IV

(Informations)

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

PARLEMENT EUROPÉEN

DÉCISION DU BUREAU DU PARLEMENT EUROPÉEN

du 6 juin 2011

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

(2011/C 190/02)

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»), il est nécessaire de réviser la décision du Bureau du 13 novembre 2006 sur la réglementation relative au traitement administratif des documents confidentiels.

(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 de l'article 15 du traité sur le fonctionnement de l'Union européenne ni du règlement (CE) nº 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission [2].

(5) Les dispositions de la présente décision sont arrêtées sans préjudice de l'article 16 du traité sur le fonctionnement de l'Union européenne ni du règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données [3],

A ADOPTÉ LA PRÉSENTE DÉCISION

Article premier

Objectif

La présente décision régit la création, la réception, la transmission et le stockage des informations confidentielles par le Parlement européen en vue d'assurer une protection appropriée de leur caractère confidentiel. Elle met en œuvre, en particulier, l'annexe 2 de l'accord-cadre.

[1] JO L 304 du 20.11.2010, p. 47.

[2] JO L 145 du 31.5.2001, p. 43.

[3] JO L 8 du 12.1.2001, p. 1.

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 de l'UE» et «autres informations confidentielles» non classifiées;

c) «informations classifiées de l'UE»: 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 pourrait porter 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, organismes et agences établis en vertu ou sur la base des traités ou qu'elles proviennent d'États membres, d'États tiers ou d'organisations internationales. Á cet égard:

— «TRÈS SECRET UE/EU TOP SECRET» est la classification pour les informations et matériels 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» est la classification pour les informations et matériels 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» est la classification pour les informations et matériels 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» est la classification pour les informations et matériels dont la divulgation non autorisée pourrait être défavorable aux intérêts de l'Union ou d'un ou plusieurs des États membres.

d) «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;

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

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

g) «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;

h) «autorisation»: une décision (décision d'habilitation) 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 travaillant pour les groupes politiques, permet à un individu d'accéder à des informations classifiées de l'UE 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;

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

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

k) «autorité d'origine»: l'auteur, dûment autorisé, d'une information classifiée de l'UE ou de toute autre information confidentielle;

l) «consignes de sécurité»: les mesures techniques de mise en œuvre établies à l'annexe II [1].

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 conformément à ces principes de base et normes minimales, qui vise à faciliter le travail parlementaire et administratif tout en assurant la protection de toute information confidentielle traitée par le Parlement européen, dans le plein respect des règles établies par l'autorité d'origine de cette information comme prévu dans les consignes de sécurité.

Le traitement des informations confidentielles par des systèmes d'information automatisés (SI) du Parlement européen est mis en œuvre conformément au concept d'assurance de l'information (AI) comme prévu dans les consignes de sécurité.

[1] Annexe à adopter.

3. Les députés au Parlement européen peuvent consulter les informations classifiées jusques et y compris au niveau «CONFIDENTIEL UE/EU CONFIDENTIAL» sans habilitation de sécurité. Pour les informations classifiées «CONFIDENTIEL UE/EU CONFIDENTIAL», ils signent une déclaration solennelle par laquelle ils s'engagent à ne pas communiquer le contenu de ces informations à des tiers. Les informations classifiées au-dessus du niveau «CONFIDENTIEL UE/EU CONFIDENTIAL» sont uniquement communiquées aux députés qui disposent de l'habilitation de sécurité du niveau approprié.

4. 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.

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 selon ce que prévoient les consignes de sécurité.

2. Lorsqu'elle crée une information classifiée, l'autorité d'origine applique le niveau de classification approprié, conformément aux normes internationales et définitions énoncées à l'annexe I. L'autorité d'origine définit aussi, en règle générale, les destinataires qui doivent être autorisés à consulter cette information, en fonction du niveau de classification. Cette information est communiquée au Service des informations confidentielles (SIC) lors du dépôt du document auprès du SIC.

3. Les informations confidentielles couvertes par le secret professionnel sont traitées conformément aux instructions de traitement définies dans les consignes de sécurité.

Article 5

Réception d'informations confidentielles par le Parlement européen

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

— en ce qui concerne les informations confidentielles de l'UE du niveau «RESTREINT UE/EU RESTRICTED» et les autres informations confidentielles, au secrétariat de l'organe/titulaire d'un mandat au sein du Parlement qui a présenté la demande,

— en ce qui concerne les informations confidentielles de l'UE classifiées au niveau «CONFIDENTIEL UE/EU CONFIDENTIAL» et au-delà, au SIC.

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

3. Dans le cas d'informations confidentielles communiquées par la Commission conformément à l'accord-cadre, les modalités convenues au sens du point 3.2. de l'annexe II de l'accord-cadre (fixées d'un commun accord et concernant les destinataires, la procédure de consultation, c'est-à-dire une salle de lecture sécurisée et des réunions à huis clos, ou d'autres questions) prévues pour préserver la confidentialité des informations sont déposées, avec les informations confidentielles, auprès du secrétariat de l'organe/du titulaire d'un mandat au sein du Parlement européen ou du SIC lorsque les informations sont classifiées «CONFIDENTIEL UE/EU CONFIDENTIAL» ou au-delà.

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. Les informations classifiées de l'UE classifiées au niveau «TRÈS SECRET UE/EU TOP SECRET» sont transmises au Parlement européen selon d'autres modalités, à convenir entre l'organe/titulaire d'un mandat au sein du Parlement européen qui a présenté la demande d'informations et l'institution de l'Union ou l'État membre qui les détient. Un comité de surveillance est établi par la Conférence des présidents. Il vise à assurer un niveau de protection correspondant à ce niveau de classification.

Article 6

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

Le Parlement européen peut, avec le consentement de l'autorité d'origine, transmettre des informations classifiées de l'UE à d'autres institutions, organes, organismes et agences établis en vertu ou sur la base des traités ou aux États membres à la condition qu'ils garantissent que, lors du traitement des informations classifiées de l'UE, des règles équivalentes à celles fixées par la présente décision sont respectées dans leurs services et leurs locaux.

Article 7

Stockage et consultation des informations confidentielles dans des zones sécurisées (salles de lecture sécurisée)

1. Les salles de lecture sécurisées permettent un stockage sécurisé et ne comportent ni photocopieurs, ni téléphones, ni télécopieurs, ni scanners, ni aucun autre moyen technique de reproduction ou de transmission de documents.

2. L'accès à une salle de lecture sécurisée est régi par les conditions suivantes:

a) Seules les personnes ci-après y ont accès:

— les députés au Parlement européen, les fonctionnaires du Parlement européen et les autres employés du Parlement travaillant pour les groupes politiques, dûment identifiés conformément aux modalités visées à l'article 4, paragraphe 2, ou à l'article 5, paragraphes 3 et 4;

— les fonctionnaires du Parlement européen chargés de la gestion du SIC;

— si nécessaire, les fonctionnaires du Parlement européen responsables de la sécurité et de la protection contre l'incendie.

Le nettoyage de la zone sécurisée se fait uniquement en la présence et sous la surveillance étroite d'un fonctionnaire travaillant au SIC.

b) Chaque personne qui souhaite avoir accès à des informations confidentielles communique à l'avance son nom au SIC. Le SIC vérifie l'identité de chaque personne présentant une demande de consultation d'informations confidentielles et vérifie, le cas échéant, que cette personne possède une habilitation de sécurité du niveau requis et est autorisée à effectuer cette consultation conformément aux modalités visées à l'article 4, paragraphe 2, ou à l'article 5, paragraphes 3 et 4;

c) Le SIC est habilité à refuser l'accès de la salle à toute personne non autorisée à y pénétrer en vertu des points a) et b). Toute contestation de la décision du SIC est soumise au président dans le cas des députés au Parlement européen, et au secrétaire général dans les autres cas.

3. Les conditions ci-après régissent la consultation d'informations confidentielles dans la salle de lecture sécurisée:

a) Les personnes autorisées à consulter les informations et ayant introduit la demande visée au paragraphe 2, point b), doivent se présenter auprès du SIC.

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 la salle de lecture sécurisée, en présence d'un fonctionnaire du SIC.

Le fonctionnaire informe la personne ainsi autorisée de ses obligations et lui fait notamment signer une déclaration sur l'honneur qui l'engage à ne pas en divulguer le contenu à un tiers;

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

c) Avant d'autoriser une personne à quitter la salle de lecture sécurisée, le fonctionnaire du SIC visé au point a) s'assure que les informations confidentielles consultées sont toujours présentes, intactes et complètes.

4. En cas de manquements aux règles définies ci-dessus, le fonctionnaire responsable du SIC en informe le secrétaire général, qui en réfère au président au cas où l'auteur des manquements est un député au Parlement européen.

Article 8

Normes minimales applicables à d'autres consultations d'informations confidentielles

1. S'agissant du traitement administratif d'informations confidentielles lors d'une réunion à huis clos, le secrétariat de l'organe/du titulaire d'un mandat au sein du Parlement européen responsable de la réunion veille à ce que:

— seules les personnes désignées pour participer à la réunion et possédant le niveau d'habilitation de sécurité requis soient autorisées à pénétrer dans la salle de réunion;

— tous les documents soient numérotés, distribués au début de la réunion et récupérés à la fin et aucune note, photocopie ou photographie de ces documents ne soit prise;

— le procès-verbal de la réunion ne mentionne pas le contenu de la discussion sur les informations qui ont été examinées selon la procédure confidentielle;

— les informations confidentielles communiquées oralement à des destinataires au Parlement européen soient soumises à un niveau de protection équivalent à celui appliqué aux informations confidentielles ayant la forme d'un écrit. Une déclaration sur l'honneur portant engagement des destinataires de ces informations de ne pas les divulguer à des tiers peut notamment être prévue.

2. Les règles suivantes s'appliquent au traitement administratif des informations confidentielles, en dehors des réunions à huis clos, par le secrétariat de l'organe/du titulaire d'un mandat au sein du Parlement européen:

— les documents sur support papier sont remis en mains propres au chef du secrétariat, qui les enregistre et fournit un accusé de réception;

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

— sans préjudice du traitement administratif des informations confidentielles lors d'une réunion à huis clos, tel que décrit au paragraphe 1, en aucun cas ces informations ne peuvent être reproduites, sauvegardées sur un autre support ou transmises à quiconque;

— l'accès à ces documents est limité à leurs destinataires et se fait, conformément aux modalités visées à l'article 4, paragraphe 2, ou à l'article 5, paragraphes 3 ou 4, sous le contrôle du secrétariat;

— le secrétariat tient un relevé des personnes ayant consulté les documents, qui indique la date et l'heure de la consultation. Ce relevé est transmis au SIC en vue de l'établissement du rapport annuel visé à l'article 12.

Article 9

Archivage des informations confidentielles

1. Un système d'archivage sécurisé est assuré dans les locaux du Parlement européen.

Les informations confidentielles définitivement déposées auprès du SIC ou du secrétariat de l'organe/du titulaire d'un mandat au sein du Parlement européen sont transférées vers les archives sécurisées du SIC six mois après la dernière consultation et, au plus tard, un an après leur dépôt.

2. Le SIC est responsable de la gestion des archives sécurisées, conformément aux normes en matière d'archivage.

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

— 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;

— la demande de consultation de ces informations doit être présentée au SIC qui assurera le transfert du document vers la salle de lecture sécurisée;

— les procédures et conditions applicables à la consultation des informations confidentielles, définies à l'article 7, sont d'application.

Article 10

Déclassement et déclassification d'informations classifiées de l'UE

1. Les informations classifiées de l'UE ne peuvent être déclassées ou déclassifiées qu'avec l'autorisation de l'autorité d'origine et, si nécessaire, après consultation des autres parties intéressées. 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.

2. La déclassification des documents conservés dans les archives sécurisées intervient au plus tard à l'issue d'un délai de 30 ans, conformément aux dispositions du règlement (CEE, Euratom) n° 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.

Article 11

Violations de la confidentialité

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

2. Les violations commises par le personnel entraînent 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) n° 259/68 du Conseil [2] (ci-après dénommés «statut des fonctionnaires»).

3. Le président et le secrétaire général diligentent les enquêtes nécessaires.

Article 12

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 présente un rapport annuel au Bureau sur l'application de la présente décision.

[1] JO L 43 du 15.2.1983, p. 1.
[2] JO L 56 du 4.3.1968, p. 1.

Article 13

Dispositions transitoires et finales

1. Les informations confidentielles se trouvant au SIC ou dans les archives avant l'application de la présente décision sont classifiées au niveau «RESTREINT UE/EU RESTRICTED» par défaut, à moins que l'autorité d'origine décide de ne pas les classifier ou de les classifier à un niveau de classification supérieur ou d'y apposer un marquage dans un délai d'un an à compter de l'entrée en vigueur de la présente décision.

2. Si l'autorité d'origine décide de classifier ces informations confidentielles à un niveau supérieur, elles sont classifiées au niveau le plus bas possible par l'autorité d'origine ou ses délégués, en liaison avec le SIC et conformément aux critères énoncés à l'annexe I.

3. La décision du Bureau du 13 novembre 2006 sur la réglementation relative au traitement administratif des documents confidentiels est abrogée.

4. La décision du Bureau du 24 octobre 2005 chargeant le secrétaire général de constituer un comité de déclassification et d'adopter des décisions en matière de déclassification est abrogée.

Article 14

Entrée en vigueur

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

2. Elle s'applique à compter du 1er juillet 2011.

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 à respecter par le Parlement européen dans tous les lieux de travail ainsi que par tout destinataire d'informations classifiées de l'UE 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. Elles sont complétées par les 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 généraux

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.

Le principe de 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. Ce principe implique également que 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, il implique que les manquements aux règles de sécurité commis dans le domaine de responsabilité du Parlement européen doivent être traités conformément à la politique du Parlement européen en matière de mesures disciplinaires.

Le principe de 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. Ce principe implique également la nécessité de disposer d'orientations écrites claires pour la mise en œuvre des mesures de sécurité.

Le principe de 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.

Le principe de 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. Le principe de proportionnalité signifie que les activités de sécurité doivent être strictement limitées à ce qui est absolument nécessaire et que les mesures de sécurité doivent être proportionnelles aux intérêts à protéger et 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) au sein du Parlement européen, un service INFOSEC d'assurance de la sécurité des informations chargé de travailler avec l'autorité responsable de la sécurité concernée pour fournir des informations et des avis sur les menaces d'ordre technique pesant sur la sécurité et sur les moyens de s'en protéger;

b) 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 classifiées de l'UE et des autres informations confidentielles contre l'espionnage, la compromission ou la divulgation non autorisée;

b) la protection des informations classifiées de l'UE 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 de l'UE 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 de ses conséquences, la réalisation d'enquêtes de sécurité et l'adoption des mesures correctives nécessaires.

4.2. *Classification*

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 fondamental 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; un système similaire de classification est utilisé 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 locaux les plus importants contenant des informations classifiées de l'UE et, à l'intérieur de ces locaux, les éléments les plus sensibles.

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. Lorsqu'un certain nombre d'éléments d'informations sont regroupés, le niveau de classification à appliquer à l'ensemble est au moins égal au degré le plus élevé de classification appliqué individuellement à ces éléments. 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 de l'UE, aux supports des informations classifiées de l'UE, 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 de repérer les personnes dont le poste 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 (c'est-à-dire empêcher 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) de toutes les informations confidentielles, classifiées ou non, et en particulier des informations 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 observées par tout destinataire d'une information classifiée de l'UE, 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 organismes extérieurs que pour autant qu'ils assurent 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 de l'UE doivent recevoir, lors de leur entrée en fonction puis à intervalles réguliers, un exposé très complet des mesures de sécurité nécessaires et des procédures en vigueur à cet égard. Ces personnes doivent certifier 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. S'il s'avère 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 de l'UE.

7.1. *Exigences en matière de protection*

Le degré de sécurité physique à mettre en œuvre pour assurer la protection des informations classifiées de l'UE doit être proportionnel 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 de l'UE 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 de l'UE, 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 de l'UE et des systèmes de communication et d'information sécurisés doivent être défendus contre les accès non autorisés.

La nature de la protection des informations classifiées de l'UE, 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 c), 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. Cet identifiant est «JUSQU'À/AU … (heure/date)» ou «JUSQU'À/AU … (événement)».

Des identifiants de sécurité complémentaires tels que CRYPTO ou tout autre identifiant de sécurité reconnu par l'Union sont utilisés lorsque sont nécessaires une diffusion limitée et un traitement spécial qui s'ajoutent à ceux qu'exige la classification de sécurité.

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

8.2. *Marquages*

Un marquage peut être utilisé pour préciser 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 ne saurait être utilisé en lieu et place d'une classification.

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

La classification est apposée de la manière suivante:

a) sur les documents classifiés «RESTREINT UE/EU RESTRICTED», par un procédé mécanique ou électronique;

b) sur les documents classifiés «CONFIDENTIEL UE/EU CONFIDENTIAL», par un procédé mécanique, à la main ou par impression sur du papier enregistré revêtu d'un cachet pré-imprimé;

c) sur les documents classifiés «SECRET UE/EU SECRET» et «TRÈS SECRET UE/EU TOP SECRET», par voie mécanique ou à la main.

Les identifiants de sécurité sont apposés juste sous la classification, par les mêmes moyens que pour l'apposition des classifications.

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 documents «TRÈS SECRET UE/EU TOP SECRET» est limité au strict minimum et les noms de ces personnes sont consignés sur une liste établie par le SIC.

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 c). Il importe que la classification soit utilisée à bon escient et avec modération, en particulier pour la classification «TRÈS SECRET UE/EU TOP SECRET».

Les lettres ou notes d'envoi accompagnant des pièces jointes portent 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 tenir compte des diverses règles susmentionnées et se garder de toute tendance à la surclassification comme à 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 des mesures de sécurité prises pour la protection des informations classifiées de l'UE sont menées par la direction du Parlement européen en charge de la sécurité, qui peut être assistée dans cette tâche par le SIC.

La direction du Parlement européen en charge de la sécurité et les services de sécurité d'autres institutions, organes, organismes et agences établis en vertu ou sur la base des traités détenant des informations classifiées de l'UE peuvent également convenir de procéder à des évaluations par les pairs des mesures de sécurité prises pour assurer la protection des informations classifiées de l'UE.

10. **Procédure de déclassification**

10.1. Le SIC examine les informations classifiées de l'UE et adresse des propositions quant à la déclassification à l'autorité d'origine du document au plus tard la 25e année suivant la date de création du document. Les documents qui ne sont pas déclassifiés lors du premier examen sont réexaminés régulièrement, et ce au moins tous les cinq ans.

10.2. Outre aux documents effectivement conservés dans les archives sécurisées et dûment classifiés, le processus de déclassification peut également être appliqué à d'autres informations confidentielles conservées soit dans les archives sécurisées, soit par le centre archivistique et documentaire (CARDOC).

10.3. Il incombe au SIC, agissant pour le compte de l'autorité d'origine, d'informer les destinataires du document du changement de classification, 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 marquages pouvant apparaître sur le document.

10.5. 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 le SIC.

10.6. Le texte du document déclassifié 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, le SIC consulte le tiers concerné avant de procéder à la déclassification. Le tiers dispose de 8 semaines pour présenter des observations;

b) s'agissant des exceptions concernant la vie privée et l'intégrité de l'individu, la procédure de déclassification tient compte, en particulier, de l'accord de la personne concernée, de l'impossibilité d'identifier la personne concernée et/ou du fait que cette personne n'est plus en vie;

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. Eu égard aux prérogatives et aux compétences du Parlement européen, les députés bénéficient sans habilitation de sécurité d'un accès aux informations classifiées de l'UE allant jusqu'au niveau «CONFIDENTIEL UE/EU CONFIDENTIAL» inclus. Pour les informations classifiées «CONFIDENTIEL UE/EU CONFIDENTIAL», ils signent une déclaration solennelle par laquelle ils s'engagent à ne divulguer le contenu de ces informations à aucun tiers.

11.2. Pour pouvoir accéder aux informations classifiées «TRÈS SECRET UE/EU TOP SECRET» ou «SECRET UE/EU SECRET», les députés au Parlement européen doivent avoir été autorisés à cet effet conformément à la procédure décrite aux points 11.3 et 11.4.

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 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 du Parlement européen en charge de la sécurité 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 aux autorités nationales compétentes le niveau de classification des informations que le député au Parlement européen concerné aurait à connaître, de sorte que ces autorités puissent mener la procédure d'enquête.

11.11. L'ensemble du déroulement et des résultats de la procédure d'enquête de sécurité menée par les autorités nationales compétentes 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 les autorités nationales compétentes de l'État membre émettent un avis positif, le président peut octroyer l'autorisation au député au Parlement européen concerné.

11.13. Un avis négatif des autorités nationales compétentes 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 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 les autorités nationales compétentes et en l'absence de réaction de celles-ci 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 comme «TRÈS SECRET UE/EU TOP SECRET».

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 «TRÈS SECRET UE/EU TOP SECRET», «SECRET UE/EU SECRET» et «CONFIDENTIEL UE/EU CONFIDENTIAL», les personnes visées au point 12.1 doivent avoir été autorisées 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 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 du Parlement européen en charge de la sécurité 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 de la personne concernée 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 «CONFIDENTIEL UE/EU CONFIDENTIAL» ou au-delà.

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 aux autorités nationales compétentes le niveau de classification des informations que la personne concernée aurait à connaître, de sorte que ces autorités puissent 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 les autorités nationales compétentes 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 les autorités nationales compétentes de l'État membre émettent un avis positif, le secrétaire général peut octroyer l'autorisation à la personne concernée.

12.13. Un avis négatif des autorités nationales compétentes 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 aux autorités nationales compétentes 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 les autorités nationales compétentes et en l'absence de réaction de celles-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 comme «TRÈS SECRET UE/EU TOP SECRET».