurité du SEAE en conformité avec la présente décision après qu'une HSP a été délivrée par les autorités compétentes d'un État membre, 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 — voir article 2 de l'annexe A I;

«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;

«autorité d'origine», l'institution, l'organe ou l'organisme de l'UE, l'État membre, le pays tiers ou l'organisation internationale sous l'autorité de laquelle les informations classifiées ont été créées et/ou introduites dans les structures de l'UE;

«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;

«communication des risques», le fait de sensibiliser la communauté des utilisateurs du SIC aux risques, d'informer les autorités d'homologation de ces risques et de faire rapport à leur sujet aux autorités responsables de l'exploitation;

«compromission d'ICUE», la divulgation totale ou partielle d'ICUE à des personnes ou entités non autorisées — voir article 8, paragraphe 2;

«contractant», une personne ou une entité juridique dotées de la capacité juridique de conclure des contrats;

«contrat classifié», un contrat conclu par le SEAE 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 SEAE 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 nécessite ou implique l'accès à des informations classifiées de l'Union européenne ou la production 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;

«énoncé des impératifs de sécurité propres à un système» (SSRS), ensemble contraignant de principes de sécurité à respecter et d'impératifs de sécurité détaillés à mettre en œuvre, sous-tendant la procédure de certification et d'accréditation des SIC;

«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», l'application de procédures permettant de garder la trace du cycle de vie d'une information, y compris de sa diffusion et de sa destruction. Voir annexe A III, paragraphe 21;

«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;

«évaluation des risques», le fait de 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;

«gestion des informations classifiées», 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 5, 6 et 8 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, le traitement, le stockage et la destruction des ICUE — voir article 7, paragraphe 1, de l'annexe A;

«guide de 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 re-classifiés ou déclassés; lorsqu'il existe, le GCS fait partie de l'AS — voir annexe A V, section II;

«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) 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»;

«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), 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 — voir article 2, point f);

«infraction», un acte ou une omission commis par une personne qui est contraire aux règles de sécurité énoncées dans la présente décision et/ou aux politiques ou lignes directrices en matière de sécurité énonçant les éventuelles mesures nécessaires à sa mise en œuvre;

«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», aux fins de la présente décision, 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 — voir annexe A IV, paragraphe 31;

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

«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», 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;

— en ce qui concerne l'accès à des informations CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, ont fait l'objet d'une habilitation de sécurité du niveau correspondant, ou ont été dûment autorisées en vertu de leurs fonctions conformément aux lois et réglementations nationales; et

— été informées de leurs responsabilités —

voir article 5, paragraphe 1, de l'annexe A;

«opération PSDC», une opération militaire ou civile de gestion de crise mise en place en vertu du titre V, chapitre 2, du TUE;

«procédures d'exploitation de sécurité» (SecOPs), description des mesures de mises en œuvre de la politique de sécurité à adopter, des procédures d'exploitation à suivre et des responsabilités du personnel;

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

«produits cryptographiques», 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;

«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;

«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», 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 — voir article 9, paragraphe 1, de l'annexe A;

«sécurité physique», l'application de mesures physiques et techniques de protection pour dissuader l'accès non autorisé aux ICUE — voir article 6 de l'annexe A;

«système d'information et de communication» (SIC), tout système permettant le traitement d'informations sous forme électronique. Un système d'information et de communication comprend l'ensemble des moyens nécessaires pour le faire fonctionner, y compris l'infrastructure, l'organisation, le personnel et les ressources d'information; voir article 8, paragraphe 2, de l'annexe A;

«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;

«traitement des risques», le fait d'atténuer, d'éliminer, de réduire (par un ensemble approprié de mesures sur le plan technique, physique ou au niveau de l'organisation ou des procédures), de transférer ou de surveiller les risques;

«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.

INFORMATIONS PROVENANT DES ÉTATS MEMBRES

Renseignements communiqués par les États membres sur les aides d'État accordées conformément au règlement (CE) n° 800/2008 de la Commission déclarant certaines catégories d'aide compatibles avec le marché commun en application des articles 87 et 88 du traité (règlement général d'exemption par catégorie)

(Texte présentant de l'intérêt pour l'EEE)

(2013/C 190/02)

Numéro de référence de l'aide d'État	SA.30208 (X 17/10)
État membre	Pays-Bas
Numéro de référence de l'État membre	Verlenging O&Oprogramma SKB
Nom de la région (NUTS)	Régions non assistées
Organe octroyant l'aide	Ministerie VROM/BJZ Internationaal Postbus 20951 IPC 880 2500 EZ Den Haag e-mail: djz.internationaal@minvrom.nl www.minvrom.nl
Titre de la mesure d'aide	Subsidie onderzoeks- en ontwikkelingsprogramma Stichting Kennisontwikkeling en Kennisoverdracht Bodem 2010-2014
Base juridique nationale (référence à la publication officielle nationale concernée)	Individueel subsidiebesluit op grond van de Algemene wet bestuursrecht en het Besluit Milieusubsidies
Type de mesure	Aide ad hoc
Modification d'une mesure d'aide existante	Prolongation N 230/1999
Date d'octroi	A partir de 8.12.2009
Secteur(s) économique(s) concerné(s)	Secteurs économiques éligibles au bénéfice de l'aide
Type de bénéficiaire	PME,grande entreprise
Montant total de l'aide ad hoc accordée à l'entreprise	EUR 10,00 (millions)
Pour les garanties	EUR 10,00 (millions)
Instrument d'aide (art. 5)	Subvention directe
Référence à la décision de la Commission	—
Si cofinancement par des fonds communautaires	—

Objectifs	Intensité maximale de l'aide en % ou montant maximal de l'aide en devise nationale	Suppléments pour PME en %
Développement expérimental [art. 31, paragraphe 2, point c)]	25 %	20 %
Aides aux études de faisabilité technique (art. 32)	75 %	—
Recherche fondamentale [art. 31, paragraphe 2, point a)]	100 %	—
Recherche industrielle [art. 31, paragraphe 2, point b)]	50 %	20 %

Lien internet vers le texte intégral de la mesure d'aide:

http://www.rijksoverheid.nl/documenten-en-publicaties/brieven/2009/12/08/subsidieaanvraag-stichting-kennisontwikkeling-en-kennisoverdracht-bodem-skb-programma-2010-2014.html

http://www.rijksoverheid.nl/documenten-en-publicaties/brieven/2010/01/26/aanvullende-voorwaarden-groepsvrijstellingsverordening-bij-subsidieaanvraag-stichting-kennisontwikkeling-en-kennisoverdracht-bodem-skb-programma-2010-2014.html

Numéro de référence de l'aide d'État	SA.36154 (13/X)
État membre	Pays-Bas
Numéro de référence de l'État membre	—
Nom de la région (NUTS)	NEDERLAND Article 107(3)(c),Régions non assistées
Organe octroyant l'aide	Ministerie van Financiën Korte Voorhout 7 2511 CW Den Haag www.overheid.nl
Titre de la mesure d'aide	Teruggaafregeling energiebelasting op elektriciteit voor energie-intensieve bedrijven
Base juridique nationale (référence à la publication officielle nationale concernée)	Artikel VIIc Belastingplan 2013 (Stb 2012, 668) en inwerkingtreding bij Koninklijk Besluit (Stb 2012, 672)
Type de mesure	Régime d'aide
Modification d'une mesure d'aide existante	—
Durée	1.1.2013-31.12.2020
Secteur(s) économique(s) concerné(s)	Secteurs économiques éligibles au bénéfice de l'aide
Type de bénéficiaire	grande entreprise
Montant annuel total du budget prévu au titre du régime	EUR 6,50 (millions)
Pour les garanties	EUR 6,50 (millions)
Instrument d'aide (art. 5)	Autre forme d'avantage fiscal
Référence à la décision de la Commission	—
Si cofinancement par des fonds communautaires	—

Objectifs	Intensité maximale de l'aide en % ou montant maximal de l'aide en devise nationale	Suppléments pour PME en %
Aides sous forme de réductions de taxes environnementales (art. 25)	110 000 EUR	—

Lien internet vers le texte intégral de la mesure d'aide:

https://zoek.officielebekendmakingen.nl/stb-2012-668.html?zoekcriteria=%3fzkt%3dUitgebreid%26pst%3dStaatsblad%26dpr%3dAlle%26spd%3d20130128%26epd%3d20130128%26jgp%3d2012%26nrp%3d668%26sdt%3dDatumUitgifte%26planId%3d%26pnr%3d1%26rpp%3d10&resultIndex=0&sorttype=1&sortorder=4

http:/www.overheid.nl -> Staatsblad -> jaargang 2012 + nummer 668

https://zoek.officielebekendmakingen.nl/stb-2012-672.html?zoekcriteria=%3fzkt%3dUitgebreid%26pst%3dStaatsblad%26dpr%3dAlle%26spd%3d20130128%26epd%3d20130128%26jgp%3d2012%26nrp%3d672%26sdt%3dDatumUitgifte%26planId%3d%26pnr%3d1%26rpp%3d10&resultIndex=0&sorttype=1&sortorder=4

http:/www.overheid.nl -> Staatsblad -> jaargang 2012 + nummer 672

Numéro de référence de l'aide d'État	SA.36370 (13/X)
État membre	Pologne
Numéro de référence de l'État membre	PL
Nom de la région (NUTS)	Jeleniogórsko-walbrzyski Article 107(3)(a)
Organe octroyant l'aide	Minister Gospodarki PL. Trzech Krzyży 3/5 www.mg.gov.pl
Titre de la mesure d'aide	Mando Corporation Poland Sp. z o.o.
Base juridique nationale (référence à la publication officielle nationale concernée)	„Program wspierania inwestycji o istotnym znaczeniu dla gospodarki polskiej na lata 2011-2020", przyjęty przez Radę Ministrów w dniu 5 lipca 2011 (Uchwała Rady Ministrów Nr 122/2011) na podstawie art. 19 ust. 2 ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (Dz. U. z 2009 r. Nr 84, poz. 712 i Nr 157, poz. 1241) zmieniony uchwałą Rady Ministrów z dnia 20 marca 2012 r. (Nr 39/2012).
Type de mesure	Aide ad hoc
Modification d'une mesure d'aide existante	—
Date d'octroi	A partir de 28.11.2012
Secteur(s) économique(s) concerné(s)	Fabrication d'autres équipements automobiles
Type de bénéficiaire	grande entreprise — Mando Corporation Poland Sp. z o.o.
Montant total de l'aide ad hoc accordée à l'entreprise	PLN 15,11 (millions)
Pour les garanties	PLN 15,11 (millions)
Instrument d'aide (art. 5)	Subvention directe
Référence à la décision de la Commission	—
Si cofinancement par des fonds communautaires	—

Objectifs	Intensité maximale de l'aide en % ou montant maximal de l'aide en devise nationale	Suppléments pour PME en %
Aides ad hoc (art.13.1)	3,9 %	0 %

Lien internet vers le texte intégral de la mesure d'aide:

http://www.mg.gov.pl/Wspieranie+przedsiebiorczosci/Wsparcie+finansowe+i+inwestycje/Pomoc+na+inwestycje+o+istotnym+znaczeniu+dla+gospodarki

---

Numéro de référence de l'aide d'État	SA.36382 (13/X)
État membre	Autriche
Numéro de référence de l'État membre	—
Nom de la région (NUTS)	WIEN Régions non assistées

Organe octroyant l'aide	MA 5 der Stadt Wien Ebendorferstraße 2, 1082 Wien www.wien.gv.at
Titre de la mesure d'aide	WIEN WORK — Integrativer Betrieb, Förderung Ausbildungs- und Produktionsstätte für behinderte Personen, Förderung gem. Art 42 AGVO
Base juridique nationale (référence à la publication officielle nationale concernée)	Beschluss des Wiener Gemeinderates vom 1.3.2013, siehe beigefügte Anlagen
Type de mesure	Aide ad hoc
Modification d'une mesure d'aide existante	—
Date d'octroi	A partir de 1.3.2013
Secteur(s) économique(s) concerné(s)	Secteurs économiques éligibles au bénéfice de l'aide
Type de bénéficiaire	grande entreprise — Wien Work — Integrative Betriebe und AusbildungsGmbH, Gemeinnützige GmbH., Unterneghmensgegenstand:
Montant total de l'aide ad hoc accordée à l'entreprise	EUR 5,00 (millions)
Pour les garanties	EUR 5,00 (millions)
Instrument d'aide (art. 5)	Subvention directe
Référence à la décision de la Commission	—
Si cofinancement par des fonds communautaires	—

Objectifs	Intensité maximale de l'aide en % ou montant maximal de l'aide en devise nationale	Suppléments pour PME en %
Aides destinées à compenser les surcoûts liés à l'emploi de travailleurs handicapés (art. 42)	81 %	—

Lien internet vers le texte intégral de la mesure d'aide:

https://www.wien.gv.at/infodat/ergdt?detvid=103242

Numéro de référence de l'aide d'État	SA.36383 (13/X)
État membre	Royaume-Uni
Numéro de référence de l'État membre	N/A
Nom de la région (NUTS)	NORTHERN IRELAND Article 107(3)(c)
Organe octroyant l'aide	Department of Agriculture and Rural Development (Northern Ireland) DARD Science, Evidence and Innovation Policy Division Room 359 Dundonald House Belfast BT4 3SB http://www.dardni.gov.uk/
Titre de la mesure d'aide	Agricultural Research and Development Scheme (Northern Ireland) 2013 — 2020
Base juridique nationale (référence à la publication officielle nationale concernée)	Agriculture Act (Northern Ireland) 1949 Agriculture (Northern Ireland) Order 2004

Type de mesure	Régime d'aide
Modification d'une mesure d'aide existante	—
Durée	1.4.2013-31.3.2020
Secteur(s) économique(s) concerné(s)	Culture et production animale, chasse et services annexes
Type de bénéficiaire	PME,grande entreprise
Montant annuel total du budget prévu au titre du régime	GBP 1,00 (millions)
Pour les garanties	GBP 1,00 (millions)
Instrument d'aide (art. 5)	Subvention directe
Référence à la décision de la Commission	—
Si cofinancement par des fonds communautaires	—

Objectifs	Intensité maximale de l'aide en % ou montant maximal de l'aide en devise nationale	Suppléments pour PME en %
Aides à la recherche et au développement dans les secteurs de l'agriculture et de la pêche (art. 34)	100 %	—

Lien internet vers le texte intégral de la mesure d'aide:

http://www.dardni.gov.uk/index/strategies-reports-accounts/dard-research-section/agriculture-research-and-development-scheme.htm

---

Numéro de référence de l'aide d'État	SA.36496 (13/X)
État membre	Autriche
Numéro de référence de l'État membre	—
Nom de la région (NUTS)	NIEDEROESTERREICH Zones mixtes
Organe octroyant l'aide	Amt der NÖ Landesregierung Landhausplatz 1, 3109 St. Pölten www.noel.gv.at bzw. www.nafes.at
Titre de la mesure d'aide	Neufassung der NAFES-Förderungsrichtlinien
Base juridique nationale (référence à la publication officielle nationale concernée)	NAFES Förderrichtlinien (Kennzeichen: RU2-N-133/077-2012 — Beschluß der Landesregierung)
Type de mesure	Régime d'aide
Modification d'une mesure d'aide existante	—
Durée	26.2.2013-31.12.2017
Secteur(s) économique(s) concerné(s)	Secteurs économiques éligibles au bénéfice de l'aide
Type de bénéficiaire	PME
Montant annuel total du budget prévu au titre du régime	EUR 1,20 (millions)
Pour les garanties	EUR 1,20 (millions)

Instrument d'aide (art. 5)	Subvention directe	
Référence à la décision de la Commission	—	
Si cofinancement par des fonds communautaires	—	
Objectifs	Intensité maximale de l'aide en % ou montant maximal de l'aide en devise nationale	Suppléments pour PME en %
Régime d'aide	20 %	0 %
Aides à l'investissement et à l'emploi en faveur des PME (art.15)	20 %	—

Lien internet vers le texte intégral de la mesure d'aide:

http://www.nafes.at

http://www.nafes.at/foerderung/formulare_und_leitfaeden — siehe „Förderrichtlinie"

Numéro de référence de l'aide d'État	SA.36505 (13/X)
État membre	Grèce
Numéro de référence de l'État membre	GR
Nom de la région (NUTS)	KENTRIKI MAKEDONIA, DYTIKI ELLADA, ATTIKI Article 107(3)(a)
Organe octroyant l'aide	GENERAL SECRETARIAT FOR RESEARCH AND TECHNOLOGY 14-18 MESOGEION AV 115 10 ATHENS GREECE http:/www.gsrt.gr
Titre de la mesure d'aide	Funding of Research Proposals Positively Evaluated under the 5th Call of ERC Grant Schemes
Base juridique nationale (référence à la publication officielle nationale concernée)	Law 1514/1985 and its amendment, Law 3614/07 and its amendments, Ministerial Decision 14053/EIS 1749/27.3.2008 (FEK — Official Journal of Greek Government — 540/B/27.3.2008) and its amendments (43804/EYTHY 2041/7.9.2009 — FEK 1957/B/9.9.2009), 28020/EYTHI 1212/30.6.2010 — FEK 1088/B/19.7.2010), 5058/EYTHI 138/5-2-13 (FEK 292/B/13.2.2013)
Type de mesure	Régime d'aide
Modification d'une mesure d'aide existante	—
Durée	20.3.2013-31.12.2015
Secteur(s) économique(s) concerné(s)	Recherche développement scientifique
Type de bénéficiaire	grande entreprise
Montant annuel total du budget prévu au titre du régime	EUR 0,83 (millions)
Pour les garanties	EUR 0,83 (millions)
Instrument d'aide (art. 5)	Subvention directe
Référence à la décision de la Commission	—
Si cofinancement par des fonds communautaires	ESF — EUR 2,07 (millions)

Objectifs	Intensité maximale de l'aide en % ou montant maximal de l'aide en devise nationale	Suppléments pour PME en %
Développement expérimental [art. 31, paragraphe 2, point c)]	40 %	0 %
Recherche fondamentale [art. 31, paragraphe 2, point a)]	100 %	—
Recherche industrielle [art. 31, paragraphe 2, point b)]	65 %	0 %

Lien internet vers le texte intégral de la mesure d'aide:

http://www.gsrt.gr/central.aspx?sId=108I334I1106I646I444510&olID=671&neID=673&neTa=1_300_1&ncID=0&neHC=0&tbid=0&lrID=2&oldUIID=aI671I0I108I334I1106I0I2&actionID=load&JScript=1

Δράσεις Ενίσχυσης E&T › Τρέχουσες Εθνικές Δράσεις › Ενεργές προκηρύξεις ΕΣΠΑ

Numéro de référence de l'aide d'État	SA.36530 (13/X)
État membre	Pays-Bas
Numéro de référence de l'État membre	NLD
Nom de la région (NUTS)	OVERIJSSEL Régions non assistées
Organe octroyant l'aide	Provincie Overijssel Postbus 10078 8000 GB Zwolle www.overijssel.nl
Titre de la mesure d'aide	Rijden op groen gas en electriciteit (aanschaf vrachtwagens)
Base juridique nationale (référence à la publication officielle nationale concernée)	Subsidieregeling Rijden op groen gas en electriciteit, in werking treding op 4 april 2013. Publicatie Provinciaal blad nr. 2013/0115269
Type de mesure	Régime d'aide
Modification d'une mesure d'aide existante	—
Durée	4.4.2013-31.12.2013
Secteur(s) économique(s) concerné(s)	Secteurs économiques éligibles au bénéfice de l'aide
Type de bénéficiaire	PME
Montant annuel total du budget prévu au titre du régime	EUR 0,55 (millions)
Pour les garanties	EUR 0,55 (millions)
Instrument d'aide (art. 5)	Subvention directe
Référence à la décision de la Commission	—
Si cofinancement par des fonds communautaires	—

Objectifs	Intensité maximale de l'aide en % ou montant maximal de l'aide en devise nationale	Suppléments pour PME en %
Aides à l'acquisition de nouveaux véhicules de transport qui vont au-delà des normes communautaires ou qui augmentent le niveau de protection de l'environnement en l'absence de normes communautaires (art.19)	3 %	0 %

Lien internet vers le texte intégral de la mesure d'aide:

http://www.overijssel.nl/loket/provinciale/uitvoeringsbesluit_subsidies_overijssel_2011

www.overijssel.nl, loket, provinciale regelingen, uitvoeringsbesluit subsidies Overijssel 2011, Hoofdstuk 8, paragraaf 8.11

Numéro de référence de l'aide d'État	SA.36540 (13/X)
État membre	Allemagne
Numéro de référence de l'État membre	—
Nom de la région (NUTS)	MERZIG-WADERN Régions non assistées
Organe octroyant l'aide	EVTZ Interreg IV A Großregion Préfecture de la Région Lorraine SGAR — Direction des Affaires Européennes GECT — Autorité de gestion Programme Interreg IV A Grande Région 36 place Saint Thiébault BP 71014 F-57034 METZ Cedex 1 www.interreg-4agr.eu
Titre de la mesure d'aide	Initiative Précise: Initiative zur Optimierung der präzisen elektrochemischen Prozesse für industrielle Serienfertigung in der Großregion
Base juridique nationale (référence à la publication officielle nationale concernée)	Gesetz Nr. 938 betreffend Haushaltsordnung des Saarlandes (LHO) Vom 3. November 1971 in der Fassung der Bekanntmachung vom 5. November 1999 (Amtsbl. des Saarlandes 2000 S. 194), zuletzt geändert durch Art. 5 des Gesetzes vom 1. Dezember 2011 (Amtsbl. des Saarlandes I S. 556)
Type de mesure	Aide ad hoc
Modification d'une mesure d'aide existante	—
Date d'octroi	A partir de 22.11.2012
Secteur(s) économique(s) concerné(s)	Fabrication d'autres articles de robinetterie
Type de bénéficiaire	PME — MHA Zentgraf GmbH & Co.KG
Montant total de l'aide ad hoc accordée à l'entreprise	EUR 0,20 (millions)
Pour les garanties	EUR 0,20 (millions)
Instrument d'aide (art. 5)	Subvention directe
Référence à la décision de la Commission	—
Si cofinancement par des fonds communautaires	103 GR 1 1 223 — EUR 0,20 (millions)

Objectifs	Intensité maximale de l'aide en % ou montant maximal de l'aide en devise nationale	Suppléments pour PME en %
Recherche industrielle [art. 31, paragraphe 2, point b)]	50 %	0 %

Lien internet vers le texte intégral de la mesure d'aide:

http://www.interreg-4agr.eu/de/projet-liste.php#

Numéro de référence de l'aide d'État	SA.36551 (13/X)
État membre	Italie
Numéro de référence de l'État membre	ITD5
Nom de la région (NUTS)	EMILIA-ROMAGNA Zones mixtes
Organe octroyant l'aide	Direzione Attività Produttive, Commercio e Turismo della Regione Emilia-Romagna/Direzione Generale A Direzione Attività Produttive: Viale Aldo Moro, 44 — 40127 Bologna Direzione Ambiente: Viale Aldo Moro n. 8 — 40127 Bologna http://fesr.regione.emilia-romagna.it/che-cose-il-por-fesr/assi-pagine/asse-3-qualificazione-energetico-ambientale-e-sviluppo-sostenibile www.ermesambiente.it
Titre de la mesure d'aide	POR FESR 2007-2013 — Asse III, Attività III 1.2 e Piano di Azione ambientale per un futuro sostenibile 2008-2010: Modalità e criteri per la concessione di contributi finalizzati alla rimozione dell'amianto dagli edifici, la coibentazione degli edifici e l'installazione di pannelli solari fotovoltaici
Base juridique nationale (référence à la publication officielle nationale concernée)	Delibera della Giunta Regionale del 10 gennaio 2011 n. 15 pubblicata sul BURER n. 14 del 27 gennaio 2011 (parte seconda)
Type de mesure	Régime d'aide
Modification d'une mesure d'aide existante	—
Durée	15.11.2012-30.9.2013
Secteur(s) économique(s) concerné(s)	Secteurs économiques éligibles au bénéfice de l'aide
Type de bénéficiaire	PME
Montant annuel total du budget prévu au titre du régime	EUR 1,02 (millions)
Pour les garanties	EUR 1,02 (millions)
Instrument d'aide (art. 5)	Subvention directe
Référence à la décision de la Commission	—
Si cofinancement par des fonds communautaires	POR FESR «Competitività regionale e occupazione» 2007-2013 regione Emilia-Romagna Decisione C(2007) 3875 — 7.8.2007 Codice CCI n. 2007 IT 16 2 PO 002 — EUR 0,33 (millions)

Objectifs	Intensité maximale de l'aide en % ou montant maximal de l'aide en devise nationale	Suppléments pour PME en %
Aides environnementales en faveur des investissements dans la promotion de l'énergie produite à partir de sources d'énergie renouvelables (art. 23)	45 %	0 %
Aides à l'investissement permettant aux entreprises de dépasser les normes communautaires ou d'augmenter le niveau de protection de l'environnement en l'absence de normes communautaires (art. 18)	45 %	0 %
Aides environnementales en faveur des investissements dans les économies d'énergie (art. 21)	45 %	0 %

Lien internet vers le texte intégral de la mesure d'aide:

http://fesr.regione.emilia-romagna.it/finanziamenti/bandi/bando-fotovoltaico-amianto

Numéro de référence de l'aide d'État	SA.36555 (13/X)
État membre	Pays-Bas
Numéro de référence de l'État membre	Subsidie Energiesprong Flevogebouw
Nom de la région (NUTS)	OVERIJSSEL Régions non assistées
Organe octroyant l'aide	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Directie CZW Postbus 20011 2500 EA Den Haag email: angelique.herwijnen@minbzk.nl www.rijksoverheid.nl/ministeries/bzk
Titre de la mesure d'aide	Subsidie energiesprong Consortium Flevogebouw Zwolle
Base juridique nationale (référence à la publication officielle nationale concernée)	Subsidiebesluit experimenten en kennisoverdracht wonen Geldend op 18.4.2013 http://wetten.overheid.nl/BWBR0020333/geldigheidsdatum_18-04-2013 Regeling Subsidiebesluit experimenten en kennisoverdracht wonen Geldend op 18.4.2013 http://wetten.overheid.nl/BWBR0020311/geldigheidsdatum_18-04-2013
Type de mesure	Aide ad hoc
Modification d'une mesure d'aide existante	—
Date d'octroi	A partir de 21.2.2013
Secteur(s) économique(s) concerné(s)	Travaux de plomberie et installation de chauffage et de conditionnement d'air, Promotion immobilière, Construction de bâtiments résidentiels et non résidentiels
Type de bénéficiaire	PME,grande entreprise — Bemog Projectontwikkeling; Nikkels Bouwbedrijf; Seinen Energy solutions; Brenorm Installatiegroep
Montant total de l'aide ad hoc accordée à l'entreprise	EUR 0,18 (millions)
Pour les garanties	EUR 0,18 (millions)
Instrument d'aide (art. 5)	Subvention directe
Référence à la décision de la Commission	—
Si cofinancement par des fonds communautaires	—

Objectifs	Intensité maximale de l'aide en % ou montant maximal de l'aide en devise nationale	Suppléments pour PME en %
Aides environnementales en faveur des investissements dans les économies d'énergie (art. 21)	40 %	0 %

Lien internet vers le texte intégral de la mesure d'aide:

http://www.rijksoverheid.nl/documenten-en-publicaties/besluiten/2013/03/14/beschikking-subsidie-energiesprong-flevogebouw.html

---

Numéro de référence de l'aide d'État	SA.36572 (13/X)
État membre	Espagne
Numéro de référence de l'État membre	ES51
Nom de la région (NUTS)	CATALUNA Zones mixtes

Organe octroyant l'aide	Departamento de Empresa y Ocupación; Dirección general de Economía Social y Cooperativa i Trabajo Au Sepúlveda, 148-150 08011 Barcelona http://www.gencat.cat/temes/cat/treball.htm
Titre de la mesure d'aide	Acciones relativas a las unidades de apoyo a la actividad profesional en el marco de servicios de ayuda personal y social a las personas con discapacidad en los centros especiales de empleo.
Base juridique nationale (référence à la publication officielle nationale concernée)	Orden EMO/66/2012, de 21 de marzo, por la que se aprueban las bases reguladoras para la concesión de subvenciones destinadas a la realización de acciones relativas a las unidades de apoyo a la actividad profesional en el marco de los servicios de ajuste personal y social de las personas con discapacidad en los centros especiales de empleo, y se abre la convocatoria para el año 2012. RESOLUCIÓN EMO/577/2013, de 19 de marzo, de convocatoria para el año 2013
Type de mesure	Régime d'aide
Modification d'une mesure d'aide existante	—
Durée	1.1.2012-31.12.2013
Secteur(s) économique(s) concerné(s)	Secteurs économiques éligibles au bénéfice de l'aide
Type de bénéficiaire	PME,grande entreprise
Montant annuel total du budget prévu au titre du régime	EUR 41,00 (millions)
Pour les garanties	EUR 41,00 (millions)
Instrument d'aide (art. 5)	Subvention directe
Référence à la décision de la Commission	—
Si cofinancement par des fonds communautaires	—

Objectifs	Intensité maximale de l'aide en % ou montant maximal de l'aide en devise nationale	Suppléments pour PME en %
Aides destinées à compenser les surcoûts liés à l'emploi de travailleurs handicapés (art. 42)	70 %	—

Lien internet vers le texte intégral de la mesure d'aide:

http://portaldogc.gencat.cat/utilsEADOP/PDF/6095/1232356.pdf

http://portaldogc.gencat.cat/utilsEADOP/PDF/6341/1291415.pdf

Numéro de référence de l'aide d'État	SA.36583 (13/X)
État membre	Hongrie
Numéro de référence de l'État membre	—
Nom de la région (NUTS)	Hungary Article 107(3)(a),Article 107(3)(c)
Organe octroyant l'aide	Garantiqa Hitelgarancia Zrt. 1082 Budapest, Kisfaludy u. 32. www.garantiqa.hu
Titre de la mesure d'aide	A Garantiqa Hitelgarancia Zrt által kezességvállalási díj csökkentése formájában nyújtott beruházási támogatás

Base juridique nationale (référence à la publication officielle nationale concernée)	2008. évi CII. törvény a Magyar Köztársaság 2009. évi költségvetéséről, 2012. évi CCIV törvény a Magyar Köztársaság 2013. évi költségvetéséről, 48/2002. (XII.28) PM rendelet a költségvetési viszontgaranciavállalásának és érvényesítésének részletes szabályairól
Type de mesure	Régime d'aide
Modification d'une mesure d'aide existante	—
Durée	13.5.2009-31.12.2013
Secteur(s) économique(s) concerné(s)	Secteurs économiques éligibles au bénéfice de l'aide
Type de bénéficiaire	PME
Montant annuel total du budget prévu au titre du régime	HUF 6 000,00 (millions)
Pour les garanties	HUF 6 000,00 (millions)
Instrument d'aide (art. 5)	Garantie
Référence à la décision de la Commission	—
Si cofinancement par des fonds communautaires	—

Objectifs	Intensité maximale de l'aide en % ou montant maximal de l'aide en devise nationale	Suppléments pour PME en %
Aides à l'acquisition de nouveaux véhicules de transport qui vont au-delà des normes communautaires ou qui augmentent le niveau de protection de l'environnement en l'absence de normes communautaires (art.19)	35 %	20 %
Aides environnementales en faveur des investissements dans les économies d'énergie (art. 21)	60 %	20 %
Aides environnementales en faveur des investissements dans la promotion de l'énergie produite à partir de sources d'énergie renouvelables (art. 23)	45 %	20 %
Recherche fondamentale [art. 31, paragraphe 2, point a)]	100 %	—
Recherche industrielle [art. 31, paragraphe 2, point b)]	50 %	20 %
Développement expérimental [art. 31, paragraphe 2, point c)]	25 %	20 %
Régime d'aide	50 %	20 %
Aides à l'investissement permettant aux entreprises de dépasser les normes communautaires ou d'augmenter le niveau de protection de l'environnement en l'absence de normes communautaires (art. 18)	35 %	20 %

Lien internet vers le texte intégral de la mesure d'aide:

http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0800102.TV

http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200204.TV

http://www.njt.hu/cgi_bin/njt_doc.cgi?docid=65457.92922

http://www.garantiqa.hu/hu/letoltheto-dokumentumok/uzletszabalyzataink

http://www.njt.hu/cgi_bin/njt_doc.cgi?docid=65457.92920

Numéro de référence de l'aide d'État	SA.36607 (13/X)
État membre	Espagne
Numéro de référence de l'État membre	—
Nom de la région (NUTS)	GALICIA Article 107(3)(a)
Organe octroyant l'aide	Instituto Enerxético de Galicia (Inega) C/ Avelino Pousa Antelo, núm. 5 15707 (San Lázaro) Santiago de Compostela (A Coruña) http://www.inega.es/?idioma=es
Titre de la mesure d'aide	Ayudas del Inega para proyectos de energías renovables
Base juridique nationale (référence à la publication officielle nationale concernée)	Resolución de 9 de abril de 2013 [Diario Oficial de Galicia (DOG) núm.73, de 16 de abril] por la que se establecen las bases reguladoras y se anuncia la convocatoria de subvenciones para el año 2013 a proyectos de energías renovables, con financiación procedente de fondos comunitarios derivados del Programa Operativo Feder Galicia 2007-2013
Type de mesure	Régime d'aide
Modification d'une mesure d'aide existante	—
Durée	22.4.2013-31.10.2013
Secteur(s) économique(s) concerné(s)	Secteurs économiques éligibles au bénéfice de l'aide
Type de bénéficiaire	PME,grande entreprise
Montant annuel total du budget prévu au titre du régime	EUR 2,10 (millions)
Pour les garanties	EUR 2,10 (millions)
Instrument d'aide (art. 5)	Subvention directe
Référence à la décision de la Commission	—
Si cofinancement par des fonds communautaires	Feder 2007-2013 — EUR 1,10 (millions)

Objectifs	Intensité maximale de l'aide en % ou montant maximal de l'aide en devise nationale	Suppléments pour PME en %
Aides environnementales en faveur des investissements dans la promotion de l'énergie produite à partir de sources d'énergie renouvelables (art. 23)	45 %	20 %

Lien internet vers le texte intégral de la mesure d'aide:

http://www.xunta.es/dog/Publicados/2013/20130416/AnuncioO3G1-090413-0001_es.pdf

---

Numéro de référence de l'aide d'État	SA.36611 (13/X)
État membre	Allemagne
Numéro de référence de l'État membre	612-40306-BY/0008
Nom de la région (NUTS)	BAYERN Article 107(3)(c)

Organe octroyant l'aide	Technologie- und Förderzentrum im Kompetenzzentrum für Nachwachsende Rohstoffe Schulgasse 18, 94315 Straubing www.tfz.bayern.de
Titre de la mesure d'aide	Bayern: Demonstrationsmaßnahmen zur Nutzung von Biomasse als regenerativer Energieträger (BioSol)
Base juridique nationale (référence à la publication officielle nationale concernée)	Richtlinie zur Förderung von Demonstrationsvorhaben zur Nutzung von Biomasse als regenerativer Energieträger (BioSol), Art. 23 und 44 der Bayerischen Haushaltsordnung und die Verwaltungsvorschriften hierzu.
Type de mesure	Régime d'aide
Modification d'une mesure d'aide existante	—
Durée	1.5.2013-30.6.2014
Secteur(s) économique(s) concerné(s)	Secteurs économiques éligibles au bénéfice de l'aide
Type de bénéficiaire	PME,grande entreprise
Montant annuel total du budget prévu au titre du régime	EUR 0,70 (millions)
Pour les garanties	EUR 0,70 (millions)
Instrument d'aide (art. 5)	Subvention directe
Référence à la décision de la Commission	—
Si cofinancement par des fonds communautaires	—

Objectifs	Intensité maximale de l'aide en % ou montant maximal de l'aide en devise nationale	Suppléments pour PME en %
Aides environnementales en faveur des investissements dans la promotion de l'énergie produite à partir de sources d'énergie renouvelables (art. 23)	30 %	10 %

Lien internet vers le texte intégral de la mesure d'aide:

http://www.stmelf.bayern.de/mam/cms01/agrarpolitik/dateien/b_rili_biosol_2013.pdf

---

Numéro de référence de l'aide d'État	SA.36747 (13/X)
État membre	Royaume-Uni
Numéro de référence de l'État membre	—
Nom de la région (NUTS)	UNITED KINGDOM Article 107(3)(a),Article 107(3)(c),Régions non assistées,Zones mixtes
Organe octroyant l'aide	Department of Energy and Climate Change 3 Whitehall Place, London, SW1A 2AW https://www.gov.uk/renewable-heat-premium-payment-scheme#overview
Titre de la mesure d'aide	Amalgamation of all previous and future phases of Renewable Heat Premium Payment — Social Housing Competitions
Base juridique nationale (référence à la publication officielle nationale concernée)	Section 153 of Environmental Protection Act 1990

Type de mesure	Régime d'aide	
Modification d'une mesure d'aide existante	SA.36747 replaces SA.34995, SA.35310, SA.34994, SA.35312, SA.34795, SA.34996 and SA.35311.	
Durée	15.8.2011-30.6.2014	
Secteur(s) économique(s) concerné(s)	Travaux de plomberie et installation de chauffage et de conditionnement d'air	
Type de bénéficiaire	PME,grande entreprise	
Montant annuel total du budget prévu au titre du régime	GBP 23,22 (millions)	
Pour les garanties	GBP 23,22 (millions)	
Instrument d'aide (art. 5)	Subvention directe	
Référence à la décision de la Commission	—	
Si cofinancement par des fonds communautaires	—	
Objectifs	Intensité maximale de l'aide en % ou montant maximal de l'aide en devise nationale	Suppléments pour PME en %
Aides environnementales en faveur des investissements dans les économies d'énergie (art. 21)	60 %	20 %

Lien internet vers le texte intégral de la mesure d'aide:

https://www.gov.uk/renewable-heat-premium-payment-scheme#overview

Renseignements communiqués par les États membres sur les aides d'État accordées conformément au règlement (CE) nº 1857/2006 de la Commission concernant l'application des articles 87 et 88 du traité aux aides d'État accordées aux petites et moyennes entreprises actives dans la production de produits agricoles et modifiant le règlement (CE) nº 70/2001

(2013/C 190/03)

Aide nº: SA.36717 (13/XA)

État membre: Espagne

Région: ASTURIAS

Intitulé du régime d'aide ou nom de l'entreprise bénéficiaire de l'aide individuelle: Asociación de Criadores de Gochu Asturcelta (ACGA)

Base juridique: Convenio de colaboración con la Asociación de Criadores de Gochu Asturcelta para el mantenimiento del libro genealógicoy el desarrollo del programa de conservación de dicha raza en 2013.

Dépenses annuelles prévues dans le cadre du régime d'aide ou montant total de l'aide individuelle octroyée à l'entreprise bénéficiaire: Montant total de l'aide ad hoc accordée à l'entreprise: EUR 0,01 (millions)

Intensité maximale des aides: 100,00 %

Durée du régime d'aide ou de l'aide individuelle: 18.6.2013-31.12.2013

Objectif de l'aide: Assistance technique (article 15 du règl. (CE) nº 1857/2006), Secteur de l'élevage (article 16 du règl. (CE) nº 1857/2006)

Secteur(s) concerné(s): Élevage de porcins

Nom et adresse de l'autorité responsable:

Consejería de Agroganadería y Recursos Autóctonos del Principado de Asturias
C/ Coronel Aranda, s/n, 3ª planta
33005 Oviedo — ASTURIAS

Adresse du site web:

http://www.asturias.es/Asturias/descargas/PDF_TEMAS/Ganaderia/ayudas/genetica/acga.pdf

Autres informations: —

Aide nº: SA.36718 (13/XA)

État membre: Espagne

Région: ASTURIAS

Intitulé du régime d'aide ou nom de l'entreprise bénéficiaire de l'aide individuelle: Asociación de Criadores de Cabra Bermeya (ACRIBER)

Base juridique: Convenio de colaboración con la Asociación de Criadores de Cabra Bermeya para el mantenimiento del libro genealógico y el desarrollo del programa de conservación de dicha raza en 2013.

Dépenses annuelles prévues dans le cadre du régime d'aide ou montant total de l'aide individuelle octroyée à l'entreprise bénéficiaire: Montant total de l'aide ad hoc accordée à l'entreprise: EUR 0,01 (millions)

Intensité maximale des aides: 100,00 %

Durée du régime d'aide ou de l'aide individuelle: 18.6.2013-31.12.2013

Objectif de l'aide: Assistance technique (article 15 du règl. (CE) nº 1857/2006), Secteur de l'élevage (article 16 du règl. (CE) nº 1857/2006)

Secteur(s) concerné(s): Élevage d'ovins et de caprins

Nom et adresse de l'autorité responsable:

Consejería de Agroganadería y Recursos Autóctonos del Principado de Asturias
C/ Coronel Aranda, s/n, 3ª planta
33005 Oviedo — ASTURIAS

Adresse du site web:

http://www.asturias.es/Asturias/descargas/PDF_TEMAS/Ganaderia/ayudas/genetica/acriber.pdf

Autres informations: —

Aide nº: SA.36719 (13/XA)

État membre: Espagne

Région: ASTURIAS

Intitulé du régime d'aide ou nom de l'entreprise bénéficiaire de l'aide individuelle: Ayudas al sector ganadero en forma de servicios prestados por Asturiana de Control Lechero, Cooperativa Limitada (ASCOL)

Base juridique: Convenio de colaboración con la Cooperativa Asturiana de Control Lechero (ASCOL) para el desarrollo de un programa de mejora genética de la cabaña ganadera asturiana de raza firsona durante el año 2013.

Dépenses annuelles prévues dans le cadre du régime d'aide ou montant total de l'aide individuelle octroyée à l'entreprise bénéficiaire: Montant annuel total du budget prévu au titre du régime: EUR 0,44 (millions)

Intensité maximale des aides: 100,00 %

Durée du régime d'aide ou de l'aide individuelle: 14.6.2013-31.12.2013

Objectif de l'aide: Assistance technique (article 15 du règl. (CE) nº 1857/2006), Secteur de l'élevage (article 16 du règl. (CE) nº 1857/2006)

Secteur(s) concerné(s): Élevage de vaches laitières

Nom et adresse de l'autorité responsable:

Consejería de Agroganadería y Recursos Autóctonos del Principado de Asturias
C/ Coronel Aranda, s/n, 3ª planta
33005 — Oviedo — ASTURIAS

Adresse du site web:

http://www.asturias.es/Asturias/descargas/PDF_TEMAS/Ganaderia/ayudas/genetica/ascol.pdf

Autres informations: —

Aide nº: SA.36720 (13/XA)

État membre: Espagne

Région: ASTURIAS

Intitulé du régime d'aide ou nom de l'entreprise bénéficiaire de l'aide individuelle: Asociación española de criadores de ganado vacuno selecto de raza Asturiana de los Valles (ASESAVA)

Base juridique: Convenio de colaboración con la Asociación española de criadores de ganado vacuno selecto de raza Asturiana de los Valles para el mantenimiento del libro genealógico y el desarrollo del programa de mejora genética de dicha raza en 2013.

Dépenses annuelles prévues dans le cadre du régime d'aide ou montant total de l'aide individuelle octroyée à l'entreprise bénéficiaire: Montant annuel total du budget prévu au titre du régime: EUR 0,48 (millions)

Intensité maximale des aides: 100,00 %

Durée du régime d'aide ou de l'aide individuelle: 14.6.2013-31.12.2013

Objectif de l'aide: Assistance technique (article 15 du règl. (CE) nº 1857/2006), Secteur de l'élevage (article 16 du règl. (CE) nº 1857/2006)

Secteur(s) concerné(s): Élevage d'autres bovins et de buffles

Nom et adresse de l'autorité responsable:

Consejería de Agroganadería y Recursos Autóctonos del Principado de Asturias
C/ Coronel Aranda, s/n, 3ª planta
33005 Oviedo — ASTURIAS

Adresse du site web:

http://www.asturias.es/Asturias/descargas/PDF_TEMAS/Ganaderia/ayudas/genetica/aseava.pdf

Autres informations: —

Aide nº: SA.36721 (13/XA)

État membre: Espagne

Région: ASTURIAS

Intitulé du régime d'aide ou nom de l'entreprise bénéficiaire de l'aide individuelle: Asociación Española de Criadores de Ganado Vacuno Selecto de raza Asturiana de la Montaña (ASEAMO)

Base juridique: Convenio de colaboración con la Asociación Española de Criadores de Ganado Vacuno Selecto de raza Asturiana de la Montaña para el mantenimiento del libro genealógico y del desarrollo de un programa de conservación de dicha raza en 2013.

Dépenses annuelles prévues dans le cadre du régime d'aide ou montant total de l'aide individuelle octroyée à l'entreprise bénéficiaire: Montant annuel total du budget prévu au titre du régime: EUR 0,13 (millions)

Intensité maximale des aides: 100,00 %

Durée du régime d'aide ou de l'aide individuelle: 14.6.2013-31.12.2013

Objectif de l'aide: Assistance technique (article 15 du règl. (CE) nº 1857/2006), Secteur de l'élevage (article 16 du règl. (CE) nº 1857/2006)

Secteur(s) concerné(s): Élevage d'autres bovins et de buffles

Nom et adresse de l'autorité responsable:

Consejería de Agroganadería y Recursos Autóctonos del Principado de Asturias
C/ Coronel Aranda, s/n, 3ª planta
33005 Oviedo — ASTURIAS

Adresse du site web:

http://www.asturias.es/Asturias/descargas/PDF_TEMAS/Ganaderia/ayudas/genetica/aseamo.pdf

Autres informations: —

Aide nº: SA.36722 (13/XA)

État membre: Espagne

Région: ASTURIAS

Intitulé du régime d'aide ou nom de l'entreprise bénéficiaire de l'aide individuelle: Asociación de Criadores de Oveya Xalda de Asturias (ACOXA)

Base juridique: Convenio de colaboración con la Asociación de Criadores de Oveya Xalda de Asturias para el mantenimiento del libro genealógico y el desarrollo del programa de conservación de dicha raza durante 2013.

Dépenses annuelles prévues dans le cadre du régime d'aide ou montant total de l'aide individuelle octroyée à l'entreprise bénéficiaire: Montant total de l'aide ad hoc accordée à l'entreprise: EUR 0,03 (millions)

Intensité maximale des aides: 100,00 %

Durée du régime d'aide ou de l'aide individuelle: 18.6.2013-31.12.2013

Objectif de l'aide: Assistance technique (article 15 du règl. (CE) nº 1857/2006), Secteur de l'élevage (article 16 du règl. (CE) nº 1857/2006)

Secteur(s) concerné(s): Élevage d'ovins et de caprins

Nom et adresse de l'autorité responsable:

Consejería de Agroganadería y Recursos Autóctonos del Principado de Asturias
C/ Coronel Aranda, s/n, 3ª planta
33005 — Oviedo — ASTURIAS

Adresse du site web:

http://www.asturias.es/Asturias/descargas/PDF_TEMAS/Ganaderia/ayudas/genetica/acoxa.pdf

Autres informations: —

Aide nº: SA.36723 (13/XA)

État membre: Espagne

Région: ASTURIAS

Intitulé du régime d'aide ou nom de l'entreprise bénéficiaire de l'aide individuelle: Asociación de Criadores de Pita Pinta Asturiana (ACPPA)

Base juridique: Convenio de colaboración con la Asociación de Criadores de Pita Pinta Asturiana para el mantenimiento del libro genealógico y el desarrollo del programa de conservación de dicha raza en 2013.

Dépenses annuelles prévues dans le cadre du régime d'aide ou montant total de l'aide individuelle octroyée à l'entreprise bénéficiaire: Montant annuel total du budget prévu au titre du régime: EUR 0,01 (millions)

Intensité maximale des aides: 100,00 %

Durée du régime d'aide ou de l'aide individuelle: 14.6.2013-31.12.2013

Objectif de l'aide: Assistance technique (article 15 du règl. (CE) nº 1857/2006), Secteur de l'élevage (article 16 du règl. (CE) nº 1857/2006)

Secteur(s) concerné(s): Élevage de volailles

Nom et adresse de l'autorité responsable:

Consejería de Agroganadería y Recursos Autóctonos del Principado de Asturias
C/ Coronel Aranda, s/n, 3ª planta
33005 Oviedo — ASTURIAS

Adresse du site web:

http://www.asturias.es/Asturias/descargas/PDF_TEMAS/Ganaderia/ayudas/genetica/acppa.pdf

Autres informations: —

Aide nº: SA.36724 (13/XA)

État membre: Espagne

Région: ASTURIAS

Intitulé du régime d'aide ou nom de l'entreprise bénéficiaire de l'aide individuelle: Asociación de Criadores de Ponis de Raza Asturcón (ACPRA)

Base juridique: Convenio de colaboración con la Asociación de Criadores de Ponis de Raza Asturcón para el mantenimiento del libro genealógico y el desarrollo del programa de conservación de dicha raza en 2013.

Dépenses annuelles prévues dans le cadre du régime d'aide ou montant total de l'aide individuelle octroyée à l'entreprise bénéficiaire: Montant annuel total du budget prévu au titre du régime: EUR 0,13 (millions)

Intensité maximale des aides: 100,00 %

Durée du régime d'aide ou de l'aide individuelle: 14.6.2013-31.12.2013

Objectif de l'aide: Assistance technique (article 15 du règl. (CE) nº 1857/2006), Secteur de l'élevage (article 16 du règl. (CE) nº 1857/2006)

Secteur(s) concerné(s): Élevage de chevaux et d'autres équidés

Nom et adresse de l'autorité responsable:

Consejería de Agroganadería y Recursos Autóctonos del Principado de Asturias
C/ Coronel Aranda, s/n, 3ª planta
33005 Oviedo — ASTURIAS

Adresse du site web:

http://www.asturias.es/Asturias/descargas/PDF_TEMAS/Ganaderia/ayudas/genetica/acpra.pdf

Autres informations: —

Renseignements communiqués par les États membres sur les aides d'État accordées conformément au règlement (CE) nº 800/2008 de la Commission déclarant certaines catégories d'aide compatibles avec le marché commun en application des articles 87 et 88 du traité (règlement général d'exemption par catégorie)

(Texte présentant de l'intérêt pour l'EEE)

(2013/C 190/04)

Reference number of the State Aid	SA.36385 (13/X)
Member State	Latvia
Member State reference number	—
Name of the Region (NUTS)	Latvia Article 107(3)(a)
Granting authority	valsts aģentūra "Latvijas Investīciju un attīstības aģentūra" Pērses iela 2, Rīga, Latvija, LV-1442 www.liaa.gov.lv
Title of the aid measure	Atbalsts darba vietu radīšanai
National legal basis (Reference to the relevant national official publication)	2012.gada 13.marta Ministru kabineta noteikumi Nr.179 "Noteikumi par darbības programmas "Cilvēkresursi un nodarbinātība" papildinājuma 1.3.1.1.6.apakšaktivitāti "Atbalsts darba vietu radīšanai"" Darbības programma "Cilvēkresursi un nodarbinātība" (638. – 641. punkts) Darbības programmas "Cilvēkresursi un nodarbinātība" papildinājums (208.7. – 208.12. punkts)
Type of measure	Scheme
Amendment of an existing aid measure	—
Duration	1.11.2012-31.12.2013
Economic sector(s) concerned	All economic sectors eligible to receive aid
Type of beneficiary	SME,large enterprise
Annual overall amount of the budget planned under the scheme	LVL 7,00 (in millions)
For guarantees	LVL 7,00 (in millions)
Aid Instrument (Article 5)	Direct grant
Reference to the Commission Decision	—
If co-financed by Community funds	Komisijas lēmums 18.12.2007 ar ko pieņem darbības programmu Kopienas palīdzībai no Eiropas Sociālā fonda atbilstīgi konverģences mērķim Latvijas reģionos CCI 2007LV051PO001. – LVL 3,00 (in millions)

Objectives	Maximum aid intensity in % or Maximum aid amount in national currency	SME-bonuses in %
General training (Art. 38(2))	50 %	0 %
Scheme	50 %	0 %
Specific training (Art. 38(1))	25 %	0 %

Web link to the full text of the aid measure:

http://www.likumi.lv/doc.php?id=246032#top

Reference number of the State Aid	SA.36580 (13/X)
Member State	Germany
Member State reference number	—
Name of the Region (NUTS)	DEUTSCHLAND Article 107(3)(a),Article 107(3)(c),Non-assisted areas,Mixed
Granting authority	KfW Bankengruppe Palmengartenstraße 5-9, 60325 Frankfurt www.kfw.de
Title of the aid measure	KfW-Programm Erneuerbare Energien „Speicher“
National legal basis (Reference to the relevant national official publication)	KfW-Gesetz, BGBI. I S.2427, Programmmerkblatt „KfW-Programm Erneuerbare Energien ‚Speicher‘“
Type of measure	Scheme
Amendment of an existing aid measure	—
Duration	1.5.2013-31.12.2013
Economic sector(s) concerned	All economic sectors eligible to receive aid
Type of beneficiary	SME,large enterprise
Annual overall amount of the budget planned under the scheme	EUR 25,00 (in millions)
For guarantees	EUR 25,00 (in millions)
Aid Instrument (Article 5)	Direct grant, Soft loan
Reference to the Commission Decision	—
If co-financed by Community funds	—

Objectives	Maximum aid intensity in % or Maximum aid amount in national currency	SME-bonuses in %
SME investment and employment aid (Art.15)	20 %	—
Environmental investment aid for the promotion of energy from renewable energy sources (Art. 23)	45 %	20 %

Web link to the full text of the aid measure:

https://www.kfw.de/media/pdf/download_center/foerderprogramme__inlandsfoerderung_/pdf_dokumente_2/6000002700_M_275_Speicher.pdf

---

Reference number of the State Aid	SA.36584 (13/X)
Member State	Italy
Member State reference number	—
Name of the Region (NUTS)	ABRUZZO Article 107(3)(c),Non-assisted areas

Granting authority	GIUNTA REGIONALE — DIREZIONE SVILUPPO ECONOMICO E TURISMO VIA PASSOLANCIANO N. 75 65127 PESCARA — ITALIA http://www.regione.abruzzo.it/portale/index.asp
Title of the aid measure	BANDO PER LA PROMOZIONE SUL PROPRIO TERRITORIO REGIONALE DI INIZIATIVE DI LOCALIZZAZIONE, AMPLIAMENTO E AMMODERNAMENTO DI UNITA INDUSTRIALI, ATTRAVERSO CONTRATTI DI SVILUPPO LOCALI — TITOLO IV PROGETTI DI RICERCA INDUSTRIALE E SVILUPPO SPERIMENTALE
National legal basis (Reference to the relevant national official publication)	PAR FA ABRUZZO 2007-2013 APPROVATO CON D.G.R. N. 458 DEL 4 LUGLIO 2011 E MODIFICATO CON D.G.R. N. 556 DELL'8 AGOSTO 2011 CON ALLEGATO A. PRESA D'ATTO DA PARTE DEL CIPE CON DELIBERAZIONE DEL 30.9.2011 G.U. SERIE GENERALE N. 47 DEL 25.2.2012.
Type of measure	Scheme
Amendment of an existing aid measure	—
Duration	29.3.2013-30.6.2014
Economic sector(s) concerned	MANUFACTURING
Type of beneficiary	SME,large enterprise
Annual overall amount of the budget planned under the scheme	EUR 10,00 (in millions)
For guarantees	EUR 10,00 (in millions)
Aid Instrument (Article 5)	Direct grant
Reference to the Commission Decision	—
If co-financed by Community funds	—

Objectives	Maximum aid intensity in % or Maximum aid amount in national currency	SME-bonuses in %
Industrial research (Art. 31(2)(b))	50 %	20 %
Experimental development (Art. 31(2)(c))	25 %	20 %

Web link to the full text of the aid measure:

http://www.regione.abruzzo.it/portale/index.asp?modello=avvisoSing&servizio=le&stileDiv=sequence&template=default&tom=2497&b=avviso

http://bura.regione.abruzzo.it/bollettinoaccess.aspx?id=49993&tipo=Speciali&numero=35&data=29+Marzo+2013

Reference number of the State Aid	SA.36585 (13/X)
Member State	Italy
Member State reference number	—
Name of the Region (NUTS)	ABRUZZO Non-assisted areas

Granting authority	GIUNTA REGIONALE — DIREZIONE SVILUPPO ECONOMICO E TURISMO VIA PASSOLANCIANO N. 75 65127 PESCARA — ITALIA http://www.regione.abruzzo.it/portale/index.asp
Title of the aid measure	BANDO PER LA PROMOZIONE SUL PROPRIO TERRITORIO REGIONALE DI INIZIATIVE DI LOCALIZZAZIONE, AMPLIAMENTO E AMMODERNAMENTO DI UNITA INDUSTRIALI, ATTRAVERSO CONTRATTI DI SVILUPPO LOCALI — TITOLO III PROGETTI RELATIVI AD INVESTIMENTI IN AREE DIVERSE DA QUELLE DI CUI ALL'ART. 107 3, C) TFUE
National legal basis (Reference to the relevant national official publication)	PAR FAS ABRUZZO 2007-2013 APPROVATO CON D.G.R. N. 458 DEL 4 LUGLIO 2011 E MODIFICATO CON D.G.R. N. 556 DELL'8 AGOSTO 2011 CON ALLEGATO A. PRESA D'ATTO DA PARTE DEL CIPE CON DELIBERAZIONE 30.9.2011 G.U. SERIE GENERALE N. 47 DEL 25.2.2012
Type of measure	Scheme
Amendment of an existing aid measure	—
Duration	29.3.2013-30.6.2014
Economic sector(s) concerned	MANUFACTURING
Type of beneficiary	SME
Annual overall amount of the budget planned under the scheme	EUR 10,00 (in millions)
For guarantees	EUR 10,00 (in millions)
Aid Instrument (Article 5)	Direct grant
Reference to the Commission Decision	—
If co-financed by Community funds	—

Objectives	Maximum aid intensity in % or Maximum aid amount in national currency	SME-bonuses in %
SME investment and employment aid (Art.15)	20 %	—

Web link to the full text of the aid measure:

http://www.regione.abruzzo.it/portale/index.asp?modello=avvisoSing&servizio=le&stileDiv=sequence&template=default&tom=2497&b=avviso

http://bura.regione.abruzzo.it/bollettinoaccess.aspx?id=49993&tipo=Speciali&numero=35&data=29+Marzo+2013

Reference number of the State Aid	SA.36586 (13/X)
Member State	Italy
Member State reference number	—
Name of the Region (NUTS)	ABRUZZO Article 107(3)(c)

Granting authority	GIUNTA REGIONALE — DIREZIONE SVILUPPO ECONOMICO E TURISMO VIA PASSOLANCIANO N. 75 65127 PESCARA — ITALIA http://www.regione.abruzzo.it/portale/index.asp
Title of the aid measure	BANDO PER LA PROMOZIONE SUL PROPRIO TERRITORIO REGIONALE DI INIZIATIVE DI LOCALIZZAZIONE, AMPLIAMENTO E AMMODERNAMENTO DI UNITA INDUSTRIALI, ATTRAVERSO CONTRATTI DI SVILUPPO LOCALI — TITOLO II — PROGETTI RELATIVI AD INVESTIMENTI NELLE AREE 107 3, C) TFUE
National legal basis (Reference to the relevant national official publication)	PAR FAS ABRUZZO 2007-2013 APPROVATO CON D.G.R. n.458 del 4 luglio 2011 E MODIFICATO CON D.G.R. n.556 dell'8 Agosto 2011 con allegato A. PRESA D'ATTO DA PARTE DEL CIPE CON DELIBERAZIONE DEL 30.9.2011 G.U. SERIE GENERALE N. 47 DEL 25.2.2012
Type of measure	Scheme
Amendment of an existing aid measure	—
Duration	29.3.2013-30.6.2014
Economic sector(s) concerned	MANUFACTURING
Type of beneficiary	SME,large enterprise
Annual overall amount of the budget planned under the scheme	EUR 10,00 (in millions)
For guarantees	EUR 10,00 (in millions)
Aid Instrument (Article 5)	Direct grant
Reference to the Commission Decision	—
If co-financed by Community funds	—

Objectives	Maximum aid intensity in % or Maximum aid amount in national currency	SME-bonuses in %
Scheme	15 %	20 %

Web link to the full text of the aid measure:

http://www.regione.abruzzo.it/portale/index.asp?modello=avvisoSing&servizio=le&stileDiv=sequence&template=default&tom=2497&b=avviso

http://bura.regione.abruzzo.it/bollettinoaccess.aspx?id=49993&tipo=Speciali&numero=35&data=29+Marzo+2013

V

(Avis)

PROCÉDURES RELATIVES À LA MISE EN ŒUVRE DE LA POLITIQUE DE CONCURRENCE

COMMISSION EUROPÉENNE

AIDE D'ÉTAT — RÉPUBLIQUE HELLÉNIQUE

Aide d'État nº SA.31155 (2013/C) (ex 2013/NN) (ex 2010/N) — Aide d'État en faveur d'Hellenic Postbank S.A. consistant en la création et la capitalisation de la banque-relais «New Hellenic Postbank S.A.»

Invitation à présenter des observations conformément à l'article 108, paragraphe 2, du TFUE

(Texte présentant de l'intérêt pour l'EEE)

(2013/C 190/05)

Par lettre du 6 mai 2013, reproduite dans la langue faisant foi dans les pages qui suivent le présent résumé, la Commission a notifié à la République hellénique sa décision d'ouvrir la procédure prévue à l'article 108, paragraphe 2, du TFUE à l'égard de l'aide/la mesure susmentionnée.

Les parties intéressées peuvent transmettre leurs observations sur les mesures d'aide à l'égard desquelles la Commission ouvre la procédure dans un délai d'un mois suivant la date de publication du présent résumé et de la lettre qui suit, à l'adresse suivante:

Commission européenne
Direction générale de la concurrence
Greffe des aides d'État
1049 Bruxelles
BELGIQUE

Fax +32 22961242

Ces observations seront communiquées à la République hellénique. Le traitement confidentiel de l'identité de la partie intéressée qui présente les observations peut être demandé par écrit, en spécifiant les motifs de la demande.

TEXTE DU RÉSUMÉ

PROCÉDURES

Le 18 janvier 2013, les autorités grecques ont créé un établissement de crédit temporaire appelé «New TT Hellenic Postbank S.A.» (ci-après «New TT»), auquel ont été transférées les activités commerciales saines de l'ancienne TT Hellenic Postbank S.A. (ci-après «TT»). Dans ce contexte, New TT a reçu une aide d'État d'un montant de 4,6 milliards d'euros du Fonds hellénique de stabilité financière (ci-après le «HFSF»).

TT avait également bénéficié, le 25 mai 2009, d'un apport en capital de 224,96 millions d'euros au titre du régime grec de recapitalisation [1]. En outre, la Commission a autorisé pour une durée de 6 mois, par décision du 16 mai 2012 [2] concernant l'aide d'État SA.34115 (2012/NN) relative à la résolution de la défaillance de T Bank S.A. effectuée en décembre 2011, une aide d'environ 678 millions d'euros visant à faciliter la résolution d'une défaillance, la jugeant compatible avec le marché intérieur sur la base de l'article 107, paragraphe 3, point b), du traité sur le fonctionnement de l'Union européenne (ci-après le «TFUE»).

[1] Voir la décision de la Commission du 19 novembre 2008 concernant l'aide d'État N 560/2008 «Support Measures for the Credit Institutions in Greece», JO C 125 du 5.6.2009, p. 6. Le régime a été prolongé à plusieurs reprises.

[2] Décision de la Commission du 16 mai 2012 dans l'affaire SA.34115 (2012/NN) «Résolution de la défaillance de T Bank», JO C 284 du 20.9.2012, p. 9.

DESCRIPTION DES MESURES À L'ÉGARD DESQUELLES LA COMMISSION OUVRE LA PROCÉDURE

Premièrement, le HFSF a apporté à New TT, le 18 janvier 2013, un capital initial de 500 millions d'euros.

Deuxièmement, comme les activités transférées de TT à New TT contenaient des actifs inférieurs d'un montant de 4,1 milliards d'euros aux passifs, le HFSF a couvert le «déficit de financement» qui en découlait en émettant des obligations du FESF d'un montant total de 4,1 milliards d'euros en faveur de New TT.

Troisièmement, TT a bénéficié, le 25 mai 2009, d'un apport en capital de 224,96 millions d'euros au titre du régime grec.

Quatrièmement, la Banque de Grèce a procédé, le 17 décembre 2011, à la résolution de la défaillance de T Bank en ordonnant le transfert de ses actifs et de ses passifs à TT. Comme la valeur des passifs transférés était supérieure à celle des actifs transférés, le déficit de financement de 676 956 514 euros qui en résultait a été couvert conformément aux dispositions concernées par le mécanisme de résolution du Fonds grec de garantie des dépôts et des investissements (ci-après le «HDIGF»).

APPRÉCIATION DES MESURES

Premièrement, en ce qui concerne (i) l'apport en capital de 0,5 milliard d'euros et (ii) la couverture du déficit de financement d'un montant de 4,1 milliards d'euros par le HFSF en faveur de New TT, la Commission considère ces deux mesures d'aide comme des aides d'État au sens de l'article 107, paragraphe 1, du TFUE. Deuxièmement, pour ce qui est de la recapitalisation de TT effectuée en 2009, la Commission a déjà conclu, dans sa décision autorisant le régime ([3]), que la recapitalisation accordée au titre de ce dernier constituerait une aide d'État. Troisièmement, en ce qui concerne l'aide visant à faciliter la résolution d'une défaillance, accordée à T-Bank, la Commission a établi, dans sa décision du 16 mai 2012 ([4]), que l'intervention du mécanisme de résolution du HDIGF constituait une aide d'État.

La base juridique de l'appréciation des mesures est l'article 107, paragraphe 3, point b) du TFUE.

En ce qui concerne la compatibilité des mesures susmentionnées avec l'article 107, paragraphe 3, point b), du TFUE, la Commission l'apprécie sur la base de la communication bancaire ([5]), de la communication sur la recapitalisation ([6]) et de la communication sur la restructuration des banques ([7]).

En ce qui concerne la compatibilité des mesures, la Commission estime que l'apport en capital et la couverture du déficit de financement de New TT constituent des formes d'aide au sauvetage appropriées pour atteindre l'objectif de rétablissement de la stabilité financière dans le système bancaire grec et l'économie grecque dans son ensemble. La Commission doute toutefois, à ce stade, que le montant de 4,6 milliards d'euros (0,5 milliard sous la forme de capitaux et 4,1 milliards sous la forme d'une couverture du déficit de financement) soit limité au minimum nécessaire et invite les parties intéressées à formuler des observations sur ce point. La Commission considère en outre que les deux mesures sont proportionnées en tant qu'aides au sauvetage à court terme, mais exige l'instauration rapide de mesures visant à éviter que l'aide ne soit utilisée pour financer la croissance ou des mesures qui ne sont pas strictement indispensables au rétablissement de la rentabilité.

En ce qui concerne le rétablissement de la viabilité à long terme conformément à la communication sur la restructuration des banques, la Commission doute de la capacité de New TT à y parvenir par ses propres moyens, comme prévu dans le plan de restructuration communiqué à la Commission le 29 janvier 2013 et actualisé en mars 2013. Les mesures proposées dans le plan de restructuration pour générer des bénéfices à l'avenir semblent très limitées. Ces doutes concernent en particulier la faible réduction des effectifs de personnel et du nombre de succursales ainsi que le recours limité aux synergies possibles, à savoir la pleine intégration de T Bank. Dans ce contexte, la Commission doute que New TT dispose des ressources nécessaires pour atteindre les objectifs fixés dans le plan de restructuration et, plus précisément, pour réaliser les bénéfices prévus. Le risque existe donc que New TT devienne finalement une banque-relais régulièrement dépendante des aides de l'État. Aussi la Commission estime-t-elle, à ce stade, que la réintégration de TT dans une société financière rentable de plus grande taille accroîtrait les perspectives de rentabilité de New TT. La Commission invite les parties intéressées à formuler leurs observations au sujet de ces doutes.

En ce qui concerne le partage des charges et la limitation de l'aide au minimum nécessaire, la Commission doute que l'aide soit limitée à ce minimum. Elle doute en particulier que les coûts de restructuration soient limités au minimum car New TT doit être restructurée sur une base autonome, ce qui gonflera ces coûts. La Commission invite les parties intéressées à formuler leurs observations sur ce point.

([3]) Voir la note de bas de page n° 1.
([4]) Voir la note de bas de page n° 2.
([5]) Communication de la Commission intitulée «Application des règles en matière d'aides d'État aux mesures prises en rapport avec les institutions financières dans le contexte de la crise financière mondiale», JO C 270 du 25.10.2008, p. 8.
([6]) Communication de la Commission intitulée «Recapitalisation des établissements financiers dans le contexte de la crise financière actuelle: limitation de l'aide au minimum nécessaire et garde-fous contre les distorsions indues de concurrence», JO C 10 du 15.1.2009, p. 2.
([7]) Communication de la Commission intitulée «Retour à la viabilité et appréciation, conformément aux règles relatives aux aides d'État, des mesures de restructuration prises dans le secteur financier dans le contexte de la crise actuelle», JO C 195 du 19.8.2009, p. 9.

La Commission fait en outre observer qu'une grande partie des pertes encourues par TT ces dernières années provient d'une remise de dette en faveur de l'État, en l'occurrence par la participation des créanciers privés et par la vente d'obligations d'État grecques à l'État largement sous le pair à la fin de 2012. Ces mesures pourraient être considérées comme étant équivalentes à un paiement par TT à l'État et justifier par conséquent une rémunération inférieure sur l'aide à la recapitalisation octroyée par la suite par l'État pour couvrir les déficits en fonds propres générés par la remise de dette en faveur de l'État. Les parties intéressées sont invitées à présenter leurs observations sur ce point de vue.

En ce qui concerne la distorsion de concurrence, il convient de noter que TT détenait beaucoup plus d'obligations d'État grecques, par rapport à sa taille, que d'autres banques grecques. La Commission considère à ce stade qu'un investissement d'une telle ampleur dans ces obligations pourrait dénoter une prise de risques inappropriée. La Commission invite les parties intéressées à formuler leurs observations sur ce point également.

Conformément à l'article 14 du règlement (CE) n° 659/1999 du Conseil, toute aide illégale pourra faire l'objet d'une récupération auprès de son bénéficiaire.

TEXTE DE LA LETTRE

«The Commission wishes to inform the Hellenic Republic that, having examined the information supplied by your authorities on the aid measures referred to above, it has decided to initiate the procedure laid down in Article 108(2) of the Treaty on the Functioning of the European Union ("**TFEU**").

1. **PROCEDURE**

(1) On 19 November 2008 ([8]), the Commission approved the Greek support measures for the credit institutions designed to ensure the stability of the Greek financial system (the "**Scheme**").

(2) On 25 May 2009, TT Hellenic Postbank S.A. ("**TT**") received a capital injection of EUR 224.96 million under the Scheme.

(3) The Greek authorities submitted information to the Commission on TT in February, March, May and June 2010.

(4) By letter of 30 June 2010, the Commission's services requested the restructuring plan for TT to be submitted by 1 September 2010.

(5) By letter of 22 July 2010, the Greek authorities requested an extension of the deadline for the submission of the restructuring plan until 30 September 2010. The Commission services agreed to the extension of the deadline on 23 August 2010.

(6) On 1 October 2010, the Greek authorities submitted the initial restructuring plan for TT.

(7) The restructuring plan was discussed between the Greek authorities and the Commission services in a series of meetings, teleconferences and other information exchanges between October 2010 and May 2011, in particular - amongst others - on 6 and 14 October 2010, 8 November 2010, 27 December 2010, 26 January 2011, 23 March 2011 and 13 April 2011.

(8) On 17 December 2011, the Bank of Greece ("**BoG**") proceeded with the resolution of T Bank S.A. ("**T Bank**") by ordering a transfer of its good assets and liabilities to TT, which was already a shareholder of T Bank (holding around 32.9 % of its shares).

(9) In March 2012, Greece and the EU/ECB/IMF updated the Memorandum of Economic and Financial Policies ("**MEFP**"). The MEFP sets out, among other economic and financial policies, that the Greek authorities have initiated an orderly resolution of TT through a Purchase and Assumption ("**P&A**") transaction. TT had been classified as non-viable in the framework of the viability assessment of all the Greek banks carried out by the BoG and its advisors, in consultation with the EU/ECB/IMF.

(10) By decision of 16 May 2012 in State aid case SA.34115 (2012/NN) on the Resolution of T Bank ([9]), the Commission authorised an intervention by the Resolution scheme of the Hellenic Deposit and Investment Guarantee Fund ("**HDIGF**") for an amount of EUR 676 956 514 as compatible with the internal market on the basis of Article 107(3)(b) TFEU for a period of six months. In that decision, the Commission required the Greek authorities to submit an updated restructuring plan for TT within six months. That plan was to take into account the integration of T Bank's activities into TT. In the decision of 16 May 2012 the Commission could not definitively conclude on the compatibility of the resolution aid to T Bank since the buyer of the bank's activities – TT – was itself an aided bank on which the Commission had not yet taken a decision on its restructuring, as well as on the restoration of TT's long-term viability. The Commission could therefore not conclude on whether the transfer of T Bank to TT was an adequate way to restore the viability of the transferred entity.

(11) Further correspondence took place between the Greek authorities and the Commission services between May and December 2012.

(12) In January 2013, the Greek authorities submitted a draft restructuring plan for a bridge bank of TT. Due to the absence of buyers for TT, no P&A transaction (as envisaged in the MEFP) could take place and the creation of a bridge bank was considered as the only remaining solution for the resolution of TT. The bridge bank received aid from the Hellenic Financial Stability Fund ([10]) ("**HFSF**") which (a) covered the so-called "funding gap" of the transferred perimeter and (b) provided the bridge bank with initial share capital.

(13) The establishment of the bridge bank and its restructuring plan were discussed by the Greek authorities and the Commission services in a series of meetings, teleconferences and other information exchanges between

([8]) See Commission decision of 19 November 2008 in State aid N 560/2008 "Support Measures for the Credit Institutions in Greece", OJ C 125, 05.06.2009, p. 6. The scheme has been prolonged several times. The last updated scheme is in place until 30 June 2013. See Commission decision of 22 January 2013 in State aid SA.35999 (2012/N) "Prolongation of the Guarantee Scheme and the Bond Loans Scheme for Credit Institutions in Greece", not yet published.

([9]) Commission decision of 16 May 2012 in case SA.34115 (2012/NN) "Resolution of T Bank", OJ C 284, 20.09.2012, p. 9.

([10]) The HFSF is a Fund originally established by Law 3864/2010 of the Greek Parliament. The Fund's resources stem from the financial support mechanism to Greece and its capital is gradually paid up by the Greek State. It is set up for a limited duration until 30 June 2017. For more details, see inter alia, Commission decision of 3 September 2010 in State Aid case N 328/2010 "Recapitalisation of credit institutions in Greece under the Financial Stability Fund (FSF)", OJ C 316, 20.11.2010, p. 7.

January and March 2013, in particular - amongst others – on 8, 11, 15, 22, 23 and 30 January and 12 March 2013.

(14) For reasons of urgency, the Hellenic Republic exceptionally accepts that the present decision is adopted in the English language.

2. DESCRIPTION

2.1 TT Hellenic Postbank S.A.

(15) TT was established in 1902 under the framework of the Hellenic Post Office Organisation. Until 2006, TT was a State-controlled special credit institution with activities limited to the granting of mortgages and consumer loans to public servants and publicly-owned companies. After having acquired a banking licence in 2006, TT expanded its activities to corporate finance and retail lending. In the same year, TT became listed on the Athens Stock Exchange through a public offering of 34.84 % of its existing shares. The Hellenic Republic remained its largest shareholder.

(16) TT has a market share of 6 % in terms of deposits in Greece.

(17) In 2009, when it received its first recapitalisation, TT had 146 own branches and 2 554 employees. TT had a balance sheet showing total assets of approximately EUR 16 billion and risk weighted assets ("**RWA**") of EUR 7.5 billion.

(18) TT has a cooperation agreement with the Hellenic Post Office to market its products in approximately 800 branches of the latter. The contribution of that additional network to TT's services is 7 % of TT's total deposit base (which amounted to approximately EUR 12 billion in 2009).

(19) Compared to its size, TT has a relatively large deposit base. TT had a loan-to-deposit ratio of less than 100 % in 2009.

(20) On 25 May 2009, TT got a capital injection of EUR 224.96 million (corresponding to circa 2.9 % of its RWA at that time) under the Scheme ([11]) because its bank capital adequacy ratio ("**CAR**") was under the 10% minimum threshold set by the BoG for it.

(21) On 3 July 2009, TT issued common shares in amount of EUR 526.3 million, which were then placed on the market. After the completion of the capital increases of May and July 2009, the bank's CAR amounted to approximately 17 %. TT's shareholding structure following the share capital increase of July 2009 was as follows: the Hellenic State with 44.04 % of which 10% was held through the Hellenic Post Office; individuals with 24.9 %; legal entities (domestic) owning 22.04 %; legal entities (international) owning 7.81 % and; own shares corresponding to 1.21 % ownership.

([11]) See footnote 1.

(22) In April 2010, TT acquired 32.9 % of the share capital of Aspis Bank for an amount of EUR 28.56 million. After the acquisition, Aspis Bank was rebranded as T Bank. When that bank was acquired by TT, it was in a poor economic situation with the lowest capital adequacy among the Greek banks, insufficient liquidity and profitability.

(23) Other participations held by TT are: (i) Post insurance (50 % shareholding), a company promoting and selling insurance and banc assurance products; and (ii) Attica Bank (22.4 % shareholding), one of the smallest banks (1.1 % market share in terms of total assets) in Greece.

(24) On 17 December 2011, the BoG proceeded with the resolution of T Bank through a transfer order of its assets and liabilities to TT and at the same time, with the withdrawal of T Bank's license. T Bank was put into liquidation. TT acquired the package of assets and liabilities of T Bank as it had made the highest bid in the framework of an unconditional tender procedure open to other banks. The value of the net assets transferred from T Bank to TT at the resolution date amounted to EUR 1.5 billion ([12]). TT took over 75 branches with 853 employees of T Bank.

(25) As a result, TT's total assets increased by 16 % to EUR 18 billion and its deposits by 15 % to EUR 13.5 billion, compared to the standalone basis ([13]). The acquisition of T Bank's assets had a negative impact on TT's capital adequacy due to the capital shortage of T Bank. However, TT's CAR stayed well above supervisory limit at the time as, on the consolidated basis, its CAR amounted to 15.7 %.

(26) In March 2012, the BoG, based on an own 'viability framework' methodology applied to the entire Greek banking system, declared TT to be an unviable bank as it was highly unlikely that TT could remain viable under its current state. The situation of TT gave rise several concerns. Firstly, TT booked an exceptionally high loss in 2011, due to the Private Sector Involvement ([14]) ("**PSI**"). TT had held a portfolio of Greek government bonds ("**GGB**") which, compared to its balance sheet size, was much higher than that of the other Greek banks. As a result of that very large loss, TT's capital became deeply negative. Secondly, TT faced a structural problem of a low profitability which had lasted since 2008.

([12]) Bain&Company assessment report regarding policies and procedures required to ensure effective liquidating bank asset management and recovery of February 2013.

([13]) Financial impact analysis of the proposed merger between TT and T Bank performed by BoG, 19 July 2011

([14]) Private Sector Involvement (PSI): negotiation between the Greek authorities and its private creditors which aimed to achieve a partial waiver of the Greek government debt by its private creditors on a voluntary basis. The PSI is extraordinary in nature and had a considerable impact on Greek banks. A series of banks made losses stemming from PSI. Those developments are described in more detail for instance in points 12 and 13 of the following document: "*The Second Economic Adjustment Programme for Greece – March 2012*", also available on http://ec.europa.eu/economy_finance/publications/occasional_paper/2012/op94_en.htm.

(27) The updated MEFP of March 2012 gives a preference to an orderly resolution of TT via a P&A transaction, implying that TT's good assets and liabilities would be put for sale to another existing bank. For that purpose, the BoG launched a call for an expression of interest to third parties for acquiring TT's good assets in December 2012. Three Greek banks expressed preliminary informal interest; however, by the deadline of 11 January 2013 for submitting binding offers, the Greek authorities had not received any such offers.

(28) Therefore, in the absence of buyers, the Greek authorities considered that the creation of a bridge bank was the only remaining solution for the resolution of TT.

2.2. **New TT Hellenic Postbank S.A.**

(29) On 18 January 2013, in the context of the Greek resolution framework ([15]) and in line with the provisions in the MEFP regarding the resolution of TT by January 2013, the Greek authorities announced the immediate creation and capitalisation of a temporary credit institution (a bridge bank) "New TT Hellenic Postbank S.A." ("**New TT**"), following a decree adopted by the Ministry of Finance ([16]) on a proposal by the BoG. In that context, the HFSF covered the so-called "funding gap" of the transferred perimeter *i.e.* the difference between the fair value of the assets transferred to New TT and the nominal value of the liabilities transferred to it. Since the former is lower than the latter, New TT had received a package having a negative value, which was compensated by a grant from the HFSF. In addition, the HFSF provided initial share capital to New TT amounting to EUR 500 million, fully and immediately paid up by the HFSF. As a consequence, HFSF is the sole shareholder of New TT. TT's bank licence was terminated.

(30) TT's sound business activities were transferred to New TT, in accordance with the recommendation of the BoG ([17]). Therefore, all the contractual relationships of TT with third parties were transferred to New TT. New TT received TT assets and liabilities such as cash, retail deposits and performing loans, central bank funding, GGB and T-Bills. Overall, EUR 10.8 billion assets ("**Transferred Assets**") were transferred to New TT.

(31) A total amount of EUR 1.2 billion net assets were left into TT. In particular, non-performing loans, tax assets and liabilities of TT, and levies and duties of any kind were included in "non-transferred" items. Those residual assets remaining in TT will be resolved through liquidation.

([15]) See the Greek law 4021/2011 on Bank Restructuring and the Law 3864/2010 on the Hellenic Financial Stability Fund. The Law 4021 of October 2011 amends the existing Greek banking legislation by providing for recovery as well as for resolution measures for credit institutions seated in Greece.

([16]) Decree 2124/B.95 of the Hellenic Republic Ministry of Finance of 18 January 2013 establishing an interim credit institution by the name of "New TT Hellenic Postbank S.A.".

([17]) See Bank of Greece Resolution Measures Committee Decision 7/2/18.01.2013 on the authorisation of the interim credit institution by the name of "New TT Hellenic Postbank S.A." and Resolution Measures Committee Decision 7/3/18/01.2013 on the withdrawal of the authorization of the credit institution by name of "TT Hellenic Postbank S.A." and placing thereof under liquidation.

(32) New TT was only fully operational as from 21 January 2013 as the operations of New TT were suspended from 4 to 21 January due to a strike of its employees. After the trade unions approved the tentative deal as regards the employment contracts, the operations of New TT could be resumed.

(33) On 30 January 2013, New TT signed new contracts with all the employees of TT. In that context, New TT reduced its annual personnel costs on average by 30% and started with 2 998 employees of TT as well as another 358 outsourced employees, resulting in a total bank staff of 3 356. New TT has a network of 217 branches and 300 automated teller machines ("ATM").

2.3 **New TT's restructuring plan**

(34) On 29 January 2013, the Greek authorities submitted an initial restructuring plan for New TT. The draft was updated in March 2013. The plan foresees the restructuring to take place between 2013 and 2017 ("the restructuring period")

(35) The main strategic objective of New TT is to improve the bank's investor attractiveness and financial results with the aim of selling it to a third party. For that purpose, New TT's restructuring plan foresees an employee cost reduction with the implementation of a Voluntary Retirement Scheme ("**VRS**"), as well as operating cost reductions assuming a steady amount of assets.

(36) Firstly, the VRS targets between 520 and 900 exits at a cost of approximately EUR 39 - 45 million, depending on the take-up by employees. A fully subscribed VRS would allow for annual savings of EUR 22 million. However, it is currently not clear when the VRS will be implemented. Moreover, there is still no concrete plan on the table as regards the future of the 358 outsourced staff that New TT employs.

(37) In a base scenario assuming the implementation of the VRS, the restructuring plan foresees a steady number of employees of 2 478 during the restructuring period. According to the plan, the number of branches will also remain steady, at 197 during the same period, resulting in 12.6 employees per branch as from 2013 until 2017. 20 branches have been closed since the creation of New TT.

(38) Secondly, regarding the reduction of operating costs, an agreement with the Hellenic Post Office has been achieved in order to reduce the network usage cost. In addition, New TT has already simplified its organizational structure, reducing its seven main divisions to five, a 29 % reduction in the number of departments. The plan also foresees a reduction in marketing and promotional costs. Non-essential on-going projects will be, or already have been, stopped.

(39) Furthermore, New TT intends to re-price its loans and deposits in order to achieve a significant increase in its net interest income. On that basis, the plan foresees that New TT would become profitable again in 2014-2015. In the base scenario, its net interest income would

increase from EUR 132 million in 2013 to EUR 325 million in 2017, while its total operating income would increase from EUR 156 million in 2013 to EUR 339 million in 2017. New TT's personal expenses would be reduced to EUR 80 million in 2017, against equivalent expenses of EUR 149 million in 2012 for TT. Other operating costs would decrease by approximately 15 % from EUR 95 million in 2012 (compared to TT) to an annual average of EUR 80 million in the period 2015-2017. New TT's profit after tax would amount to EUR 123 million in 2017, resulting in a return on equity ("**RoE**") of 15.2 % in 2017.

(40) As regards assets, New TT aims to have a relatively steady amount of total assets, of around EUR 12.5 billion during the restructuring period. New TT intends to shift its assets mix from core lending activities of mortgages and consumer loans into corporate banking. New TT's corporate lending activities are expected to double in the restructuring period, *i.e.* from EUR 1 billion to EUR 2.1 billion.

(41) As regards funding, the ECB's exposure will be totally eliminated and 100 % of emergency liquidity assistance ("**ELA**") funding dependence will be replaced with market funding. The bank's deposit base will, on the other hand, remain stable.

2.4. **Aid measures**

(42) There are four aid measures which are relevant to the situation of TT, which will be described in chronological order. Firstly, on 25 May 2009, TT got a capital injection of EUR 224.96 million (corresponding to approximately 2.9 % of the bank's RWA at that time) in the form of preference shares under the Scheme ([18]) ("**measure C**"). The injection was made because TT's CAR amounted to 8 %, which was below the minimum threshold of 10 % set by the BoG. The measure increased TT's CAR from 8.74 % (as of March 2009) to 10.96 %.

(43) That capital injection took the form of the issuance by TT of 60 800 000 non-voting, non-listed, non-transferable, tax deductible, non-cumulative preference shares. The issue price of EUR 3.70 for each share was fully subscribed and paid by the Hellenic Republic with bonds of equivalent value ([19]). Those preference shares pay a non-cumulative dividend of 10 %, subject to meeting the minimum CAR requirements set by the BoG and to the availability of after-tax net profits or distributable reserves in accordance with article 44a of C.L. 2190/1920. During the five years following the issuance of the preference shares, the Greek Ministry of Finance could either convert the preference shares into ordinary shares in case of insufficient regulatory capital, or redeem TT's preference shares.

(44) Secondly, on 17 December 2011, the BoG proceeded with the resolution of T Bank by ordering the transfer of its assets and liabilities to TT and withdrawing T Bank's license, in accordance with the law on resolution (Law 4021/2011). T Bank was put into liquidation. In that context, the fair value of the liabilities transferred from T Bank to TT amounted to EUR 2 160 182 164 and the fair value of the transferred assets amounted to EUR 1 483 225 650. The difference was a so-called "funding gap" of EUR 676 956 514, which was covered by the Resolution Scheme of the HDIGF ("**measure D**"). ([20])

(45) Thirdly, on 18 January 2013, the HFSF provided New TT with its initial capital of EUR 500 million, in exchange for which the HFSF received common shares with a nominal value of EUR 1 each ("**measure A**").

(46) Finally, the Transferred Activities from TT to New TT contained a funding gap of EUR 4.1 billion resulting from the difference between assets and liabilities. As a result, the HFSF, by taking over the obligations of the HDIGF (in line with the provisions of L. 4051/2012 which clarify that, as from February 2012, the HFSF will take over HDIGF's obligation), made up for that funding gap by granting EFSF bonds worth EUR 4.1 billion to New TT ("**measure B**"). The measure was granted on 18 January 2013.

(47) Table 1 summarizes those four aid measures.

Table 1: **Overview of the aid measures**

	Nature of aid	Legal entity which formally received the aid measure	Aid amount (in EUR million)
Measure A	Recapitalisation	New TT (bridge bank)	500
Measure B	Funding gap	New TT (bridge bank)	4 100
Aid to the other entities			
Measure C	Recapitalisation	TT	224.96
Measure D	Funding gap	TT	678

3. **ASSESSMENT**

3.1 **Existence of State aid within the meaning of Article 107(1) TFEU and quantity of State aid**

(48) The Commission has to first assess whether measures A, B, C and D constitute State aid within the meaning of Article 107 (1) TFEU. According to that provision, State aid is any aid granted by a Member State or through State resources in any form whatsoever which distorts, or threatens to distort, competition by favouring certain undertakings or the production of certain goods, in so far as it affects trade between Member States.

([18]) See footnote 1.

([19]) Under Law 3723/2008.

([20]) In 2011, a resolution branch was created in the HDIGF with the adoption of the Resolution Framework in Greece. According to law 4021/2011, in the case of a transfer order: '*In case the value of the liabilities transferred to the transferee-credit institution exceeds the value of the assets transferred, the Bank of Greece shall determine the difference, to be covered as follows: a) the Depositors Branch of the HDIGF shall pay an amount equal to the value of the guaranteed deposits after deduction of the value of the transferred assets and b) the Resolution Branch of HDIGF shall pay the surplus.*'

Measure A

(49) The Commission notes that the capital injection by the HFSF into New TT, amounting to EUR 500 million (Measure A), was provided by the HFSF, an entity set up and financed by the Greek State. In the Commission decision approving the recapitalisations under the HFSF as compatible State aid ([21]), the Commission notes that the HFSF receives its resources from the State and its activities are considered imputable to the State. It will stay in place until 2017 and after that its profits or losses will be borne by the State. ([22]) In the present case, the Commission similarly concludes that measure A was financed by the State or through State resources.

(50) The Commission further notes that the capital injection provided a selective advantage to New TT, since it was a measure concerning New TT alone which enabled it to obtain capital it could not have found on the market. Given TT's precarious financial situation and the challenging economic situation in Greece which directly affects the banking sector, it is highly doubtful that any private investor would have injected capital into New TT under those conditions.

(51) Furthermore, New TT, although a bridge bank, competes with other banks amongst which are subsidiaries and branches of foreign banks. Even if there has been a general withdrawal of foreign banks from the Greek market (e.g. sale of their Greek banking activities by Credit Agricole, Société Générale and BCP), any selective advantage may affect the timing and condition of a return of some foreign banks to the Greek market. Therefore, the capital injection may have an effect on trade and may also distort competition between the Member States.

(52) The Commission concludes therefore that the capital injection by the HFSF into New TT constitutes State aid for the purposes of Article 107(1) TFEU.

Measure B

(53) As regards measure B, the Commission notes that it was also granted by the HFSF. Therefore, on the basis of the above argument for measure A as described in the recital 49, the Commission considers that measure B contains State resources and is imputable to the State.

(54) As regards the existence of a selective advantage, it should be recalled that measure B is a grant by the HFSF to New TT that covers a funding gap between the fair value of the assets transferred from TT and the nominal value of the transferred liabilities. Because that package of assets and liabilities had a negative value of more than EUR 4 billion, if measure B had not been granted to New TT, it would not have been possible to transfer TT's activities to another legal entity. They would then have been left in the liquidated TT and hence discontinued. Measure B thus allows the continuation within New TT of the economic activities previously carried out within TT. As measure concerns the transferred activities of TT and no other market operator it is by definition selective. The Commission considers New TT to be the economic beneficiary of the measure as it harbours TT's economic activities which continue to exist thanks to measure B.

(55) In its earlier decisions ([23]) on resolution supported by State measures, the Commission already observed that all the key productive banking assets (employees, branches, deposits, part of the loans, as well as central services and infrastructure) were transferred to the bridge bank or to the buying bank. No private investor would have made such an investment if the funding gap was not covered.

(56) Measure B distorts competition and affects trade for the reasons already developed in respect of measure A at recital 51. That selective advantage distorts competition by keeping the transferred activities alive and allowing them to continue competing on the market ([24]), when the BoG declared TT to be unviable.

(57) The Commission concludes therefore that the capital injection into New TT by the HFSF aimed at covering the funding gap constitutes State aid falling for the purposes of Article 107(1) TFEU.

Measure C

(58) As regards the recapitalisation of TT in 2009 (Measure C), that capital injection was granted under the Scheme ([25]). In the decision approving the Scheme, the Commission already concluded that recapitalisations granted under that Scheme would constitute State aid.

Measure D

(59) The Commission recalls that it has already established in its decision of 16 May 2012 ([26]) that measure D, the intervention by the Resolution scheme of the HDIGF in the amount of approximately EUR 0.68 billion in favour of T Bank's assets which were transferred to TT, constitutes State aid.

([21]) Commission decision of 3 September 2010 in State Aid case N 328/2010 "Recapitalisation of credit institutions in Greece under the Financial Stability Fund (FSF)", OJ C 316, 20.11.2010, p. 7.

([22]) More specifically, recital 46 of the Commission decision of 3 September 2010 in State Aid case N 328/2010 states that: '*The qualification of a measure as State aid first of all presupposes that the aid must be imputable to the State and financed by a Member State or through State resources. Neither imputability nor the presence of State resources are put into question by the fact that the Fund is independent. It is true that according to settled case-law regarding public undertakings it is not sufficient that the State is in a position to control a public undertaking and to exercise a dominant influence over its operations, but an actual exercise of that control must exist. However, in the present case the Fund is not acting as a public undertaking and its activities cannot be considered as falling into the sphere of a commercial market operator. Instead, the Fund is solely executing a public task. In addition it can be noted that the capital of the Fund is fully and solely paid by the Greek State, all seven members of the Fund's Board shall be appointed by a decision of the Minister of Finance and the Fund shall enjoy all the administrative, financial and judicial immunities applicable to the State.*'

([23]) See footnotes 14 and 15.

([24]) See by analogy Commission decision of 25.01.2010 in the State aid case NN 19/2009 – Restructuring aid to Dunfermline Building Society, recital 51; Commission decision of 25.10.2010 in State aid case N 560/2009 – Aid for the liquidation of Fionia bank, recital 56; Commission decision of 8.11.2010 in State aid case N 392/2010 – Restructuring of CajaSur, recital 52.

([25]) See footnote 1.

([26]) See footnote 2.

3.2 **Compatibility of the aid**

3.2.1. *Legal basis for the compatibility assessment*

(60) Article 107(3)(b) TFEU provides the legal basis for the Commission to declare aid compatible with the internal market if it is intended "to remedy a serious disturbance in the economy of a Member State". The Commission has acknowledged in several recent Greek State aid cases in the banking sector that there is a threat of serious disturbance in the Greek economy and that State support of banks is suitable to remedy that disturbance. ([27]) Despite a slow global economic recovery that has taken hold since the beginning of 2010, the Commission still considers that the requirements for State aid to be approved pursuant to Article 107(3)(b) TFEU are fulfilled in view of the reappearance of stress in financial markets. In December 2011 the Commission confirmed that view by adopting the Communication ([28]) on the application, from 1 January 2012, of State aid rules to support measures in favour of banks in the context of the financial crisis which prolongs the application of those State aid rules.

(61) In the light of the foregoing considerations, the Commission accepts that the capital injections by the HFSF (measure A) and the grant by the HFSF to cover the funding gap (measure B) can be analysed as State aid measures taken to avoid a serious disturbance in the economy of Hellenic Republic. In its decisions on the Scheme and on the resolution of T Bank, respectively, the Commission had already accepted that Article 107(3)(b) TFEU was the appropriate legal instrument to assess the recapitalisation of TT (measure C) and the resolution aid to T Bank (measure D).

3.2.2. *Compatibility assessment*

(62) The compatibility of the measures A, B, C and D with Article 107(3)(b) TFEU are assessed by the Commission in light of the Banking Communication ([29]), the Recapitalisation Communication ([30]) and the Restructuring Communication ([31]).

(63) In line with the general principles underlying the State aid rules of the Treaty and taking into account the global financial crisis and the systemic risk associated with it, the Banking Communication (point 15) requires that all measures have to be:

a. *Appropriate*: The aid has to be well-targeted in order to be able to achieve effectively the objective of remedying a serious disturbance in the economy;

b. *Necessary*: The aid measure must, in its amount and form, be necessary to achieve its legitimate purpose of remedying a serious disturbance in the economy and must, therefore, not exceed the necessary minimum amount to attain that effect;

c. *Proportionate to the challenge faced*: The distortions of competition resulting from the aid granted must be avoided or minimized as far as possible. Therefore, the aid measures must be designed in such a way as to minimize negative spill-over effects on competitors, other sectors and other Member States.

(64) The Recapitalisation Communication further details the level of remuneration required for State capital injections.

(65) Finally, the Commission should assess the measures under the Restructuring Communication, according to which a restructuring plan needs to: (i) demonstrate how the bank will restore long-term viability without State aid as soon as possible; (ii) address moral hazard by imposing appropriate own contribution ("burden-sharing") by the aid beneficiary to the restructuring costs; as well as (iii) ensure a competitive banking sector by limiting distortions of competition resulting from the aid granted, to the minimum necessary.

3.2.3. *Compatibility with the Banking and Recapitalisation Communications*

(66) The Commission will first assess whether measures A and B can be temporarily approved as rescue aid. It will then review the situation as regards the compatibility of measures C and D.

a. *Appropriateness of measures A and B*

(67) As regards the measure A, the capital injection from the HFSF was needed in order to have capital in New TT and to enable New TT to adhere to the minimum capital adequacy ratio set by the BoG.

(68) The Commission considers that the capital injection of EUR 500 million is appropriate as rescue aid since it enabled the transfer of the economic activities of TT to New TT. Hence, the economic activities have not been wound-up. An immediate winding-up of TT's activities could have led to a bank run and could have triggered a serious disturbance on the Greek financial markets. A serious disturbance on the Greek financial markets could be avoided through the creation of New TT and the transfer of TT's economic activities into New TT.

(69) On that basis, the Commission finds that the measure A is appropriate as rescue aid.

(70) As regards measure B, the intervention by HFSF was needed in order to fill the gap between the fair value of TT's assets and the nominal value of its liabilities which were transferred to New TT.

([27]) Commission decision of 22 January 2013 in State aid SA.35999 (2012/N) "Prolongation of the Guarantee Scheme and the Bond Loans Scheme for Credit Institutions in Greece", not yet published, Commission decision of 16 May 2012 "Resolution of T Bank",

([28]) Commission communication on the application, from 1 January 2012, of State aid rules to support measures in favour of banks in the context of the financial crisis, OJ C 356, 6.12.2011, p. 7

([29]) Communication from the Commission - The application of State aid rules to measures taken in relation to financial institutions in the context of the current global financial crisis, OJ C 270, 25.10.2008, p. 8.

([30]) Communication from the Commission - The recapitalisation of financial institutions in the current financial crisis: limitation of aid to the minimum necessary and safeguards against undue distortions of competition, OJ C 10, 15.1.2009, p. 2.

([31]) Commission Communication - The return to viability and the assessment of restructuring measures in the financial sector in the current crisis under the State aid rules, OJ C 195, 19.8.2009, p. 9.

(71) The Commission considers that measure B is appropriate as rescue aid because it helps keep alive TT's economic activities which were transferred to New TT. Without measure B, those activities would not have been able to continue, as TT was on the verge of bankruptcy and in current difficult market conditions no bank would have acquired a package having a negative value (i.e. with the fair value of the assets lower than the fair value of the liabilities). The measure thereby ensures that financial stability in Greece is maintained in the short-term. On that basis, the Commission finds that the measure B is appropriate as rescue aid.

b. *Necessity of measures A and B – limitation of the aid to the minimum*

(72) According to the Banking Communication, the aid measure must, in its amount and form, be necessary to achieve the objective. It implies that the capital injection must be of the minimum amount necessary to reach the objective.

(73) As regards measure A, the Commission has doubts that the amount is limited to the minimum necessary because the Member State envisages as one possible option that New TT is to be restructured on a stand-alone basis. The Commission doubts that the bank can be viable on a stand-alone basis. Hence, the Commission is of the opinion that State aid may be used for an option which is not realistic in the long-term. The Commission is of the opinion that the Hellenic Republic should also assess other options, which might be less expensive than the stand-alone option. At this stage the Commission is of the preliminary view that the stand-alone option might not be the cheapest option available and therefore it doubts that the State aid is limited to the minimum necessary. The Commission invites interested parties to provide comments on that issue.

(74) As regards measure B, the Commission doubts that the amount exactly covers the difference between the fair value of the transferred assets and the nominal value of the transferred liabilities. That amount may be excessive. Therefore, the Commission would ask for more detailed information regarding the exact amount of assets and liabilities that were and were not transferred to New TT, as well as additional information regarding the pricing model used.

(75) Furthermore, regarding the remuneration of measures A and B, the Commission has doubts on whether New TT will be able to sufficiently remunerate the State for the aid it received. The Commission observes that, in line with the Recapitalisation Communication, any recapitalisation of banks should, in principle, reflect the risk profile of the beneficiary, *i.e.* not fundamentally sound banks or, unviable banks, should pay higher remuneration than those that are fundamentally sound. The Commission notes that capital assistance to a bank which is unable to sufficiently remunerate the State for the received recapitalisation may only be accepted upon condition that (i) either the bank is wound-up, or (ii) a far-reaching restructuring plan is set-up, including a change in management and corporate governance where appropriate. In the present case, the Commission has doubts on whether New TT is a fundamentally sound bank and observes that New TT is not able to remunerate the measure A, the recapitalisation. In addition, no remuneration is foreseen for measure B, in the sense that the State did not receive any ownership rights in exchange. The coverage of the funding gap is therefore a definitive cost for the State without offsetting future revenues.

(76) In conclusion, on a preliminary basis, the Commission considers that the forms taken by measures A and B to be necessary as rescue aid to achieve the objective of restoring financial stability in the Greek banking system and economy as a whole.

(77) However, at this stage, the Commission doubts whether the amount of EUR 4.6 billion (measures A and B) is limited to the minimum. The Commission underlines that the absence of remuneration triggers a need for in-depth restructuring.

c. *Proportionality of measures A and B – measures limiting negative spill-over effects*

(78) The Commission notes that the legal entity TT will be liquidated and will exit the market. However, thanks to measures A and B, the economic activities of TT continue to exist in New TT, thereby producing negative spill-over effects. New TT should be rapidly subject to measures that will limit negative spill-over effects.

(79) The Commission considers that measures A and B are proportionate as rescue aid in the short-term, but require measures to be introduced rapidly to ensure aid is not used to fund growth or measures not strictly necessary to restore viability.

d. *Compatibility of measures C and D*

(80) For measure C, the Greek authorities submitted a restructuring plan for TT Bank on 1 October 2010 in line with the requirement of the Scheme. Because of the rapid and substantial changes in the Greek banking sector since then, while there have been extensive exchanges between the Greek authorities and the Commission services, it has not yet been possible to take a final view on that restructuring plan. In the meanwhile, the situation of TT Bank has altered so significantly that the restructuring plan which was submitted in 2010 is no longer pertinent. It is therefore necessary, in line with point 16 of the Restructuring Communication, to examine measure C in light of the updated restructuring plan presented in March 2013.

(81) In its decision of 16 May 2012, the Commission temporarily approved measure D, the resolution aid of T Bank, as compatible rescue aid for six months as from the date of adoption of that decision on the basis that the Greek authorities would submit to the Commission, within that six-month period, an updated restructuring plan for TT which took into account the integration of T Bank's activities into TT. In that decision of 16 May 2012, the Commission could not conclude that the transfer of T Bank's activities into TT allowed the restoration of their viability since TT was itself an aided bank required to submit a restructuring plan. The Commission could therefore not give a definitive approval of the aid to T Bank's activities which were transferred to TT.

(82) The decision of 16 May 2012 further concluded that the temporary authorisation of the aid would be automatically prolonged on submission of an updated restructuring until the Commission reached a final restructuring decision on TT's restructuring plan. ([32])

(83) The Commission first notes that no standalone restructuring plan for TT was submitted by the Greek authorities by the end of the six-month period. While the Commission regrets that omission by the Greek authorities, it accepts that delayed submission was understandable since, as indicated previously, it has been required in the meantime in the MEFP that TT be resolved. Moreover, the Greek authorities submitted a restructuring plan for New TT in January 2013 which deals with the activities transferred from T Bank to TT. It is therefore necessary to examine the compatibility of measure D as restructuring aid in light of the compliance with the Restructuring Communication of the plan submitted by the Greek authorities in January 2013 and updated in March 2013. Until the Commission has taken a final decision on measures A, B, C and D as restructuring aid, the Commission considers that Measure D can be approved provisionally as rescue aid.

3.2.4. *Compatibility with the Restructuring Communication*

(84) Because measures A, B, C and D all have the effect of allowing New TT to continue to operate on the market, the Commission must assess them individually and in combination in order to ensure that, as indicated in its Restructuring Communication, the restructuring plan will restore the viability of the company within a reasonable time span, that the aid granted by the measures is limited to the minimum necessary and ensures adequate burden-sharing, and that such aid is accompanied by measures which sufficiently limit distortions of competition.

3.2.4.1. *Restoration of long-term viability*

(85) Under the HFSF law, the HFSF has the obligation to sell the shares it owns in any bridge bank after a number of years. Since the obligation is only to sell the shares, it can be a sale to any type of investor. Thus the sale does not necessarily entail the integration of New TT into a larger banking group; New TT could remain a standalone bank with only change being that it would have a new shareholder, for instance, a private equity group. Given the uncertainty about the type of the future owner, the notified restructuring plan is based on the continuation of the operations of the bank on a stand-alone basis, *i.e.* not merged into a larger bank.

(86) As the Commission has indicated in its Restructuring Communication, the restructuring plan must restore the viability of the company within a reasonable time span. In that regard, the Commission notes positively that New TT reduced on average by 30 % annual personnel costs in January 2013.

(87) However, the Commission has doubts that New TT will be able to restore its long-term viability on a stand-alone basis, as planned in the restructuring plan submitted to the Commission.

(88) According to the restructuring plan, New TT plans to be profitable as of 2014. However, the proposed measures to generate profits in the future are very limited. Firstly, it is not clear whether New TT will manage to further reduce its personnel. Currently, the bank seems overstaffed compared to the services New TT offers. Moreover, the implementation of the VRS is uncertain as regards the timing and the acceptance rate by the employees. In that context, the VRS targets up to 900 potential persons and New TT plans to reduce headcount by approximately 520, as described in recital (36). No further steps are proposed in the restructuring plan to reduce personnel costs. For instance, no further indications are given as regards the future of 358 outsourced staff.

(89) As regards branches, no further closure of branches is foreseen beyond the closing of 20 branches already implemented since the creation of the bridge bank. Additionally, the branches of TT are in the main cities, especially in the Attica region. TT took over T Bank in 2011, which had a similar concentration of branches presence in the Attica region. A rationalisation of the branch network did not take place after the acquisition of T Bank. T Bank seems to remain operating as a separate entity, on a separate IT-platform as well as having a different risk management system. Therefore, the Commission has doubts whether the potential to achieve synergies has been used. It doubts that viability can be restored by keeping T Bank separate, which was itself a non-viable bank.

(90) Beside those limited cost-cutting measures, New TT's restructuring plan foresees re-pricing of loans and deposits. New TT aims at decreasing the deposit margins on existing deposits while, at the same time, increasing loan margins on new loan production. In that respect, the restructuring plan foresees that the interest margins paid by New TT on deposits will be decreased by 150 basis points ("**bp**") during 2013-2014 and a further 60 bp during 2015-2017. Loan margins will on the other hand increase by 70bp during 2013-2017. On that basis the interest income of New TT would significantly increase from EUR 433 million in 2013 to EUR 615 million in 2017. However, the Commission doubts that such ambitious re-pricing can be successfully implemented without losing a significant amount of customers and without making risky lending.

(91) In that respect, the Commission observes that New TT intends to double its corporate loan book. However, it is not clear how New TT intends to achieve that significant increase. In the past the corporate segment was relatively small compared to the other activities of TT because TT entered that segment only in 2009. That loan portfolio has generated significant losses since then. It is therefore doubtful whether New TT has the expertise to grow in that segment on a viable and profitable basis.

(92) Therefore it is questionable whether New TT has the resources to achieve the increase of income planned in the restructuring plan.

([32]) See recitals (59)-(61) from Commission decision of 16 May 2012 "Resolution of T Bank".

(93) Net interest income is an important income driver. If New TT does not manage to achieve the planned strong growth rate, it will not achieve the planned future profits or it will generate further losses in the future.

(94) There is therefore a risk of New TT ending up as a bridge bank, repeatedly relying on State aid.

(95) The Commission is at this stage of the opinion that the reintegration of TT into a larger viable financial company would increase the viability prospects of New TT. It would allow significant rationalisation of costs, would facilitate the re-pricing of deposits and of new loans, and would allow a wider range of products to be offered to customers, thereby achieving higher income through cross-selling.

(96) The Restructuring Communication provides that if a bank cannot return to viability on a stand-alone basis, viability can be restored through a sale and integration into a larger entity. In that respect, point 17 of the Restructuring Communication clarifies that *the sale of an ailing bank to another financial institution can contribute to restoring long-term viability, if the purchaser is viable and capable of absorbing the transfer of the ailing bank and may help restoring market confidence*.

(97) In conclusion, the Commission doubts that the restructuring plan submitted to the Commission on 29 January 2013 and updated in March 2013 will restore New TT's long-term viability. It therefore doubts that measures A and B can be found compatible with the Restructuring Communication.

(98) Since the Commission has doubts about the restoration of the long-term viability of New TT which harbours the economic activities previously carried out within TT, including T Bank, the Commission has also to open a formal investigation procedure on whether measure D (coverage of the funding gap granted to the transferred activities of T Bank) and measure C (the recapitalisation of TT in 2009) offered a long-term solution for New TT's viability and hereby invites the Greek authorities to submit further information on that subject.

3.2.4.2 *Burden-sharing and limitation of the aid to the minimum necessary*

(99) The Commission has doubts that the aid is limited to the minimum. In particular, the Commission doubts that the restructuring costs are limited to the minimum, because New TT is restructured on a stand-alone basis, which inflates the restructuring costs. The Commission doubts that New TT can be made viable on a stand-alone basis without incurring high costs, in particular to develop a sustainable personnel strategy, optimize the branch network, shift its assets mix to corporate lending and integrate T Bank, which includes developing a viable IT infrastructure and risk management structure. At this stage the Commission considers that the stand-alone option might not be the cheapest option and doubts that the State aid is limited to the minimum.

(100) Concerning burden-sharing of shareholders and subordinated debt holders, the Commission notes that the shareholders and subordinated debt holders were not transferred to New TT but have remained in the entity in liquidation. Therefore, there is a high probability that they will lose their investments. That burden-sharing reduces the aid amount needed. Hence, the Commission considers that sufficient burden-sharing of shareholders and subordinated debt holders is achieved.

(101) As regards the remuneration of the aid, the Greek State could expect to recover only part of the capital injections by the HFSF amounting to a total of EUR 500 million (Measure A). There will be no remuneration for the HFSF for covering the funding gap between assets and liabilities (Measure B). Further there is a very small likelihood of recovering much of the amount contributed by the HFSF. It is therefore highly probable that the EUR 4.1 billion granted is definitively lost.

(102) Therefore the Commission considers that the burden-sharing, even if it probably represents the maximum of what is feasible for that distressed bank *i.e.* New TT, does not seem to meet the Communication's requirements. If that is the case, the absence of remuneration triggers the need for in-depth restructuring, both in terms of viability measures and in terms of measures to limit distortions of competition.

(103) The Commission observes that a large part of the losses incurred in the last years stems from a waiver of debt in favour of the State *i.e.* through the PSI and through the sale of GGB to the State at a deep discount to par at the end of 2012. Those measures could be considered as equivalent to a payment by the bank to the State and therefore justify a lower remuneration on the subsequent recapitalisation aid granted by the State to cover the capital holes stemming from the debt waiver in favour of the State. The Member State authorities and interested parties are invited to comment on that view.

3.2.4.3 *Distortion of competition*

(104) New TT has received EUR 4.6 billion of aid (EUR 0.5 billion in form of capital and 4.1 billion in form of "funding gap" coverage) which is a considerable amount of aid. That aid represents more than 70% of TT's RWA and more than 90% of New TT's RWA. Further the Commission notes that TT (which is the legal entity which previously performed the activities which are now harboured in New TT) had received aid in the past: TT received under the Scheme [33] a first capital injection of EUR 224.96 million in form of preference shares (measure C). Furthermore, on the resolution of T Bank, the transferred activities of T Bank, which were transferred to TT, received a resolution aid of approximately EUR 678 million (measure D). Such amounts of aid normally call for a deep restructuring and reduction of the market presence of the bank. Those requirements are even more acute if there is no remuneration of the aid, most of which will never be recovered. At the same time, a significant part of the losses which the bank incurred in recent years do not seem to stem from

[33] See footnote 1.

risk-taking activities but from the holding of government bonds. That factor may justify the view that the aid is creating fewer distortions of competition. However, it has also to be observed that TT was holding proportionally to its size far more GGBs than the other banks in Greece. At this stage, the Commission considers that apparently excessive investment in GGBs could reflect some inappropriate risk-taking. The authorities and interested parties are invited to comment on that view.

(105) In terms of market presence, the Commission observes that the creation of the bridge bank is not a real resolution of TT as the restructuring plan of New TT foresees that New TT remains on the market nearly as TT was before.

(106) TT was a medium-sized bank in Greece (approximately 6 % in terms of deposits). TT's assets and liabilities transferred into New TT are relatively small when compared with the size of the Greek banking system. Also, the bank has no foreign activities. Therefore, despite the exceptionally large aid amount, the distortions of competition caused by the aid to New TT could be considered to be rather limited.

(107) However, to limit the risk that New TT would offer interest rates on deposits which are much higher than the interest rates on deposits of most of the competitors, a price leadership ban may be contemplated for New TT. Such a price leadership ban would decrease the probability that New TT uses the State aid to pay high interest rates and distorts competition on the market for deposits. Furthermore, to ensure that New TT does not expand its business and to limit the competition distortions, the Commission is of the view that some behavioural measures such as an acquisition ban and a ban on strong growth in lending would seem necessary.

(108) At this stage, the Commission therefore doubts that sufficient measures are taken to limit undue distortions of competition.

3.3 **Conclusion**

(109) In the light of the foregoing considerations, the Commission decides that measures A, B, C and D constitute State aid within the meaning of Article 107(1) TFEU and approves them provisionally as rescue aid. It doubts that those measures may be found compatible with the internal market pursuant to Article 107(3)(b) TFEU as restructuring aid, as they do not seem to comply with the requirements of the Restructuring Communication.

The Commission has accordingly decided to consider the aid to be temporarily compatible with the internal market within the meaning of Article 107(1) TFEU. Moreover, and in the light of the foregoing considerations, the Commission, acting under the procedure laid down in Article 108(2) of the TFEU, requests the Hellenic Republic to submit its comments and to provide all such information as may help to assess the restructuring aid, within one month of the date of receipt of this letter. In particular, it requests the Hellenic Republic to submit a new restructuring plan for New TT which addresses the Commission's doubts expressed in this decision. It requests your authorities to forward a copy of this letter to the potential recipient of the aid immediately.

The Commission wishes to draw the attention of the Hellenic Republic to Article 14 of Council Regulation (EC) No 659/1999, which provides that all unlawful aid may be recovered from the recipient.

Finally, the Commission warns the Hellenic Republic that it will inform interested parties by publishing this letter and a meaningful summary of it in the *Official Journal of the European Union*. It will also inform interested parties in the EFTA countries which are signatories to the EEA Agreement, by publication of a notice in the EEA Supplement to the *Official Journal of the European Union* and will inform the EFTA Surveillance Authority by sending a copy of this letter. All such interested parties will be invited to submit their comments within one month of the date of such publication.»

Prix d'abonnement 2013 (hors TVA, frais de port pour expédition normale inclus)

Journal officiel de l'UE, séries L + C, édition papier uniquement	22 langues officielles de l'UE	1 300 EUR par an
Journal officiel de l'UE, séries L + C, papier + DVD annuel	22 langues officielles de l'UE	1 420 EUR par an
Journal officiel de l'UE, série L, édition papier uniquement	22 langues officielles de l'UE	910 EUR par an
Journal officiel de l'UE, séries L + C, DVD mensuel (cumulatif)	22 langues officielles de l'UE	100 EUR par an
Supplément au Journal officiel (série S — Marchés publics et adjudications), DVD, une édition par semaine	Multilingue: 23 langues officielles de l'UE	200 EUR par an
Journal officiel de l'UE, série C — Concours	Langues selon concours	50 EUR par an

L'abonnement au *Journal officiel de l'Union européenne,* qui paraît dans les langues officielles de l'Union européenne, est disponible dans 22 versions linguistiques. Il comprend les séries L (Législation) et C (Communications et informations).

Chaque version linguistique fait l'objet d'un abonnement séparé.

Conformément au règlement (CE) nº 920/2005 du Conseil, publié au Journal officiel L 156 du 18 juin 2005, stipulant que les institutions de l'Union européenne ne sont temporairement pas liées par l'obligation de rédiger tous les actes en irlandais et de les publier dans cette langue, les Journaux officiels publiés en langue irlandaise sont commercialisés à part.

L'abonnement au Supplément au Journal officiel (série S — Marchés publics et adjudications) regroupe la totalité des 23 versions linguistiques officielles en un DVD multilingue unique.

Sur simple demande, l'abonnement au *Journal officiel de l'Union européenne* donne droit à la réception des diverses annexes du Journal officiel. Les abonnés sont avertis de la parution des annexes grâce à un «Avis au lecteur» inséré dans le *Journal officiel de l'Union européenne*.

Ventes et abonnements

Les abonnements aux diverses publications payantes, comme l'abonnement au *Journal officiel de l'Union européenne*, sont disponibles auprès de nos bureaux de vente. La liste des bureaux de vente est disponible à l'adresse suivante:

http://publications.europa.eu/others/agents/index_fr.htm

EUR-Lex (http://eur-lex.europa.eu) offre un accès direct et gratuit au droit de l'Union européenne. Ce site permet de consulter le *Journal officiel de l'Union européenne* et inclut également les traités, la législation, la jurisprudence et les actes préparatoires de la législation.

Pour en savoir plus sur l'Union européenne, consultez: http://europa.eu

Office des publications de l'Union européenne
2985 Luxembourg
LUXEMBOURG

FR