1.4.2014 FR Journal officiel de l'Union européenne C 96/1

II

(Communications)

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

PARLEMENT EUROPÉEN

DÉCISION DU BUREAU DU PARLEMENT EUROPÉEN

du 15 avril 2013

concernant les règles applicables au traitement des informations confidentielles par le Parlement européen

(2014/C 96/01)

LE BUREAU DU PARLEMENT EUROPÉEN,

vu l'article 23, paragraphe 12, du règlement du Parlement européen,

Considérant ce qui suit:

(1) Vu l'accord-cadre sur les relations entre le Parlement européen et la Commission européenne [1], signé le 20 octobre 2010 (ci-après dénommé «accord-cadre»), et l'accord interinstitutionnel entre le Parlement européen et le Conseil relatif à la transmission au Parlement européen et au traitement par celui-ci des informations classifiées détenues par le Conseil concernant d'autres questions que celles relevant de la politique étrangère et de sécurité commune [2], signé le 12 mars 2014, («l'accord interinstitutionnel»), il est nécessaire de définir des règles spécifiques sur le traitement des informations confidentielles par le Parlement européen.

(2) Le traité de Lisbonne confère de nouvelles tâches au Parlement européen et, afin de développer les activités du Parlement dans les domaines qui exigent un certain degré de confidentialité, il est nécessaire d'établir des principes de base, des normes minimales de sécurité et des procédures appropriées pour le traitement des informations confidentielles, y compris des informations classifiées, par le Parlement européen.

(3) Les règles établies par la présente décision visent à garantir des normes de protection équivalentes et une compatibilité avec les réglementations adoptées par d'autres institutions, organes, organismes et agences établis en vertu ou sur la base des traités ou par les États membres, afin de faciliter le bon fonctionnement du processus décisionnel de l'Union européenne.

(4) Les dispositions de la présente décision sont arrêtées sans préjudice des règles actuelles et futures sur l'accès aux documents adoptées conformément à l'article 15 du traité sur le fonctionnement de l'Union européenne (TFUE).

[1] JO L 304 du 20.11.2010, p. 47.
[2] JO C 95, 1.4.2014, p. 1.

(5) Les dispositions de la présente décision sont arrêtées sans préjudice des règles actuelles et futures sur la protection des données personnelles adoptées conformément à l'article 16 du traité sur le fonctionnement de l'Union européenne (TFUE),

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Objectif

La présente décision régit la gestion et le traitement des informations confidentielles par le Parlement européen, y compris la création, la réception, la transmission et le stockage de ces informations en vue d'assurer une protection appropriée de leur caractère confidentiel. Elle met en œuvre l'accord interinstitutionnel et l'accord-cadre, l'annexe II de celui-ci en particulier.

Article 2

Définitions

Aux fins de la présente décision, on entend par:

a) «information»: toute information écrite ou orale, quel qu'en soit le support ou l'auteur;

b) «informations confidentielles»: «informations classifiées» et «autres informations confidentielles» non classifiées;

c) «informations classifiées»: «informations classifiées de l'UE» et «informations classifiées équivalentes»;

d) «informations classifiées de l'UE» (ICUE): toute information et tout matériel classifiés «TRÈS SECRET UE/EU TOP SECRET», «SECRET UE/EU SECRET», «CONFIDENTIEL UE/EU CONFIDENTIAL» ou «RESTREINT UE/EU RESTRICTED», dont la divulgation non autorisée porterait atteinte à des degrés divers aux intérêts de l'Union, ou à ceux d'un ou plusieurs de ses États membres, que ces informations aient leur origine au sein des institutions, organes ou agences établis en vertu ou sur la base des traités. À cet égard, les informations et le matériel classifiés au niveau:

— «TRÈS SECRET UE/EU TOP SECRET» sont des informations et du matériel dont la divulgation non autorisée pourrait causer un préjudice exceptionnellement grave aux intérêts essentiels de l'Union ou d'un ou plusieurs des États membres,

— «SECRET UE/EU SECRET» sont des informations et du matériel dont la divulgation non autorisée pourrait nuire gravement aux intérêts essentiels de l'Union ou d'un ou plusieurs des États membres,

— «CONFIDENTIEL UE/EU CONFIDENTIAL» sont des informations et du matériel dont la divulgation non autorisée pourrait nuire aux intérêts essentiels de l'Union ou d'un ou plusieurs des États membres;

— «RESTREINT UE/EU RESTRICTED» sont des informations et du matériel dont la divulgation non autorisée pourrait être défavorable aux intérêts de l'Union ou d'un ou plusieurs des États membres;

e) «informations classifiées équivalentes»: informations classifiées transmises par des États membres, des États tiers ou des organisations internationales, qui portent un marquage de classification de sécurité équivalent à l'un des marquages de classification de sécurité utilisé pour les ICUE et qui ont été transmises au Parlement européen par le Conseil ou la Commission;

f) «autres informations confidentielles»: toutes autres informations confidentielles non classifiées, y compris les informations couvertes par les règles relatives à la protection des données ou par l'obligation de secret professionnel, qu'elles aient leur origine au sein du Parlement européen ou qu'elles aient été transmises au Parlement européen par d'autres institutions, organes, organismes et agences établis en vertu ou sur la base des traités ou par les États membres;

g) «document»: toute information enregistrée, quelles que soient sa forme physique ou ses caractéristiques;

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

i) «besoin d'en connaître»: la nécessité, pour une personne, d'accéder à des informations confidentielles pour pouvoir s'acquitter d'une fonction officielle ou d'une tâche donnée;

j) «autorisation»: une décision par laquelle le Président, si elle concerne les députés au Parlement européen, ou le Secrétaire général, si elle concerne les fonctionnaires du Parlement européen et autres employés du Parlement européen travaillant pour les groupes politiques, permet à un individu d'accéder à des informations classifiées jusqu'à un niveau donné, sur la base du résultat positif d'une enquête de sécurité (vérification) effectuée par une autorité nationale au titre du droit national et conformément aux dispositions de l'annexe I, partie 2;

k) «déclassement»: une diminution du niveau de la classification;

l) «déclassification»: la suppression de toute classification;

m) «marquage»: un signe apposé à «d'autres informations confidentielles» destiné à identifier des instructions concrètes prédéfinies sur leur traitement ou le domaine couvert par un document donné. Il peut aussi être apposé à des informations classifiées afin d'imposer des exigences supplémentaires pour leur traitement.

n) «retrait de marquage»: la suppression de tout marquage;

o) «autorité d'origine»: l'auteur, dûment autorisé, d'une information confidentielle;

p) «consignes de sécurité»: les mesures de mise en œuvre établies à l'annexe II;

q) «instructions de traitement»: les instructions techniques données aux services du Parlement sur la gestion des informations confidentielles.

Article 3

Principes de base et normes minimales

1. Le traitement des informations confidentielles par le Parlement européen obéit aux principes de base et normes minimales fixés à l'annexe I, partie 1.

2. Le Parlement européen met en place un système de gestion de la sécurité des informations (SGSI) conformément à des principes de base et des normes minimales. Le SGSI se compose de notices de sécurité, d'instructions de manipulation et de règles de procédure pertinentes. L'objectif du SGSI est de faciliter le travail administratif et parlementaire tout en garantissant la protection de toute information confidentielle traitée par le Parlement, dans le respect des règles établies par l'autorité d'origine de cette information décrites dans les consignes de sécurité. Le SGSI comprend les consignes de sécurité, les instructions de traitement et les dispositions applicables du règlement.

Le traitement des informations confidentielles par le biais du système informatique et de communication automatisé (SIC) du Parlement européen est mis en œuvre conformément au concept d'assurance information, inscrit dans la consigne de sécurité n° 3

3. Les députés au Parlement européen peuvent consulter les informations classifiées jusque et y compris au niveau RESTREINT UE/EU RESTRICTED sans habilitation de sécurité.

4. Quand les informations en question sont classifiées au niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou à son équivalent, l'accès à ces informations est accordé aux membres du Parlement européen qui ont été autorisés par le Président conformément au paragraphe 5 ou après avoir signé une déclaration solennelle de non-divulgation du contenu de ces informations à des tiers, du respect de l'obligation de protéger les informations classifiées au niveau CONFIDENTIEL UE/EU CONFIDENTIAL et de reconnaissance des conséquences en cas de manquement.

5. Quand lesdites informations sont classifiées au niveau SECRET UE/EU SECRET, au niveau TRÈS SECRET/EU TOP SECRET ou à leurs équivalents, l'accès à ces informations est accordé aux députés au Parlement européen autorisés par le Président du Parlement européen après:

a) qu'ils aient reçu l'habilitation de sécurité nécessaire, conformément à l'annexe I, partie 2, de la présente décision, ou

b) qu'une autorité nationale compétente a fait savoir qu'ils sont dûment autorisés en vertu de leurs fonctions, conformément aux dispositions législatives nationales.

6. Avant de se voir accorder l'accès à une information classifiée, les députés au Parlement européen sont informés des responsabilités qui leur incombent en matière de protection de cette information et prennent acte de leurs responsabilités quant à la protection de ces informations, conformément à l'annexe I. ils sont aussi informés des moyens d'assurer cette protection.

7. Les fonctionnaires du Parlement européen et les autres employés du Parlement travaillant pour les groupes politiques peuvent consulter des informations confidentielles s'ils ont un «besoin d'en connaître» avéré et peuvent consulter les informations classifiées au-dessus du niveau RESTREINT UE/EU RESTRICTED s'ils disposent de l'habilitation de sécurité du niveau approprié. L'accès aux informations classifiées est accordé uniquement s'ils ont été informés de, et ont reçu des instructions écrites sur, leurs responsabilités en matière de protection de cette information et les moyens d'assurer cette protection, et aussi s'ils ont signé une déclaration par laquelle ils accusent réception de ces instructions et s'engagent à les respecter conformément aux présentes règles.

Article 4

Création d'informations confidentielles et traitement administratif par le Parlement européen

1. Le Président du Parlement européen, les présidents des commissions parlementaires concernées et le Secrétaire général et/ou toute personne qu'il a dûment autorisée par écrit peuvent créer des informations confidentielles et/ou classifier des informations tel que cela est prévu par les consignes de sécurité.

2. Lorsqu'elle crée une information classifiée, l'autorité d'origine applique le degré de classification approprié, conformément aux normes internationales et définitions établies à l'annexe I de la présente décision du Bureau. L'autorité d'origine définit aussi, en règle générale, les destinataires qui sont habilités à consulter cette information, en fonction du niveau de classification. Cette information est communiquée à l'unité Informations classifiées (UIC) lors du dépôt du document auprès de l'UIC.

3. Les autres informations confidentielles couvertes par le secret professionnel sont traitées conformément aux annexes I et II et aux instructions de traitement.

Article 5

Réception d'informations confidentielles par le Parlement européen

1. Les informations confidentielles reçues par le Parlement européen sont communiquées comme suit:

a) les informations classifiées au niveau RESTREINT UE/EU RESTRICTED ou à son équivalent et les autres informations confidentielles: au secrétariat de l'organe/du titulaire d'un mandat au sein du Parlement qui a présenté la demande, ou directement à l'UIC,

b) les informations classifiées aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET ou à leurs équivalents: à l'UIC.

2. L'enregistrement, le stockage et la traçabilité des informations confidentielles sont assurés, selon le cas, soit par le secrétariat de l'organe/titulaire d'un mandat au sein du Parlement européen qui a reçu les informations, soit par l'UIC.

3. Les modalités convenues à établir de commun accord afin de préserver la confidentialité des informations, dans le cas d'informations confidentielles communiquées par la Commission sur la base du point 3.2 de l'annexe II de l'accord-cadre, ou, dans le cas d'informations classifiées transmises par le Conseil conformément à l'article 5, paragraphe 4, de l'accord interinstitutionnel, sont déposées, avec les informations confidentielles, auprès du secrétariat de l'organe parlementaire/de la personne mandatée ou de l'UIC, selon le cas.

4. Les modalités visées au paragraphe 3 peuvent également être appliquées *mutatis mutandis* à la communication d'informations confidentielles par d'autres institutions, organes, organismes et agences établis en vertu ou sur la base des traités ou par les États membres.

5. Afin de garantir un niveau de protection proportionné au niveau de classification «TRÈS SECRET UE/EU TOP SECRET» ou à son équivalent, la Conférence des présidents établit un comité de surveillance. Les informations classifiées au niveau TRÈS SECRET UE/EU TOP SECRET ou à son équivalent sont communiquées au Parlement européen selon d'autres modalités, à convenir entre le Parlement européen et l'institution de l'Union de laquelle les informations sont reçues.

Article 6

Communication d'informations classifiées par le Parlement européen à des tiers

Le Parlement européen peut, avec le consentement écrit préalable de l'autorité d'origine ou de l'institution de l'Union qui a communiqué les informations classifiées au Parlement européen, selon le cas, transmettre de telles informations classifiées à des tiers à la condition qu'ils garantissent que, lors du traitement de telles informations, des règles équivalentes à celles fixées par la présente décision sont respectées dans leurs services et leurs locaux.

Article 7

Installations sécurisées

1. Aux fins de la gestion des informations confidentielles, le Parlement européen établit une zone sécurisée et des salles de lecture sécurisées.

2. La zone sécurisée prévoit des installations pour l'enregistrement, la consultation, l'archivage, la transmission et le traitement des informations classifiées. Elle comprend, entre autres, une salle de lecture sécurisée et une salle de réunion pour la consultation des informations classifiées et est gérée par l'UIC.

3. En dehors de la zone sécurisée, des salles de lecture sécurisées peuvent être créées, afin de permettre la consultation des informations classifiées au niveau RESTREINT UE/UE RESTRICTED ou à son équivalent, et d'«autres informations confidentielles». Ces salles de lecture sécurisées sont gérées par les services compétents des secrétariats des organes ou titulaires d'un mandat du Parlement ou par l'UIC, selon le cas. Elles ne comportent ni photocopieurs, ni téléphones, ni fax, ni scanners ni autre moyen technique de reproduction ou de transmission de documents.

Article 8

Enregistrement, traitement et stockage des informations confidentielles

1. Les informations classifiées au niveau RESTREINT UE/EU RESTRICTED ou à son équivalent et les «autres informations confidentielles» peuvent être enregistrées et stockées par les services compétents des secrétariats des organes ou titulaires d'un mandat du Parlement ou par l'UIC, en fonction de la personne qui a reçu les informations.

2. Les conditions suivantes s'appliquent au traitement des informations classifiées au niveau RESTREINT UE/EU RESTRICTED ou à son équivalent et des «autres informations confidentielles»:

a) les documents sont remis en mains propres au chef du secrétariat, qui les enregistre et fournit un accusé de réception;

b) lorsqu'ils ne sont pas effectivement utilisés, ces documents sont tenus dans un lieu fermé à clé, sous la responsabilité du secrétariat;

c) en aucun cas les informations ne sont sauvegardées sur un autre support ou transmises à quiconque. De tels documents peuvent seulement être reproduits à l'aide de matériel dûment homologué, comme défini dans les consignes de sécurité;

d) l'accès à ces informations est limité aux personnes désignées par l'autorité d'origine ou par l'institution de l'Union qui a communiqué les informations au Parlement européen, conformément aux modalités visées à l'article 4, paragraphe 2, ou à l'article 5, paragraphes 3, 4 et 5;

e) le secrétariat de l'organe/titulaire d'un mandat parlementaire tient un registre des personnes ayant consulté les informations, qui indique la date et l'heure de la consultation, and transmettent le registre à l'UIC lors du dépôt des informations auprès de l'UIC.

3. Les informations classifiées au niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET ou à leurs niveau équivalents sont enregistrées, traitées et stockées par l'UIC dans la zone sécurisée, conformément au niveau de classification donné et comme défini dans les consignes de sécurité.

4. En cas de manquements aux règles définies aux paragraphes 1 à 3, le fonctionnaire responsable du secrétariat de l'organe/titulaire d'un mandat du Parlement européen ou de l'UIC, selon le cas, en informe le Secrétaire général, qui en réfère au Président au cas où un député au Parlement européen est concerné.

Article 9

Accès aux installations sécurisées

1. Seules les personnes ci-après ont accès à la zone sécurisée:

a) les personnes qui, conformément à l'article 3, paragraphes 4 à 7 sont autorisées à consulter les informations qui y sont détenues et qui ont introduit une demande en vertu de l'article 10, paragraphe 1;

b) les personnes qui, conformément à l'article 4, paragraphe 1, sont autorisées à créer des informations classifiées et qui ont introduit une demande en vertu de l'article 10, paragraphe 1;

c) les fonctionnaires du Parlement européen de l'UIC;

d) les fonctionnaires du Parlement européen gestionnaires du SIC;

e) les fonctionnaires du Parlement européen responsables de la sécurité et de la protection contre l'incendie, si nécessaire;

f) le personnel de nettoyage, mais uniquement en la présence et sous la surveillance étroite d'un fonctionnaire de l'UIC.

2. L'UIC peut refuser l'accès à la zone sécurisée à toute personne non autorisée à entrer. Toute contestation de la décision de l'UIC est soumise au Président dans le cas de demande d'accès émanant des députés au Parlement européen, et au Secrétaire général dans les autres cas.

3. Le Secrétaire général peut autoriser une réunion pour un nombre limité de personnes dans la salle de réunion située au sein de la zone sécurisée.

4. Seules les personnes ci-après ont accès à une salle de lecture sécurisée:

a) les députés au Parlement européen, les fonctionnaires du Parlement européen et les autres employés du Parlement européen travaillant pour les groupes politiques, dûment identifiés aux fins de la consultation ou de la création des informations confidentielles;

b) les fonctionnaires du Parlement européen chargés de la gestion du SIC, les fonctionnaires du secrétariat de l'organe/titulaire d'un mandat du Parlement européen qui a reçu les informations et les fonctionnaires de l'UIC;

c) quand cela est nécessaire, les fonctionnaires du Parlement européen responsables de la sécurité et de la protection contre l'incendie;

d) le personnel de nettoyage, mais uniquement en la présence et sous la surveillance étroite d'un fonctionnaire travaillant au secrétariat de l'organe/titulaire d'un mandat du Parlement européen ou à l'UIC, selon le cas.

5. Le secrétariat compétent de l'organe/du titulaire d'un mandat du Parlement européen ou l'UIC, selon le cas, peut refuser l'accès d'une salle de lecture sécurisée à toute personne non autorisée. Toute contestation d'un tel refus d'accès est soumise au Président dans le cas de demande d'accès émanant des députés au Parlement européen, et au Secrétaire général dans les autres cas.

Article 10

Consultation ou création d'informations confidentielles dans les installations sécurisées

1. Toute personne qui souhaite consulter ou créer des informations confidentielles dans la zone sécurisée communique à l'avance son nom à l'UIC. L'UIC vérifie l'identité de cette personne présentant une demande et vérifie qu'elle est autorisée, conformément aux modalités visées à l'article 3, paragraphes 3 à 7, à l'article 4, paragraphe 1, ou à l'article 5, paragraphes 3, 4 et 5, à consulter ou à créer des informations confidentielles.

2. Toute personne qui souhaite, conformément à l'article 3, paragraphes 3 et 7, consulter des informations confidentielles classifiées au niveau RESTREINT UE/EU RESTRICTED ou à son équivalent, ou d'«autres informations confidentielles» dans une salle de lecture sécurisée, communique à l'avance son nom aux services compétents des secrétariats de l'organe/du titulaire d'un mandat du Parlement européen ou à l'UIC.

3. Sauf dans des circonstances exceptionnelles (par exemple lorsqu'un grand nombre de demandes de consultation est introduit dans un court laps de temps), une seule personne à la fois est autorisée à consulter des informations confidentielles dans l'installation sécurisée, en présence d'un fonctionnaire du secrétariat de l'organe/du titulaire d'un mandat du Parlement européen ou de l'UIC.

4. Pendant la période de consultation, ne sont autorisés ni les contacts avec l'extérieur (y compris par l'usage du téléphone ou d'autres outils technologiques), ni la prise de notes, ni la photocopie ou la photographie des informations confidentielles consultées.

5. Avant d'autoriser une personne à quitter l'installation sécurisée, le fonctionnaire du secrétariat de l'organe/du titulaire d'un mandat du Parlement européen ou de l'UIC s'assure que les informations confidentielles consultées sont toujours présentes, intactes et complètes.

6. En cas de manquements aux règles définies ci-dessus, le fonctionnaire du secrétariat de l'organe/titulaire d'un mandat du Parlement européen ou de l'UIC informe le Secrétaire général qui en référera au Président au cas où un député au Parlement européen est concerné.

Article 11

Normes minimales applicables à la consultation d'informations confidentielles lors d'une réunion à huis clos à l'extérieur des installations sécurisées

1. Les informations classifiées au niveau RESTREINT UE/EU RESTRICTED ou à son équivalent et d'autres informations confidentielles peuvent être consultées par des membres de commissions parlementaires ou d'autres organes politiques et administratifs du Parlement européen lors d'une réunion à huis clos à l'extérieur des installations sécurisées.

2. Dans le cas prévu au paragraphe 1, le secrétariat de l'organe/du titulaire d'un mandat au sein du Parlement européen responsable de la réunion veille à ce que les conditions suivantes soient respectées, à savoir:

a) seules les personnes désignées pour participer à la réunion par la présidence de la commission compétente ou de l'organe compétent sont autorisées à pénétrer dans la salle de réunion;

b) tous les documents sont numérotés, distribués au début de la réunion et récupérés à la fin et aucune note, photocopie ou photographie de ces documents n'est prise;

c) le procès-verbal de la réunion ne mentionne pas le contenu de la discussion sur les informations qui ont été examinées. Seule la décision, si décision il y a, peut figurer au procès-verbal;

d) les informations confidentielles communiquées oralement à des destinataires au Parlement européen sont soumises à un niveau de protection équivalent à celui appliqué aux informations confidentielles ayant la forme d'un écrit;

e) aucun document supplémentaire ne peut être détenu dans les salles de réunion;

f) seul le nombre nécessaire de copies des documents est distribué aux participants et aux interprètes au début de la réunion;

g) l'état de classification ou de marquage des documents est précisé par la présidence de la réunion au début de la réunion;

h) les participants n'emportent pas de documents en dehors de la salle de réunion;

i) toutes les copies de documents sont rassemblées et comptées à la fin de la réunion par le secrétariat de l'organe/du titulaire d'un mandat du Parlement européen;

j) aucun équipement de communication électronique ou autre équipement électronique n'est introduit dans la salle de réunion lorsque les informations confidentielles en question sont consultées ou examinées.

3. Lorsque, conformément aux exceptions prévues au point 3.2.2 de l'annexe II à l'accord-cadre et à l'article 6, paragraphe 5, de l'accord interinstitutionnel, les informations classifiées au niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou à son équivalent sont examinées lors d'une réunion à huis clos, le secrétariat de l'organe/du titulaire d'un mandat du Parlement européen responsable de la réunion, outre les dispositions prévues au paragraphe 2, s'assure que les personnes désignées pour participer à la réunion satisfont aux exigences de l'article 3, paragraphes 4 et 7.

4. Dans le cas prévu au paragraphe 3, l'UIC fournit au secrétariat de l'organe/du titulaire d'un mandat du Parlement européen responsable de la réunion à huis clos, le nombre nécessaire de copies des documents à examiner, qui sont restituées à l'UIC après la réunion.

Article 12

Archivage des informations confidentielles

1. Un système d'archivage sécurisé est assuré dans la zone sécurisée. L'UIC est responsable de la gestion des archives sécurisées, conformément aux normes en matière d'archivage.

2. Les informations classifiées définitivement déposées auprès de l'UIC et les informations classifiées au niveau RESTREINT UE/EU RESTRICTED ou son équivalent qui sont déposées auprès du secrétariat de l'organe /du titulaire d'un mandat au sein du Parlement européen sont transférées vers les archives sécurisées dans la zone sécurisée six mois après la dernière consultation et, au plus tard, un an après leur dépôt. Les «autres informations confidentielles» sont archivées, à moins qu'elles ne soient déposées auprès de l'UIC, par les secrétariats de l'organe/titulaire d'un mandat du Parlement européen concerné, conformément aux règles générales relatives à la gestion des documents.

3. Les informations confidentielles conservées dans les archives sécurisées peuvent être consultées aux conditions suivantes:

a) seules sont autorisées à consulter ces informations les personnes identifiées, par leur nom ou par leur fonction, dans le document d'accompagnement établi lors du dépôt des informations;

b) la demande de consultation de ces informations est présentée à l'UIC qui assure le transfert du document vers la salle de lecture sécurisée;

c) les procédures et conditions applicables à la consultation des informations confidentielles, définies à l'article 10, s'appliquent.

Article 13

Déclassement, déclassification et retrait du marquage des informations confidentielles

1. Les informations confidentielles ne peuvent être déclassées, déclassifiées ou faire l'objet d'un retrait de marquage qu'avec l'accord préalable de l'autorité d'origine et, si nécessaire, après consultation des autres parties intéressées.

2. Le déclassement ou la déclassification fait l'objet d'une confirmation écrite. Il incombe à l'autorité d'origine d'informer ses destinataires du changement, ces derniers étant à leur tour chargés d'en aviser les destinataires successifs auxquels ils ont fait suivre l'original ou une copie du document. Dans la mesure du possible, l'autorité d'origine indique sur le document classifié la date, le délai ou l'événement à partir duquel son contenu peut être déclassé ou déclassifié. À défaut, elle réexamine la question tous les cinq ans au plus pour s'assurer que la classification initiale demeure nécessaire.

3. Les informations confidentielles conservées dans les archives sécurisées sont examinées en temps utile et au plus tard le jour du 25e anniversaire de sa création, afin de décider si elles doivent ou non être déclassifiées, déclassées ou faire l'objet d'un retrait de marquage. L'examen et la publication de telles informations ont lieu conformément aux dispositions du règlement (CEE, Euratom) no 354/83 du Conseil du 1er février 1983 concernant l'ouverture au public des archives historiques de la Communauté économique européenne et de la Communauté européenne de l'énergie atomique ([1]). L'autorité d'origine des informations classifiées ou le service qui est responsable procède à la déclassification conformément à l'annexe I, partie 1, section 10.

4. À la suite de la déclassification, les informations anciennement classifiées et conservées dans les archives sécurisées sont transférées aux archives historiques du Parlement européen pour une conservation permanente et pour un traitement ultérieur conformément aux règles applicables.

5. À la suite du retrait d'un marquage, les anciennes «autres informations confidentielles» sont soumises aux règles du Parlement européen relatives à la gestion des documents.

Article 14

Manquements aux règles de sécurité, perte ou compromission d'informations confidentielles

1. Une violation de la confidentialité en général, et de la présente décision en particulier, entraîne, dans le cas des députés au Parlement européen, l'application des dispositions pertinentes concernant les sanctions, prévues par le règlement du Parlement européen.

2. Une violation commise par un membre du personnel du parlement européen entraîne l'application des procédures et sanctions prévues respectivement par le statut des fonctionnaires et le régime applicable aux autres agents de l'Union européenne, fixés par le règlement (CEE, Euratom, CECA) no 259/68 du Conseil (ci-après dénommés «statut des fonctionnaires»).

([1]) JO L 43 du 15.2.1983, p. 1.

3. Le Président et/ou le Secrétaire général, selon le cas, diligentent les enquêtes nécessaires en cas de violation telle que définie à la consigne de sécurité n° 6.

4. Si les informations confidentielles ont été communiquées au Parlement européen par une autre institution de l'Union ou par un Etat membre, le Président et/ou le Secrétaire général, selon le cas, informent l'institution de l'Union concernée de toute perte suspecte ou avérée ou compromission d'informations classifiées et des résultats de l'enquête et des mesures prises pour empêcher une récidive.

Article 15

Adaptation de la présente décision et de ses modalités de mise en œuvre et rapport annuel sur l'application de la présente décision

1. Le Secrétaire général propose les adaptations nécessaires de la présente décision et des annexes qui la mettent en œuvre et transmet ces propositions au Bureau en vue d'une décision.

2. Le Secrétaire général est responsable de la mise en œuvre de la présente décision par les services du Parlement européen et publie les instructions de traitement sur les sujets couverts pas le SGSI, conformément aux principes établis par la présente décision.

3. Le Secrétaire général présente un rapport annuel au Bureau sur l'application de la présente décision.

Article 16

Dispositions transitoires et finales

1. Les informations non classifiées se trouvant à l'UIC ou dans d'autres archives du Parlement européen qui sont considérées comme confidentielles et datées avant le 1 avril 2014 sont considérées, aux fins de la présente décision, comme étant des «autres informations confidentielles». Leur autorité d'origine peut à tout moment réexaminer leur niveau de confidentialité.

2. Par dérogation au point a) de l'article 5, paragraphe 1, et à l'article 8, paragraphe 1, de la présente décision, pendant une période de douze mois à compter du 1 avril 2014, les informations communiquées par le Conseil conformément à l'accord interinstitutionnel qui sont classifiées au niveau RESTREINT UE/EU RESTRICTED ou à son équivalent sont déposées auprès de l'UIC, enregistrées et conservées par celle-ci. Ces informations peuvent être consultées conformément à l'article 4, paragraphe 2, point a) et c) et à l'article 5, paragraphe 4, de l'accord interinstitutionnel.

3. La décision du Bureau du 6 juin 2011 concernant les règles applicables au traitement des informations confidentielles par le Parlement européen est abrogée.

Article 17

Entrée en vigueur

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

ANNEXE I

Partie 1

PRINCIPES DE BASE ET NORMES MINIMALES DE SÉCURITÉ POUR LA PROTECTION DES INFORMATIONS CONFIDENTIELLES

1. **INTRODUCTION**

Les présentes dispositions définissent les principes de base et les normes minimales de sécurité pour la protection des informations confidentielles devant être respectés et appliqués par le Parlement européen dans tous ses lieux de travail ainsi que par tout destinataire d'informations classifiées et d'autres informations confidentielles, de manière à assurer la sécurité et de sorte que toutes les personnes concernées puissent avoir la certitude qu'une norme de protection commune est établie. Ces dispositions sont complétées par les ***consignes de sécurité inclue dans l'annexe II et d'autres*** dispositions régissant le traitement des informations confidentielles par les commissions parlementaires et les autres organes/titulaires d'un mandat au sein du Parlement européen.

2. **PRINCIPES DE BASE**

La politique de sécurité du Parlement européen fait partie intégrante de sa politique de gestion interne générale et est par conséquent basée sur les principes régissant cette politique générale. Ces principes comprennent la légalité, la transparence, la responsabilité ainsi que la subsidiarité et la proportionnalité.

La légalité implique qu'il est nécessaire de maintenir strictement dans le cadre juridique l'exécution des fonctions de sécurité, ainsi que de se conformer aux exigences juridiques applicables. En outre, les responsabilités en matière de sécurité doivent s'appuyer sur des dispositions juridiques appropriées. Les dispositions du statut des fonctionnaires s'appliquent pleinement, en particulier son article 17 concernant l'obligation de s'abstenir de toute divulgation non autorisée d'informations portées à leur connaissance dans l'exercice de leurs fonctions et son titre VI concernant le régime disciplinaire. Enfin, les manquements aux règles de sécurité commis dans le domaine de responsabilité du Parlement européen ***seront*** traités conformément ***à son règlement et*** à la politique du Parlement européen en matière de mesures disciplinaires.

La transparence implique qu'il est nécessaire d'établir des règles et dispositions de sécurité qui soient toutes caractérisées par leur clarté et d'assurer l'équilibre entre les différents services et les différents domaines (sécurité physique par opposition à la protection des données, etc.) et impose une politique cohérente et structurée de sensibilisation à la sécurité. De plus, il est nécessaire de disposer d'orientations écrites claires pour la mise en œuvre des mesures de sécurité.

La responsabilité signifie que les responsabilités dans le domaine de la sécurité doivent être clairement définies. Il implique également qu'il est nécessaire de contrôler régulièrement si ces responsabilités ont été correctement exécutées.

La subsidiarité signifie que la sécurité doit être organisée au plus bas niveau possible et au plus près des directions générales et des services du Parlement européen. La proportionnalité signifie que les activités de sécurité doivent être strictement limitées à celles qui sont absolument nécessaires et que les mesures de sécurité doivent être proportionnelles aux intérêts à protéger ainsi qu'aux menaces réelles ou potentielles qui pèsent sur ces intérêts, de manière à en organiser la protection dans des conditions imposant le moins de perturbations possible.

3. **FONDEMENTS D'UNE BONNE SÉCURITÉ DES INFORMATIONS**

Un système de sécurité des informations fiable a pour fondements:

a) un système de communication et d'information propre (SIC), qui relève de la responsabilité de l'autorité de sécurité du Parlement européen (telle que définie dans la consigne de sécurité n°1)

b) au sein du Parlement européen, l'Autorité chargée de l'assurance de l'information (telle que définie dans la consigne de sécurité n°1), chargée de travailler avec l'autorité responsable de la sécurité concernée (telle que définie dans la consigne de sécurité n° 1) pour fournir des informations et des avis sur les menaces d'ordre technique pesant sur les systèmes d'information et de communication (SIC) et sur les moyens de se protéger de ces menaces;

c) une collaboration étroite entre les services compétents du Parlement européen et les services de sécurité des autres institutions de l'Union;

4. **PRINCIPES RELATIFS À LA SÉCURITÉ DES INFORMATIONS**

4.1. ***Objectifs***

La sécurité des informations a pour objectifs principaux:

a) la protection des informations confidentielles contre l'espionnage, la compromission ou la divulgation non autorisée;

b) la sauvegarde des informations classifiées faisant l'objet de communications et transitant par des systèmes et réseaux d'information contre les menaces pesant sur leur confidentialité, leur intégrité et leur disponibilité;

c) la protection des locaux du Parlement européen abritant des informations classifiées contre les tentatives de sabotage et les actes intentionnels de détérioration;

d) en cas d'échec de la sécurité, l'évaluation du dommage causé, la limitation des conséquences, la réalisation d'enquêtes de sécurité et l'adoption des mesures correctives nécessaires.

4.2. ***Classement***

4.2.1. En matière de confidentialité, prudence et expérience sont nécessaires pour choisir les informations et matériels à protéger et pour évaluer le degré de protection à assurer. Il est essentiel que le degré de protection soit en rapport avec le caractère sensible que revêt, du point de vue de la sécurité, l'élément d'information ou le matériel à protéger. Afin d'assurer la bonne circulation des informations, doivent être évitées tant la surclassification que la sous-classification.

4.2.2. Le système de classification constitue l'instrument qui permet de mettre en œuvre les principes énoncés dans la présente section. Il convient d'adopter un système similaire pour la planification et l'organisation des mesures de lutte contre l'espionnage, le sabotage, le terrorisme et d'autres menaces de façon à protéger au mieux les installations les plus importantes contenant des informations classifiées et les éléments les plus sensibles à l'intérieur de ces installations.

4.2.3. L'autorité d'origine de l'information est seule responsable de sa classification.

4.2.4. Le niveau de classification se fonde exclusivement sur le contenu de l'information concernée.

4.2.5. Quand un certain nombre de renseignements sont regroupés, leur classification est au moins égale au degré de classification le plus élevé attribué à une partie séparée.. Il est néanmoins possible d'attribuer à un groupement d'informations une classification plus élevée que celle de ses composantes.

4.2.6 Les classifications sont attribuées uniquement en cas de nécessité et maintenues seulement aussi longtemps que nécessaire.

4.3. ***Objectifs des mesures de sécurité***

Les mesures de sécurité doivent:

a) s'appliquer à toutes les personnes ayant accès à des informations classifiées, aux supports des informations classifiées, aux autres informations confidentielles et à tous les locaux contenant de telles informations ainsi qu'aux installations importantes;

b) être conçues de façon à permettre d'identifier les personnes dont le poste (en termes d'accès, de relations ou autres) pourrait nuire à la sécurité de ces informations et des installations importantes contenant de telles informations, et de les exclure ou de les changer de poste;

c) empêcher toute personne non autorisée d'avoir accès à ces informations et aux installations qui en contiennent;

d) garantir que la diffusion de ces informations repose exclusivement sur le principe du besoin d'en connaître, qui est fondamental pour tous les aspects de la sécurité;

e) garantir l'intégrité (en empêchant l'altération, la modification non autorisée ou la destruction non autorisée) et la disponibilité (pour les personnes qui ont besoin de consulter les informations et qui y sont autorisées) d'informations confidentielles, en particulier lorsqu'elle sont stockées, traitées ou transmises sous forme électromagnétique.

5. NORMES MINIMALES COMMUNES

Le Parlement européen veille à ce que les normes minimales communes en matière de sécurité soient respectées par tout destinataire d'une information classifiée, à la fois à l'intérieur de l'institution et dans son domaine de compétence, par exemple ses services et contractants, de sorte que cette information puisse être transmise avec la certitude qu'elle sera traitée avec les mêmes précautions. Ces normes minimales doivent comprendre les critères applicables à l'habilitation de sécurité des fonctionnaires du Parlement européen et autres employés du Parlement travaillant pour les groupes politiques et les procédures à suivre pour la protection des informations confidentielles.

L'accès à ces informations ne peut être autorisé par le Parlement européen à des tiers que pour autant que ces tiers garantissent que de telles informations sont traitées conformément à des dispositions qui soient au moins strictement équivalentes aux présentes normes minimales communes.

Ces normes minimales communes sont également appliquées lorsque le Parlement charge, par contrat ou attribution, des entités industrielles ou autres de tâches qui font intervenir des informations confidentielles.

6. MESURES DE SÉCURITÉ APPLICABLES AUX FONCTIONNAIRES DU PARLEMENT EUROPÉEN ET AUX AUTRES EMPLOYÉS DU PARLEMENT TRAVAILLANT POUR LES GROUPES POLITIQUES

6.1. *Instructions de sécurité applicables aux fonctionnaires du Parlement européen et autres employés du Parlement travaillant pour les groupes politiques*

Les fonctionnaires du Parlement européen et les autres employés du Parlement travaillant pour les groupes politiques occupant un poste qui peut leur donner accès à des informations classifiées doivent recevoir, lors de leur entrée en fonction puis à intervalles réguliers, un exposé très complet des mesures de sécurité nécessaires et des procédures concernées. Ces personnes doivent confirmer par écrit avoir lu et pleinement compris les dispositions applicables en matière de sécurité.

6.2. *Responsabilités du personnel d'encadrement*

Il incombe au personnel d'encadrement de savoir quels sont les membres de leur personnel qui traitent des informations classifiées ou qui ont accès à des systèmes de communication ou d'information sécurisés ainsi que de prendre note des incidents ou des vulnérabilités apparentes pouvant avoir des répercussions sur le plan de la sécurité, et de les signaler.

6.3. *Statut, en matière de sécurité, des fonctionnaires du Parlement européen et autres employés du Parlement travaillant pour les groupes politiques*

Sont établies des procédures garantissant, si des renseignements défavorables viennent à être communiqués à propos d'un fonctionnaire du Parlement européen ou d'un autre employé du Parlement travaillant pour un groupe politique, que des mesures sont prises pour déterminer si cette personne effectue un travail lui donnant accès à des informations classifiées, ou si elle a accès à des systèmes de communication ou d'information sécurisés, et que le service compétent du Parlement européen est informé. Si l'autorité nationale de sécurité compétente indique que cette personne présente un risque pour la sécurité, elle doit être exclue ou écartée des fonctions dans lesquelles elle risquerait de nuire à la sécurité.

7. SÉCURITÉ PHYSIQUE

La sécurité physique est l'application de mesures de protection physiques et techniques en vue d'éviter l'accès non autorisé à des informations classifiées.

7.1. ***Exigences en matière de protection***

Le degré de sécurité physique à mettre en œuvre pour assurer la protection des informations classifiées doit être proportionné à la classification des informations et matériels détenus et à leur volume, ainsi qu'à la menace à laquelle ils sont exposés. Tous les détenteurs d'informations classifiées doivent se conformer à des pratiques normalisées de classification de ces informations et respecter des critères de protection communs concernant la garde, la transmission et la destruction d'informations et de matériels devant être protégés.

7.2. ***Contrôle***

Avant de laisser sans surveillance une zone contenant des informations classifiées, les personnes en ayant la garde doivent s'assurer que ces informations sont en sécurité et que tous les dispositifs de sécurité (fermetures, alarmes, etc.) sont enclenchés. Des contrôles indépendants supplémentaires doivent être effectués après les heures de bureau.

7.3. ***Sécurité des bâtiments***

Les bâtiments contenant des informations classifiées ou des systèmes de communication et d'information sécurisés doivent être défendus contre les accès non autorisés.

La nature de la protection des informations classifiées, par exemple fenêtres à barreaux, portes verrouillables, présence de gardes aux entrées, systèmes de contrôle d'entrée automatiques, inspections et patrouilles de sécurité, systèmes d'alarme, systèmes de détection des intrusions et chiens de garde, est fonction des paramètres suivants:

a) classification, volume et localisation dans le bâtiment concerné des informations et matériels à protéger;

b) qualité des meubles de sécurité contenant ces informations et matériels; et

c) caractéristiques physiques et situation du bâtiment.

La nature de la protection des systèmes de communication et d'information est fonction de l'évaluation de la valeur des actifs en jeu et des dommages potentiels en cas d'atteinte à la sécurité, des caractéristiques physiques et de la situation du bâtiment qui héberge le système concerné, ainsi que de la localisation du système dans le bâtiment.

7.4. ***Plans d'urgence***

Sont établis à l'avance des plans détaillés destinés à protéger les informations classifiées en cas d'urgence.

8. **IDENTIFIANTS DE SÉCURITÉ, MARQUAGES, APPOSITIONS ET POLITIQUE EN MATIÈRE DE CLASSIFICATION**

8.1. ***Identifiants de sécurité***

Aucune autre classification que celles définies à l'article 2, point d) n'est permise.

Pour fixer des limites à la validité d'une classification (c'est-à-dire déclassement ou déclassification automatique de l'information classifiée), il est possible d'utiliser un identifiant de sécurité convenu.

Les identifiants de sécurité ne sont utilisés qu'en association avec une classification.

Les identifiants de sécurité sont en outre réglementés dans la consigne de sécurité n° 2 et définis dans les instructions de traitement.

8.2. ***Marquages***

Un marquage est utilisé pour préciser les instructions spécifiques prédéfinies sur le traitement des informations confidentielles. Les marquages peuvent aussi indiquer le domaine couvert par un document donné, pour indiquer une diffusion particulière fondée sur le besoin d'en connaître ou (dans le cas d'une information non classifiée) pour indiquer la fin d'une interdiction.

Un marquage n'est pas une classification et n'est pas utilisé en lieu et place d'une classification.

Les marquages sont en outre réglementés dans la consigne de sécurité n° 2 et définis dans les instructions de traitement.

8.3. ***Apposition de classifications et d'identifiants de sécurité***

L'apposition de classifications et d'identifiants de sécurité et de marquages est effectuée conformément à la consigne de sécurité n° 2, section E, et aux instructions de traitement.

8.4. ***Politique en matière de classification***

8.4.1 *Généralités*

Les informations ne sont classifiées qu'en tant que de besoin. La classification est clairement et correctement indiquée et elle n'est maintenue qu'aussi longtemps que les informations doivent être protégées.

La classification des informations ainsi que tout déclassement ou déclassification ultérieurs incombent à la seule autorité d'origine.

Les fonctionnaires du Parlement européen classifient, déclassent ou déclassifient les informations sur instruction du Secrétaire général ou en vertu d'une délégation de celui-ci.

Les procédures détaillées régissant le traitement des documents classifiés sont conçues de façon à assurer à ces documents une protection adaptée aux informations qu'ils contiennent.

Le nombre de personnes autorisées à émettre des informations classifiées «TRÈS SECRET UE/EU TOP SECRET» est limité au strict minimum et les noms de ces personnes sont consignés sur une liste établie par l'UIC.

8.4.2 *Application de la classification*

La classification d'un document est déterminée par le degré de sensibilité de son contenu, conformément aux définitions données à l'article 2, point d). Il importe que la classification soit attribuée à bon escient et utilisée avec modération.

Les lettres ou notes d'envoi accompagnant des pièces jointes portent au moins le plus haut degré de classification attribué à l'une de ces pièces. L'autorité d'origine indique clairement le niveau de classification des lettres ou notes d'envoi lorsqu'elles sont séparées de leurs pièces jointes.

En déterminant la classification à attribuer à un document, l'autorité d'origine doit suivre les diverses règles susmentionnées et éviter la surclassification ou la sous-classification.

Des pages, paragraphes, sections, annexes, appendices et pièces jointes d'un document donné peuvent nécessiter une classification différente et doivent alors recevoir la classification correspondante. La classification du document dans son ensemble est celle de sa partie portant la classification la plus élevée.

9. **INSPECTIONS**

Des inspections périodiques internes des mesures de sécurité prises pour la protection des informations classifiées sont menées par la direction de la sécurité et de l'évaluation du risque qui peut demander l'assistance des autorités de sécurité du Conseil ou de la Commission.

Les autorités de sécurité et les services compétents des institutions de l'Union peuvent effectuer, dans le cadre d'une procédure convenue initiée par l'une des parties, des évaluations par les pairs des dispositions de sécurité pour la protection des informations classifiées échangées au titre des accords interinstitutionnels pertinents.

10. **PROCEDURES DE DECLASSIFICATION ET DE RETRAIT DE MARQUAGE**

10.1. L'UIC examine les informations confidentielles contenues dans son registre et demande le consentement de l'autorité d'origine à la déclassification ou au retrait de marquage du document au plus tard la 25e année suivant la date de création du document. Les documents qui ne sont pas déclassifiés ou qui n'ont pas fait l'objet d'un retrait de marquage lors du premier examen sont réexaminés régulièrement, et ce au moins tous les cinq ans. Outre aux documents effectivement conservés dans les archives sécurisées dans la zone sécurisée et dûment classifiés, le processus de retrait de marquage peut également être appliqué à d'autres informations confidentielles conservées soit dans l'organe/titulaire d'un mandat du Parlement, soit dans le service en charge des archives historiques du Parlement.

10.2 La décision concernant la déclassification ou le retrait de marquage d'un document est, en règle générale, prise uniquement par l'autorité d'origine en règle générale ou, exceptionnellement, en coopération avec l'organe/titulaire d'un mandat du Parlement détenteur de ces informations, avant que les informations qu'elle contient ne soient transférées au service responsable des archives historiques du Parlement. Les informations classifiées ne peuvent être déclassifiées ou ne peuvent se voir retirer leur marquage qu'avec l'accord préalable écrit de l'autorité d'origine. En ce qui concerne les «autres informations confidentielles», le secrétariat de l'organe/titulaire d'un mandat du Parlement qui détient de telles informations décide, en coopération avec le service détenteur de ces informations, si le marquage peut être retiré du document.

10.3. Il incombe à l'UIC, agissant pour le compte de l'autorité d'origine, d'informer les destinataires du document du changement de classification ou de marquage, ces derniers étant à leur tour chargés d'en aviser les destinataires successifs auxquels ils ont fait suivre l'original ou une copie du document.

10.4. La déclassification n'affecte aucun des identifiants de sécurité ou des marquages pouvant apparaître sur le document.

10.5. En cas de déclassification, la classification initiale figurant en tête et en pied de chaque page est barrée. La première page (page de couverture) du document porte un cachet et une référence ajoutée par l'UIC. En cas de retrait de marquage, le marquage initial figurant en tête de chaque page est barré.

10.6. Le texte du document déclassifié ou qui a fait l'objet d'un retrait de marquage est joint à la fiche électronique ou au système équivalent dans lequel il a été enregistré.

10.7. Dans le cas de documents relevant des exceptions concernant la vie privée et l'intégrité de l'individu ou les intérêts commerciaux d'une personne physique ou morale et de documents sensibles, l'article 2 du règlement (CEE, Euratom) no 354/83 s'applique.

10.8. Outre les dispositions des points 10.1 à 10.7, les règles suivantes s'appliquent:

a) dans le cas de documents de tiers, l'UIC consulte le tiers concerné avant de procéder à la déclassification ou au retrait de marquage;

b) s'agissant des exceptions concernant la vie privée et l'intégrité de l'individu, la procédure de déclassification ou de retrait de marquage tient compte, en particulier, de l'accord de la personne concernée ou, le cas échéant, de l'impossibilité d'identifier la personne concernée;

c) s'agissant de l'exception concernant les intérêts commerciaux d'une personne physique ou morale, la notification à la personne concernée peut être assurée par une publication au *Journal officiel de l'Union européenne* et cette personne dispose d'un délai de 4 semaines à compter de la date de cette publication pour présenter des observations.

Partie 2

PROCÉDURE D'HABILITATION DE SÉCURITÉ

11. **PROCÉDURE D'HABILITATION DE SÉCURITÉ POUR LES DÉPUTÉS AU PARLEMENT EUROPÉEN**

11.1. Pour pouvoir accéder aux informations classifiées au niveau confidentiel CONFIDENTIEL UE/EU CONFIDENTIAL ou à son équivalent, les députés au Parlement européen auront été autorisés à cet effet soit conformément à la procédure visée aux points 11.3 et 11.4 de la présente annexe ou sur la base d'une déclaration solennelle de non-divulgation conformément à l'article 3, paragraphe 4, de la présente décision.

11.2 Pour pouvoir accéder aux informations classifiées au niveau TRÈS SECRET UE/EU TOP SECRET, au niveau SECRET UE/EU SECRET ou à leurs équivalents, les députés au Parlement européen doivent avoir été autorisés à cet effet conformément à la procédure décrite aux points 11.3 et 11.14.

11.3. L'autorisation n'est délivrée qu'aux députés au Parlement européen qui ont fait l'objet d'une enquête de sécurité effectuée par les autorités nationales compétentes des États membres, selon la procédure visée aux points 11.9 à 11.14. Le Président est responsable de l'octroi de cette autorisation aux députés.

11.4 Le Président peut accorder l'autorisation écrite après avoir recueilli l'avis des autorités nationales compétentes des États membres sur la base de l'enquête de sécurité effectuée conformément aux points 11.8 à 11.13.

11.5. La direction de la sécurité et de l'évaluation du risque du Parlement européen tient une liste actualisée de tous les députés au Parlement européen ayant reçu une autorisation, y compris une autorisation provisoire au sens du point 11.15.

11.6. L'autorisation vaut pour une durée de cinq ans ou, si elle est plus courte, la durée des tâches qui en ont justifié l'octroi. Elle peut être renouvelée conformément à la procédure visée au point 11.4.

11.7. Le Président retire l'autorisation dès lors qu'il estime qu'il y a des motifs justifiant de le faire. Toute décision de retrait d'autorisation est notifiée au député au Parlement européen concerné, qui peut demander à être entendu par le Président avant que le retrait ne prenne effet, ainsi qu'à l'autorité nationale compétente.

11.8. L'enquête de sécurité est effectuée avec le concours du député au Parlement européen concerné et à la demande du Président. L'autorité nationale compétente aux fins de l'enquête est celle de l'État membre dont le député est ressortissant.

11.9. Dans le cadre de la procédure d'enquête, le député au Parlement européen concerné est tenu de remplir un formulaire d'information personnel.

11.10. Le Président spécifie dans sa demande à l'autorité nationale compétente le niveau de classification des informations que le député au Parlement européen concerné aurait à connaître, de sorte que cette autorité puisse mener la procédure d'enquête.

11.11 L'ensemble du déroulement et des résultats de la procédure d'enquête de sécurité menée par l'autorité nationale compétente respecte les prescriptions et réglementations en vigueur en la matière dans l'État membre concerné, y compris celles relatives aux voies de recours.

11.12. Lorsque l'autorité nationale compétente de l'État membre émet un avis positif, le Président peut octroyer l'autorisation au député au Parlement européen concerné.

11.13. Un avis négatif d'une autorité nationale compétente est notifié au député au Parlement européen concerné, qui peut demander à être entendu par le Président. Le Président peut, s'il le juge nécessaire, s'adresser aux autorités nationales compétentes afin de demander des éclaircissements complémentaires. En cas de confirmation de l'avis négatif, l'autorisation ne peut être accordée.

11.14. Tout député au Parlement européen qui est autorisé au sens du point 11.3 reçoit, au moment de l'autorisation et par la suite à intervalles réguliers, les lignes directrices nécessaires quant à la protection des informations classifiées et aux moyens de l'assurer. Il signe une déclaration confirmant qu'il a reçu ces lignes directrices.

11.15. À titre exceptionnel, le Président peut, après en avoir préalablement informé l'autorité nationale compétente et pourvu qu'aucune réaction de celle-ci n'ait été reçue dans un délai d'un mois, octroyer une autorisation provisoire à un député au Parlement européen pour une période qui ne peut excéder six mois, en attendant le résultat de l'enquête visée au point 11.11. Les autorisations provisoires ainsi octroyées ne donnent pas accès aux informations classifiées à un niveau TRÈS SECRET UE/EU TOP SECRET ou à son équivalent.

12. PROCÉDURE D'HABILITATION DE SÉCURITÉ POUR LES FONCTIONNAIRES DU PARLEMENT EUROPÉEN ET LES AUTRES EMPLOYÉS DU PARLEMENT TRAVAILLANT POUR LES GROUPES POLITIQUES

12.1. Seuls les fonctionnaires du Parlement européen et les autres employés du Parlement travaillant pour les groupes politiques qui, en raison de leurs fonctions et pour des nécessités de service, ont besoin de prendre connaissance d'informations classifiées ou d'en faire usage, peuvent avoir accès auxdites informations.

12.2. Pour pouvoir accéder aux informations classifiées aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET ou à leurs équivalents, les fonctionnaires du Parlement européen et les autres employés du Parlement travaillant pour les groupes politiques concernés auront été autorisés à cet effet conformément à la procédure décrite aux points 12.3 et 12.4.

12.3. L'autorisation n'est délivrée qu'aux personnes visées au point 12.1 qui ont fait l'objet d'une enquête de sécurité effectuée par les autorités nationales compétentes des États membres, selon la procédure visée aux points 12.9 à 12.14. Le Secrétaire général est responsable de l'octroi de l'autorisation aux fonctionnaires du Parlement européen et aux autres employés du Parlement travaillant pour les groupes politiques.

12.4. Le Secrétaire général peut accorder l'autorisation écrite après avoir recueilli l'avis des autorités nationales compétentes des États membres sur la base de l'enquête de sécurité effectuée conformément aux points 12.8 à 12.13.

12.5. La direction de la sécurité et de l'évaluation du risque du Parlement européen tient une liste actualisée de tous les postes nécessitant une habilitation de sécurité, fournie par les services concernés du Parlement européen, et de toutes les personnes ayant reçu une autorisation, y compris une autorisation provisoire au sens du point 12.15.

12.6. L'autorisation vaut pour une durée de cinq ans ou, si elle est plus courte, la durée des tâches qui en ont justifié l'octroi. Elle peut être renouvelée conformément à la procédure visée au point 12.4.

12.7. Le Secrétaire général retire l'autorisation dès lors qu'il estime qu'il y a des motifs justifiant de le faire. Toute décision de retrait d'autorisation est notifiée au fonctionnaire du Parlement européen concerné ou à l'autre employé concerné du Parlement travaillant pour un groupe politique, qui peut demander à être entendu par le Secrétaire général avant que le retrait ne prenne effet, ainsi qu'à l'autorité nationale compétente.

12.8. L'enquête de sécurité est effectuée avec le concours du fonctionnaire au Parlement européen concerné ou d'un autre employé concerné du Parlement travaillant pour les groupes politiques et à la demande du Secrétaire général. L'autorité nationale compétente aux fins de l'enquête est celle de l'État membre dont l'intéressé est ressortissant. Lorsque les lois et réglementations nationales l'autorisent, les autorités nationales compétentes peuvent mener des enquêtes sur des ressortissants étrangers qui demandent un accès à des informations classifiées aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET.

12.9. Dans le cadre de la procédure d'enquête, le fonctionnaire du Parlement européen concerné ou l'autre employé concerné du Parlement travaillant pour un groupe politique est tenu de remplir un formulaire d'information personnel.

12.10. Le Secrétaire général spécifie dans sa demande à l'autorité nationale compétente le niveau de classification des informations que le fonctionnaire du Parlement européen concerné ou un autre employé concerné du Parlement travaillant pour des groupes politiques aurait à connaître, de sorte que cette autorité puisse mener la procédure d'enquête et rendre un avis quant au niveau d'autorisation qu'il serait approprié d'accorder à la personne concernée.

12.11. L'ensemble du déroulement et des résultats de la procédure d'enquête de sécurité menée par l'autorité nationale compétente respecte les prescriptions et réglementations en vigueur en la matière dans l'État membre concerné, y compris celles relatives aux voies de recours.

12.12. Lorsque l'autorité nationale compétente de l'État membre émet un avis positif, le Secrétaire général peut octroyer l'autorisation au fonctionnaire du Parlement européen ou à un autre employé du Parlement travaillant pour des groupes politiques concerné.

12.13. Un avis négatif de l'autorité nationale compétente est notifié au fonctionnaire du Parlement européen concerné ou à l'autre employé concerné du Parlement travaillant pour un groupe politique, qui peut demander à être entendu par le Secrétaire général. Le Secrétaire général peut, s'il le juge nécessaire, s'adresser à l'autorité nationale compétente afin de demander des éclaircissements complémentaires. En cas de confirmation de l'avis négatif, l'autorisation ne peut être accordée.

12.14. Tout fonctionnaire du Parlement européen ou autre employé du Parlement travaillant pour un groupe politique, autorisé au sens des points 12.4 et 12.5, reçoit, au moment de l'autorisation et par la suite à intervalles réguliers, les instructions qui s'imposent sur la protection des informations classifiées et sur les moyens de l'assurer. Il signe une déclaration confirmant qu'il a reçu ces instructions et qu'il s'engage à les respecter.

12.15. À titre exceptionnel, le Secrétaire général peut, après en avoir préalablement informé l'autorité nationale compétente et en l'absence de réaction de celle-ci dans un délai d'un mois, octroyer une autorisation provisoire à un fonctionnaire du Parlement européen ou à un autre employé du Parlement travaillant pour un groupe politique, pour une période qui ne peut excéder six mois, en attendant le résultat de l'enquête visée au point 12.11. Les autorisations provisoires ainsi octroyées ne donnent pas accès aux informations classifiées au niveau TRÈS SECRET UE/EU TOP SECRET ou à son équivalent.

ANNEXE II

INTRODUCTION

Les dispositions ci-après définissent les consignes de sécurité qui régissent et garantissent la gestion et le traitement sécurisés des informations confidentielles par le Parlement européen. Ces consignes de sécurité, assorties des instructions de traitement, constituent le système de gestion de la sécurité des informations du Parlement européen visé à l'article 3, paragraphe 2, de la présente décision:

CONSIGNE DE SÉCURITÉ N° 1

Organisation de la sécurité au Parlement européen en matière de protection des informations confidentielles

CONSIGNE DE SÉCURITÉ N° 2

Gestion des informations confidentielles

CONSIGNE DE SÉCURITÉ N° 3

Traitement des informations confidentielles par des systèmes d'information et de communication automatisés (SIC)

CONSIGNE DE SÉCURITÉ N° 4

Sécurité physique

CONSIGNE DE SÉCURITÉ N° 5

Sécurité industrielle

CONSIGNE DE SÉCURITÉ N° 6

Manquements aux règles de sécurité, perte ou compromission d'informations confidentielles

CONSIGNE DE SÉCURITÉ N° 1

ORGANISATION DE LA SÉCURITÉ AU PARLEMENT EUROPÉEN EN MATIÈRE DE PROTECTION DES INFORMATIONS CONFIDENTIELLES

1. Le Secrétaire général veille à la mise en œuvre générale et cohérente de la présente décision.

Le Secrétaire général prend toutes les mesures nécessaires pour faire en sorte que, aux fins du traitement ou du stockage des informations confidentielles, la présente décision soit appliquée dans les locaux du Parlement par les députés au Parlement européen, par les fonctionnaires du Parlement européen, par les autres employés du Parlement qui travaillent pour les groupes politiques et par les contractants.

2. Le Secrétaire général est l'autorité de sécurité (AS). Le Secrétaire général, en cette qualité, est chargé:

2.1. de coordonner toutes les questions de sécurité liées aux activités du Parlement en ce qui concerne la protection des informations confidentielles;

2.2. de donner son accord à la mise en place d'une zone sécurisée, de salles de lecture sécurisées et d'un équipement sécurisé;

2.3. de mettre en œuvre les décisions autorisant, conformément à l'article 6 de la présente décision, la transmission d'informations classifiées par le Parlement à des tiers;

2.4. d'enquêter ou d'ordonner une enquête sur toute fuite concernant des informations confidentielles qui, à première vue, se serait produite à partir du Parlement, en liaison avec le Président du Parlement européen; quand un député au Parlement européen est concerné

2.5. d'entretenir des contacts étroits avec les autorités de sécurité des autres institutions et agences de l'Union et les autorités nationales de sécurité dans les États membres dans le but de garantir une coordination optimale des politiques de sécurité en ce qui concerne les informations classifiées;

2.6. de réexaminer constamment l'organisation et les procédures de sécurité du Parlement et de préparer les recommandations appropriées qui s'imposent;

2.7. de signaler à l'autorité nationale de sécurité (ANS) qui a mené la procédure d'enquête de sécurité, conformément à l'annexe I, partie 2, point 11.3, les cas où des informations défavorables pourraient l'affecter.

3. Quand un député au Parlement européen est concerné, le Secrétaire général exerce ses responsabilités en liaison étroite avec le Président du Parlement européen.

4. Dans l'exercice de ses responsabilités en vertu des paragraphes 2 et 3, le Secrétaire général est assisté du Secrétaire général adjoint, de la direction de la sécurité et de l'évaluation du risque, de la direction des technologies de l'information (DIT) et de l'unité des informations classifiées (UIC).

4.1. La direction de la sécurité et de l'évaluation du risque est chargée des mesures de protection personnelle et, en particulier, de la procédure d'habilitation de sécurité telle que visée à l'annexe I, partie 2. La direction de la sécurité et de l'évaluation du risque:

a) est le point de contact pour les autorités de sécurité des autres institutions de l'Union et les ANS, s'agissant des questions liées aux procédures d'habilitation de sécurité concernant les députés au Parlement européen, les fonctionnaires du Parlement européen et les autres employés du Parlement qui travaillent pour les groupes politiques;

b) fourni les informations nécessaires sur la sécurité générale en ce qui concerne les obligations de protection des informations classifiées et les conséquences de tout manquement en la matière;

c) surveille le fonctionnement de la zone sécurisée et des salles de lecture sécurisées dans les locaux du Parlement en coopération, s'il y a lieu, avec les services de sécurité des autres institutions de l'Union et les ANS;

d) vérifie, en coopération avec les autorités de sécurité des autres institutions de l'Union et les ANS, les procédures de gestion et de stockage des informations classifiées, ainsi que la zone sécurisée et les salles de lecture sécurisées dans les locaux du Parlement lorsque des informations classifiées sont traitées;

e) soumet les instructions de traitement approriées au Secrétaire général.

4.2. La DIT est responsable du traitement des informations confidentielles par les systèmes informatiques sécurisés au Parlement européen.

4.3. L'unité des informations classifiées (UIC) a pour mission:

a) d'identifier les besoins en matière de sécurité en ce qui concerne la protection effective des informations confidentielles, en étroite coopération avec direction de la sécurité et de l'évaluation du risque du Parlement et des autres institutions de l'Union;

b) d'identifier tous les aspects de la gestion et du stockage des informations confidentielles au sein du Parlement, comme indiqué dans les instructions de traitement;

c) de veiller au bon fonctionnement de la zone sécurisée;

d) de gérer ou de consulter les informations confidentielles dans la zone sécurisée ou dans la salle de lecture sécurisée de l'UIC, conformément à l'article 7, paragraphes 2 et 3, de la présente décision;

e) de gérer le registre de l'UIC;

f) de signaler à l'autorité de sécurité tout manquement à la sécurité et toute perte ou compromission, avérés ou présumés, d'informations classifiées déposées au sein de l'UIC et détenues dans la zone sécurisée ou dans la salle de lecture sécurisée de l'UIC.

5. En outre, le Secrétaire général, en tant qu'autorité de sécurité, nomme les autorités suivantes:

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

b) une autorité opérationnelle chargée de l'assurance de l'information (AOAI);

c) une autorité chargée de la distribution cryptographique (ADC);

d) une autorité Tempest (AT);

e) une autorité chargée de l'assurance de l'information (AAI).

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 tout conflit d'intérêt et tout chevauchement des tâches.

6. L'autorité d'homologation de sécurité émet un avis sur toutes les questions de sécurité liées à l'homologation de chaque système et réseau informatique au sein du Parlement:

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

6.2. en mettant 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;

6.3. en définissant une stratégie d'homologation de sécurité qui indique le niveau de précision du processus d'homologation en fonction du niveau d'assurance requis;

6.4. en étudiant et en approuvant les documents se rapportant à la sécurité, y compris en ce qui concerne la gestion des risques et les énoncés des risques résiduels, les documents concernant la vérification de la mise en œuvre des mesures de sécurité et les procédures d'exploitation de sécurité, et en veillant à ce qu'ils soient conformes aux politiques et aux règles du Parlement en matière de sécurité;

6.5. en vérifiant 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;

6.6. en définissant 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;

6.7. en approuvant, le cas échéant dans le cadre d'une approbation conjointe, l'interconnexion d'un SIC à d'autres SIC;

6.8. en approuvant les normes de sécurité des équipements techniques envisagés pour la protection et le traitement sécurisés des informations classifiées;

6.9. en s'assurant que les produits cryptographiques utilisés au sein du Parlement figurent sur la liste des produits agréés par l'Union européenne; et

6.10. en menant 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.

7. L'AOAI s'acquitte des tâches suivantes:

7.1. élaborer des documents relatifs à la sécurité de chaque système conformes à la politique et aux lignes directrices en matière de sécurité, et notamment en ce qui concerne le risque résiduel, les procédures d'exploitation de sécurité et le volet cryptographique du processus d'homologation des SIC;

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

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

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

7.5. 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;

7.6. dispenser une formation sur l'assurance de l'information propre à chaque SIC;

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

8. L'ADC s'acquitte des tâches suivantes:

8.1. gérer le matériel cryptographique de l'Union européenne et en rendre compte;

8.2. veiller, en étroite coopération avec l'AHS, à ce que les procédures appropriées soient mises en place et à ce que les projets soient appliqués pour rendre compte de tout le matériel cryptographique de l'Union et en assurer la manutention, le stockage et la diffusion en toute sécurité; et

8.3. assurer le transfert et la reprise du matériel cryptographique de l'Union européenne auprès des personnes ou des services utilisateurs.

9. L'AT est chargée de veiller à la conformité des SIC aux stratégies et instructions de traitement Tempest. Elle approuve les contre-mesures Tempest pour les installations et les produits destinés à protéger les informations classifiées jusqu'à un certain niveau de classification dans leur environnement opérationnel.

10. L'AAI est responsable de tous les aspects de la gestion et du traitement des informations confidentielles au sein du Parlement et, en particulier:

10.1 de définir la sécurité et les lignes directrices de sécurité en matière d'assurance de l'information et d'en surveiller l'efficacité et la pertinence;

10.2. de conserver et de gérer les données techniques relatives aux produits cryptographiques;

10.3. de veiller à ce que les mesures en matière d'assurance de l'information sélectionnées aux fins de la protection des informations classifiées soient conformes aux orientations pertinentes régissant leur éligibilité et leur sélection;

10.4. de veiller à ce que les produits cryptographiques soient sélectionnés conformément aux orientations régissant leur éligibilité et leur sélection;

10.5. de mener des consultations avec le fournisseur du système, les intervenants en matière de sécurité et les représentants des utilisateurs au sujet de la sécurité en matière d'assurance de l'information;

CONSIGNE DE SÉCURITÉ N° 2

GESTION DES INFORMATIONS CONFIDENTIELLES

A. **INTRODUCTION**

1. Cette consigne de sécurité n° 2 fixe les modalités de gestion, par le Parlement des informations confidentielles.

2. Lors de la création d'informations confidentielles, l'autorité d'origine évalue le niveau de confidentialité et arrête une décision fondée sur les principes définis dans cette consigne de sécurité en ce qui concerne la classification ou le marquage de ces informations.

B. **CLASSIFICATION ICUE**

3. La décision de classifier un document est arrêtée avant la création de celui-ci. À cette fin, la classification d'informations dans la catégorie des informations classifiées de l'Union européenne (ICUE) implique une évaluation préalable de leur niveau de confidentialité et une décision de l'autorité d'origine selon laquelle la divulgation non autorisée de ces informations pourrait porter atteinte, à un degré certain, aux intérêts de l'Union européenne ou à ceux de l'un ou de plusieurs de ses États membres ou de ses individus.

4. Dès que la décision de classifier les informations est arrêtée, une deuxième évaluation préalable est effectuée pour déterminer le niveau de classification approprié. La classification d'un document est déterminée par le degré de sensibilité de son contenu.

5. L'autorité d'origine de l'information est seule responsable de sa classification. Les fonctionnaires du Parlement classifient les informations sur instruction du Secrétaire général ou dans le cadre d'une délégation de celui-ci.

6. La classification est utilisée à bon escient et avec modération. En déterminant la classification à attribuer à un document, l'autorité d'origine se garde de toute tendance à la surclassification comme à la sous-classification.

7. Le niveau de classification attribué aux informations détermine le niveau de protection dont elles feront l'objet en ce qui concerne la sécurité personnelle, physique et procédurale ainsi que dans le domaine de l'assurance de l'information.

8. Les informations qu'il convient de classifier doivent être marquées et traitées comme telles, quelle que soit leur forme physique. La classification doit être clairement communiquée aux destinataires, soit au moyen d'un marquage de classification de sécurité (lorsque les informations sont communiquées par écrit, que ce soit sur papier ou au sein d'un SIC), soit au moyen d'une annonce (lorsque les informations sont communiquées oralement, par exemple, lors d'une conversation ou dans le cadre d'une réunion organisée à huis clos). Une mention de classification doit être apposée de manière physique sur le matériel classifié de manière à permettre une identification aisée de la classification de sécurité.

9. Les ICUE sous forme électronique ne peuvent être créées que dans le cadre d'un SIC homologué. Les informations classifiées elles-mêmes, mais aussi les noms de fichiers et les périphériques de stockage (s'il s'agit de périphériques externes, par exemple des CD-ROM ou des clés USB), doivent porter le marquage de classification de sécurité ad hoc.

10. La classification des informations doit avoir lieu dès leur création. Par exemple, les notes personnelles, brouillons ou courriers électroniques contenant des informations qu'il convient de classifier devraient être marqués d'emblée comme des ICUE et il y a lieu de les générer et de les traiter conformément à la présente décision et aux instructions de traitement en ce qui concerne les caractéristiques physiques et techniques. Par la suite, ces informations pourront devenir un document officiel qui, à son tour, portera un marquage approprié et fera l'objet d'un traitement ad hoc. Au cours du processus de rédaction, il peut s'avérer nécessaire de réévaluer un document officiel et de lui attribuer un niveau de classification plus élevé ou moins élevé.

11. L'autorité d'origine peut décider d'attribuer un niveau de classification uniformisé à des catégories d'informations qui sont créées régulièrement au sein de ce service. Cependant, l'autorité d'origine s'assure que, ce faisant, elle ne surclassifie ou ne sous-classifie pas systématiquement des éléments d'information particuliers.

12. Les ICUE affichent toujours un marquage de classification de sécurité qui correspond à leur niveau de classification de sécurité.

B.1. ***Niveaux de classification***

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

— «TRÈS SECRET UE/EU TOP SECRET», tel que défini à l'article 2, point d), de la présente décision, dont la compromission risquerait:

a) de menacer directement la stabilité interne de l'Union, de l'un ou de plusieurs de ses États membres, de pays tiers ou d'organisations internationales;

b) de causer un préjudice exceptionnellement grave aux relations avec des pays tiers ou des organisations internationales;

c) d'entraîner directement la perte d'un grand nombre de vies humaines;

d) de causer un préjudice exceptionnellement grave à l'efficacité opérationnelle ou à la sécurité du personnel déployé des États membres ou d'autres contributeurs, ou au maintien de l'efficacité d'opérations de sécurité ou de renseignements extrêmement utiles; ou

e) de causer un grave préjudice à long terme à l'économie de l'Union ou des États membres;

— «SECRET UE/EU SECRET», tel que défini à l'article 2, point d), de la présente décision, dont la compromission risquerait:

a) de provoquer des tensions internationales;

b) de nuire gravement aux relations avec des pays tiers et des organisations internationales;

c) de menacer directement des vies humaines ou de nuire gravement à l'ordre public ou à la sécurité ou à la liberté des personnes;

d) de nuire à des négociations commerciales ou politiques importantes et de causer des problèmes opérationnels significatifs à l'Union ou à ses États membres;

e) de nuire à la sécurité opérationnelle des États membres ou à l'efficacité d'opérations de sécurité ou de renseignements très utiles;

f) de causer un préjudice matériel important aux intérêts financiers, monétaires, économiques et commerciaux de l'Union ou d'un État membre;

g) de compromettre de manière substantielle la viabilité financière de grandes organisations ou de grands opérateurs; ou

h) d'entraver gravement l'élaboration ou le fonctionnement des politiques de l'Union et d'entraîner de lourdes conséquences économiques, commerciales ou financières;

— «CONFIDENTIEL UE/EU CONFIDENTIAL», tel que défini à l'article 2, point d), de la présente décision, dont la compromission risquerait:

a) de nuire gravement aux relations diplomatiques, par exemple, dans les cas où cela pourrait donner lieu à des protestations officielles ou à d'autres sanctions;

b) de menacer la sécurité ou la liberté des personnes;

c) de mettre en péril le résultat de négociations commerciales ou politiques et de causer des problèmes opérationnels à l'Union ou à ses États membres;

d) de nuire à la sécurité opérationnelle des États membres ou à l'efficacité d'opérations de sécurité ou de renseignements;

e) de compromettre de manière substantielle la viabilité financière de grandes organisations ou de grands opérateurs;

f) de faire obstacle aux enquêtes relatives à des infractions ou à des activités terroristes ou de faciliter la commission de ces infractions ou de ces activités terroristes;

g) d'aller fortement à l'encontre des intérêts financiers, monétaires, économiques et commerciaux de l'Union ou de ses États membres;

h) d'entraver gravement l'élaboration ou le fonctionnement des politiques de l'Union et d'entraîner de lourdes conséquences économiques, commerciales ou financières;

— «RESTREINT UE/EU RESTRICTED», tel que défini à l'article 2, point d), de la présente décision, dont la compromission risquerait:

a) d'être défavorable aux intérêts généraux de l'Union;

b) de nuire aux relations diplomatiques;

c) de causer des difficultés importantes à des personnes ou à des sociétés;

d) d'être défavorable à l'Union ou à ses États membres dans le cadre de négociations commerciales ou politiques;

e) de rendre plus difficile le maintien d'une sécurité efficace au sein de l'Union ou de ses États membres;

f) d'entraver l'élaboration ou le fonctionnement efficace des politiques de l'Union;

g) de nuire au bon fonctionnement de l'Union et de ses activités;

h) de violer les engagements pris par le Parlement de préserver le statut classifié d'informations fournies par des tiers;

i) d'enfreindre les restrictions légales à la divulgation d'informations;

j) de causer des pertes financières à des personnes ou à des sociétés ou de faciliter l'obtention de gains ou d'avantages indus par celles-ci; ou

k) de nuire aux enquêtes relatives à des infractions ou de faciliter la commission de ces infractions.

B.2. ***Classification des compilations, des pages de garde et des extraits***

14. Les lettres ou notes d'envoi accompagnant des pièces jointes portent le plus haut niveau de classification attribué à l'une de ces pièces. L'autorité d'origine indique clairement le niveau de classification des lettres ou notes d'envoi lorsqu'elles sont séparées de leurs pièces jointes. Lorsque la note/lettre d'envoi ne doit pas être classifiée, elle porte le libellé définitif suivant: «Lorsqu'elle est séparée de ses pièces jointes, la présente note/lettre n'est pas classifiée.».

15. Les documents ou les dossiers dont les parties n'ont pas le même niveau de classification sont, dans la mesure du possible, structurés de telle sorte que ces parties ayant des niveaux de classification différents puissent au besoin être aisément identifiées et séparées des autres. 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.

16 Des pages, paragraphes, sections, annexes, appendices et pièces jointes d'un document donné peuvent nécessiter des niveaux de classification différents et doivent alors porter la mention correspondante. Les abréviations uniformisées peuvent être utilisées dans les documents comportant des ICUE pour indiquer le niveau de classification de sections ou blocs de texte de moins d'une page.

17. 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.

C. **AUTRES INFORMATIONS CONFIDENTIELLES**

18. Les «autres informations confidentielles» doivent porter un marquage conformément au point E de la présente consigne de sécurité et aux instructions de traitement.

D. **CREATION D'INFORMATIONS CONFIDENTIELLES**

19. Seules les personnes dûment habilitées au titre de la présente décision ou autorisées par l'autorité de sécurité peuvent créer des informations confidentielles.

20. Les informations confidentielles ne sont pas ajoutées aux systèmes Internet ou Intranet de gestion des documents.

D.1. ***Création d'ICUE***

21. Pour créer des ICUE classifiées aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, la personne concernée est habilitée au titre de la présente décision ou est d'abord en possession d'une autorisation octroyée conformément à l'article 4, paragraphe 1 de la présente décision.

22. Les ICUE classifiées aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, sont créées uniquement à l'intérieur de la zone sécurisée.

23. Les règles suivantes s'appliquent à la création d'ICUE:

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

b) chaque page est numérotée et mentionne le nombre total de pages;

c) le document porte un numéro de référence sur la première page et une indication de l'objet sur lequel il porte, qui ne constitue pas en elle-même une information classifiée à moins que ne figure une apposition en ce sens;

d) le document comporte une date sur la première page;

e) la première page de tout document classifié aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, comporte une liste de toutes les annexes et pièces jointes;

f) les documents classifiés aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET, portent un numéro d'exemplaire sur chaque page dès lors qu'ils doivent être diffusés en plusieurs exemplaires. Chaque exemplaire comporte également sur la première page le nombre total d'exemplaires et de pages, et

g) si le document fait référence à d'autres documents contenant des informations classifiées transmises par d'autres institutions de l'Union ou s'il contient des informations classifiées émanant desdits documents, il est doté du même niveau de classification que les documents en question et ne peut être diffusé, sans le consentement écrit préalable de son autorité d'origine, à d'autres personnes que celles désignées dans la liste de diffusion relative au document original ou aux documents contenant des informations classifiées.

24. L'autorité d'origine conserve le contrôle des ICUE qu'elle a créées. Son consentement écrit préalable est requis avant que les ICUE en question ne soient:

a) déclassées ou déclassifiées;

b) utilisées à d'autres fins que celles établies par l'autorité d'origine;

c) divulguées à un État tiers ou à une organisation internationale quels qu'ils soient;

d) divulguées à toute personne, institution, pays ou organisation internationales autres que les destinataires autorisés à l'origine par l'autorité d'origine à consulter les informations en question;

e) divulguées à un contractant ou futur contractant situé dans un État tiers;

f) copiées ou traduites, si les informations sont classifiées au niveau TRES SECRET UE/EU TOP SECRET;

g) détruites.

D.2. ***Création d'autres informations confidentielles***

25. Le Secrétaire général faisant fonction d'autorité de sécurité peut décider d'autoriser ou non la création d'«autres informations confidentielles» par une fonction, un service et/ou une personne donnés.

26. Les «autres informations confidentielles» portent l'un des marquages définis dans les instructions de traitement.

27. Les règles suivantes s'appliquent à la création d'«autres informations confidentielles»:

a) le marquage correspondant est indiqué en haut de la première page du document;

b) chaque page est numérotée et mentionne le nombre total de pages;

c) le document porte un numéro de référence sur la première page et une indication de l'objet sur lequel il porte;

d) le document comporte une date sur la première page, et

e) la dernière page du document contient une liste de toutes les annexes et pièces jointes.

28. La création d'«autres informations confidentielles» est soumise à des règles et procédures spécifiques exposées dans les instructions de traitement.

E. **IDENTIFIANTS ET MARQUAGES DE SECURITE**

29. Les identifiants et marquages de sécurité figurant sur les documents servent à contrôler le flux d'informations et à restreindre l'accès aux informations confidentielles sur la base du principe du «besoin d'en connaître».

30. Lorsque des identifiants et/ou marquages de sécurité sont utilisés ou apposés, il convient de prendre soin d'éviter toute confusion avec les classifications de sécurité des ICUE: RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET et TRES SECRET UE/EU TOP SECRET.

31. Des règles spécifiques relatives à l'utilisation des identifiants et marquages de sécurité, ainsi que la liste des marquages de sécurité approuvés par le Parlement européen, sont exposées dans les instructions de traitement.

E.1. ***Identifiants de sécurité***

32. Les identifiants de sécurité peuvent uniquement être utilisés en lien avec une classification de sécurité et ne sont pas appliqués séparément à des documents. Un identifiant de sécurité peut être appliqué à des ICUE afin de:

a) fixer des limites à la validité d'une classification (c'est-à-dire déclassement ou déclassification automatique de l'information classifiée);

b) limiter la diffusion desdites ICUE;

c) établir des modalités spéciales de traitement en sus de celles correspondant au niveau de classification de sécurité.

33. Les contrôles supplémentaires applicables au traitement et au stockage des documents contenant des ICUE imposent des charges supplémentaires à toutes les parties concernées. Afin de réduire à son minimum le travail requis à cet égard, il est d'usage, lorsque de tels documents sont créés, de fixer un délai ou de prévoir un événement au-delà desquels la classification expire automatiquement et les informations contenues dans le document sont déclassées ou déclassifiées.

34. Lorsqu'un document traite d'un domaine particulier de travail et que sa diffusion a besoin d'être limitée et/ou qu'il doit être soumis à des modalités spéciales de traitement, une indication à cet effet peut être ajoutée à sa classification pour aider à identifier son public cible.

E.2. ***Marquages***

35. Les marquages ne constituent pas une classification de sécurité. Ils visent à servir uniquement à fournir des instructions concrètes sur le traitement d'un document, et ne sont pas utilisés pour décrire le contenu du document en question.

36. Les marquages peuvent être appliqués séparément aux documents ou utilisés en lien avec une classification de sécurité.

37. En règle générale, les marquages sont appliqués aux informations qui sont couvertes par le secret professionnel auxquelles il est fait référence à l'article 339 du TFUE et à l'article 17 du statut, ou qui doivent être protégées par le Parlement pour des motifs juridiques, mais qui ne doivent pas nécessairement ou ne pourraient être classifiées.

E.3. ***Utilisation de marquages dans le SIC***

38. Les règles en matière d'utilisation des marquages sont également applicables dans le SIC homologué.

39. L'AHS fixe des règles spécifiques sur l'utilisation des marquages dans le SIC homologué.

F. **RECEPTION**

40. Seule l'UIC est habilitée, au sein du Parlement, à recevoir des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET ou à leurs niveaux équivalents de la part de tiers.

41. En ce qui concerne les informations classifiées au niveau RESTREINT UE/EU RESTRICTED ou à son niveau équivalent et les «autres informations confidentielles», tant l'UIC que les organes ou titulaires d'un mandat au sein du Parlement peuvent être chargés de recevoir ces informations de la part de tiers, et d'appliquer les principes fixés dans la présente consigne de sécurité.

G. **ENREGISTREMENT**

42. Par «enregistrement», on entend l'application des procédures d'enregistrement du cycle de vie des informations confidentielles, y compris leur diffusion, leur consultation et leur destruction.

43. Aux fins de la présente consigne de sécurité, on entend par «cahier d'enregistrement» un registre dans lequel sont consignées en particulier les dates et heures auxquelles:

a) des informations confidentielles arrivent dans les secrétariats respectifs d'organes ou de titulaires d'un mandat au sein du Parlement ou, le cas échéant, de l'UIC, ou en sortent;

b) une personne habilitée accède à des informations confidentielles ou en transmet; et

c) des informations confidentielles sont détruites.

44. L'autorité d'origine d'informations classifiées est chargée du marquage de la première déclaration au moment de la création d'un document contenant de telles informations. Cette déclaration est communiquée à l'UIC lorsque le document est créé.

45. Les informations classifiées au niveau CONFIDENTIEL UE/EU CONFIDENTIAL SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET ou à leurs équivalents ne peuvent être enregistrées que par l'UIC à des fins de sécurité. Les informations classifiées au niveau RESTREINT UE/EU RESTRICTED ou à son équivalent et les «autres informations confidentielles» reçues de la part de tiers sont enregistrées par le service chargé de la réception officielle du document, à savoir soit l'UIC soit le secrétariat d'organes ou de titulaires d'un mandat au sein du Parlement, à des fins administratives. Les «autres informations confidentielles» produites au sein du Parlement sont enregistrées par l'autorité d'origine, à des fins administratives.

46. Les informations classifiées aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET ou à leurs équivalents sont enregistrées en particulier au moment où:

a) elles sont produites;

b) elles arrivent à l'UIC ou en sortent; et

c) elles arrivent dans le SIC ou en sortent.

47. Les informations classifiées au niveau RESTREINT UE/EU RESTRICTED ou à son équivalent sont enregistrées en particulier au moment où:

a) elles sont produites;

b) elles arrivent dans les secrétariats respectifs d'organes ou de titulaires d'un mandat au sein du Parlement ou de l'UIC, ou en sortent; et

c) elles arrivent dans le SIC ou en sortent.

48. L'enregistrement d'informations confidentielles peut être effectué dans un cahier d'enregistrement papier ou électronique/dans un SIC.

49. Pour les informations classifiées au niveau RESTREINT UE/EU RESTRICTED ou à son équivalent et les «autres informations confidentielles», les éléments suivants, au minimum, sont consignés:

a) la date et l'heure auxquelles les informations en question arrivent dans les secrétariats respectifs d'organes ou de titulaires d'un mandat au sein du Parlement ou de l'UIC, le cas échéant, ou en sortent;

b) le titre du document, le niveau ou marquage de classification, la date d'expiration de la classification/du marquage et tout numéro de référence attribué au document.

50. Pour les informations classifiées aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET ou à leurs équivalents, les éléments suivants, au minimum, sont consignés:

a) la date et l'heure auxquelles les informations en question arrivent dans l'UIC ou en sortent;

b) le titre du document, le niveau ou marquage de classification, tout numéro de référence attribué au document et la date d'expiration de la classification/du marquage;

c) les coordonnées de l'autorité d'origine;

d) l'identité de toute personne qui obtient l'accès au document et la date de cet accès de cette personne;

e) l'indication de toute copie ou traduction du document effectuée;

f) la date et l'heure auxquelles toute copie ou traduction du document a été effectuée, auxquelles le document a quitté l'UIC ou y est retourné, et l'indication précise de l'endroit où les informations ont été envoyées et de la personne qui les a rendues;

g) la date et l'heure auxquelles le document est détruit, et par qui, conformément aux règles de sécurité du Parlement relatives à la destruction; et

h) la déclassification ou le déclassement du document.

51. Les cahiers d'enregistrement sont classifiés ou portent un marquage approprié. Les cahiers d'enregistrement d'informations classifiées au niveau TRES SECRET UE/EU TOP SECRET ou à son équivalent sont enregistrés au même niveau de classification.

52. Les informations classifiées peuvent être enregistrées:

a) dans un cahier d'enregistrement unique; ou

b) dans des cahiers d'enregistrement séparés en fonction de leur niveau de classification, du fait qu'il s'agit d'informations entrantes ou sortantes et de leur origine ou destination.

53. Dans le cas d'un traitement électronique dans le SIC, les procédures d'enregistrement peuvent être mises en œuvre au moyen de processus intervenant dans le SIC même et répondant à des exigences équivalentes à celles spécifiées plus haut. Chaque fois que des ICUE sortent du SIC, la procédure d'enregistrement décrite ci-dessus s'applique.

54. L'UIC conserve une trace de toutes les informations classifiées communiquées par le Parlement à des tiers et des informations classifiées reçues par le Parlement de la part de tiers.

55. Une fois l'enregistrement des informations classifiées aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET ou a leurs équivalents effectué, l'UIC vérifie si le destinataire dispose d'une autorisation de sécurité valide. Dans l'affirmative, le destinataire est informé par l'UIC. La consultation d'informations classifiées ne peut se faire qu'une fois que le document les contenant a été enregistré.

H. **DIFFUSION**

56. L'autorité d'origine établit la liste de diffusion initiale pour les ICUE qu'elle a créées.

57. Les informations classifiées au niveau RESTREINT UE/EU RESTRICTED et les autres informations confidentielles produites par le Parlement sont diffusées au sein du Parlement par l'autorité d'origine conformément aux instructions de traitement applicables et sur la base du principe du besoin d'en connaître. En ce qui concerne les informations classifiées aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET créées par le Parlement au sein de la zone sécurisée, la liste de diffusion (et toutes autres instructions relatives à la diffusion) est fournie à l'UIC, qui est chargée de sa gestion.

58. Les ICUE produites par le Parlement ne peuvent être diffusées à des tiers que par l'UIC, sur la base du principe du besoin d'en connaître.

59. Les informations confidentielles reçues soit par l'UIC soit par tout organe/titulaire d'un mandat au sein du Parlement qui en a fait la demande sont diffusées conformément aux instructions reçues de la part de l'autorité d'origine.

I. **TRAITEMENT, STOCKAGE ET CONSULTATION**

60. Le traitement, le stockage et la consultation d'informations confidentielles s'effectuent conformément à la consigne de sécurité n° 4 et aux instructions de traitement.

J. **COPIE/TRADUCTION/INTERPRETATION D'INFORMATIONS CLASSIFIEES**

61. Les documents contenant des informations classifiées au niveau TRES SECRET UE/EU TOP SECRET ou son équivalent ne sont ni copiés ni traduits sans le consentement écrit préalable de l'autorité d'origine. Les documents contenant des informations classifiées au niveau SECRET UE/EU SECRET à son équivalent ou classifiées au niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou à son équivalent peuvent être copiés ou traduits à la demande de leur détenteur, à condition que l'autorité d'origine ne l'ait pas interdit.

62. Chaque copie d'un document contenant des informations classifiées aux niveaux TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET EU ou CONFIDENTIEL UE/EU CONFIDENTIAL ou à leurs niveaux équivalents doit être enregistrée à des fins de sécurité.

63. Les mesures de sécurité applicables au document original contenant des informations classifiées le sont aussi à ses copies et à ses traductions.

64. Les documents envoyés par le Conseil doivent être reçus dans toutes les langues officielles.

65. Des copies et/ou traductions de documents contenant des informations classifiées peuvent être requises par l'autorité d'origine ou le détenteur d'une copie. Les copies de documents contenant des informations classifiées au niveau CONFIDENTIEL UE/EU CONFIDENTIAL SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET ou à leurs équivalents ne peuvent être produites qu'au sein de la zone sécurisée et sur des photocopieurs qui font partie d'un SIC homologué. Les copies de documents contenant des informations classifiées au niveau RESTREINT UE/EU RESTRICTED ou à son équivalent et d'autres informations confidentielles sont réalisées à l'aide d'un outil de reproduction homologué dans les locaux du Parlement.

66. Toutes les copies et traductions de tout document ou des parties de copies de documents contenant des informations confidentielles portent le marquage approprié, sont numérotées et enregistrées.

67. Il n'est pas fait davantage de copies qu'il n'est strictement nécessaire. Toutes les copies sont détruites conformément aux instructions de traitement à la fin de la période de consultation.

68. Seuls les interprètes et traducteurs qui sont des fonctionnaires du Parlement peuvent avoir accès à des informations classifiées.

69. Les interprètes et traducteurs ayant accès à des documents contenant des informations classifiées au niveau CONFIDENTIEL UE/EU CONFIDENTIAL SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET ou à leurs équivalents doivent disposer de l'habilitation de sécurité appropriée.

70. Lorsqu'ils travaillent sur des documents contenant des informations classifiées au niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET ou à leurs équivalents, les interprètes et traducteurs travaillent à l'intérieur de la zone sécurisée.

K. DECLASSEMENT, DECLASSIFICATION ET RETRAIT DE MARQUAGE D'INFORMATIONS CONFIDENTIELLES

K.1. *Principes généraux*

71. Les informations confidentielles sont déclassifiées, déclassées ou bien leur marquage est retiré lorsque leur protection n'est plus nécessaire ou n'est plus requise à l'échelon d'origine.

72. Les décisions visant à déclasser ou à déclassifier des informations contenues dans des documents produits au sein du Parlement, ou à en retirer le marquage, sont prises de façon ad hoc, par exemple en réponse à une demande d'accès de la part du public ou d'une autre institution de l'Union, ou bien à l'initiative de l'UIC ou d'un organe ou d'un titulaire d'un mandat au sein du Parlement.

73. Au moment de la création du document classifié, l'autorité d'origine d'ICUE indique, si possible, si les ICUE en question peuvent ou non être déclassées ou déclassifiées à une date donnée ou après un événement spécifique. Lorsqu'il n'est pas possible de fournir ces informations, l'autorité d'origine, l'UIC ou l'organe/titulaire d'un mandat au sein du Parlement détenant les informations procède au réexamen du niveau de classification des ICUE qu'il détient au moins une fois tous les cinq ans. En tout état de cause, les ICUE ne peuvent être déclassées ou déclassifiées sans le consentement écrit préalable de l'autorité d'origine.

74. Au cas où l'autorité d'origine de documents produits au sein du Parlement ne peut être identifiée ou retrouvée, l'autorité de sécurité procède au réexamen du niveau de classification des ICUE sur la base d'une proposition de l'organe/du titulaire d'un mandat au sein du Parlement détenteur des informations, qui peut consulter l'UIC à cet égard.

75. L'UIC ou l'organe/le titulaire du mandat au sein du Parlement qui détient les informations en question sont chargés d'informer le ou les destinataires de la déclassification ou du déclassement de ces informations, et ce ou ces destinataires sont à leur tour chargés d'informer tout destinataire ultérieur auquel ils ont envoyé le document ou auquel ils ont transmis une copie du document en question.

76. La déclassification, le déclassement ou le retrait du marquage d'informations contenues dans un document sont consignés.

K.2. *Déclassification*

77. Les ICUE peuvent être déclassifiées en totalité ou partiellement. Elles peuvent être déclassifiées partiellement lorsque la protection n'est plus jugée nécessaire pour une partie donnée du document qui les contient mais que la protection demeure justifiée pour le reste du document.

78. Lorsque le réexamen d'ICUE contenues dans un document créé au sein du Parlement donne lieu à une décision de déclassification, il convient d'examiner si le document peut être rendu public ou s'il doit porter un marquage de diffusion (et donc ne pas être rendu public).

79. En cas de déclassification d'ICUE, celle-ci est consignée dans le cahier d'enregistrement avec les données suivantes: la date de la déclassification, le nom des personnes qui ont demandé et autorisé la déclassification, le numéro de référence du document déclassifié et sa destination finale.

80. L'ancien marquage de classification figurant sur le document déclassifié et toutes ses copies est barré. Les documents et toutes leurs copies sont stockés en conséquence.

81. En cas de déclassification partielle d'informations classifiées, la partie ayant été déclassifiée est produite sous forme d'extrait et stockée en conséquence. Le service compétent enregistre:

a) la date de la déclassification partielle;

b) le nom des personnes qui ont demandé et autorisé la déclassification; et

c) le numéro de référence de l'extrait déclassifié.

K.3. ***Déclassement***

82. Après le déclassement d'informations classifiées, le document les contenant est enregistré dans les cahiers d'enregistrement correspondant à l'ancien et au nouveau niveau de classification. La date du déclassement est consignée, ainsi que le nom de la personne qui a autorisé le déclassement.

83. Le document contenant les informations déclassées ainsi que toutes les copies dudit document reçoivent le nouveau niveau de classification et sont stockés en conséquence.

L. **DESTRUCTION D'INFORMATIONS CONFIDENTIELLES**

84. Les informations confidentielles (sous forme papier ou électronique) qui ne sont plus nécessaires sont détruites ou effacées, conformément aux instructions de traitement et aux règles pertinentes en matière d'archivage.

85. Les informations classifiées aux niveaux TRES SECRET UE/EU TOP SECRET ou SECRET UE/EU SECRET ou à leurs équivalents sont détruites par l'UIC en présence d'un témoin titulaire d'une habilitation de sécurité correspondant au moins au niveau de classification des informations faisant l'objet de la destruction.

86. Les informations classifiées au niveau TRES SECRET UE/EU TOP SECRET ou à son équivalent ne sont pas détruites sans le consentement écrit préalable de l'autorité d'origine.

87. Les informations classifiées au niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou à son équivalent sont détruites et éliminées par l'UIC à la demande de l'autorité d'origine ou d'une autorité compétente. Les cahiers d'enregistrement et autres registres sont actualisés en conséquence. Les informations classifiées au niveau RESTREINT UE/EU RESTRICTED ou à son équivalent sont détruites et éliminées soit par l'UIC soit par l'organe/titulaire d'un mandat pertinent au sein du Parlement.

88. Le fonctionnaire chargé de la destruction et le témoin de celle-ci signent un certificat de destruction, qui doit être classé et archivé à l'UIC. L'UIC conserve, avec les formulaires de diffusion, les certificats de destruction des informations classifiées au niveau TRES SECRET UE/EU TOP SECRET ou à son équivalent pendant au moins dix ans, et ceux des informations classifiées au niveau SECRET UE/EU SECRET ou à son équivalent ainsi que ceux des informations classifiées au niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou à son niveau équivalent pendant au moins cinq ans.

89. Les documents contenant des informations classifiées sont détruits à l'aide de méthodes répondant aux normes applicables de l'Union ou de normes équivalentes pour empêcher leur reconstitution totale ou partielle.

90. La destruction de supports de stockage informatique utilisés pour les informations classifiées est effectuée conformément aux instructions de traitement applicables.

91. La destruction d'informations classifiées est consignée dans le cahier d'enregistrement correspondant avec les données suivantes:

a) la date et l'heure de la destruction;

b) le nom du fonctionnaire chargé de la destruction;

c) l'identification du document ou des copies détruits;

d) le format physique d'origine des ICUE détruites;

e) les moyens de destruction employés; et

f) le lieu de destruction.

M. **ARCHIVAGE**

92. Les informations classifiées, y compris toutes les notes/lettres de couverture, toutes les annexes, tous les récépissés de dépôt et/ou toutes les autres parties du dossier sont transférées vers les archives sécurisées de la zone sécurisée six mois après leur dernière consultation et, au plus tard, un an après leur dépôt. Les instructions de traitement exposent des règles détaillées sur l'archivage des informations classifiées.

93. En ce qui concerne les «autres informations confidentielles», les règles générales sur la gestion des documents s'appliquent sans préjudice d'autres dispositions spécifiques relatives à leur traitement.

CONSIGNE DE SÉCURITÉ 3

TRAITEMENT DES INFORMATIONS CONFIDENTIELLES AU MOYEN DE SYSTÈMES AUTOMATISÉS D'INFORMATION ET DE COMMUNICATION (SIC)

A. **ASSURANCE DES INFORMATIONS CLASSIFÉES TRAITÉES DANS DES SYSTÈMES D'INFORMATION**

1. Par «assurance de l'information» (AI) dans le domaine des systèmes d'information, on entend la certitude que ces systèmes protégeront les informations classifiées qu'ils traitent, qu'ils fonctionneront comme ils le doivent et qu'ils fonctionneront sous le contrôle d'utilisateurs légitimes.que cela est nécessaire. Une AI efficace garantit des niveaux appropriés de confidentialité, d'intégrité, de disponibilité, de non-répudiation et d'authenticité. L'AI s'articule autour d'un processus de gestion des risques.

2. Par «système d'information et de communication» (SIC) dédié au traitement d'informations classifiées, on entend un système capable de gérer des informations sous forme électronique. Un tel système d'information comprend l'ensemble des moyens nécessaires pour le faire fonctionner, y compris l'infrastructure, l'organisation, le personnel et les ressources d'information.

3. Les SIC traitent les informations classifiées en respectant la notion d'AI.

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

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

a) authenticité: garantie que l'information est véridique et émane de sources dignes de foi;

b) disponibilité: caractéristique de l'information selon laquelle elle est accessible et utilisable, à la demande d'une entité autorisée;

c) confidentialité: propriété selon laquelle les informations ne sont pas divulguées à des personnes ou à des entités non autorisées et l'accès à ces informations n'est pas accordé à des processus non autorisés;

d) intégrité: propriété consistant à préserver l'exactitude et le caractère complet des informations et éléments;

e) non-répudiation: la possibilité de prouver qu'une action ou un événement a eu lieu, de sorte que la possibilité de nier par la suite l'existence de cet action ou évènement est exclue.

B. **PRINCIPES D'ASSURANCE DE L'INFORMATION**

6. Les dispositions énoncées ci-après constituent les éléments fondamentaux permettant de garantir la sécurité de tout SIC traitant des informations classées. 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.

B.1. ***Gestion des risques de sécurité***

7. 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 conformément à la consigne de sécurité 1, sur la base d'une procédure d'évaluation des risques ayant fait ses preuves, transparente et pouvant être parfaitement comprise. Le domaine d'application du SIC et ses ressources sont clairement définis dès le début du processus de gestion des risques.

8. Les autorités compétentes visées dans la consigne de sécurité 1 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 réexaminent régulièrement l'évaluation de la vulnérabilité afin de suivre l'évolution de la technologie de l'information.

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

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

B.2. ***Sécurité du SIC tout au long de son cycle de vie***

11. Assurer la sécurité d'un SIC tout au long de son cycle de vie, de sa mise en service à son retrait, est une obligation.

12. 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.

13. Le SIC, y compris les mesures de sécurité techniques et non techniques dont il fait l'objet, est soumis à des essais de sécurité au cours du processus d'homologation afin de s'assurer que le niveau d'assurance requis est atteint et de vérifier que le CIS et ses mesures de sécurité techniques et non techniques sont correctement mis en œuvre, intégrés et configurés.

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

15. Les documents relatifs à la sécurité du 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.

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

B.3. ***Bonnes pratiques***

17. L'autorité chargée de l'assurance de l'information définit les bonnes pratiques visant à protéger les informations classifiées traitées par le SIC. Les lignes directrices concernant les bonnes pratiques énoncent les mesures visant à assurer la sécurité du SIC sur le plan technique et physique ainsi qu'au niveau de l'organisation et des procédures, dont l'efficacité dans la lutte contre certaines menaces et vulnérabilités a été démontrée.

18. La protection des informations classifiées traitées par le SIC met à profit les enseignements tirés par les entités associées à l'AI.

19. La diffusion et la mise en œuvre ultérieure des bonnes pratiques contribuent à atteindre un niveau équivalent d'assurance dans les SIC, exploités par le secrétariat du Parlement, traitant des informations classifiées.

B.4. ***Sécurité en profondeur***

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

a) la dissuasion: mesures de sécurité visant à dissuader un éventuel ennemi de projeter une attaque contre le SIC;

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

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

d) la résistance: 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; ainsi que

e) le rétablissement: mesures de sécurité visant à rétablir la sécurité du SIC.

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

21. Les autorités compétentes, visées dans la consigne de sécurité 1, s'assurent qu'elles sont en mesure de faire face aux incidents dont l'ampleur dépasse les limites de l'organisation, de manière à coordonner les réactions et d'échanger des informations sur ces incidents et l'ensemble des risques qui en découlent (capacités de réaction informatique en cas d'urgence).

B.5. ***Principes du minimalisme et du moindre privilège***

22. De manière à éviter les risques superflus, seuls sont mis en œuvre les fonctions, dispositifs et services indispensables pour répondre aux exigences opérationnelles.

23. Les utilisateurs d'un SIC et les processus automatisés se voient uniquement accorder des droits d'accès, des privilèges ou des autorisations requis 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.

B.6. ***Sensibilisation à l'assurance de l'information***

24. 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, tous les acteurs intervenant dans le cycle de vie d'un SIC, y compris les utilisateurs, doivent bien percevoir:

a) l'ampleur des dommages que des défaillances en matière de sécurité peuvent provoquer sur les SIC traitant des informations classifiées;

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

c) la responsabilité et l'obligation de rendre des comptes qui leur incombent en matière de sécurité du SIC au regard des fonctions qui sont les leurs dans le cadre des systèmes et processus.

25. 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, les députés au Parlement européen et les utilisateurs du SIC.

B.7. ***Évaluation et homologation des produits de sécurité informatique***

26. Les SIC traitant des informations classifiées aux niveaux CONFIDENTIEL UE/ EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET ou à leurs équivalents sont protégés de telle manière que les informations ne peuvent pas être compromises par des émissions électromagnétiques non intentionnelles («mesures de sécurité Tempest»).

27. Lorsque la protection des informations classifiées est assurée par des produits cryptographiques, ces produits sont certifiés par l'AHS comme produits cryptographiques homologués par l'UE.

28. Il convient, lors de la transmission des informations classifiées par voie électronique, de mettre en œuvre des produits cryptographiques homologués UE. Nonobstant cette exigence, des procédures spécifiques peuvent être appliquées en cas d'urgence ou dans le cadre de configurations techniques spécifiques comme le prévoient les points 41 à 44.

29. 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.

30. 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.

31. L'AHS approuve les lignes directrices applicables en matière de sécurité pour ce qui est de la qualification et de l'homologation des produits de sécurité informatique non cryptographiques.

B.8. ***Transmission à l'intérieur de la zone sécurisée***

32. Lorsque la transmission d'informations classifiées s'effectue uniquement à l'intérieur de la zone sécurisée, une diffusion non cryptée ou d'un niveau de cryptage inférieur peut être envisagée au regard des résultats d'un processus de gestion des risques et avec l'accord de l'AHS.

B.9. ***Interconnexion sécurisée des SIC***

33. 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 de façon unidirectionnelle ou multidirectionnelle.

34. 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 avec tout autre SIC.

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

a) les autorités compétentes définissent et approuvent les conditions opérationnelles et commerciales que doivent remplir ces interconnexions;

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

c) des services de protection (SP) sont mis en place à la périphérie du SIC.

36. Il ne peut y avoir aucune interconnexion entre un SIC homologué et un réseau non protégé ou public, sauf lorsque le SIC comporte des systèmes de protection homologués installés 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 compétente chargée de l'assurance de l'information et approuvées par l'AHS compétente.

37. Lorsque le réseau public non protégé sert uniquement aux fins de la transmission et les données sont cryptées au moyen d'un produit cryptographique de l'Union certifié conformément au point 27, une telle connexion n'est pas considérée comme une interconnexion.

38. Est interdite l'interconnection directe ou en cascade à un réseau non protégé ou public d'un SIC homologué pour traiter des informations classifiées au niveau TRÈS SECRET UE/ EU TOP SECRET ou à son équivalent ainsi que des informations classifiées au niveau SECRET UE/EU SECRET ou à son équivalent.

B.10. ***Support de données informatiques***

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

40. Les supports de données informatiques sont réutilisés, déclassés ou déclassifiés conformément aux instructions de traitement.

B.11. ***Situations d'urgence***

41. Les procédures spécifiques décrites ci-après peuvent être appliquées dans les situations d'urgence, telles que les crises, les conflits ou les guerres, imminentes ou effectives, ou dans des circonstances opérationnelles exceptionnelles.

42. Les informations classifiées peuvent, avec le consentement de l'autorité compétente, être transmises au moyen de produits cryptographiques homologués pour un niveau de classification inférieur ou sans faire l'objet d'un cryptage 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 cryptage nécessaire ou ne possèdent aucun dispositif de cryptage; ainsi que

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

43. Les informations classifiées transmises dans les conditions visées au point 41 ne portent aucun marquage ni indication qui les distinguerait d'informations non classifiées ou pouvant être protégées à l'aide d'un dispositif de cryptage disponible. Les destinataires sont informés, sans délai et par d'autres moyens, du niveau de classification.

44. Lorsque des informations sont transmises en application des parapgraphes 41 et 42, un rapport est par la suite adressé à ce sujet à l'autorité compétente.

CONSIGNE DE SÉCURITÉ 4

SÉCURITÉ PHYSIQUE

A. **INTRODUCTION**

La présente consigne de sécurité énonce les principes de sécurité sous-tendant la mise en place d'un environnement sécurisé compatible avec le traitement d'informations confidentielles au sein du Parlement. Ces principes, notamment leur aspect technique, sont complétés par les instructions de traitement.

B. **GESTION DES RISQUES DE SÉCURITÉ**

1. Les risques pesant sur les informations classifiées sont gérés dans le cadre d'une procédure spécifique. Cette dernière vise à déterminer les risques connus pesant sur la sécurité, à définir des mesures de sécurité permettant de ramener ces risques à un niveau acceptable conformément aux principes de base et aux normes minimales énoncés dans la présente consigne de sécurité et à appliquer ces mesures en faisant sienne la notion de défense en profondeur, définie dans la consigne de sécurité 3. L'efficacité de telles mesures fait l'objet d'une évaluation constante.

2. Les mesures de sécurité applicables à la protection des informations classifiées 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 documents ainsi qu'à leur volume, au lieu et à la construction des installations hébergeant des informations classifiées et à la menace, évaluée à l'échelle locale, que représentent les activités malveillantes ou criminelles, notamment l'espionnage, le sabotage et le terrorisme.

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

4. Des mesures de prévention et de rétablissement visant à limiter autant que possible l'impact de défaillances ou d'incidents graves sur le traitement et le stockage des informations classifiées sont prévues dans les plans de continuité des opérations.

C. **PRINCIPES GÉNÉRAUX**

5. Le niveau de classification ou d'indication des informations détermine le niveau de protection applicable en matière de sécurité physique.

6. Les informations qu'il convient de classifier doivent être marquées et traitées comme telles, quelle que soit leur forme physique. La classification doit être clairement communiquée aux destinataires, soit au moyen d'un marquage de classification (lorsque les informations sont communiquées par écrit, que ce soit sur papier ou dans le cadre d'un SIC), soit au moyen d'une annonce (lorsque les informations sont communiquées oralement, par exemple lors d'une conversation ou dans le cadre d'une présentation). Une mention de classification doit être apposée de manière physique sur le document classifié de manière à permettre une identification aisée de la classification de sécurité.

7. Les informations classées confidentielles ne doivent, sous aucun prétexte, être lues dans des lieux publics (trains, avions, cafés, bars, etc.) où elles peuvent être visualisées par un tiers n'ayant pas vocation à en prendre connaissance. Ces informations ne doivent pas être laissées sans surveillance dans les lieux publics.

D. **RESPONSABILITÉS**

8. Il incombe à l'unité «Informations classifiées» (UIC) d'assurer la sécurité physique des informations confidentielles déposées et traitées dans ses installations sécurisées. L'UIC est par ailleurs responsable de la gestion de ses installations sécurisées.

9. Lors du traitement tant des informations classifiées au niveau RESTREINT UE/ EU RESTRICTED ou à son équivalent que des informations classifiées «autres informations confidentielles», la sécurité physique relève de la responsabilité de l'organe ou du titulaire d'un mandat au sein du Parlement correspondant.

10. La direction de la sécurité et de l'évaluation des risques veille à la sécurité du personnel et aux habilitations de sécurité nécessaires pour permettre le traitement sécurisé des informations confidentielles au sein du Parlement européen.

11. La direction des technologies de l'information (DIT) exerce une mission de conseil et veille à ce que tout SIC créé ou mis en œuvre respecte intégralement la consigne de sécurité 3 ainsi que les instructions de traitement correspondantes.

E. **INSTALLATIONS SÉCURISÉES**

12. Il est possible de mettre en place des installations sécurisées spécifiques au titre des normes techniques de sécurité pour autant qu'elles soient conformes au niveau de confidentialité attribué aux informations en vertu de l'article 7.

13. Les installations sécurisées sont certifiées par l'AHS et validées par l'AS.

F. **CONSULTATION DES INFORMATIONS CONFIDENTIELLES**

14. Si des informations classifiées au niveau RESTREINT UE/EU RESTRICTED ou à son équivalent, ou des informations classifiées «autres informations confidentielles», doivent être consultées hors de la zone sécurisée alors qu'elles ont été déposées auprès de l'UIC, cette dernière en transmet une copie au service autorisé approprié qui veille à ce que la consultation et le traitement desdites informations soient conformes à l'article 8, paragraphe 2, et à l'article 10 de la présente décision ainsi qu'aux instructions de traitement applicables en la matière.

15. Si des informations classifiées au niveau RESTREINT UE/EU RESTRICTED ou à son équivalent, ou des informations classifiées «autres informations confidentielles», sont déposées auprès d'un organe ou d'un titulaire de mandat au sein du Parlement autre que l'UIC, il incombe au secrétariat de cet organe ou à ce titulaire de mandat de veiller à ce que la consultation et le traitement desdites informations soient effectués en conformité avec l'article 7, paragraphe 3, à l'article 8, paragraphes 1, 2 et 4, à l'article 9, paragraphes 3 à 5, à l'article 10, paragraphes 2 à 6, et à l'article 11 de la présente décision ainsi qu'aux instructions de traitement applicables.

16. Si des informations classifiées aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET ou à leurs équivalents sont consultées dans la zone sécurisée, il incombe à l'UCI de veiller à ce que la consultation et le traitement desdites informations soient conformes aux articles 9 et 10 de la présente décision ainsi qu'aux instructions de traitement applicables.

G. **SÉCURITÉ TECHNIQUE**

17. Les mesures afférentes à la sécurité technique relèvent de la responsabilité de l'AHS, à qui il appartient de définir, dans les instructions de traitement, les normes particulières qui doivent s'appliquer en la matière

18. Les salles de lecture sécurisées réservées, en vertu de l'article 7, paragraphe 3, de la présente décision, à la consultation des informations classifiées au niveau RESTREINT UE/ EU RESTRICTED ou de niveau équivalent, ainsi que des informations classifiées «autres informations confidentielles», doivent satisfaire aux normes particulières prévues dans les instructions de traitement en matière de sécurité technique.

19. La zone sécurisée visée à l'article 7, paragraphe 2, de la présente décision, comprend les installations suivantes:

a) un sas de sécurité («SAS») qu'il convient d'installer conformément aux mesures de sécurité technique prévues dans les instructions de traitement; les accès à ce sas sont consignés; le sas de sécurité satisfait aux normes élevées d'identification des personnes et prévoit l'enregistrement des accès, un dispositif de vidéosurveillance, un espace sécurisé pour déposer les effets personnels interdits dans les salles sécurisées (téléphones, stylos, etc.);

b) une salle de communication permettant d'envoyer et de recevoir des informations classifiées, notamment des informations classifiées cryptées, conformément à la consigne de sécurité 3 et aux instructions de traitement correspondantes;

c) des archives sécurisées équipées d'éléments de rangement homologués et certifiés utilisés séparément pour stocker les informations classifiées aux niveaux RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL et/ou CONFIDENTIEL UE/EU CONFIDENTIAL ou à leurs équivalents; il appartient de stocker les informations classifiées au niveau TRÈS SECRET UE/EU TOP SECRET ou à son équivalent dans une salle séparée et de les placer dans un élément de rangement certifié particulier; le seul équipement additionnel autorisé dans cette salle est le bureau d'aide permettant à l'UIC de gérer les archives;

d) une salle d'enregistrement mettant à disposition le matériel nécessaire pour permettre un enregistrement papier ou électronique, et équipée ainsi des outils sécurisés indispensables pour installer le SIC souhaité; seule la salle d'enregistrement est habilitée à héberger des appareils de reproduction validés et homologués (copies papier ou sous forme électronique). Les instructions de traitement précisent quels sont les appareils de reproduction qui sont réputés homologués et validés. La salle d'enregistrement présente également les capacités indispensables pour stocker et gérer le matériel homologué nécessaire au marquage, à la duplication et à la diffusion des informations classifiées sous forme physique, selon leur niveau de classification. L'UCI définit toujours le matériel qui est homologué, qui doit par ailleurs être validé par l'AHS en accord avec l'avis de l'autorité opérationnelle chargée de l'assurance de l'information. Cette salle doit également accueillir le matériel de destruction homologué et validé pour le niveau de classification le plus élevé, comme décrit dans les instructions de traitement; la traduction des informations classifiées aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET ou à leurs équivalents doit s'effectuer dans la salle d'enregistrement en utilisant le système approprié et homologué; la salle d'enregistrement doit être équipée de postes de travail permettant à deux traducteurs au maximum de travailler simultanément sur le même document; un membre de l'unité «Informations classifiées» doit être présent;

e) une salle de lecture permettant aux personnes dûment autorisées de consulter individuellement les informations classifiées; la salle de lecture doit permettre d'accueillir deux personnes, dont un membre de l'UCI qui doit être présent durant l'ensemble de la consultation; le niveau de sécurité de cette salle est prévu pour les informations classifiées aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET ou à leurs équivalents. La salle de lecture peut accueillir du matériel Tempest conforme au niveau de classification desdites informations pour permettre, si nécessaire, une consultation par voie électronique;

f) une salle de réunion pouvant accueillir jusqu'à 25 personnes consultant des informations classifiées aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET ou à leurs équivalents; la salle de réunion est équipée d'installations techniques sécurisées et certifiées permettant d'interpréter dans et depuis un maximum de deux langues. Quand elle n'accueille pas de réunion, cette salle peut également servir de salle de lecture supplémentaire dédiée à la consultation individuelle; l'UIC peut, dans des cas exceptionnels, autoriser la consultation des informations classifiées par plus d'une personne autorisée, sous réserve que le niveau d'habilitation et le besoin d'en prendre connaissance soient identiques pour l'ensemble des personnes présentes dans la pièce. Le nombre de personnes autorisées à consulter simultanément des informations classifiées ne peut excéder quatre; il convient alors de renforcer la présence des agents de l'UCI;

g) des locaux techniques sécurisés pour entreposer tout le matériel technique en liaison avec la sécurité de la zone sécurisée et des serveurs informatiques sécurisés.

20. La zone sécurisée satisfait aux normes internationales applicables en la matière et fait l'objet d'une certification par la direction de la sécurité et de l'évaluation des risques. La zone sécurisée prévoit au moins les équipements de sécurité technique suivants:

a) systèmes d'alarme et de sécurité;

b) dispositif de sécurité et systèmes d'urgence (système d'alerte bidirectionnel);

c) système de CCTV;

d) système de détection des intrusions;

e) contrôle d'accès (notamment système biométrique de sécurité);

f) éléments de rangement;

g) casiers;

h) dispositif de protection anti-électromagnétique.

21. L'AHS peut, en étroite coopération avec l'unité «Informations classifiées», ajouter, après avis favorable de l'AS, des mesures afférentes à la sécurité technique.

22. Les équipements d'infrastructure peuvent être reliés aux systèmes de gestion générale du bâtiment accueillant la zone sécurisée. Le dispositif de sécurité gérant le contrôle d'accès et le SIC doit toutefois être indépendant des autres systèmes existant au sein du Parlement européen.

H. **INSPECTIONS DE LA ZONE SÉCURISÉE**

23. La zone sécurisée est régulièrement inspectée par l'AHS et à la demande de l'unité «Informations classifiées».

24. L'AHS établit et tient à jour la liste des éléments à vérifier au cours d'une inspection, conformément aux instructions de traitement.

I. **TRANSPORT DES INFORMATIONS CONFIDENTIELLES**

25. Les informations confidentielles sont transportées à l'abri des regards et ne comportent aucune indication du caractère confidentiel de leur contenu, conformément aux instructions de traitement.

26. Seuls les huissiers et les membres du personnel disposant de l'habilitation de sécurité correspondante peuvent transporter des informations classifiées aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET ou à leurs équivalents.

27. Le transport par courrier externe ou par porteur à l'extérieur d'un bâtiment n'est effectué que s'il répond aux conditions prévues dans les instructions de traitement.

28. Les informations classifiées aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET ou à leurs équivalents ne sont jamais envoyées par courrier électronique ou par télécopie, même s'il existe un système de messagerie électronique «sécurisée» ou de télécopie chiffrée. Les informations classifiées au niveau RESTREINT UE/EU RESTRICTED ou à un niveau équivalent ainsi que les autres informations confidentielles peuvent être envoyées par courrier électronique à l'aide d'un système de chiffrage homologué.

J. **STOCKAGE DES INFORMATIONS CONFIDENTIELLES**

29. Le niveau de classification ou d'indication des informations confidentielles détermine le niveau de protection applicable en vue de leur stockage, qui doit être effectué dans du matériel certifié à cet effet, conformément aux instructions de traitement.

30. Les informations classifiées au niveau RESTREINT UE/EU RESTRICTED ou à son équivalent ainsi que les «autres informations confidentielles»:

a) sont stockées dans une armoire standard métallique fermée à clé, soit dans un bureau soit dans une zone de travail, lorsqu'ils ne sont pas effectivement utilisés;

b) ne sont pas laissées sans surveillance, sauf si elles sont soigneusement rangées sous clé.

c) ne sont pas laissées sur un bureau, une table, etc. de sorte qu'une personne non autorisée, par exemple un visiteur, un agent d'entretien, un agent de maintenance etc. pourrait les lire ou les emporter;

d) ne sont montrées ou exposées à aucune personne non autorisée.

31. Les informations confidentielles classifiées au niveau RESTREINT EU/EU RESTRICTED ou à son niveau équivalent ainsi que les «autres informations confidentielles» sont stockées uniquement au secrétariat des organes/titulaires d'un mandat au sein du Parlement, ou dans l'unité «Informations classifiées», conformément aux instructions de traitement.

32. Les informations confidentielles classifiées aux niveaux CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET ou à leurs équivalents:

a) sont stockées dans la zone sécurisée, dans un meuble de sécurité ou une chambre forte. À titre exceptionnel, par exemple si l'unité «Informations classifiées» est fermée, elles peuvent être stockées dans un coffre-fort au sein des services de sécurité;

b) ne sont jamais laissées sans surveillance dans la zone sécurisée sans avoir été auparavant mises sous clé dans un coffre-fort homologué (même en cas d'absence de très courte durée);

c) ne sont pas laissées sur un bureau, une table, etc. de sorte qu'une personne non autorisée pourrait les lire ou les emporter, même si l'agent responsable de l'unité «Informations classifiées» est présent dans la pièce.

Si un document comportant des informations classifiées est généré sous forme électronique à l'intérieur de la zone sécurisée, l'ordinateur doit être verrouillé et l'écran doit être bloqué si l'auteur du document ou l'agent responsable de l'unité «Informations classifiées» quitte la pièce (même très brièvement). Un verrouillage automatique de sécurité qui se déclenche au bout de quelques minutes n'est pas considéré comme une mesure suffisante.

CONSIGNE DE SÉCURITÉ 5

SÉCURITÉ INDUSTRIELLE

A. **INTRODUCTION**

1. La présente consigne de sécurité concerne uniquement les informations classifiées.

2. Elle contient les dispositions d'application des normes communes minimales figurant à l'annexe I, partie I, de la présente décision.

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

4. Le Parlement européen, en tant qu'autorité contractante, 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.

B. **ASPECTS LIÉS À LA SÉCURITÉ DANS UN CONTRAT CLASSIFIÉ**

B.1. ***Guide de la classification de sécurité (GCS)***

5. Avant de lancer un appel d'offres ou en vue de l'attribution d'un contrat classifié ou avant d'attribuer un tel contrat, le Parlement européen, en tant qu'autorité contractante, détermine le niveau de classification de sécurité de toute information devant être fournie aux soumissionnaires et aux contractants ainsi que de toute information devant être créée pour le contractant. À cet effet, le Parlement européen élabore un guide de la classification de sécurité (GCS), qui sera utilisé aux fins de l'exécution du contrat.

6. La détermination du niveau de classification de sécurité des différents éléments d'un contrat classifié obéit aux principes suivants:

a) pour élaborer un GCS, le Parlement européen tient compte de tous les aspects pertinents en matière de sécurité, y compris du niveau de classification de sécurité attribué aux informations fournies et approuvées par leur auteur aux fins de leur utilisation dans le cadre du contrat;

b) le niveau général de classification du contrat ne peut pas être inférieur au niveau de classification le plus élevé de l'un de ses éléments.

B.2. ***Annexe de sécurité (AS)***

7. Les exigences de sécurité propres à un contrat figurent dans une AS. Le cas échéant, celle-ci contient le GCS et fait partie intégrante du contrat ou du contrat de sous-traitance classifié.

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

B.3. ***Instructions de sécurité relatives à un programme/un projet (ISP)***

9. En fonction de la portée des programmes ou des projets prévoyant l'accès à des informations classifiées de l'Union européenne, leur traitement ou leur stockage, l'autorité contractante chargée du projet ou du programme concerné peut définir des instructions de sécurité spécifiques à ce programme/un projet (ISP).

C. **HABILITATION DE SECURITÉ D'INSTALLATION (HSI)**

10. L'ANS ou toute autre autorité de sécurité compétente d'un État membre délivre une HSI pour indiquer, conformément aux dispositions législatives et réglementaires nationales, qu'une entité industrielle ou autre est en mesure, dans ses installations, de protéger des informations classifiées de l'Union européenne au niveau de classification CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET. La preuve de la délivrance de l'HSI est communiquée au Parlement européen, autorité contractante, avant que le contractant ou sous-traitant, ou le contractant ou sous-traitant potentiel, ne reçoive les informations classifiées de l'Union européenne ou l'autorisation d'accéder à celles-ci.

11. L'ANS:

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

b) analyse les éléments relatifs à la propriété, au contrôle de l'entité et/ou à toute possibilité d'influence indue pouvant être considérés comme un risque de sécurité;

c) s'assure que l'entité industrielle ou toute autre entité a mis en place, dans ses installations, un système de sécurité qui comporte toutes les mesures de sécurité appropriées pour protéger des informations ou des documents classifiés au niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou au niveau SECRET UE/EU SECRET, conformément aux exigences de la présente décision;

d) s'assure que le statut, au regard de la sécurité, du personnel d'encadrement, des propriétaires et des employés qui doivent avoir accès à des documents classifiés au niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou au niveau SECRET UE/EU SECRET a été établi conformément aux exigences de la présente décision; et

e) vérifie que l'entité industrielle ou toute autre entité a nommé un agent chargé de la sécurité des installations et responsable, vis-à-vis de sa direction, du respect des obligations de sécurité dans l'entité.

12. S'il y a lieu, le Parlement européen, en sa qualité d'autorité contractante, informe l'ANS ou toute autre autorité de sécurité compétente qu'une HSI est exigée dans la phase précontractuelle ou pour l'exécution du contrat. Une HSI ou une habilitation de sécurité du personnel (HSP) est exigée dans la phase précontractuelle si des informations classifiées «CONFIDENTIEL UE/EU CONFIDENTIAL» ou «SECRET UE/EU SECRET» doivent être communiquées durant la procédure de soumission des offres.

13. L'autorité contractante n'attribue pas de contrat classifié au soumissionnaire sélectionné avant que l'ANS ou toute autre autorité de sécurité compétente de l'État membre dans lequel le contractant ou le sous-traitant concerné est immatriculé, ne lui ait confirmé la délivrance d'une HSI appropriée.

14. Toute autorité de sécurité compétente ayant délivré une HSI notifie au Parlement européen les modifications éventuellement apportées à ladite HSI. S'il s'agit d'un contrat de sous-traitance, l'autorité de sécurité compétente en est dûment informée.

15. Le retrait d'une HSI par l'ANS concernée ou toute autre autorité de sécurité compétente constitue un motif suffisant habilitant le Parlement européen, en sa qualité d'autorité contractante, à résilier un contrat classifié ou à exclure un soumissionnaire de la procédure d'appel d'offres.

D. **CONTRATS ET CONTRATS DE SOUS-TRAITANCE CLASSIFIÉS**

16. Lorsque des informations classifiées sont communiquées aux soumissionnaires potentiels durant la phase précontractuelle, l'appel d'offres contient une disposition imposant au soumissionnaire qui ne présente pas d'offre ou qui n'est pas sélectionné de restituer tous les documents classifiés dans un délai donné.

17. Après l'attribution d'un contrat ou d'un contrat de sous-traitance classifié, le Parlement européen, en sa qualité d'autorité contractante, notifie les dispositions de sécurité figurant dans le contrat classifié à l'ANS dont relève le contractant ou le sous-traitant et/ou à toute autre autorité de sécurité compétente.

18. Lorsqu'il est mis fin à un contrat ou un contrat de sous-traitance classifié, le Parlement européen, en sa qualité d'autorité contractante (ou, le cas échéant, l'autorité de sécurité compétente s'il s'agit d'un contrat de sous-traitance) avertit immédiatement l'ANS 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 toute information classifiée qu'il a en sa possession, dès que le contrat ou le contrat de sous-traitance classifié prend fin.

20. L'AS contient des dispositions spéciales relatives à la suppression d'informations classifiées durant l'exécution du contrat ou à l'expiration de celui-ci.

21. Lorsque le contractant ou le sous-traitant est autorisé à conserver des informations classifiées après l'expiration d'un contrat, les normes minimales figurant dans la présente décision doivent continuer à être respectées et la confidentialité des informations classifiées de l'Union européenne est protégée par le contractant ou le sous-traitant.

22. Les conditions de sous-traitance par un contractant sont définies dans l'offre et le contrat.

23. Un contractant doit obtenir l'autorisation du Parlement européen, 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 tiers qui n'a pas conclu avec l'Union européenne d'accord sur la sécurité des informations.

24. Le contractant veille à ce que toutes les activités de sous-traitance soient réalisées conformément aux normes minimales définies dans la présente décision et s'abstient de fournir des informations classifiées de l'Union européenne à un sous-traitant sans l'autorisation écrite préalable de l'autorité contractante.

25. L'autorité contractante exerce les droits détenus par l'auteur d'informations classifiées qui sont créées ou traitées par le contractant ou le sous-traitant.

E. VISITES LIÉES À DES CONTRATS CLASSIFIÉS

26. Lorsque le Parlement européen, les contractants ou les sous-traitants sollicitent l'accès à des informations classifiées au niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou au niveau SECRET UE/EU SECRET dans les locaux de l'autre partie aux fins de l'exécution d'un contrat classifié, les visites sont organisées en liaison avec les ANS ou toute autre autorité de sécurité compétente concernée. Toutefois, dans le cadre de projets spécifiques, les ANS peuvent également convenir d'une procédure permettant d'organiser directement ces visites.

27. Pour avoir accès aux informations classifiées liées au contrat attribué par le Parlement européen, les visiteurs doivent détenir une HSP appropriée et avoir vocation à en prendre connaissance.

28. Les visiteurs ont accès uniquement aux informations classifiées qui sont liées à l'objectif de la visite.

F. TRANSMISSION ET TRANSPORT DES INFORMATIONS CLASSIFIÉES

29. En ce qui concerne la transmission d'informations classifiées par voie électronique, les dispositions correspondantes de la consigne de sécurité 3 s'appliquent.

30. En ce qui concerne le transport d'informations classifiées, les dispositions correspondantes de la consigne de sécurité 4 et des instructions de traitement s'appliquent.

31. En ce qui concerne le transport par fret de matériel classifié, les principes ci-après s'appliquent pour déterminer les mesures de sécurité:

a) la sécurité est assurée à tous les étapes du transport, du lieu d'origine jusqu'à la destination finale;

b) le degré de protection affecté à un envoi est déterminé en fonction du niveau de classification le plus élevé des documents qu'il contient;

c) le cas échéant, une HSI est délivrée aux sociétés assurant le transport; le personnel de manutention reçoit alors une habilitation de sécurité conformément à l'annexe I;

d) avant tout déplacement transfrontalier de documents classifiés au niveau CONFIDENTIEL UE/EU CONFIDENTIAL, au niveau SECRET UE/EU SECRET ou à leurs équivalents, un plan de transport est établi par l'expéditeur et approuvé par le Secrétaire général;

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

f) les itinéraires passent, autant que possible, par le territoire des États membres.

G. **TRANSFERT D'INFORMATIONS CLASSIFIÉES AUX CONTRACTANTS ÉTABLIS DANS DES ÉTATS TIERS**

32. Les informations classifiées sont transférées aux contractants et sous-traitants établis dans des États tiers conformément aux mesures de sécurité convenues entre le Parlement européen, en sa qualité d'autorité contractante, et l'État tiers concerné dans lequel le contractant est immatriculé.

H. **TRAITEMENT ET STOCKAGE D'INFORMATIONS CLASSIFIÉES AU NIVEAU RESTREINT UE/EU RESTRICTED**

33. En liaison, s'il y a lieu, avec l'ANS de l'État membre concerné, le Parlement européen, en sa qualité d'autorité contractante, est habilité, en vertu de dispositions contractuelles, à effectuer des visites dans les installations des contractants/sous-traitants afin de s'assurer de la mise en place, comme l'exige le contrat, des mesures de sécurité applicables aux fins de la protection des informations classifiées de l'Union européenne de niveau RESTREINT UE/EU RESTRICTED.

34. Dans la mesure nécessaire, en vertu des dispositions légales et réglementaires nationales, les ANS, ou toutes autres autorités de sécurité compétentes, doivent être informées par le Parlement européen, autorité contractante, des contrats ou contrats de sous-traitance contenant des informations classifiées au niveau RESTREINT UE/EU RESTRICTED.

35. Les contractants ou sous-traitants et leur personnel ne sont pas tenus de posséder une HSI ou une HSP pour les contrats attribués par le Parlement européen qui contiennent des informations classifiées au niveau RESTREINT UE/EU RESTRICTED.

36. Le Parlement européen, en sa qualité d'autorité contractante, examine les réponses aux appels d'offres portant sur des contrats prévoyant l'accès à des informations classifiées au niveau RESTREINT UE/EU RESTRICTED, nonobstant les exigences liées aux HSIs ou HSPs que les dispositions législatives et réglementaires nationales sont susceptibles de prévoir.

37. Les conditions de sous-traitance par un contractant sont définies dans l'offre et le contrat.

38. Si un contrat prévoit le traitement d'informations classifiées au niveau RESTREINT UE/EU RESTRICTED au moyen de systèmes de communication et d'information exploités par un contractant, le Parlement européen, en sa qualité d'autorité contractante, veille à ce que les exigences techniques et administratives d'homologation desdits systèmes, proportionnées au risque évalué à l'aune de tous les facteurs pertinents, soient précisées dans le contrat. La portée de l'homologation desdits systèmes est fixée d'un commun accord par l'autorité contractante et l'ANS/ASD compétente.

CONSIGNE DE SÉCURITÉ 6

INFRACTIONS À LA SÉCURITÉ, PERTE OU COMPROMISSION D'INFORMATIONS CLASSIFIÉES

1. Une infraction à la sécurité est la conséquence d'un acte ou d'une omission contraire à la présente décision qui pourrait mettre en péril ou compromettre des informations confidentielles.

2. Des informations confidentielles sont compromises lorsque des personnes non autorisées — c'est-à-dire des personnes qui n'ont pas l'habilitation de sécurité correspondante ou n'ont pas vocation à prendre connaissance de telles informations — se les approprient en totalité ou en partie ou lorsqu'il est vraisemblable qu'elles se les soient appropriées.

3. Des informations confidentielles peuvent être compromises à la suite d'une inattention, d'une négligence ou d'une indiscrétion et à cause d'activités menées par des services qui prennent l'Union pour cible ou par des organisations subversives.

4. Lorsque le Secrétaire général constate ou apprend l'existence avérée ou alléguée d'une infraction à la sécurité, de la perte ou de la compromission d'informations confidentielles, il lui incombe:

a) d'établir les faits;

b) d'évaluer et de réduire au minimum les dommages occasionnés;

c) de prendre des mesures pour éviter que les faits ne se reproduisent;

d) d'informer l'autorité compétente de l'État tiers ou de l'État membre qui a créé ou transmis les informations confidentielles.

Lorsqu'un député au Parlement européen est concerné, le Secrétaire général collabore avec le Président du Parlement européen.

Si les informations sont transmises par les autres institutions de l'Union, le Secrétaire général se conforme aux mesures de sécurité appropriées relatives aux informations classifiées ainsi qu'aux modalités prévues par l'accord-cadre conclu avec la Commission ou par l'accord interinstitutionnel conclu avec le Conseil.

5. Toutes les personnes chargées de traiter des informations confidentielles reçoivent d'amples instructions sur les procédures de sécurité, les risques liés à une conversation indiscrète et à leurs relations avec les médias. Le cas échéant, elles signent une déclaration par laquelle elles s'engagent à ne pas révéler à des tiers le contenu des informations confidentielles, à respecter l'obligation de protéger ces dernières et à supporter les conséquences de tout manquement. L'accès à des informations classifiées ou leur utilisation par une personne n'ayant ni reçu les instructions précitées ni signé la déclaration y afférente est considéré comme une infraction à la sécurité.

6. Les députés au Parlement européen, les fonctionnaires du Parlement et les autres agents du Parlement au service des groupes politiques ou de contractants informent immédiatement le Secrétaire général de toute infraction à la sécurité, perte ou compromission d'informations confidentielles dont ils peuvent avoir connaissance.

7. Toute personne responsable de la compromission d'informations confidentielles est passible de sanctions disciplinaires conformément aux dispositions réglementaires applicables. De telles sanctions, son adoptée sans préjudice de poursuites judiciaires qui peuvent être entamées conformément à la législation applicable.

8. Sous réserve d'autres poursuites judiciaires, les infractions commises par des fonctionnaires du Parlement et d'autres agents du Parlement européen travaillant pour des groupes politiques entraînent l'application des procédures et des sanctions prévues par au titre VI du statut du personnel.

9. Sans préjudice d'autres poursuites judiciaires, les infractions commises par des députés au Parlement européen sont traitées conformément à l'article 9, paragraphe 2, ainsi que des articles 152, 153 et 154 du règlement.