COM(2022) 119 final

ASSEMBLÉE NATIONALE

QUINZIÈME LÉGISLATURE

SÉNAT

SESSION ORDINAIRE DE 2021/2022

Reçu à la Présidence de l'Assemblée nationale
le 30 mars 2022

Enregistré à la Présidence du Sénat
le 30 mars 2022

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT

Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à la sécurité de l'information dans les institutions, organes et organismes de l'Union

E 16609

Conseil de
l'Union européenne

Bruxelles, le 28 mars 2022
(OR. en)

7670/22

Dossier interinstitutionnel:
2022/0084(COD)

CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34

PROPOSITION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	22 mars 2022
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	COM(2022) 119 final
Objet:	Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à la sécurité de l'information dans les institutions, organes et organismes de l'Union

Les délégations trouveront ci-joint le document COM(2022) 119 final.

p.j.: COM(2022) 119 final

COMMISSION
EUROPÉENNE

Bruxelles, le 22.3.2022
COM(2022) 119 final

2022/0084 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

relatif à la sécurité de l'information dans les institutions, organes et organismes de l'Union

{SWD(2022) 65 final} - {SWD(2022) 66 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

La présente proposition fait partie de la stratégie de l'UE pour l'union de la sécurité[1] adoptée par la Commission le 24 juillet 2020 et énonçant l'engagement pris par cette dernière d'apporter la valeur ajoutée de l'Union européenne aux efforts nationaux dans le domaine de la sécurité. Cet engagement inclut notamment l'initiative visant à rationaliser les cadres juridiques internes relatifs à la sécurité de l'information dans l'ensemble des institutions et organes de l'Union.

L'un des grands objectifs du programme stratégique pour 2019-2024 adopté par le Conseil européen en juin 2019 est la protection de nos sociétés contre les menaces en perpétuelle évolution visant les informations traitées par les institutions et les organes. Dans ses conclusions[2], le Conseil européen a notamment invité «les institutions de l'UE, ainsi que les États membres, à œuvrer à des mesures visant à renforcer la résilience et à améliorer la culture de sécurité de l'UE face aux menaces cyber et hybrides émanant de l'extérieur de l'UE, et à mieux protéger les réseaux d'information et de communication de l'UE, ainsi que ses processus décisionnels, contre les actes de malveillance de tout type».

Dans le même ordre d'idées, le Conseil des affaires générales de décembre 2019[3] a conclu que les institutions et organes de l'UE, soutenus par les États membres, devraient élaborer et mettre en œuvre un ensemble complet de mesures visant à garantir leur sécurité. Cette conclusion fait écho à une demande formulée depuis longtemps par le comité de sécurité du Conseil visant à étudier l'adoption d'un socle commun de règles de sécurité pour le Conseil, la Commission et le Service européen pour l'action extérieure[4].

Actuellement, soit les institutions et organes de l'Union possèdent leurs propres règles en matière de sécurité de l'information, fondées sur leur règlement de procédure ou leur acte fondateur, soit ils ne disposent d'aucune règle en la matière. C'est surtout le cas de certaines petites entités, qui ne possèdent aucune politique officielle en matière de sécurité de l'information.

En raison des volumes toujours plus conséquents d'informations sensibles non classifiées et d'informations classifiées de l'Union européenne (ci-après les «ICUE») que les institutions et organes de l'Union doivent se partager, et compte tenu de l'évolution spectaculaire des menaces, l'administration européenne est exposée à des attaques dans tous ses domaines d'activité. Les informations traitées par nos institutions et organes intéressent au plus haut point les acteurs malveillants, et elles doivent être correctement protégées, ce qui nécessite une action rapide afin d'améliorer leur protection.

Dès lors, et afin d'accroître la protection des informations traitées par l'administration européenne, la présente initiative vise à rationaliser les différents cadres juridiques des institutions et organes de l'Union dans ce domaine, grâce aux mesures suivantes:

- définir des catégories d'informations exhaustives et harmonisées, ainsi que des règles communes à toutes les institutions et tous les organes de l'Union en matière de traitement;

---

1 Communication relative à la stratégie de l'UE pour l'union de la sécurité, COM(2020) 605, 24 juillet 2020 (priorité stratégique «Un environnement de sécurité à l'épreuve du temps»).

2 EUCO 9/19.

3 14972/19.

4 WK 10563/2018 INIT section 9.

- établir un système rationalisé de coopération entre les institutions et organes de l'Union dans le domaine de la sécurité de l'information, capable de favoriser une culture cohérente de la sécurité de l'information dans l'ensemble de l'administration européenne;
- moderniser les politiques en matière de sécurité de l'information à tous les niveaux de classification/de catégorisation, pour l'ensemble des institutions et organes de l'Union, en tenant compte de la transformation numérique et du développement du télétravail en tant que pratique structurelle.

- **Cohérence avec les dispositions existantes dans le domaine d'action**

La présente initiative s'inscrit dans un vaste ensemble de politiques de l'Union dans le domaine de la sécurité et de la sécurité de l'information.

En 2016, le Parlement européen et le Conseil ont adopté une directive[5] concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. Cette directive constituait la première mesure législative adoptée au niveau de l'Union afin d'améliorer la coopération entre les États membres en matière de cybersécurité. Si la Commission a adopté, en décembre 2020, une proposition en vue de procéder à une révision de cet instrument, en introduisant des mesures de surveillance destinées aux autorités nationales, l'administration de l'Union ne relève toujours pas de son champ d'application.

Dans le même ordre d'idées, et afin de compléter les efforts des États membres dans le domaine de la sécurité, il est capital que les institutions et organes de l'Union assurent un niveau élevé de protection de leurs informations et des systèmes d'information et de communication s'y rapportant, afin de garantir la sécurité de l'information.

En juillet 2020, la Commission a adopté la stratégie pour l'union de la sécurité[6], incluant un engagement global, de la part des États membres, de compléter les efforts des États membres dans tous les domaines relatifs à la sécurité. Cette stratégie porte sur la période 2020-2025 et comporte quatre grands piliers d'action: un environnement de sécurité à l'épreuve du temps, faire face à l'évolution des menaces, protéger l'Europe contre le terrorisme et la criminalité organisée, et un solide écosystème européen de la sécurité. Plusieurs des thèmes abordés dans le cadre de ces piliers sont axés sur la sécurité de l'information, la cybersécurité, la coopération et l'échange d'informations et les infrastructures critiques.

Conformément à la stratégie pour l'union de la sécurité, la Commission européenne propose la création d'un ensemble minimal de règles en matière de sécurité de l'information destinées à l'ensemble des institutions et organes de l'Union, qui entraînera l'établissement de normes communes élevées et obligatoires en vue de l'échange sécurisé d'informations. Cette initiative représente l'engagement des institutions et organes d'établir au sein de l'administration européenne le même niveau d'ambition dans le domaine de la sécurité que celui exigé des États membres.

Le 16 décembre 2020, la Commission et le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité ont présenté une nouvelle stratégie de cybersécurité de l'UE[7]. Cette stratégie définit des priorités et des actions clés visant à accroître la résilience,

---

5 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

6 C(2020)605.

7 Stratégie de cybersécurité de l'UE pour la décennie numérique | «Façonner l'avenir numérique de l'Europe» (europa.eu), qui inclut une communication conjointe avec le haut représentant de l'Union

l'autonomie, le rôle de chef de file et les capacités opérationnelles de l'Europe face aux menaces complexes et croissantes auxquelles font face ses réseaux et ses systèmes d'information, ainsi qu'à promouvoir un cyberespace ouvert et mondial et les partenariats internationaux noués dans ce cyberespace. Il est tout aussi important que les institutions et organes de l'Union contribuent à la réalisation de ces priorités en définissant des exigences équivalentes tant dans le domaine de la sécurité de l'information que dans le domaine de la cybersécurité.

Cette proposition, associée à la proposition de règlement établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union, vise à compléter le cadre réglementaire de la stratégie pour l'union de la sécurité par des exigences spécifiquement destinées à l'administration européenne. Compte tenu des interconnexions qui existent entre la sécurité de l'information et la cybersécurité, il y a lieu de garantir une approche cohérente de la protection des informations non classifiées entre ces deux propositions.

- **Cohérence avec les autres politiques de l'Union**

La présente initiative tient également compte des autres politiques de l'Union pertinentes pour la sécurité de l'information.

Dans le domaine de la protection des données, l'instrument concerné, applicable à l'administration de l'Union européenne et de la Communauté européenne de l'énergie atomique («Euratom), est le règlement (UE) 2018/1725 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données[8]. De la même manière, il y a lieu d'indiquer que, pour certaines institutions et certains organes de l'Union, les législateurs de l'Union ont adopté des règles pertinentes spécifiques pour la protection des données à caractère personnel.

Dans le domaine de la transparence, la présente proposition s'appuie sur les principes consacrés dans le règlement (CE) nº 1049/2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission[9] en ce qui concerne d'autres règles pertinentes.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

- **Base juridique**

Eu égard à l'objectif et au contenu de la présente proposition, sa base juridique la plus appropriée est l'article 298 du traité sur le fonctionnement de l'Union européenne (TFUE) et l'article 106 *bis* du traité instituant la Communauté européenne de l'énergie atomique.

L'article 298 du TFUE a été introduit par le traité de Lisbonne et permet aux législateurs d'établir des dispositions afin de créer une administration efficace et indépendante qui soutiendra les institutions, organes et organismes dans l'exercice de leur mission.

---

pour les affaires étrangères et la politique de sécurité [JOIN(2020)18] ainsi qu'une directive révisée sur la sécurité des réseaux et de l'information (SRI) [COM(2020)823].

8 Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

9 Règlement (CE) nº 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (JO L 145 du 31.5.2001, p. 43).

Une administration efficace et indépendante a besoin que la sécurité de ses informations soit garantie. Pour mener à bien leur mission, les institutions et organes de l'Union doivent disposer d'un environnement sûr pour les informations qu'ils traitent et stockent au quotidien. En outre, fournir un ensemble de normes de base communes obligatoires pour tous garantirait un niveau de sécurité élevé, réduirait le risque de maillons faibles dans le soutien de l'interopérabilité entre les institutions et organes et permettrait de tirer profit de synergies, ce qui améliorerait ainsi la résilience de l'administration face aux menaces en évolution.

Par ailleurs, dans le but général de parvenir à un niveau élevé commun de sécurité pour les ICUE et les informations non classifiées traitées et stockées par les institutions et organes de l'Union, la présente proposition permet à l'administration européenne de mieux se protéger contre les ingérences externes et les activités d'espionnage.

L'article 298 du TFUE permet à l'Union d'établir des règles communes à l'ensemble de l'administration européenne afin de faire en sorte que l'ensemble des institutions et organes de l'Union traitent de manière similaire les ICUE et les informations non classifiées. Le règlement établit par conséquent des règles applicables à l'administration et ne peut imposer indirectement des obligations qu'aux personnes qui exécutent des tâches au nom de cette administration ou sur une base contractuelle (à l'exception des commissaires, des représentants des États membres agissant au sein du Conseil, des députés du Parlement européen, des juges des tribunaux de l'Union et des membres de la Cour des comptes européenne).

Conformément à l'article 298 du TFUE, le Parlement européen et le Conseil statuent par voie de règlements conformément à la procédure législative ordinaire.

La présente proposition nécessite une base juridique supplémentaire, étant donné qu'elle couvre également les informations relatives à certaines activités de la Communauté européenne de l'énergie atomique. Ces informations ne sont pas des informations classifiées d'Euratom, mais elles sont traitées par les institutions et organes de l'Union sous le régime général des ICUE.

Cette base juridique supplémentaire est l'article 106 *bis* du traité instituant la Communauté européenne de l'énergie atomique, qui rend l'article 298 du TFUE également applicable aux activités d'Euratom susmentionnées.

- **Subsidiarité (en cas de compétence non exclusive)**

Conformément au principe de subsidiarité énoncé à l'article 5, paragraphe 3, du traité sur l'Union européenne, une action au niveau de l'Union ne devrait être entreprise que si les objectifs envisagés ne peuvent pas être réalisés de manière suffisante par les États membres, mais peuvent l'être mieux, en raison des dimensions ou des effets de l'action envisagée, au niveau de l'Union.

Étant donné que seule l'Union peut adopter des règles régissant les ICUE et les informations sensibles non classifiées traitées et stockées par les institutions et organes de l'Union, le principe de subsidiarité ne s'applique pas.

- **Proportionnalité**

L'établissement d'une base de référence commune à l'ensemble des institutions et organes de l'Union en matière de sécurité de l'information est nécessaire pour favoriser une administration indépendante et efficace.

Conformément au principe de proportionnalité énoncé à l'article 5, paragraphe 4, du TUE, les dispositions du règlement ne sont pas excessivement normatives et laissent une marge pour la

définition de différents niveaux d'action spécifique, en fonction du degré de maturité en matière de sécurité de chaque institution ou organe de l'Union.

En outre, la solution a une incidence limitée sur les droits fondamentaux des individus. Partant, la proposition n'excède pas ce qui est nécessaire pour répondre au problème de l'absence de socle de règles commun à l'ensemble des institutions et organes de l'Union en matière de sécurité de l'information.

- **Choix de l'instrument**

Un règlement fondé sur l'article 298 du TFUE est considéré comme l'instrument juridique approprié.

Le choix du règlement en tant qu'instrument juridique se justifie par la prédominance d'éléments qui requièrent une application uniforme ne laissant aucune marge de mise en œuvre aux institutions et organes de l'Union et créant un cadre entièrement horizontal.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

- **Évaluations ex post/bilans de qualité de la législation existante**

Sans objet

- **Consultation des parties intéressées**

La Commission a mené une vaste consultation des principales parties intéressées sur différents aspects ayant trait aux règles des institutions et organes de l'Union en matière de sécurité de l'information. Le but général de ces activités de consultation était de recueillir des contributions pertinentes pour la préparation d'une initiative législative relative à des règles communes à l'ensemble des institutions et organes de l'Union en matière de sécurité de l'information. Les consultations ont visé à recueillir des contributions sur:

- les problèmes liés à l'actuel cadre de sécurité de l'information au sein des institutions et organes de l'Union qui devraient, selon les parties intéressées, être abordés dans l'initiative;
- la pertinence, l'efficacité, l'efficience et la valeur ajoutée de l'initiative;
- les incidences attendues de l'initiative, ainsi que ses éventuelles autres conséquences pour les parties intéressées.

En préparation de la présente proposition législative, la Commission a consulté les catégories suivantes de parties intéressées:

1. institutions, organes et organismes de l'Union;
2. autorités nationales de sécurité des États membres;
3. experts chercheurs du CCR.

Compte tenu de la spécificité de la présente initiative, qui s'applique exclusivement aux institutions et organes de l'Union, en n'ayant que très peu d'incidences sur les citoyens et entreprises européens, les services de la Commission ont choisi de recueillir en priorité les points de vue des groupes de parties intéressées concernés. Dès lors, **aucune consultation publique n'a été menée** spécifiquement pour cette initiative législative.

Au cours du processus de consultation, les services de la Commission ont utilisé les **méthodes et formes de consultation** suivantes:

1. la possibilité pour toutes les parties intéressées de fournir un retour d'informations sur l'analyse d'impact initiale en utilisant la plateforme «Donnez votre avis» de la Commission;
2. un questionnaire ciblé adressé aux experts des institutions et organes de l'Union en matière de sécurité des informations au moyen d'une enquête en ligne de l'UE;
3. un questionnaire ciblé adressé aux autorités nationales de sécurité des États membres au moyen d'une enquête en ligne de l'UE;
4. une demande d'évaluation personnalisée des risques pour les principales ressources de sécurité de l'information, et
5. de nombreuses réunions et de nombreux échanges avec les homologues des institutions, organes et organismes, ainsi qu'avec les autorités nationales de sécurité des États membres.

Parmi les principales contributions fournies dans le cadre des activités de consultation, la Commission attire l'attention sur les suivantes:

- la fragmentation des cadres juridiques applicables de nos institutions et organes engendre une duplication significative des efforts visant à créer et à maintenir des règles internes, ainsi qu'une non-interopérabilité des pratiques de traitement des informations. Pour les États membres, la diversité de ces règles exacerbe les risques d'incompréhensions, de mauvaises interprétations et de non-conformités;
- l'établissement d'une base de référence en matière de sécurité de l'information commune à l'ensemble des institutions et organes de l'Union créerait un écosystème de règles de sécurité standardisées et de bonnes pratiques mises en œuvre; il convient toutefois de tenir compte de la diversité et des différents environnements opérationnels de chaque institution ou organe de l'Union, et l'adoption de solutions locales devrait être autorisée;
- la présente initiative doit respecter l'autonomie et les différents niveaux de maturité, en matière de sécurité, des institutions et organes de l'Union, qui resteront entièrement responsables de l'organisation de la sécurité de l'information;
- **Obtention et utilisation d'expertise**

La Commission a utilisé ses propres ressources pour procéder à la consultation des parties intéressées. La direction «Sécurité» de la DG HR a effectué le travail connexe relatif aux enquêtes, aux vidéoconférences et autres ateliers. Cette tâche a supposé à la fois la sélection de participants et l'organisation d'événements ainsi que le traitement des contributions reçues.

Le Centre commun de recherche (JRC) a réalisé une évaluation des risques pour les principales ressources de sécurité de l'information; cette évaluation a servi de base à l'analyse d'impact.

- **Analyse d'impact**

La présente initiative s'adresse exclusivement aux institutions et organes de l'Union et a peu d'incidences sur les États membres et leurs citoyens. Il n'a donc pas été nécessaire de procéder à une analyse d'impact approfondie, étant donné qu'il n'y avait aucune incidence significative ou clairement détectable sur les citoyens et les entreprises. Une feuille de route exhaustive a été publiée sur le site web Europa; celle-ci regroupait les retours d'informations fournis par les parties prenantes concernées.

- **Réglementation affûtée et simplification**

Sans objet

- **Droits fondamentaux**

L'Union européenne a la volonté de respecter des normes élevées de protection des droits fondamentaux. La présente initiative garantit le plein respect des droits fondamentaux tels que consacrés dans la Charte des droits fondamentaux de l'Union européenne[10], à savoir:

- le droit à une bonne administration[11]

En améliorant la sécurité des informations qu'ils traitent dans le cadre de la gestion des affaires des citoyens européens, les institutions et organes de l'Union contribuent à la réalisation du principe de bonne administration;

- la protection des données à caractère personnel[12]

Toutes les opérations de traitement de données à caractère personnel réalisées dans le cadre de la présente proposition seraient effectuées dans des environnements de confiance et dans le plein respect du règlement (UE) 2018/1725 du Parlement européen et du Conseil;

- le droit d'accès aux documents[13]

L'accès du public aux ICUE et aux documents sensibles non classifiés demeure entièrement régi par le règlement (CE) nº 1049/2001 du Parlement européen et du Conseil;

- le droit de propriété intellectuelle[14]

Lors du traitement et du stockage d'informations non classifiées et d'ICUE, les institutions et organes de l'Union protègent la propriété intellectuelle conformément à la directive 2001/29/CE du Parlement européen et du Conseil[15];

- la liberté d'expression et d'information[16]

Si toute personne dispose de la liberté de recevoir et de partager des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques, cela n'empêche pas l'Union d'établir les conditions d'accès, de traitement et de stockage de certains types d'informations, en fonction de leur niveau de confidentialité.

L'exercice de ces libertés peut être soumis à des conditions et restrictions prévues par la loi et nécessaires dans une société démocratique, afin d'empêcher la divulgation d'informations confidentielles dans l'intérêt de la sécurité de l'Union.

4. INCIDENCE BUDGÉTAIRE

La présente proposition nécessite l'affectation d'un fonctionnaire AD et d'un assistant AST au secrétariat permanent du groupe de coordination assuré par la Commission, au sein de la direction de la sécurité de la direction générale des ressources humaines et de la sécurité.

---

10 Charte des droits fondamentaux de l'Union européenne (JO C 326 du 26.10.2012, p. 391).

11 Article 41 de la Charte des droits fondamentaux de l'Union européenne.

12 Article 8 de la Charte des droits fondamentaux de l'Union européenne.

13 Article 42 de la Charte des droits fondamentaux de l'Union européenne.

14 Article 17 de la Charte des droits fondamentaux de l'Union européenne.

15 Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société d'information (JO L 167 du 22.6.2001, p. 10).

16 Article 11 de la Charte des droits fondamentaux de l'Union européenne.

Les institutions et organes devraient réaliser des économies de coûts grâce aux tâches partagées et collaboratives, ainsi qu'en évitant d'éventuels préjudices économiques découlant d'incidents de sécurité grâce aux améliorations de la sécurité de l'information. Par ailleurs, les efforts financiers nécessaires à la mise en œuvre de la nouvelle législation peuvent être couverts dans le cadre des programmes d'amélioration de la sécurité de l'information existant dans chaque institution ou chaque organe de l'Union.

5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

La proposition prévoit l'obligation pour la Commission de rendre compte tous les trois ans au Parlement européen et au Conseil sur la mise en œuvre du règlement, y compris sur le fonctionnement de la gouvernance établie par ce dernier.

En outre, tous les cinq ans, la Commission procède à l'évaluation du règlement afin d'apprécier sa performance réelle et, sur cette base, de déterminer si une quelconque modification de la législation est nécessaire.

- **Explication détaillée de certaines dispositions de la proposition**

La proposition s'articule autour des exigences à respecter en ce qui concerne le traitement et le stockage des informations non classifiées et des ICUE, qui constituent l'objet principal de l'initiative et dont la protection renforcée représente la finalité sous-tendant l'initiative.

Objet et champ d'application (article 1er et article 2)

Le règlement est destiné à créer un ensemble minimal de règles en matière de sécurité de l'information applicables à l'ensemble des institutions et organes de l'Union.

Il s'applique à toutes les informations traitées et stockées par les institutions et organes de l'Union, y compris celles relatives aux activités de la Communauté européenne de l'énergie atomique, autres que les informations classifiées d'Euratom. Le règlement couvre à la fois les informations non classifiées et les ICUE.

Définitions et principes généraux (articles 3 à 5)

Les définitions fournies à l'article 3 sont fondées sur les règles en vigueur en matière de sécurité de l'information adoptées séparément par les institutions et organes de l'Union.

Outre les principes généraux de la législation de l'Union, à savoir la transparence, la proportionnalité, l'efficacité et la responsabilité, le règlement établit les principales lignes directrices contraignantes à observer, telles que la mise en œuvre par chaque institution ou organe de l'Union d'un processus séparé de gestion des risques liés à la sécurité de l'information et l'évaluation de leurs informations en vue de les catégoriser correctement.

Gouvernance et organisation de la sécurité (articles 6 à 8)

L'ensemble des institutions et organes de l'Union coopèrent au sein d'un groupe interinstitutionnel de coordination pour la sécurité de l'information, qui agit par consensus et dans l'intérêt commun des institutions et organes de l'Union.

Le groupe de coordination rassemble les autorités de sécurité de l'ensemble des institutions et organes et élabore des documents d'orientation sur la mise en œuvre du règlement. Il échange régulièrement avec les autorités nationales de sécurité des États membres, rassemblées au sein d'un comité de sécurité de l'information.

Cinq sous-groupes composés d'experts représentant différentes institutions et différents organes sont créés en vue de rationaliser les procédures et les autres aspects pratiques liés à la sécurité de l'information.

Chaque institution ou organe de l'Union est tenu de désigner une autorité de sécurité, responsable de la définition et de la mise en œuvre des politiques internes en matière de sécurité de l'information. L'autorité de sécurité établit des fonctions spécifiques, telles que l'autorité chargée de l'assurance de l'information, l'autorité opérationnelle chargée de l'assurance de l'information, l'autorité d'homologation de sécurité, l'autorité TEMPEST, l'autorité d'agrément cryptographique et l'autorité de distribution cryptographique, qui peuvent être déléguées à une autre institution ou un autre organe pour des raisons d'efficience ou de ressources.

Assurance de l'information et systèmes d'information et de communication (articles 9 à 11)

Le règlement établit un sous-groupe sur l'assurance de l'information ayant pour objectif d'améliorer la cohérence dans l'ensemble des institutions et organes de l'Union entre les règles relatives à la sécurité de l'information et la base de référence en cybersécurité définie par le règlement établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union.

Les institutions et organes de l'Union sont tenus de respecter les principes mentionnés dans ces articles et d'adopter des règles internes séparées pour certaines mesures de sécurité, adaptées à leur propre environnement de sécurité.

Informations non classifiées (articles 12 à 17 et annexe I)

Le règlement prévoit trois catégories d'informations non classifiées: les informations destinées à un usage public, les informations ordinaires et les informations sensibles non classifiées. Toutes les catégories sont définies, tandis que des marquages et des conditions de traitement sont établis afin de protéger ces informations.

Afin de coordonner les travaux sur les équivalences entre les catégories spécifiques établies par certaines institutions et certains organes de l'Union et les catégories communes prévues dans le règlement, la proposition établit un sous-groupe sur les informations non classifiées.

ICUE (articles 18 à 58 et annexes II à VI)

Ce chapitre, le plus volumineux de la proposition, est divisé en sept sections: dispositions générales, sécurité du personnel, sécurité physique, gestion des ICUE, protection dans les systèmes d'information et de communication, sécurité industrielle et partage d'ICUE et échange d'informations classifiées.

La section relative aux dispositions générales prévoit quatre niveaux d'ICUE: TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL et RESTREINT UE/EU RESTRICTED. Elle prévoit également l'obligation pour les institutions et organes de l'Union de prendre les mesures de sécurité nécessaires en fonction des résultats d'un processus de gestion des risques liés à la sécurité de l'information.

Les sections restantes sont toutes axées sur les normes de protection des ICUE, en fonction de l'aspect spécifique considéré. Les modalités de cette protection des ICUE sont précisées dans les annexes II à V. L'annexe VI fournit le tableau d'équivalence entre les ICUE et les classifications de sécurité des États membres et de la Communauté européenne de l'énergie atomique.

Afin de rationaliser les processus pertinents dans ce domaine et d'éviter la duplication des efforts, le règlement établit des sous-groupes sur l'assurance de l'information, sur les informations non classifiées, sur la sécurité physique, sur l'homologation des systèmes d'information et de communication traitant et stockant des ICUE ainsi que sur le partage d'ICUE et l'échange d'informations classifiées.

Dispositions finales (articles 59 à 62)

Les dispositions finales assurent la transition entre les règles et procédures actuelles et le nouveau cadre juridique établi par le règlement. Elles concernent les règles internes en matière de sécurité de l'information actuellement applicables dans les institutions et organes de l'Union, la reconnaissance des visites d'évaluation effectuées avant l'entrée en application du règlement, le traitement des arrangements administratifs précédemment conclus et le maintien des cadres de sécurité spécifiques applicables aux conventions de subvention.

Le règlement doit entrer en application deux ans après sa date d'entrée en vigueur.

2022/0084 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

relatif à la sécurité de l'information dans les institutions, organes et organismes de l'Union

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 298,

vu le traité instituant la Communauté européenne de l'énergie atomique, et notamment son article 106 *bis*,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) Actuellement, les institutions et organes de l'Union possèdent leurs propres règles en matière de sécurité de l'information, fondées sur leur règlement de procédure ou leur acte fondateur, ou ne disposent d'aucune règle en la matière. Dans ce contexte, chaque institution ou organe de l'Union consacre des efforts conséquents à l'adoption d'approches différentes, ce qui donne lieu à une situation dans laquelle les échanges d'informations ne sont pas toujours fiables. L'absence d'approche commune entrave le déploiement d'outils communs fondés sur un ensemble concerté de règles tenant compte des besoins de sécurité des informations à protéger.

(2) Bien que des progrès aient été réalisés en vue d'une plus grande cohérence des règles relatives à la protection des informations classifiées de l'Union européenne («ICUE») et des informations non classifiées, l'interopérabilité des systèmes concernés reste limitée, ce qui empêche un transfert fluide des informations entre les institutions et organes de l'Union. Il convient dès lors d'entreprendre des efforts supplémentaires afin de permettre la mise en œuvre d'une approche interinstitutionnelle du partage d'ICUE et d'informations sensibles non classifiées, incluant des catégories communes d'informations et des principes clés communs pour leur traitement. Une base de référence devrait également être envisagée afin de simplifier les procédures de partage d'ICUE et d'informations sensibles non classifiées entre les institutions et organes de l'Union et avec les États membres.

(3) Il convient par conséquent d'établir des règles pertinentes assurant un niveau commun de sécurité de l'information dans l'ensemble des institutions et organes de l'Union. Ces règles devraient constituer un cadre général exhaustif et cohérent pour la protection des ICUE et des informations non classifiées, et devraient assurer une équivalence des principes de base et des normes minimales.

(4) La récente pandémie a modifié de manière significative les pratiques de travail, les outils de communication à distance devenant la règle. En conséquence, de nombreuses procédures qui étaient encore au moins partiellement exécutées sur papier ont été

rapidement adaptées afin de permettre le traitement et les échanges électroniques d'informations. Ces évolutions rendent nécessaires des modifications du traitement et de la protection des informations. Le présent règlement tient compte des nouvelles pratiques de travail.

(5) En créant un niveau minimal commun de protection pour les ICUE et les informations non classifiées, le présent règlement contribue à garantir que les institutions et organes de l'Union disposent du soutien d'une administration efficace et indépendante dans l'exercice de leurs missions. Parallèlement, chaque institution ou organe de l'Union conserve son autonomie pour déterminer les modalités de mise en œuvre des règles énoncées dans le présent règlement, en fonction de ses propres besoins de sécurité. Le présent règlement n'empêche en aucun cas les institutions et organes de l'Union de remplir la mission qui leur est confiée par la législation de l'Union, ni ne porte atteinte à leur autonomie institutionnelle.

(6) Le présent règlement est sans préjudice du règlement (Euratom) nº 3/1958[17], du règlement nº 31 (C.E.E), 11 (C.E.E.A.) fixant le statut des fonctionnaires et le régime applicable aux autres agents de la Communauté économique européenne et de la Communauté européenne de l'énergie atomique[18], du règlement (CE) nº 1049/2001 du Parlement européen et du Conseil[19], du règlement (UE) 2018/1725 du Parlement européen et du Conseil[20], du règlement (CEE, Euratom) nº 354/83 du Conseil[21], du règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil[22], du règlement (UE) 2021/697 du Parlement européen et du Conseil[23] et du règlement (UE) […] du Parlement européen et du Conseil établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union[24].

(7) Afin de préserver les spécificités des activités de la Communauté européenne de l'énergie atomique régies par le règlement nº 3/1958 du Conseil de la Communauté européenne de l'énergie atomique[25], le présent règlement ne devrait pas s'appliquer

---

17 Règlement (Euratom) nº 3/1958 portant application de l'article 24 du traité instituant la Communauté européenne de l'énergie atomique (JO 17 du 6.10.1958, p. 406).

18 JO L 45 du 14.6.1962, p. 1385.

19 Règlement (CE) nº 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (JO L 145 du 31.5.2001, p. 43).

20 Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

21 Règlement (CEE, Euratom) nº 354/83 du Conseil du 1er février 1983 concernant l'ouverture au public des archives historiques de la Communauté économique européenne et de la Communauté européenne de l'énergie atomique (JO L 43 du 15.2.1983, p. 1).

22 Règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil du 18 juillet 2018 relatif aux règles financières applicables au budget général de l'Union, modifiant les règlements (UE) nº 1296/2013, (UE) nº 1301/2013, (UE) nº 1303/2013, (UE) nº 1304/2013, (UE) nº 1309/2013, (UE) nº 1316/2013, (UE) nº 223/2014, (UE) nº 283/2014 et la décision nº 541/2014/UE, et abrogeant le règlement (UE, Euratom) nº 966/2012 (JO L 193 du 30.7.2018, p. 1).

23 Règlement (UE) 2021/697 du Parlement européen et du Conseil du 29 avril 2021 établissant le Fonds européen de la défense et abrogeant le règlement (UE) 2018/1092 (JO L 170 du 12.5.2021, p. 149).

24 Règlement […] du Parlement européen et du Conseil établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union, à adopter.

25 CEEA Conseil: règlement nº 3 portant application de l'article 24 du traité instituant la Communauté européenne de l'énergie atomique (JO 17 du 6.10.1958, p. 406).

aux informations classifiées d'Euratom. Toutefois, l'ensemble des informations relatives aux autres activités d'Euratom non couvertes par le règlement nº 3/1958 devraient relever du champ d'application du présent règlement.

(8) Afin d'établir une structure formelle de coopération entre les institutions et organes de l'Union dans le domaine de la sécurité de l'information, il est nécessaire de créer un groupe interinstitutionnel de coordination (ci-après le «groupe de coordination») dans lequel seront représentées les autorités de sécurité de l'ensemble des institutions et organes de l'Union. Sans disposer de pouvoirs décisionnels, le groupe de coordination devrait améliorer la cohérence des politiques dans le domaine de la sécurité de l'information et devrait contribuer à l'harmonisation des procédures et outils de sécurité de l'information dans l'ensemble des institutions et organes de l'Union.

(9) Les travaux du groupe de coordination doivent être soutenus par des experts de différents domaines de la sécurité de l'information: catégorisation et marquage, systèmes d'information et de communication, homologation, sécurité physique, partage d'ICUE et échange d'informations classifiées. Afin d'éviter la duplication des efforts entre les institutions et organes de l'Union, des sous-groupes thématiques devraient être créés. En outre, au besoin, le groupe de coordination devrait être en mesure de créer d'autres sous-groupes chargés de tâches spécifiques.

(10) Le groupe de coordination devrait coopérer étroitement avec les autorités nationales de sécurité des États membres afin d'améliorer la sécurité de l'information dans l'Union. Un comité de sécurité de l'information des États membres devrait dès lors être créé afin de fournir des conseils au groupe de coordination.

(11) Si les organes communs représentant l'ensemble des institutions et organes de l'Union sont créés conformément au principe de coopération, chaque institution ou organe devrait conserver l'entière responsabilité de la sécurité de l'information au sein de son organisation. Chaque institution ou organe de l'Union devrait disposer d'une autorité de sécurité et, le cas échéant, d'autres autorités investies de responsabilités spécifiques en matière de sécurité de l'information.

(12) Le principe de gestion des risques liés à la sécurité de l'information devrait être au cœur de la politique à élaborer par chaque institution ou organe de l'Union dans ce domaine. Si les exigences minimales établies dans le présent règlement doivent être remplies, chaque institution ou organe de l'Union devrait adopter des mesures de sécurité spécifiques pour la protection des informations en fonction des résultats d'une évaluation interne des risques. De la même manière, les moyens techniques mis en œuvre pour protéger les informations devraient être adaptés à la situation spécifique de chaque institution ou organe.

(13) Compte tenu de la diversité des catégories d'informations non classifiées que les institutions et organes de l'Union ont définies sur la base de leurs propres règles en matière de sécurité de l'information et afin d'éviter des retards dans la mise en œuvre du présent règlement, les institutions et organes de l'Union devraient pouvoir conserver leur propre système de marquage pour leurs besoins internes ou pour échanger des informations avec leurs homologues spécifiques d'autres institutions et organes ou des États membres.

(14) Afin de s'adapter aux nouvelles pratiques de télétravail, les réseaux utilisés pour se connecter aux services d'accès à distance des institutions et organes de l'Union devraient être protégés par des mesures de sécurité adéquates.

(15) Les institutions et organes de l'Union ayant fréquemment recours à des contractants et à l'externalisation, il est important d'établir des dispositions communes pour le personnel des contractants exécutant des tâches en rapport avec la sécurité de l'information.

(16) Les règles matérielles figurant dans les règlements intérieurs de différentes institutions et différents organes de l'Union concernant l'accès aux ICUE sont actuellement alignées, mais elles présentent des différences significatives en ce qui concerne les dénominations et les procédures exigées. Cela crée une charge pour les autorités nationales de sécurité des États membres, qui doivent s'adapter aux différentes exigences. Il est donc nécessaire de prévoir un glossaire commun et des procédures communes dans le domaine de la sécurité du personnel, ce qui simplifiera la coopération avec les autorités nationales de sécurité des États membres et limitera le risque de compromission d'ICUE.

(17) Compte tenu de la disparité des ressources entre les institutions et organes de l'Union, et afin de rationaliser leurs procédures et pratiques pertinentes, les tâches d'habilitation de sécurité peuvent être confiées à la Commission afin d'assurer la continuité d'une pratique ancienne dans le domaine des habilitations de sécurité et de contribuer à la centralisation des tâches assignées à chaque autorité de sécurité.

(18) La protection des ICUE est également assurée par des mesures techniques et organisationnelles applicables aux locaux, aux bâtiments, aux salles, aux bureaux ou aux établissements des institutions et organes de l'Union dans lesquels des ICUE sont discutées, traitées ou stockées. Le présent règlement prévoit la mise en œuvre d'un processus de gestion de la sécurité de l'information dans le domaine de la sécurité physique qui permettrait aux institutions et organes de l'Union de sélectionner les mesures de sécurité appropriées pour leurs sites.

(19) L'ensemble des institutions et organes de l'Union qui traitent et stockent des ICUE devraient créer des zones physiquement protégées sur leurs sites, afin de garantir le même niveau de protection pour les catégories pertinentes d'ICUE qui y sont traitées et stockées. Ces zones devraient être désignées comme zones administratives et zones sécurisées et respecter des normes minimales communes pour la protection des ICUE.

(20) Le contrôle de l'autorité d'origine est un principe important de la gestion des ICUE; il doit donc être clairement énoncé et mis en œuvre. À cet égard, la création d'ICUE confère à l'autorité d'origine une responsabilité qui devrait couvrir l'ensemble du cycle de vie du document ICUE concerné.

(21) Les institutions et organes de l'Union ont toujours élaboré leurs systèmes d'information et de communication de manière autonome, sans accorder une attention suffisante à l'interopérabilité de ces systèmes dans l'ensemble des institutions et organes de l'Union. Il est donc nécessaire de définir des exigences minimales de sécurité concernant les systèmes d'information et de communication (SIC) traitant et stockant à la fois des ICUE et des informations non classifiées dans le but de garantir un échange fluide d'informations avec les parties prenantes concernées.

(22) Afin de parvenir à une norme unique pour l'homologation des SIC qui traitent et stockent des ICUE, les institutions et organes de l'Union devraient travailler ensemble au sein d'un groupe créé à cet effet. Il est recommandé que l'ensemble des institutions et organes utilisent cette norme afin de contribuer à un niveau général de protection des ICUE. Toutefois, en ce qui concerne l'autonomie organisationnelle, la décision reste du ressort de l'autorité compétente de chaque institution ou organe.

(23) L'ensemble des institutions et organes de l'Union devraient suivre les mêmes procédures et appliquer les mêmes mesures au moment d'octroyer et d'exécuter des contrats classifiés ou des conventions de subvention classifiées. Il est donc nécessaire de préciser clairement à la fois les éléments obligatoires et les éléments facultatifs des contrats classifiés ou des conventions de subvention classifiées. Toutefois, les mesures adoptées pour la protection des ICUE dans le cadre des contrats classifiés ou des conventions de subvention classifiées devraient tenir compte des règles déjà élaborées séparément dans ce domaine par les institutions et organes de l'Union en collaboration avec les États membres.

(24) La coopération étroite entre les institutions et organes de l'Union, ainsi que la multitude de synergies créées entre eux, suppose le partage d'une grande quantité d'informations. Dans l'intérêt de la sécurité des informations classifiées, il y a lieu d'évaluer la fiabilité d'une institution ou d'un organe de l'Union avant que cette institution ou cet organe traite et stocke un niveau donné d'ICUE.

(25) En outre, le partage d'ICUE entre les institutions et organes de l'Union et l'échange d'informations classifiées avec des organisations internationales et des pays tiers devraient également être régis par des mesures de sécurité appropriées afin de garantir la protection de ces informations. Lorsque des accords en matière de sécurité de l'information sont envisagés, les dispositions de l'article 218 du traité devraient s'appliquer.

(26) Les accords en matière de sécurité de l'information sont censés établir le cadre juridique global de l'échange d'informations classifiées de l'Union avec les pays tiers et les organisations internationales; il est également nécessaire de prévoir la possibilité pour les institutions et organes de l'Union de conclure des arrangements administratifs avec un homologue donné d'un pays tiers ou d'une organisation internationale aux fins de l'échange d'ICUE.

(27) Le présent règlement établit un cadre commun à l'ensemble des institutions et organes de l'Union. Afin d'éviter d'imposer une charge administrative excessive aux institutions et organes de l'Union au moment d'adapter leurs règles de sécurité internes aux règles établies dans le présent règlement, ce dernier devrait entrer en application dans les deux ans suivant son entrée en vigueur.

(28) Conformément aux points 22 et 23 de l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer»[26], la Commission devrait évaluer le présent règlement afin d'examiner ses effets concrets et la nécessité d'une action supplémentaire. La Commission devrait présenter au Parlement européen et au Conseil un rapport sur la mise en œuvre du présent règlement au plus tard trois ans à partir de sa date d'application.

(29) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42 du règlement (UE) 2018/1725 du Parlement européen et du Conseil[27] et a rendu un avis le […],

---

[26] Accord interinstitutionnel entre le Parlement européen, le Conseil de l'Union européenne et la Commission européenne «Mieux légiférer» (JO L 123 du 12.5.2016, p. 1).

[27] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018).

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Chapitre 1
Dispositions générales

Article premier

Objet

1. Le présent règlement établit des règles en matière de sécurité de l'information destinées à l'ensemble des institutions et organes de l'Union.

Article 2

Champ d'application

1. Le présent règlement s'applique à toutes les informations traitées et stockées par les institutions et organes de l'Union, y compris celles relatives aux activités de la Communauté européenne de l'énergie atomique, autres que les informations classifiées d'Euratom.

2. Il s'applique aux niveaux de confidentialité de l'information suivants:

   a) trois niveaux d'informations non classifiées: usage public, ordinaire et sensible non classifié;

   b) quatre niveaux d'informations classifiées de l'UE: RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET.

3. Ces niveaux sont définis en fonction du préjudice qu'une divulgation non autorisée pourrait causer aux intérêts publics et privés légitimes, y compris ceux de l'Union, des institutions et organes de l'Union, des États membres ou d'autres parties prenantes concernées, afin que des mesures de protection appropriées puissent être mises en œuvre.

Article 3

Définitions

Aux fins du présent règlement, on entend par:

   a) «information»: toute donnée orale, visuelle, électronique, magnétique ou physique, ou qui se présente sous la forme de matériel, d'équipement ou de technologie, y compris les reproductions, les traductions et le matériel en cours de développement;

   b) «sécurité de l'information»: le fait de garantir l'authenticité, la disponibilité, la confidentialité, l'intégrité et la non-répudiation des informations;

   c) «traitement» d'informations: l'ensemble des actions dont les informations sont susceptibles de faire l'objet tout au long de leur cycle de vie. Sont ainsi visés la création, la collecte, l'enregistrement et l'attribution d'un niveau de confidentialité à ces informations, ainsi que leur traitement, leur affichage, leur consultation, leur transport, leur transmission, leur déclassement, leur déclassification, leur archivage et leur destruction;

d) «stockage»: le fait de conserver des informations sur tout type de support afin d'en assurer la disponibilité pour un usage ultérieur;

e) «institutions et organes de l'Union»: les institutions, organes et organismes de l'Union créés par le traité sur l'Union européenne, le traité sur le fonctionnement de l'Union européenne, le traité instituant la Communauté européenne de l'énergie atomique ou un acte législatif, ou en vertu de ces actes;

f) «informations classifiées d'Euratom»: les informations au sens du règlement nº 3/1958 du Conseil de la Communauté européenne de l'énergie atomique;

g) «autorité de sécurité»: la fonction de sécurité de chaque institution ou organe de l'Union, désignée conformément au règlement intérieur ou à l'acte fondateur de l'institution ou organe concerné;

h) «processus de gestion des risques liés à la sécurité de l'information»: l'ensemble de la procédure consistant à identifier, contrôler et limiter les événements aléatoires susceptibles d'avoir des répercussions sur la sécurité d'une organisation ou des systèmes qu'elle utilise. La procédure couvre l'ensemble des activités liées aux risques, y compris l'évaluation, le traitement, l'acceptation et la communication;

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

j) «procédures d'exploitation de sécurité»: un ensemble de procédures documentées, telles que visées à l'annexe III, destinées à l'exploitation d'une zone sécurisée, d'un système d'information et de communication ou d'une autre ressource ou d'un autre service lié à la sécurité afin d'en assurer l'efficacité;

k) «système d'information et de communication» ou «SIC»: tout système permettant le traitement et le stockage d'informations sous forme électronique, avec l'ensemble des moyens nécessaires pour le faire fonctionner;

l) «assurance de l'information»: la certitude que les systèmes d'information et de communication protégeront les informations traitées et stockées et fonctionneront comme ils le doivent, quand ils le doivent, sous le contrôle d'utilisateurs légitimes, tout en assurant des niveaux appropriés d'authenticité, de disponibilité, de confidentialité, d'intégrité et de non-répudiation;

m) «homologation»: l'agrément formel, par l'autorité d'homologation de sécurité, d'un système d'information et de communication pour traiter un niveau prédéfini d'ICUE ou d'une zone sécurisée pour stocker un niveau prédéfini d'ICUE;

n) «processus d'homologation»: les étapes et tâches requises avant l'homologation;

o) «mesures de sécurité TEMPEST»: les mesures destinées à protéger tout SIC traitant et stockant des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification plus élevé contre la compromission de ces informations par des émissions électromagnétiques non intentionnelles;

p) «CERT-EU»: le Centre de cybersécurité pour les institutions et organes de l'Union au sens du règlement (UE) […] du Parlement européen et du Conseil établissant des mesures destinées à assurer un niveau élevé de cybersécurité dans les institutions, organes et organismes de l'Union;

q) «incident de sécurité de l'information»: tout événement susceptible de compromettre l'authenticité, la disponibilité, la confidentialité, l'intégrité ou la non-répudiation des informations stockées, transmises ou traitées;

r) «besoin d'en connaître»: la nécessité pour une personne d'accéder à certaines informations traitées ou stockées par une institution ou un organe de l'Union afin d'exécuter les tâches de l'institution ou de l'organe de l'Union en question;

s) «confiance zéro»: un modèle de sécurité, un ensemble de principes de conception de systèmes et une stratégie coordonnée de gestion des systèmes et de la cybersécurité fondés sur la reconnaissance de l'existence de menaces à l'intérieur et à l'extérieur des limites des réseaux traditionnels;

t) «timbre»: une étiquette apposée sur les informations afin de veiller à ce que des mesures de sécurité appropriées soient appliquées;

u) «timbre de sécurité»: un timbre indiquant le niveau de confidentialité des informations;

v) «timbre de diffusion»: un timbre indiquant les destinataires prévus des informations au sein de l'institution ou de l'organe de l'Union d'origine;

w) «timbre d'autorisation de divulgation»: un timbre indiquant les destinataires autorisés en dehors de l'institution ou de l'organe de l'Union d'origine;

x) «propriétaire de système»: la personne chargée de l'ensemble des procédures d'acquisition, de développement, d'intégration, de modification, d'exploitation, de maintenance et de démantèlement d'un système d'information et de communication;

y) «menace pour la sécurité de l'information»: tout événement ou agent raisonnablement susceptible de nuire à la sécurité de l'information s'il ne fait pas l'objet d'une riposte et d'un contrôle;

z) «vulnérabilité»: une faille, une susceptibilité ou un défaut d'un actif, d'un système, d'un processus ou d'un contrôle qui peuvent être exploités par une ou plusieurs menaces;

aa) «risque»: l'effet préjudiciable potentiel d'une menace donnée, susceptible d'exploiter les vulnérabilités internes et externes d'une institution ou d'un organe de l'Union ou des systèmes que celle-ci ou celui-ci utilise, en portant ainsi préjudice aux intérêts publics et privés légitimes, mesuré en tenant compte à la fois de la probabilité de voir se concrétiser des menaces et de l'incidence de celles-ci;

ab) «risque résiduel»: le risque qui subsiste après la mise en œuvre des mesures de sécurité;

ac) «évaluation des risques»: le fait de déterminer les menaces et les vulnérabilités et de procéder à l'analyse des risques correspondants, c'est-à-dire d'examiner leur probabilité et leur impact;

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

ae) «certificat de cybersécurité européen»: un certificat au sens de l'article 2, paragraphe 11, du règlement (UE) 2019/881[28];

af) «détenteur»: une personne dûment autorisée qui, sur la base d'un besoin d'en connaître avéré, est en possession d'un élément d'ICUE et à laquelle il incombe par conséquent d'en assurer la protection;

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

ah) «informations classifiées de l'Union européenne» ou «ICUE»: toute information ou tout matériel identifié comme tel par la classification de sécurité de l'Union européenne, dont la divulgation non autorisée pourrait porter atteinte à des degrés divers aux intérêts de l'Union, ou à ceux d'un ou de plusieurs de ses États membres;

ai) «autorisation d'accès aux ICUE»: une décision d'une autorité de sécurité attestant qu'un fonctionnaire ou un autre agent d'une institution ou d'un organe de l'Union ou un expert national détaché auprès d'une institution ou d'un organe de l'Union peut être autorisé à avoir accès aux ICUE jusqu'à un niveau de classification donné et pendant une période donnée;

aj) «autorité nationale de sécurité», ou «ANS»: une autorité gouvernementale d'un État membre responsable en dernier ressort de la sécurité des informations classifiées dans cet État membre;

ak) «autorité de sécurité désignée», ou «ASD»: l'autorité d'un État membre (l'ANS ou toute autre autorité compétente) chargée de fournir des orientations et une aide pour la mise en œuvre de la sécurité industrielle et/ou des procédures d'habilitation;

al) «enquête de sécurité»: les procédures d'enquête menées par l'autorité compétente d'un État membre, dans le respect de ses dispositions législatives et réglementaires nationales, en vue d'obtenir l'assurance qu'il n'existe pas de renseignements défavorables de nature à empêcher une personne d'obtenir une habilitation de sécurité jusqu'à un niveau déterminé (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur);

am) «sécurité physique»: l'application de mesures physiques, techniques et organisationnelles aux locaux, aux bâtiments, aux salles, aux bureaux et aux établissements d'une institution ou d'un organe de l'Union nécessitant une protection contre les accès non autorisés aux informations qui y sont traitées, stockées ou discutées;

an) «sites»: les locaux, les bâtiments, les salles, les bureaux et les établissements d'une institution ou d'un organe de l'Union;

[28] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

ao) «défense en profondeur»: un type de sécurité consistant à utiliser plusieurs niveaux indépendants de contrôles de sécurité de manière à ce qu'en cas d'échec de l'un d'entre eux, un autre soit opérationnel;

ap) «matériel cryptographique»: les algorithmes cryptographiques, les modules matériels et logiciels cryptographiques, et les produits comprenant les modalités de mise en œuvre et la documentation y relative, ainsi que les éléments de mise à la clé;

aq) «produit cryptographique»: un produit dont la fonction première et principale est la fourniture de services de sécurité (authenticité, disponibilité, confidentialité, intégrité et non-répudiation) par l'intermédiaire d'un ou de plusieurs mécanismes cryptographiques;

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

as) «document»: tout contenu, quel que soit son support (papier, électronique; magnétique ou autre), sous forme écrite ou sous forme d'enregistrement visuel ou audiovisuel;

at) «enregistrement à des fins de sécurité»: l'application de procédures permettant de garder la trace du cycle de vie d'un matériel, y compris de sa diffusion et de sa destruction;

au) «déclassification»: la suppression de toute classification de sécurité;

av) «déclassement»: le passage à un niveau de classification de sécurité inférieur;

aw) «contrat classifié»: un contrat-cadre ou un contrat, tel que défini dans le règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil, conclu par une institution ou un organe de l'Union avec un contractant en vue de la fourniture de biens meubles ou immeubles, de la réalisation de travaux ou de la prestation de services, dont l'exécution requiert ou implique le traitement, y compris la création, ou le stockage d'ICUE;

ax) «convention de subvention classifiée»: une convention aux termes de laquelle une institution ou un organe de l'Union octroie une subvention, telle que définie dans le titre VIII du règlement (UE, Euratom) 2018/1046, et dont l'exécution nécessite ou implique le traitement, y compris la création, ou le stockage d'ICUE;

ay) «contrat de sous-traitance classifié»: un contrat conclu par un contractant ou un bénéficiaire d'une institution ou d'un organe de l'Union avec un sous-traitant en vue de la fourniture de biens meubles ou immeubles, de la réalisation de travaux ou de la prestation de services, dont l'exécution nécessite ou implique le traitement, y compris la création, ou le stockage d'ICUE;

az) «instructions de sécurité relatives à un programme/un projet», ou «ISP»: une liste des procédures de sécurité appliquées à un programme ou à un projet spécifique en vue d'uniformiser ces procédures;

ba) «annexe de sécurité», ou «AS»: un ensemble de conditions contractuelles spéciales, établi par l'autorité contractante ou octroyant la subvention, qui fait partie intégrante de tout contrat classifié ou de toute convention de subvention

classifiée impliquant l'accès à des ICUE ou la création de telles informations, dans lequel sont définis les conditions de sécurité et les éléments du contrat ou de la subvention qui doivent être protégés pour des raisons de sécurité;

bb) «guide de la classification de sécurité», ou «GCS»: un document qui décrit les éléments d'un programme, d'un projet, d'un contrat ou d'une convention de subvention qui sont classifiés, et précise les niveaux de classification de sécurité applicables.

Article 4

Principes généraux

1. Chaque institution ou organe de l'Union est responsable de la mise en œuvre des dispositions du présent règlement au sein de son organisation et tient compte à cet égard de son propre processus de gestion des risques liés à la sécurité de l'information.

2. Le non-respect du présent règlement, en particulier la divulgation non autorisée d'informations présentant les niveaux de confidentialité visés à l'article 2, paragraphe 2, à l'exception des informations destinées à un usage public, donne lieu à une enquête et peut engager la responsabilité du personnel conformément aux dispositions des traités ou aux règles applicables au personnel correspondantes.

3. Les institutions et organes de l'Union évaluent toutes les informations qu'ils traitent et stockent afin de les catégoriser conformément aux niveaux de confidentialité visés à l'article 2, paragraphe 2.

4. Les institutions et organes de l'Union déterminent les besoins de sécurité de toutes les informations qu'ils traitent et stockent en tenant compte des aspects suivants:

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

   b) la disponibilité: le fait que l'information est accessible et utilisable, à la demande d'une entité autorisée;

   c) la confidentialité: la non-divulgation des informations à des personnes, à des entités ou à des processus non autorisés;

   d) l'intégrité: le fait que les informations sont complètes et que le caractère complet des informations est préservé;

   e) la non-répudiation: la possibilité de prouver qu'une action ou qu'un événement a eu lieu, de sorte que cette action ou cet événement ne peut être contesté par la suite;

5. Pour chaque système d'information et de communication placé sous leur responsabilité, les institutions et organes de l'Union déterminent le niveau de confidentialité le plus élevé que ce système peut traiter et stocker, procèdent à une évaluation des risques pour la sécurité de l'information et assurent un suivi régulier des besoins de sécurité et de la mise en œuvre adéquate des mesures de protection définies.

6. L'ensemble des institutions et organes de l'Union fournissent des activités de formation et de sensibilisation sur la manière dont les informations non classifiées et les ICUE doivent être traitées et stockées.

Les institutions et organes de l'Union qui traitent et stockent des ICUE organisent au moins une fois tous les cinq ans une formation obligatoire pour l'ensemble des personnes autorisées à accéder à des ICUE. Les institutions et organes de l'Union concernés organisent une formation spécifique pour les fonctions spécifiques investies de tâches liées à la sécurité de l'information.

Les institutions et organes de l'Union peuvent coordonner ces activités de formation et de sensibilisation avec d'autres institutions et organes de l'Union.

Article 5

Processus de gestion des risques liés à la sécurité de l'information

1. Chaque institution ou organe de l'Union établit un processus de gestion des risques liés à la sécurité de l'information pour la protection des informations qu'il traite et stocke.

2. Le processus de gestion des risques liés à la sécurité de l'information comporte les étapes suivantes:

   a) détection des menaces et vulnérabilités;

   b) évaluation des risques;

   c) traitement des risques;

   d) acceptation des risques;

   e) communication sur les risques.

3. Le processus de gestion des risques liés à la sécurité de l'information tient compte de tous les facteurs pertinents pour l'institution ou l'organe concernés, et notamment:

   a) du niveau de confidentialité des informations et des obligations juridiques s'y rapportant;

   b) de la forme et de la quantité des informations et des établissements ou SIC où les informations sont traitées et stockées;

   c) des personnes accédant aux informations sur site ou à distance;

   d) de l'environnement et de la structure des bâtiments ou des zones où sont stockées les informations;

   e) des menaces que les cyberattaques, les attaques de la chaîne d'approvisionnement, l'espionnage, les actes de sabotage, le terrorisme et les activités subversives ou autres activités criminelles constituent pour l'Union, les institutions et organes de l'Union ou les États membres;

   f) de la continuité des activités et du rétablissement après sinistre;

   g) des résultats des inspections, audits ou visites d'évaluation, le cas échéant.

Chapitre 2
Gouvernance et organisation de la sécurité

Article 6

Groupe interinstitutionnel de coordination pour la sécurité de l'information

1. Un groupe interinstitutionnel de coordination pour la sécurité de l'information (ci-après le «groupe de coordination») est institué.

   Ce groupe est composé de l'ensemble des autorités de sécurité des institutions et organes de l'Union. Il a pour mission de définir la politique commune de ces institutions et organes dans le domaine de la sécurité de l'information.

2. Agissant d'un commun accord et dans l'intérêt commun de l'ensemble des institutions et organes de l'Union, le groupe de coordination:

   a) adopte son règlement intérieur et ses objectifs et priorités annuels communs;

   b) adopte des décisions sur la création de sous-groupes thématiques et leur mandat;

   c) rédige des documents d'orientation sur la mise en œuvre du présent règlement, en coopération avec le conseil interinstitutionnel de cybersécurité visé à l'article 9 du règlement (UE) […] établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union, le cas échéant;

   d) crée des plateformes destinées spécifiquement au partage de bonnes pratiques et de connaissances sur les thèmes communs pertinents pour la sécurité de l'information ainsi qu'à la fourniture d'une assistance en cas d'incidents de sécurité de l'information;

   e) veille à ce que les mesures de sécurité soient coordonnées, au besoin, avec les autorités nationales de sécurité compétentes aux fins de la protection des ICUE.

3. Le groupe de coordination désigne un président et deux vice-présidents parmi ses membres, pour une période de trois ans.

4. Le groupe de coordination se réunit au moins une fois par an à l'initiative de son président ou sur demande d'une institution ou d'un organe de l'Union.

5. Le groupe de coordination dispose du soutien administratif d'un secrétariat permanent assuré par la Commission.

6. Chaque institution ou organe de l'Union est dûment représenté au sein du groupe de coordination et, le cas échéant, des sous-groupes thématiques.

7. Les institutions et organes de l'Union informent le groupe de coordination de toute évolution politique significative, au sein de leur organisation, concernant la sécurité de l'information.

8. Dans l'exécution des tâches visées au paragraphe 2, point e), le groupe de coordination est assisté d'un comité de sécurité de l'information. Ce comité est composé d'un représentant de chaque autorité nationale de sécurité et présidé par le secrétariat du groupe de coordination, visé au paragraphe 5. Le comité de sécurité de l'information joue un rôle consultatif.

Article 7

Sous-groupes thématiques

1. Le groupe de coordination crée les sous-groupes thématiques permanents suivants afin de faciliter la mise en œuvre du présent règlement:

   a) un sous-groupe sur l'assurance de l'information;

b) un sous-groupe sur les informations non classifiées;

c) un sous-groupe sur la sécurité physique;

d) un sous-groupe sur l'homologation des systèmes d'information et de communication traitant et stockant des ICUE;

e) un sous-groupe sur le partage d'ICUE et l'échange d'informations classifiées.

2. Le cas échéant, le groupe de coordination peut créer des sous-groupes ad hoc investis d'une tâche spécifique et pour une durée limitée.

3. Sauf disposition contraire dans leur mandat, l'adhésion aux sous-groupes est ouverte à tous les représentants de l'institution ou de l'organe de l'Union concerné. Les membres des sous-groupes sont des experts du domaine de compétence concerné.

4. Le secrétariat du groupe de coordination, visé à l'article 5, paragraphe 5, soutient les travaux de tous les sous-groupes et assure la communication entre ses membres.

Article 8

ORGANISATION DE LA SÉCURITÉ

1. Chaque institution ou organe de l'Union désigne une autorité de sécurité assumant les responsabilités énoncées dans le présent règlement et, le cas échéant, dans ses propres règles de sécurité internes. Dans l'exécution de ses tâches, chaque autorité de sécurité dispose du soutien du service ou de l'agent chargé des tâches liées à la sécurité de l'information.

2. Au besoin, l'autorité de sécurité de chaque institution ou organe de l'Union adopte des modalités d'exécution internes pour la protection des informations, en fonction de la mission spécifique attribuée à cette institution ou à cet organe par le droit de l'Union, et sur la base de son autonomie institutionnelle.

3. S'il y a lieu, chaque autorité de sécurité exerce les fonctions suivantes:

a) l'autorité chargée de l'assurance de l'information définit les politiques et les lignes directrices de sécurité en matière d'assurance de l'information, et en surveille l'efficacité et la pertinence;

b) l'autorité opérationnelle chargée de l'assurance de l'information est responsable de l'élaboration des documents relatifs à la sécurité, en particulier des procédures d'exploitation de sécurité et du volet cryptographique du processus d'homologation des systèmes d'information et de communication;

c) l'autorité d'homologation de sécurité est responsable de l'homologation des zones sécurisées et des SIC traitant et stockant des ICUE;

d) l'autorité TEMPEST est responsable de l'approbation des mesures adoptées afin d'assurer la protection contre la compromission des ICUE par des émissions électromagnétiques non intentionnelles;

e) l'autorité d'agrément cryptographique est responsable de l'approbation de l'utilisation de technologies de chiffrement sur demande du propriétaire du système;

f) l'autorité de distribution cryptographique est responsable de la distribution du matériel cryptographique utilisé pour protéger les ICUE (matériels de

chiffrement, clés cryptographiques, certificats et authentificateurs connexes) aux utilisateurs concernés.

4. Les responsabilités relatives à une ou plusieurs des fonctions visées au paragraphe 3 peuvent être déléguées à une autre institution ou à un autre organe de l'Union dès lors qu'une organisation décentralisée de la sécurité offre un gain d'efficacité, de temps et de ressources significatif.

Chapitre 3
Assurance de l'information et systèmes d'information et de communication (SIC)

Article 9

Principes d'assurance de l'information

1. L'évaluation des besoins en matière de sécurité de l'information est prise en considération dès le début de la création de tous les SIC, y compris les SIC internes, externalisés et hybrides, ou au stade de la passation de marchés.

2. Tout SIC traitant et stockant des ICUE est homologué conformément au chapitre 5, section 5. Tout SIC traitant et stockant des informations sensibles non classifiées respecte les exigences minimales relatives aux informations sensibles non classifiées dans les SIC énoncées au chapitre 4.

Article 10

Sous-groupe sur l'assurance de l'information

1. Le sous-groupe sur l'assurance de l'information visé à l'article 7, paragraphe 1, point a), assume les rôles et responsabilités suivants:

   a) fournir des orientations et des bonnes pratiques concernant le marquage, le traitement et le stockage d'informations dans les SIC, en étroite coopération avec le conseil interinstitutionnel de cybersécurité visé à l'article 9 du règlement (UE) [XXX] établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union;

   b) établir un système de métadonnées pour les marquages et toutes les informations techniques nécessaires pour contribuer à un échange d'informations fluide et interopérable entre les institutions et organes de l'Union, lors de l'interconnexion de leurs SIC respectifs;

   c) favoriser la cohérence, dans l'ensemble des institutions et organes de l'Union, entre les règles relatives à la sécurité de l'information et la base de référence en cybersécurité, visée à l'article 5 du règlement (UE) [XXX] établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union.

Article 11

Exigences applicables aux systèmes d'information et de communication

1. Les institutions et organes de l'Union informent les utilisateurs des niveaux de confidentialité des informations pouvant être traitées et stockées dans un SIC. Lorsqu'un SIC traite et stocke des informations de plusieurs niveaux de confidentialité, des métadonnées et des marquages visuels sont utilisés pour qu'il soit possible de distinguer ces différents niveaux.

2. Les institutions et organes de l'Union procèdent à l'identification des utilisateurs de SIC avant de leur accorder l'accès à un niveau de confidentialité autre que celui des informations destinées à un usage public. Les utilisateurs sont authentifiés à un niveau d'assurance approprié par rapport au niveau de confidentialité. Le cas échéant, un système d'identification sécurisé commun est utilisé.

3. Des journaux de sécurité adéquats sont tenus pour l'ensemble des SIC afin de garantir des enquêtes rapides en cas de manquement aux exigences ou de fuite d'informations. Ces journaux sont tenus pendant une période établie dans l'évaluation d'impact sur l'activité ou dans les politiques applicables en matière de sécurité, de manière non répudiable.

   Lorsqu'un SIC traite et stocke des ICUE, des journaux sur le besoin d'en connaître et l'accès aux informations sont tenus jusqu'à la déclassification des informations. Les journaux de sécurité sont accessibles et consultables par l'autorité de sécurité.

4. Les institutions et organes de l'Union adoptent des règles internes concernant la sécurité des SIC afin de préciser les mesures de sécurité appropriées à adopter en fonction des besoins de sécurité des informations qui doivent être traitées et stockées, et compte tenu des territoires sur lesquels les informations sont stockées, transmises et traitées. Le cas échéant, ces mesures incluent:

   a) des restrictions de la localisation géographique;

   b) la prise en considération des éventuels conflits d'intérêts, boycotts ou sanctions concernant les contractants;

   c) des dispositions contractuelles visant à assurer la sécurité de l'information;

   d) le chiffrement des informations au repos et en transit;

   e) des restrictions à l'accessibilité des informations des institutions et organes de l'Union par le personnel des contractants;

   f) la protection des données à caractère personnel conformément à la législation applicable en la matière.

5. Les institutions et organes de l'Union gèrent leurs SIC conformément aux principes suivants:

   a) il existe pour chaque SIC un propriétaire du système ou une autorité opérationnelle chargée de l'assurance de l'information responsable de sa sécurité;

   b) un processus de gestion des risques liés à la sécurité de l'information couvrant les aspects relatifs à la sécurité de l'information est mis en œuvre;

   c) les exigences de sécurité et les procédures d'exploitation de sécurité sont formellement définies, mises en œuvre, contrôlées et révisées;

   d) les incidents de sécurité de l'information sont consignés officiellement et font l'objet d'un suivi, conformément au règlement (UE) [XXX] établissant des

mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union.

Chapitre 4
Informations non classifiées

Article 12

Informations destinées à un usage public

1. Les informations destinées à un usage public ou à une publication officielle ou ayant déjà été divulguées, qui peuvent être partagées sans restrictions à l'intérieur ou à l'extérieur des institutions et organes de l'Union, sont classées, traitées et stockées en tant qu'informations destinées à un usage public.
2. Les institutions et organes de l'Union peuvent apposer le timbre «PUBLIC USE» sur les informations visées au paragraphe 1.
3. L'ensemble des institutions et organes de l'Union veillent à l'intégrité et à la disponibilité des informations destinées à un usage public en prenant des mesures appropriées en fonction de leurs besoins de sécurité.

Article 13

Informations ordinaires

1. Les informations destinées à être utilisées par une institution ou un organe de l'Union dans l'exercice de ses fonctions et qui ne sont ni des informations sensibles non classifiées ni des informations destinées à un usage public sont catégorisées, traitées et stockées en tant qu'informations ordinaires. Cette catégorie couvre l'ensemble des informations ordinaires de niveau opérationnel traitées dans l'institution ou organe de l'Union concerné.
2. Les informations ordinaires peuvent être munies d'un timbre visuel ou sous forme de métadonnée lorsque cela est nécessaire pour assurer leur protection, en particulier lorsqu'elles sont partagées en dehors des institutions et organes de l'Union. Le timbre «EU NORMAL» ou «nom ou acronyme de l'institution ou organe de l'Union NORMAL» (adapté au cas par cas) est alors utilisé.
3. Les institutions et organes de l'Union définissent des mesures de protection standard pour les informations ordinaires en tenant compte des orientations du sous-groupe sur les informations non classifiées ainsi que de tout risque spécifique lié à leurs missions et activités.
4. Les informations ordinaires ne sont échangées en dehors des institutions et organes de l'Union qu'avec des personnes physiques ou morales ayant un besoin d'en connaître.

Article 14

Informations sensibles non classifiées

1. Les institutions et organes de l'Union catégorisent, traitent et stockent en tant qu'informations sensibles non classifiées toutes les informations qui ne sont pas classifiées mais doivent être protégées en raison d'obligations juridiques ou du

préjudice que leur divulgation non autorisée pourrait causer à des intérêts publics et privés légitimes, y compris ceux des institutions et organes de l'Union, des États membres ou de particuliers.

2. Chaque institution ou organe de l'Union identifie les informations sensibles non classifiées en leur apposant un timbre de sécurité visible et définit les instructions de traitement correspondantes conformément à l'annexe I.

3. Les institutions et organes de l'Union protègent les informations sensibles non classifiées en appliquant des mesures appropriées pour leur traitement et leur stockage. Ces informations ne peuvent être rendues accessibles, au sein des institutions et organes de l'Union, qu'aux personnes ayant un besoin d'en connaître aux fins de l'exécution des tâches qui leur sont confiées.

4. Les informations sensibles non classifiées ne sont échangées en dehors des institutions et organes de l'Union qu'avec des personnes physiques et morales ayant un besoin d'en connaître, dans le respect des instructions de traitement accompagnant ces informations. Toutes les parties concernées sont informées des instructions de traitement appropriées.

Article 15

Protection des informations non classifiées et interopérabilité

1. Les institutions et organes de l'Union établissent des procédures pour le signalement et la gestion de tout incident avéré ou suspecté qui pourrait entraîner la compromission de la sécurité d'informations non classifiées.

2. Le cas échéant, les institutions et organes de l'Union utilisent les timbres prévus aux articles 12, 13 et 14. À titre exceptionnel, ils peuvent utiliser d'autres marquages équivalents en interne et avec leurs homologues spécifiques d'autres institutions et organes de l'Union ou des États membres, avec l'accord de toutes les parties. Cette exception est notifiée au sous-groupe sur les informations non classifiées, visé à l'article 7, paragraphe 1, point b).

3. Des garanties contractuelles sont établies afin d'assurer la protection des informations normales et sensibles non classifiées traitées par des services externalisés. Ces garanties sont conçues de manière à assurer au moins un niveau de protection équivalent à celui fourni par le présent règlement et incluent des engagements en matière de confidentialité et de non-divulgation qui doivent être signés par tous les fournisseurs de services pertinents intervenant dans la fourniture des systèmes externalisés.

Article 16

Sous-groupe sur les informations non classifiées

1. Le sous-groupe sur les informations non classifiées visé à l'article 7, paragraphe 1, point b), assume les rôles et responsabilités suivants:

   a) rationaliser les procédures relatives au traitement et au stockage des informations non classifiées et préparer les orientations pertinentes en la matière;

b) assurer une coordination avec le sous-groupe sur l'assurance de l'information visé à l'article 7, paragraphe 1, point a), concernant les questions qui portent sur les systèmes traitant et stockant des informations non classifiées;

c) préparer des instructions de traitement pour les différents niveaux de confidentialité des informations non classifiées;

d) aider les institutions et organes de l'Union à établir les équivalences entre leurs catégories spécifiques d'informations non classifiées et celles prévues aux articles 12, 13 et 14;

e) faciliter le partage d'informations non classifiées entre les institutions et organes de l'Union, en fournissant une assistance et des orientations.

Article 17

Traitement et stockage des informations sensibles non classifiées dans les SIC

1. Les institutions et organes de l'Union veillent à ce que les SIC satisfassent aux exigences minimales suivantes lorsqu'ils traitent et stockent des informations sensibles non classifiées:

a) une authentification forte est mise en œuvre pour l'accès aux informations sensibles non classifiées et ces informations sont chiffrées lors de leur transmission et pendant leur stockage;

b) les clés de chiffrement utilisées pour le stockage sont placées sous la responsabilité de l'institution ou organe de l'Union responsable de l'exploitation du SIC;

c) les informations sensibles non classifiées sont stockées et traitées dans l'Union;

d) des dispositions contractuelles couvrant la sécurité du personnel, des ressources et des informations sont incluses dans tous les contrats d'externalisation;

e) des métadonnées interopérables sont utilisées pour consigner le niveau de confidentialité des documents électroniques et faciliter l'automatisation des mesures de sécurité;

f) les institutions et organes de l'Union mettent en œuvre des mesures de prévention et de détection des fuites de données afin de protéger les informations sensibles non classifiées;

g) des équipements de sécurité ayant reçu un certificat de cybersécurité européen sont utilisés, lorsqu'ils sont disponibles;

h) les mesures de sécurité sont mises en œuvre sur la base des principes du besoin d'en connaître et de la confiance zéro afin de réduire au minimum l'accès aux informations sensibles non classifiées par les fournisseurs de services et les contractants.

2. Toute dérogation aux exigences minimales énoncées au paragraphe 1 est soumise à l'approbation du niveau d'encadrement approprié de l'institution ou de l'organe de l'Union concerné, sur la base d'une évaluation des risques couvrant les risques juridiques et techniques pour la sécurité des informations sensibles non classifiées.

3. L'autorité chargée de l'assurance de l'information de l'institution ou de l'organe de l'Union concerné peut vérifier le respect des principes énoncés au paragraphe 1 à tout moment du cycle de vie d'un SIC.

Chapitre 5
ICUE

SECTION 1
DISPOSITIONS GENERALES

Article 18

Classifications et marquages de sécurité

1. Les ICUE relèvent de l'un des niveaux de classification suivants et sont marquées comme suit:

   a) TRÈS SECRET UE/EU TOP SECRET: informations et matériels dont la divulgation non autorisée pourrait causer un préjudice exceptionnellement grave aux intérêts essentiels de l'Union ou d'un ou de plusieurs de ses États membres;

   b) SECRET UE/EU SECRET: informations et matériels dont la divulgation non autorisée pourrait nuire gravement aux intérêts essentiels de l'Union ou d'un ou de plusieurs de ses États membres;

   c) CONFIDENTIEL UE/EU CONFIDENTIAL: informations et matériels dont la divulgation non autorisée pourrait nuire aux intérêts essentiels de l'Union ou d'un ou de plusieurs de ses États membres;

   d) RESTREINT UE/EU RESTRICTED: informations et matériels dont la divulgation non autorisée pourrait être défavorable aux intérêts de l'Union ou d'un ou de plusieurs de ses États membres.

2. Le groupe de coordination adopte des documents d'orientation sur la création et la classification des ICUE.

Article 19

Adéquation au traitement et au stockage des ICUE

1. Toute institution ou tout organe de l'Union peut traiter et stocker des ICUE lorsque l'entité remplit les conditions suivantes:

   a) elle établit des règles et des procédures conformément au présent règlement, garantissant la protection des informations pour un niveau de classification donné; et

   b) elle a fait l'objet d'une visite d'évaluation conformément à l'article 53 et a par la suite reçu une certification concernant sa capacité à protéger les ICUE conformément au présent règlement et, le cas échéant, à toute autre règle ou procédure applicable.

2. Les conditions énoncées au paragraphe 1 sont réputées remplies par défaut par les membres du sous-groupe sur le partage d'ICUE et l'échange d'informations classifiées visé à l'article 7, paragraphe 1, point e).

Article 20

Protection des ICUE

1. Il incombe au détenteur de tout élément d'ICUE de le protéger.

2. Lorsque les États membres introduisent des informations classifiées, portant un marquage national de classification de sécurité, dans les structures ou réseaux d'une institution ou d'un organe de l'Union, cette institution ou cet organe protège lesdites informations conformément au marquage de classification correspondant établi dans l'accord entre les États membres de l'Union européenne, réunis au sein du Conseil, relatif à la protection des informations classifiées échangées dans l'intérêt de l'Union européenne[29]. Le tableau d'équivalence correspondant est inclus à l'annexe VI du présent règlement.

3. Un ensemble d'ICUE peut justifier un niveau de protection correspondant à une classification plus élevée que celle appliquée à ses différentes composantes.

Article 21

Processus de gestion des risques liés à la sécurité des ICUE

1. L'autorité de sécurité de chaque institution ou organe de l'Union approuve les mesures de sécurité destinées à protéger les ICUE tout au long de leur cycle de vie sur la base des résultats d'une évaluation des risques réalisée par l'institution ou organe de l'Union concerné.

2. Les mesures de sécurité adoptées par chaque institution ou organe de l'Union sont proportionnées au niveau de classification des informations traitées et stockées, à la forme sous laquelle elles se présentent ainsi qu'à leur volume, à l'emplacement et aux caractéristiques de protection des établissements où des ICUE sont traitées et stockées, et à la menace évaluée à l'échelle locale que représentent les activités malveillantes ou criminelles.

3. L'ensemble des institutions et organes de l'Union établissent:

   a) des plans d'urgence pour assurer la sécurité des ICUE en cas d'urgence;

   b) des plans de continuité des activités incluant des mesures de prévention et de retour aux conditions opérationnelles afin de limiter l'impact de défaillances graves ou de graves incidents de sécurité sur le traitement et le stockage des ICUE.

Article 22

Infractions à la sécurité et compromission des ICUE

1. Un acte ou une omission d'une institution ou d'un organe de l'Union, ou d'une personne, qui est contraire au présent règlement est considéré comme une infraction à la sécurité.

2. Des ICUE sont réputées avoir été compromises lorsque, à la suite d'une infraction, elles ont été divulguées, en totalité ou en partie, à une ou plusieurs personnes non autorisées à y accéder.

3. Toute compromission d'ICUE, réelle ou présumée, est immédiatement signalée à l'autorité de sécurité de l'institution ou organe de l'Union concerné, qui mène une enquête de sécurité et adopte au minimum les mesures suivantes:

[29] JO C 202 du 8.7.2011, p. 13.

a) en informer l'autorité d'origine;

b) faire en sorte qu'une enquête soit menée par des membres du personnel n'étant pas directement concernés par l'infraction afin d'établir les faits;

c) évaluer le préjudice éventuel causé aux intérêts de l'Union ou des États membres;

d) prendre des mesures appropriées pour éviter que les faits ne se reproduisent;

e) informer les autorités compétentes de la compromission réelle ou présumée et des mesures prises.

SECTION 2
SECURITE DU PERSONNEL

Article 23

Principes de base

1. L'autorité de sécurité d'une institution ou d'un organe de l'Union peut accorder à des personnes un accès à des ICUE lorsque toutes les conditions suivantes sont remplies:

   a) les personnes ont un besoin d'en connaître;

   b) elles ont été informées des règles et procédures de sécurité applicables à la protection des ICUE ainsi que des normes et lignes directrices correspondantes en matière de sécurité, et ont reconnu par écrit les responsabilités qui leur incombent en matière de protection de ces informations;

   c) pour les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification plus élevé, les personnes se sont vu délivrer une habilitation de sécurité et ont reçu une autorisation du niveau correspondant.

2. Les institutions et organes de l'Union tiennent compte de la loyauté, de l'intégrité et de la fiabilité d'une personne telles qu'établies au moyen d'une enquête de sécurité menée par les autorités compétentes de l'État membre dont le demandeur est citoyen ou ressortissant.

3. Les institutions et organes de l'Union peuvent accepter des habilitations de sécurité de pays tiers et d'organisations internationales avec lesquels l'Union a conclu un accord sur la sécurité des informations.

4. Les institutions et organes de l'Union peuvent gérer les processus d'habilitation de manière autonome ou solliciter la conclusion d'un accord de niveau de service avec la Commission aux fins de la délivrance d'habilitations de sécurité.

   Lorsqu'un accord de niveau de service est conclu, l'autorité de sécurité de la Commission fait office de point de contact entre les bureaux de sécurité de l'institution ou de l'organe de l'Union concerné et les autorités nationales compétentes des États membres pour toutes les questions relevant de l'habilitation de sécurité.

5. L'autorité de sécurité de chaque institution ou organe de l'Union tient des registres de ses habilitations de sécurité, de ses réunions d'information, de ses déclarations écrites et de ses autorisations d'accès aux ICUE.

6. Les institutions et organes de l'Union qui concluent un accord de niveau de service avec la Commission mettent les registres pertinents à la disposition de l'autorité de sécurité de la Commission en ce qui concerne, au minimum, le niveau de classification des ICUE auxquelles la personne peut être autorisée à avoir accès, la date de délivrance de l'autorisation d'accès aux ICUE et la période de validité de cette autorisation. Ces registres sont accessibles aux autres institutions et organes de l'Union ayant conclu un accord de niveau de service, lorsque cela se justifie.

Article 24

Autorisation d'accéder aux ICUE

1. Chaque institution ou organe de l'Union répertorie, au sein de son organisation, les postes nécessitant l'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification plus élevé pour permettre au détenteur de s'acquitter de ses tâches.
2. Lorsqu'une personne doit être autorisée à accéder à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification plus élevé, l'institution ou l'organe concerné informe l'autorité de sécurité compétente, qui procède aux formalités exigées au point 1 de l'annexe II.
3. L'autorité de sécurité de chaque institution ou organe de l'Union est responsable de la délivrance, de la suspension, du retrait et du renouvellement des autorisations d'accès à des ICUE pour son personnel.
4. Dans des circonstances exceptionnelles, lorsque cela est dûment justifié dans l'intérêt du service et en attendant l'achèvement de l'enquête de sécurité complète, l'autorité de sécurité d'une institution ou d'un organe de l'Union peut accorder à titre temporaire à des personnes l'autorisation d'accéder à des ICUE pour un poste déterminé, sans préjudice des dispositions concernant le renouvellement des autorisations d'accéder à des ICUE et après vérification par l'autorité nationale compétente de sécurité.
5. Les institutions et organes de l'Union suivent les procédures de gestion des autorisations d'accès à des ICUE énoncées à l'annexe II.

Article 25

Reconnaissance des autorisations d'accéder à des ICUE

1. Une autorisation d'accéder à des ICUE jusqu'au niveau de classification spécifique est valide dans toute institution ou tout organe de l'Union auquel la personne est affectée.
2. Les institutions et organes de l'Union acceptent les autorisations d'accès aux ICUE accordées par d'autres institutions ou organes de l'Union.
3. Lorsque le titulaire d'une autorisation d'accès aux ICUE accède à un emploi dans une autre institution ou un autre organe de l'Union, cette institution ou cet organe notifie à l'ANS concernée le changement d'employeur, par l'intermédiaire de l'autorité de sécurité compétente.

Article 26

Réunions d'information sur les ICUE

1. L'autorité de sécurité d'une institution ou d'un organe de l'Union informe toutes les personnes ayant besoin d'accéder à des ICUE des éventuelles menaces pour la sécurité ainsi que de leur obligation de signaler toute activité suspecte. Cette information est donnée avant que l'accès aux ICUE ne soit accordé et, par la suite, au moins une fois tous les cinq ans.

2. Après avoir été informées conformément au paragraphe 1, toutes les personnes concernées reconnaissent par écrit qu'elles ont compris leurs obligations en matière de protection des ICUE et les conséquences qui pourraient résulter si des ICUE devaient être compromises.

3. L'information visée au paragraphe 1 contient les éléments suivants:

   a) toute personne responsable d'une violation des règles de sécurité énoncées dans le présent règlement est passible d'une sanction disciplinaire conformément aux dispositions législatives et réglementaires applicables;

   b) toute personne responsable de la compromission ou de la perte d'ICUE peut être passible de sanctions disciplinaires ou peut faire l'objet d'une action en justice conformément aux dispositions législatives et réglementaires applicables.

4. Lorsque des personnes auxquelles a été délivrée une autorisation d'accéder à des ICUE n'ont plus besoin d'un tel accès, les institutions et organes de l'Union veillent à ce qu'elles soient informées, et, le cas échéant, reconnaissent par écrit qu'elles ont l'obligation de continuer à protéger les ICUE.

5. La tâche de création et de gestion des réunions d'information sur les ICUE peut être partagée entre les institutions et organes de l'Union pour autant que leurs besoins spécifiques soient pris en considération.

SECTION 3
SECURITE PHYSIQUE

Article 27

Principes de base

1. Chaque institution et chaque organe de l'Union détermine les mesures de sécurité physique appropriées pour ses sites, conformément à l'annexe III et au principe de défense en profondeur, sur la base d'une évaluation des risques réalisée par son autorité de sécurité. Les objectifs des mesures sont les suivants:

   a) empêcher tout accès aux ICUE ou toute intrusion par la force;

   b) dissuader, empêcher et détecter les actes non autorisés et répondre aux incidents de sécurité le plus rapidement possible;

   c) permettre d'établir une distinction entre les membres du personnel au regard de l'accès aux ICUE sur la base de leur besoin d'en connaître et, le cas échéant, de leur habilitation de sécurité.

2. Les institutions et organes de l'Union mettent en place des mesures de sécurité physique pour tous les sites où des ICUE sont discutées, stockées ou traitées, y compris les zones où se trouvent les systèmes d'information et de communication visés à la section 5 du présent chapitre.

3. Seuls les équipements de sécurité approuvés par l'autorité de sécurité d'une institution ou d'un organe de l'Union sont utilisés pour la protection physique d'informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification plus élevé.

4. Les institutions et organes de l'Union peuvent partager des zones sécurisées, telles que visées à l'annexe III, pour le traitement et le stockage d'ICUE, moyennant la conclusion d'un accord.

Article 28

Sous-groupe sur la sécurité physique

1. Le sous-groupe sur la sécurité physique visé à l'article 7, paragraphe 1, point c), assume les rôles et responsabilités suivants:

   a) préparation des documents d'orientation relatifs aux questions de sécurité physique;

   b) définition des critères de sécurité généraux à remplir pour l'achat d'équipements tels que des meubles de sécurité, des déchiqueteuses, des serrures de porte, des systèmes électroniques de contrôle des accès, des systèmes de détection des intrusions et des systèmes d'alarme pour la protection physique des ICUE;

   c) fourniture d'une assistance aux institutions et organes de l'Union pour déterminer les mesures de sécurité appropriées pour leurs sites;

   d) proposition de mesures compensatoires pour la protection des ICUE lorsque celles-ci sont traitées en dehors des zones physiquement protégées d'une institution ou d'un organe de l'Union.

Article 29

Protection physique des ICUE

1. Afin d'assurer la protection physique des ICUE, les institutions et organes de l'Union instaurent les zones physiquement protégées suivantes:

   a) des zones administratives, telles que visées à l'annexe III;

   b) le cas échéant, des zones sécurisées, incluant des zones sécurisées de catégorie I, des zones sécurisées de catégorie II et des zones sécurisées du point de vue technique, telles que visées à l'annexe III.

2. L'autorité de sécurité de l'institution ou de l'organe de l'Union concerné procède à une inspection interne afin de vérifier si les conditions de la désignation d'une zone comme zone administrative ou zone sécurisée, énoncées à l'annexe III, sont réunies. Lorsque le rapport d'inspection indique que ces conditions sont remplies, l'autorité de sécurité peut délivrer une homologation permettant à la zone sécurisée de protéger des ICUE jusqu'au niveau déterminé pendant une période maximale de cinq ans.

   L'autorité de sécurité de l'institution ou organe de l'Union concerné est responsable de l'exécution du processus de réhomologation de ses zones sécurisées, avant l'expiration de l'homologation ou chaque fois que des changements sont intervenus au sein de la zone homologuée.

3. Chaque institution ou organe de l'Union adopte des procédures de gestion des clés et des combinaisons pour les bureaux, les salles, les chambres fortes et les meubles de sécurité pour le niveau CONFIDENTIEL UE/EU-CONFIDENTIAL et les niveaux supérieurs.

4. L'autorité de sécurité peut autoriser des fouilles aux entrées et aux sorties afin de prévenir et de détecter l'introduction non autorisée de matériel dans des sites ou le retrait non autorisé de toute ICUE des sites.

5. Les institutions et organes de l'Union établissent les mesures de protection physique des ICUE conformément à l'annexe III.

SECTION 4
GESTION DES ICUE

Article 30

Principes de base

1. Les institutions et organes de l'Union enregistrent, consignent, conservent et, à terme, éliminent, échantillonnent ou transfèrent leurs documents ICUE vers les archives pertinentes conformément à la politique et aux règles de conservation applicables spécifiquement aux dossiers de chaque institution ou organe de l'Union.

2. Toute institution ou tout organe de l'Union qui est l'autorité d'origine des ICUE détermine la classification de sécurité de ces informations dès leur création et conformément à l'article 18, paragraphe 1.

3. Les institutions et organes de l'Union communiquent clairement le niveau de classification aux destinataires, au moyen d'un marquage de classification ou d'une annonce, lorsque les informations sont transmises sous forme orale.

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

5. Les institutions et organes de l'Union adoptent les mesures de gestion des ICUE conformément à l'annexe IV.

Article 31

Création d'ICUE

2. Les institutions et organes de l'Union sous l'autorité desquels des ICUE sont créées veillent à ce que les exigences suivantes soient respectées:

a) sur chaque page est apposé un timbre indiquant clairement le niveau de classification;

b) chaque page est numérotée;

c) le document porte un numéro de référence, le cas échéant un numéro d'enregistrement et un sujet qui n'est pas lui-même une ICUE, sauf s'il s'est vu apposer un timbre à ce titre;

d) le document porte la date de sa création.

e) toutes les annexes et pièces jointes sont énumérées, si possible sur la première page;

f) les documents classifiés SECRET UE/EU SECRET ou d'un niveau de classification supérieur portent un numéro d'exemplaire sur chaque page lorsqu'ils doivent être diffusés en plusieurs exemplaires. Les copies électroniques diffusées en dehors du système de détention se voient apposer un identifiant unique basé sur une signature électronique.

Article 32

Contrôle de l'autorité d'origine

1. L'institution ou organe de l'Union sous l'autorité de laquelle ou duquel un document ICUE est créé exerce le contrôle de l'autorité d'origine sur ce document. L'autorité d'origine détermine le niveau de classification du document et est responsable de sa diffusion initiale. Sans préjudice du règlement nº 1049/2001, le consentement préalable écrit de l'autorité d'origine est sollicité avant que les informations puissent être:

   a) déclassifiées ou déclassées;

   b) utilisées à d'autres fins que celles qui sont fixées par l'autorité d'origine;

   c) transmises à une entité située en dehors de l'institution ou de l'organe de l'Union détenant les informations, y compris à un pays tiers ou à une organisation internationale, à une autre institution ou un autre organe de l'Union, à des États membres, à un contractant ou à un contractant potentiel, à un bénéficiaire ou à un bénéficiaire potentiel;

   d) copiées et traduites lorsqu'elles relèvent du niveau TRÈS SECRET-UE/EU-TOP SECRET.

2. Si l'autorité d'origine d'un document ICUE ne peut être identifiée, l'institution ou l'organe de l'Union qui détient ces informations classifiées exerce le contrôle de l'autorité d'origine.

3. Les autorités d'origine d'un document ICUE tiennent un registre de toute source classifiée utilisée pour produire des documents classifiés, y compris des informations sur les sources provenant d'États membres, d'organisations internationales ou de pays tiers. Le cas échéant, les informations classifiées agrégées sont marquées de façon à préserver l'identification des autorités d'origine des sources classifiées utilisées.

Article 33

Timbres de classification

1. Le cas échéant, en plus de l'un des marquages de classification de sécurité, les documents d'ICUE peuvent se voir apposer d'autres marquages, tels que des timbres de diffusion ou d'autorisation de divulgation, ou des timbres indiquant l'autorité d'origine.

2. Différentes parties d'un document ICUE peuvent nécessiter des classifications différentes et doivent alors porter le marquage afférent. 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.

3. Les documents dont toutes les parties n'ont pas le même niveau de classification sont structurés de manière à ce que les parties ayant des niveaux de classification différents puissent au besoin être aisément identifiées et séparées des autres.

Article 34

Système de bureau d'ordre pour les ICUE

1. L'ensemble des institutions et organes de l'Union qui traitent et stockent des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIEL ou d'un niveau de classification plus élevé établissent un ou plusieurs bureaux d'ordre pour les ICUE afin d'assurer leur enregistrement à des fins de sécurité chaque fois qu'elles parviennent à une institution ou un organe de l'Union ou qu'elles en sortent.
2. Tous les bureaux d'ordre pour les ICUE sont établis dans des zones sécurisées telles que définies à l'annexe III.
3. Les institutions et organes de l'Union désignent un agent contrôleur pour gérer chaque bureau d'ordre pour les ICUE. L'agent contrôleur dispose d'une habilitation de sécurité appropriée ainsi que d'une autorisation conformément à l'article 24. Les institutions et organes de l'Union veillent à la formation adéquate de leur agent contrôleur.

Article 35

Déclassement et déclassification

1. Les informations ne sont classifiées que tant qu'elles nécessitent une protection. Les ICUE qui n'ont plus besoin de la classification initiale sont déclassées à un niveau inférieur. Les ICUE qui ne doivent plus du tout être considérées comme classifiées sont déclassifiées.
2. Au moment de la création d'ICUE, l'autorité d'origine indique, si possible et notamment en ce qui concerne les informations classifiées RESTREINT UE/EU RESTRICTED, si les ICUE qui y figurent peuvent ou non être déclassées ou déclassifiées à une date donnée ou après un événement spécifique.
3. L'institution ou l'organe de l'Union d'origine est responsable de la décision relative au déclassement ou à la déclassification d'un document ICUE. Il examine les informations et évalue les risques régulièrement, tous les cinq ans au moins, en vue de déterminer si le niveau de classification initial est toujours approprié.
4. Les institutions et organes de l'Union qui détiennent des ICUE dont ils ne sont pas l'autorité d'origine ne déclassent pas et ne déclassifient pas ces documents, et ne modifient ou n'éliminent pas non plus les marquages visés à l'article 18, paragraphe 1, sans le consentement écrit préalable de l'autorité d'origine.
5. Les institutions et organes de l'Union peuvent déclasser ou déclassifier partiellement les ICUE qu'ils créent. Dans ce cas, ils produisent un extrait déclassé ou déclassifié.
6. Les institutions et organes de l'Union informent l'organisation destinataire des ICUE de leur déclassement ou déclassification.

Article 36

Marquages sur les documents déclassés et déclassifiés

1. Lorsque les institutions et organes de l'Union décident de déclassifier un document ICUE, il convient d'examiner si le document doit porter un timbre de diffusion «Informations sensibles non classifiées».

2. Le timbre de classification d'origine figurant en haut et en bas de chaque page est biffé de manière visible en utilisant la fonction «strikethrough» pour les formats électroniques, ou biffé manuellement pour les impressions. Le timbre de classification d'origine n'est pas supprimé.

3. La première page ou la page de couverture du document est revêtue d'un cachet de déclassement ou de déclassification et complétée avec les références de l'autorité responsable du déclassement ou de la déclassification et la date correspondante. Le déclassement ou la déclassification de documents ICUE électroniques est certifié par une signature électronique sous l'autorité de l'autorité d'origine.

Article 37

Destruction et suppression des ICUE

1. Tous les cinq ans au moins, les institutions et organes de l'Union examinent les ICUE, sur papier et dans les SIC, afin de déterminer si elles doivent être détruites ou supprimées. Lorsque des ICUE sont détruites ou supprimées, les institutions et organes de l'Union en informent toute personne ayant précédemment reçu ces ICUE.

2. Les institutions et organes de l'Union peuvent détruire les doubles d'ICUE qui ne sont plus nécessaires, en tenant compte des règles applicables en matière de gestion des documents pour les originaux.

3. Seul l'agent contrôleur d'une institution ou d'un organe de l'Union procède à la destruction des exemplaires papier des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification plus élevé. L'agent contrôleur actualise en conséquence les journaux tenus et les autres informations relatives aux enregistrements, en conservant les métadonnées essentielles du document détruit.

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

4. L'agent contrôleur et, le cas échéant, le témoin signent un procès-verbal de destruction qui est archivé dans le bureau d'ordre. Le procès-verbal est conservé pendant au moins cinq ans pour les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET-UE/EU-SECRET et pendant au moins dix ans pour les informations classifiées TRÈS SECRET-UE/EU-TOP SECRET.

Article 38

Évacuation et destruction d'ICUE en cas d'urgence

1. Chaque institution ou organe de l'Union élabore des plans d'évacuation et de destruction d'urgence tenant compte des conditions locales pour assurer la sauvegarde des ICUE qui présentent un risque significatif de tomber entre les mains de personnes non autorisées.

Les modalités opérationnelles des plans d'évacuation et de destruction d'urgence sont elles-mêmes classifiées RESTREINT UE/EU RESTRICTED.

2. En cas d'urgence, s'il existe un risque imminent de divulgation non autorisée d'ICUE, les institutions et organes de l'Union procèdent à l'évacuation des ICUE.

   Lorsque l'évacuation n'est pas possible, les ICUE sont détruites de manière à ne pas pouvoir être reconstituées, que ce soit entièrement ou partiellement.

3. L'autorité d'origine et le bureau d'ordre d'origine sont informés de l'évacuation ou de la destruction en urgence d'ICUE enregistrées.

4. Lorsque les plans d'urgence ont été activés, les niveaux d'ICUE les plus élevés sont évacués ou détruits en priorité, y compris les matériels de chiffrement.

Article 39

Archivage

1. Les institutions et organes de l'Union déterminent s'il y a lieu d'archiver les ICUE et, dans ce cas, à quel moment, ainsi que les mesures pratiques correspondantes à prendre, conformément à leur politique en matière de gestion des documents.

2. Les documents ICUE ne sont pas transférés aux archives historiques de l'Union européenne.

SECTION 5
PROTECTION DES ICUE TRAITEES DANS DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

Article 40

Sous-groupe sur l'homologation des systèmes d'information et de communication traitant et stockant des ICUE

Le sous-groupe sur l'homologation des SIC traitant et stockant des ICUE visé à l'article 7, paragraphe 1, point d), assume les rôles et responsabilités suivants:

a) fourniture d'une assistance aux institutions et organes de l'Union dans le cadre de leurs processus d'homologation;

b) recommandation d'une norme devant être suivie par l'ensemble des institutions et organes de l'Union pour l'homologation;

c) diffusion et partage de bonnes pratiques et d'orientations concernant l'homologation des SIC.

Article 41

Systèmes d'information et de communication

Les institutions et organes de l'Union satisfont aux exigences suivantes concernant les SIC traitant et stockant des ICUE:

a) le propriétaire du système ou l'autorité opérationnelle chargée de l'assurance de l'information consulte l'autorité d'homologation de sécurité avant d'élaborer ou d'acheter un SIC ou de permettre l'utilisation d'un SIC pour

traiter et stocker des ICUE, afin de déterminer les exigences relatives à l'homologation;

b) les principes clés de sécurité pour l'élaboration de SIC traitant et stockant des ICUE s'appliquent dès le lancement du projet, dans le cadre du processus de gestion des risques liés à la sécurité de l'information et en tenant compte des principes de besoin d'en connaître, de fonctionnalité minimale, de défense en profondeur, du moindre privilège, de séparation des fonctions et du double regard;

c) les éléments d'un SIC traitant et stockant des ICUE relatifs au stockage, au traitement central et à la gestion de réseau sont installés dans une zone sécurisée, telle que visée à l'annexe III;

d) des «mesures de sécurité TEMPEST» proportionnées au risque d'exploitation et au niveau de classification des informations sont mises en œuvre;

e) l'ensemble du personnel participant au fonctionnement d'un SIC traitant et stockant des ICUE notifie à l'autorité de sécurité et au propriétaire du système concerné ou à l'autorité opérationnelle chargée de l'assurance de l'information toutes les failles en matière de sécurité, les incidents, les infractions à la sécurité ou les compromissions du système potentiels susceptibles d'avoir un impact sur la protection du SIC et/ou des ICUE qu'il contient;

f) le cas échéant, l'autorité de sécurité notifie aux autorités de sécurité de toute autre institution ou de tout autre organe de l'Union concerné les failles en matière de sécurité ou les incidents potentiels susceptibles d'affecter leurs SIC traitant et stockant des ICUE.

Article 42

Produits cryptographiques

1. Des produits cryptographiques ayant fait l'objet d'un agrément sont utilisés pour la transmission et le stockage des ICUE par voie électronique. La liste des produits cryptographiques agréés est tenue par le Conseil, sur la base des contributions des autorités nationales de sécurité.

2. Lorsque la liste visée au paragraphe 1 n'inclut aucun produit approprié pour l'utilisation escomptée, l'autorité d'agrément cryptographique de l'institution ou organe de l'Union concerné demande un agrément à titre provisoire auprès du Conseil. Dans la mesure du possible, un produit cryptographique agréé par l'autorité nationale de sécurité d'un État membre est sélectionné.

   Le Conseil prend les mesures nécessaires pour veiller à ce qu'un produit approprié soit ajouté à la liste.

3. Les agréments de produits cryptographiques sont valables pour une durée maximale de cinq ans et font ensuite l'objet d'un réexamen annuel.

4. Le Conseil supprime de la liste des produits cryptographiques agréés tout produit cryptographique dont l'agrément national a été retiré ou a expiré.

5. Le groupe de coordination informe chaque année le Conseil des éventuels produits cryptographiques qu'il recommande pour évaluation à l'autorité d'agrément cryptographique d'un État membre, sur la base d'une enquête menée dans les institutions et organes de l'Union.

Article 43

Homologation des SIC traitant et stockant des ICUE

1. En homologuant les SIC traitant et stockant des ICUE, les institutions et organes de l'Union confirment que toutes les mesures de sécurité appropriées ont été mises en œuvre et que les ICUE et les SIC font l'objet d'un niveau suffisant de protection conformément au présent règlement.

2. Le propriétaire du SIC ou l'autorité opérationnelle chargée de l'assurance de l'information est responsable de la préparation des dossiers d'homologation et de la documentation, y compris des manuels destinés aux différents types d'utilisateurs.

3. L'autorité d'homologation de sécurité de chaque institution ou organe de l'Union est chargée d'établir un processus d'homologation indiquant clairement les conditions d'homologation que doivent remplir tous les SIC relevant de sa responsabilité.

4. Lorsqu'un SIC traitant et stockant des ICUE implique à la fois des institutions et organes de l'Union et des autorités nationales de sécurité, les institutions et organes de l'Union concernés établissent, au moyen de dispositions d'application complémentaires adoptées conformément à l'article 8, paragraphe 2, un comité conjoint d'homologation de sécurité chargé de l'homologation du système. Ce comité est composé de représentants des autorités d'homologation de sécurité des parties concernées et présidé par l'autorité d'homologation de sécurité de l'institution ou de l'organe de l'Union qui possède le SIC.

Article 44

Processus d'homologation des SIC traitant et stockant des ICUE

1. Tous les SIC traitant et stockant des ICUE font l'objet d'un processus d'homologation basé sur les principes d'assurance de l'information, dont le niveau de détail doit être proportionné au niveau de protection requis.

2. Le processus d'homologation aboutit à une déclaration d'homologation déterminant le niveau maximal de classification des informations qui peuvent être traitées et stockées dans un SIC ainsi que les modalités et les conditions correspondantes. La déclaration d'homologation repose sur la validation formelle de l'évaluation des risques et des mesures de sécurité mises en œuvre pour le SIC concerné; elle fournit les assurances suivantes:

   a) le processus de gestion des risques liés à la sécurité de l'information a été correctement mis en œuvre;

   b) le propriétaire du système ou du risque a accepté le risque résiduel en connaissance de cause;

   c) un niveau suffisant de protection du SIC et des ICUE traitées et stockées par ledit système a été atteint conformément au présent règlement.

3. L'autorité d'homologation de sécurité d'une institution ou d'un organe de l'Union procède à la validation formelle de la déclaration d'homologation. Une fois la validation réussie, l'autorité d'homologation de sécurité délivre une autorisation d'utiliser le SIC qui détermine le niveau maximal de classification des ICUE pouvant être traitées dans le SIC ainsi que les modalités et les conditions de fonctionnement correspondantes. Cette autorisation est délivrée pour une période donnée. Lorsqu'une ou plusieurs des mesures de sécurité requises ne sont pas prévues, mais que cela n'a

pas d'incidence significative sur la sécurité globale, une autorisation d'utilisation provisoire peut être délivrée, précisant les points à corriger.

4. À tout moment du cycle de vie d'un SIC, l'autorité d'homologation de sécurité de l'institution ou organe de l'Union concerné peut prendre les mesures suivantes:

   a) mettre en œuvre un processus d'homologation;

   b) procéder à un audit ou une inspection du SIC;

   c) si les conditions de fonctionnement ne sont plus satisfaites, par exemple lorsqu'un incident de sécurité a révélé une grave vulnérabilité dans le SIC, exiger l'élaboration et la mise en œuvre effective d'un plan d'amélioration de la sécurité selon un calendrier bien défini, en retirant éventuellement l'autorisation d'utiliser le SIC jusqu'à ce que les conditions de son fonctionnement soient satisfaites.

5. Le propriétaire du système ou l'autorité opérationnelle chargée de l'assurance de l'information adresse chaque année un rapport formel à l'autorité d'homologation de sécurité pendant la période de validité d'une autorisation d'utiliser le SIC, incluant un résumé des éventuels facteurs de risque, évolutions et incidents significatifs.

Article 45

Situations d'urgence

1. Les institutions et organes de l'Union peuvent mettre en œuvre des procédures spécifiques pour transmettre ou stocker des ICUE classifiées dans des situations d'urgence, telles que des crises, des conflits ou des guerres, imminents ou effectifs, ou dans des circonstances opérationnelles exceptionnelles, après avoir obtenu l'approbation de leur autorité d'agrément cryptographique.

2. Dans les circonstances visées au paragraphe 1, les ICUE peuvent être transmises au moyen de produits cryptographiques agréés pour un niveau de classification inférieur ou sans faire l'objet d'un chiffrement avec le consentement de l'autorité compétente, dans le cas où un 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 ou le destinataire ne possède pas le dispositif de chiffrement nécessaire;

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

3. Les informations classifiées transmises dans les conditions visées au paragraphe 2 ne portent aucun marquage ni indication qui les distinguerait d'informations non classifiées ou pouvant être protégées à l'aide d'un produit cryptographique disponible. Leur destinataire est informé, sans délai et par d'autres moyens, du niveau de classification.

4. Un rapport ultérieur sur la transmission d'ICUE dans les circonstances visées au paragraphe 1 est soumis à l'autorité de sécurité compétente.

SECTION 6
SECURITE INDUSTRIELLE

Article 46

Principes de base

1. Chaque institution ou organe de l'Union, en tant qu'autorité contractante ou octroyant la subvention, veille à ce que les normes minimales de sécurité industrielle prévues dans la présente section et les conditions de protection des ICUE incluses dans les contrats classifiés et les conventions de subvention classifiées énoncées à l'annexe V, soient mentionnées ou intégrées dans les contrats ou conventions de subvention et respectées lors de l'octroi de contrats classifiés ou de conventions de subvention classifiées.

2. Par «sécurité industrielle», on entend l'application de mesures visant à assurer la protection des ICUE par les personnes ou entités suivantes:

   a) en gestion directe[30], dans le cadre de contrats classifiés, par:

      i) des candidats ou des soumissionnaires tout au long de la durée de la procédure d'appel d'offres et de passation de marché,

      ii) des contractants ou des sous-traitants tout au long du cycle de vie des contrats classifiés;

   b) en gestion directe[31], dans le cadre de conventions de subvention classifiées, par:

      i) des demandeurs durant les procédures d'octroi de subventions;

      ii) des bénéficiaires tout au long du cycle de vie des conventions de subvention classifiées;

   c) en gestion indirecte, dans le cadre des conventions-cadres de partenariat financier (ci-après les «CCPF») et des conventions de contribution connexes, par les entités chargées de l'exécution tout au long du cycle de vie de ces conventions.

3. En tant qu'entité confiant l'exécution, l'institution ou l'organe de l'Union décrit les impératifs de sécurité spécifiques incombant à l'entité chargée de l'exécution, dans le chapitre de la CCPF consacré à la sécurité et les conventions de contribution connexes. Ces impératifs sont fondés sur les principes et dispositions en matière de sécurité énoncés dans le présent règlement concernant les contrats classifiés et les conventions de subvention classifiées, qui s'appliquent mutatis mutandis.

4. De tels contrats ou conventions de subvention ne doivent pas concerner des informations classifiées TRÈS SECRET UE/EU TOP SECRET.

5. Les dispositions du présent chapitre visant des contrats classifiés ou des contractants, ou des subventions classifiées ou des bénéficiaires, s'appliquent également aux contrats de sous-traitance classifiés et aux sous-traitants au sens, respectivement, des contrats classifiés ou des subventions classifiées.

---

30 Règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil.

31 Idem.

6. Les institutions et organes de l'Union, en tant qu'autorités contractantes ou octroyant la subvention, coopèrent étroitement avec les autorités de sécurité ou toute autre autorité compétente du pays sur le territoire duquel la partie contractante ou le bénéficiaire de la subvention est enregistré, ainsi qu'avec l'autorité de sécurité ou toute autre autorité compétente de l'organisation internationale contractante ou bénéficiaire de la subvention.

7. Les institutions et organes de l'Union, en tant qu'autorités contractantes ou octroyant la subvention, communiquent avec les autorités de sécurité ou toute autre autorité compétente par l'intermédiaire de leurs autorités de sécurité.

8. Les institutions et organes de l'Union, en tant qu'autorités contractantes ou octroyant la subvention, notifient aux autorités visées au paragraphe 6, par l'intermédiaire de leur autorité de sécurité, chaque signature d'un contrat classifié ou d'une convention de subvention classifiée.

   Cette notification inclut les données pertinentes telles que les noms du contractant ou des bénéficiaires, la durée du contrat classifié ou de la convention de subvention classifiée, et le niveau maximal de classification.

   Les institutions et organes de l'Union, en tant qu'autorités contractantes ou octroyant la subvention, informent les autorités visées au paragraphe 6 de toute résiliation prématurée d'un contrat classifié ou d'une convention de subvention classifiée.

9. Les institutions et organes de l'Union, en tant qu'autorités contractantes ou octroyant la subvention, ne peuvent attribuer des contrats classifiés ou des parties classifiées de subventions qu'à des entités enregistrées dans les pays tiers ou établies par les organisations internationales ayant conclu un accord sur la sécurité des informations avec l'Union. Lorsque les ICUE concernées contiennent des données à caractère personnel, tout transfert de ces dernières vers un pays tiers ou une organisation internationale est effectué conformément au règlement (UE) 2018/1725.

Article 47

Aspects liés à la sécurité dans un contrat classifié ou une convention de subvention classifiée

1. Les contrats classifiés ou les conventions de subvention classifiées incluent les aspects suivants liés à la sécurité:

   a) un guide de classification de sécurité;

   b) une annexe de sécurité.

2. Les contrats classifiés ou les conventions de subvention classifiées peuvent inclure des instructions de sécurité relatives à un programme/un projet.

Article 48

Guide de classification de sécurité

1. Avant de signer un contrat classifié ou une convention de subvention classifiée, l'institution ou l'organe de l'Union, en tant qu'autorité contractante ou octroyant la subvention, détermine la classification de sécurité de toute information devant être créée par les contractants ou bénéficiaires ou par leurs sous-traitants. À cet effet, elle ou il prépare un guide de classification de sécurité à utiliser pour l'exécution du contrat classifié ou de la convention de subvention classifiée.

2. Le guide de classification de sécurité peut être modifié tout au long du cycle de vie du programme ou du projet, tel que visé à l'article 50, du contrat ou de la convention de subvention, et les éléments d'information peuvent être reclassifiés ou déclassés.

3. Les principes suivants sont appliqués pour déterminer le niveau de classification de sécurité des différents éléments d'un contrat classifié ou d'une convention de subvention classifiée:

a) dans le cadre de l'élaboration d'un guide de classification de sécurité, l'institution ou organe de l'Union, en tant qu'autorité contractante ou octroyant la subvention, tient compte de tous les aspects pertinents en matière de sécurité, y compris de la classification de sécurité attribuée aux informations fournies et dont l'utilisation aux fins du contrat classifié ou de la convention de subvention classifiée a été approuvée par l'autorité d'origine desdites informations;

b) le niveau général de classification du contrat classifié ou de la convention de subvention classifiée ne peut pas être inférieur à la classification la plus élevée de l'un de ses éléments;

c) le cas échéant, l'institution ou organe de l'Union concerné, en tant qu'autorité contractante ou octroyant la subvention, se met en rapport, par l'intermédiaire de son autorité de sécurité, avec les autorités de sécurité ou toute autre autorité compétente du pays concerné au moment de modifier le guide de classification de sécurité.

Article 49

Annexe de sécurité

1. Chaque institution ou organe de l'Union, en tant qu'autorité contractante ou octroyant la subvention, décrit les impératifs de sécurité spécifiques du contrat classifié ou de la convention de subvention classifiée dans une annexe de sécurité. Cette annexe inclut le guide de classification de sécurité et fait partie intégrante du contrat classifié, de la convention de subvention classifiée ou du contrat de sous-traitance classifié.

2. L'annexe de sécurité contient les dispositions imposant au contractant ou au bénéficiaire, ainsi qu'à leurs sous-traitants, de respecter les dispositions établies dans le présent règlement ainsi que toute disposition d'application complémentaire adoptée en vertu de l'article 8, paragraphe 2, concernant la sécurité industrielle. L'annexe de sécurité indique clairement que le non-respect de ces dispositions peut constituer un motif suffisant de résiliation du contrat classifié ou de la convention de subvention classifiée.

Article 50

Instructions de sécurité relatives à un programme/un projet

1. Les institutions et organes de l'Union, en tant qu'autorités contractantes ou octroyant la subvention, peuvent élaborer des instructions de sécurité relatives à un programme/un projet, en étroite coopération avec leurs autorités de sécurité, en particulier pour les programmes et les projets caractérisés par l'importance de leur portée, leur échelle ou leur complexité, ou par la multitude ou la diversité des contractants, bénéficiaires et autres partenaires et acteurs impliqués.

2. L'autorité de sécurité de chaque institution ou organe de l'Union, en tant qu'autorité contractante ou octroyant la subvention, soumet les instructions de sécurité relatives à un programme/un projet spécifique, pour avis, à l'organe consultatif en matière de sécurité de l'État membre concerné, qui se compose des autorités nationales de sécurité et/ou des autorités de sécurité désignées.

Lorsqu'une institution ou un organe de l'Union ne dispose pas d'un tel organe consultatif, il soumet les instructions de sécurité relatives à un programme/un projet au comité de sécurité de l'information visé à l'article 6, paragraphe 8.

SECTION 7
PARTAGE D'ICUE ET ECHANGE D'INFORMATIONS CLASSIFIEES

Article 51

Principes de base

1. L'ensemble des institutions et organes de l'Union peuvent partager des ICUE avec les autres institutions et organes de l'Union dans les conditions énoncées à l'article 54.

2. Les institutions et organes de l'Union peuvent partager des ICUE avec les États membres et la Communauté européenne de l'énergie atomique pour autant qu'ils protègent ces informations conformément au marquage de classification correspondant établi dans l'accord entre les États membres de l'Union européenne, réunis au sein du Conseil, relatif à la protection des informations classifiées échangées dans l'intérêt de l'Union européenne, et au tableau correspondant inclus à l'annexe VI du présent règlement.

3. Les institutions et organes de l'Union n'échangent des informations classifiées qu'avec les pays tiers ou organisations internationales avec lesquels un accord sur la sécurité des informations ou un arrangement administratif a été conclu conformément aux articles 55 et 56.

Ces accords et arrangements contiennent des dispositions pour garantir que les pays tiers ou les organisations internationales qui reçoivent des ICUE en assurent une protection conforme à leur niveau de classification et à des normes minimales qui ne sont pas moins strictes que celles prévues dans le présent règlement.

4. En l'absence d'accord sur la sécurité des informations ou d'arrangement administratif, l'institution ou l'organe de l'Union peut, dans des circonstances exceptionnelles, communiquer des ICUE à une autre organisation ou un autre organe de l'Union, à un pays tiers ou à une organisation internationale conformément à l'article 58.

5. Les institutions et organes de l'Union désignent les bureaux d'ordre qui servent de principaux points d'entrée et de sortie pour les ICUE partagées avec d'autres institutions ou organes de l'Union ou pour les informations classifiées échangées avec des pays tiers et des organisations internationales.

Article 52

Sous-groupe sur le partage d'ICUE et l'échange d'informations classifiées

1. Le sous-groupe sur le partage d'ICUE et l'échange d'informations classifiées visé à l'article 7, paragraphe 1, point e), assume les rôles et responsabilités suivants:

a) organiser des visites d'évaluation dans les institutions et organes de l'Union, les pays tiers et les organisations internationales, et arrêter le programme annuel des visites;

b) préparer et effectuer les visites d'évaluation;

c) élaborer un rapport sur les résultats des visites visées au point a).

Excepté dans les cas visés à l'article 56, paragraphe 2.

2. Le sous-groupe sur le partage d'ICUE et l'échange d'informations classifiées est composé de représentants de la Commission, du Conseil et du Service européen pour l'action extérieure et travaille par consensus.

Article 53

Visites d'évaluation relatives au partage d'ICUE

1. Le sous-groupe sur le partage d'ICUE et l'échange d'informations classifiées effectue des visites d'évaluation en coopérant pleinement avec les fonctionnaires de l'institution ou de l'organe de l'Union faisant l'objet de la visite. Il peut demander l'assistance de l'ANS sur le territoire de laquelle l'institution ou l'organe de l'Union est situé.

2. Les visites d'évaluation dans les institutions et organes de l'Union concernés servent aux fins suivantes:

a) vérifier si les exigences établies dans le présent règlement pour la protection des ICUE sont respectées, et, partant, si les mesures mises en œuvre sont efficaces;

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

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

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

3. À la fin de la visite d'évaluation, le sous-groupe sur le partage d'ICUE et l'échange d'informations classifiées exécute les tâches suivantes:

a) élaborer un rapport reprenant les principales conclusions de l'évaluation;

b) recueillir l'avis du comité de sécurité de l'information, visé à l'article 6, paragraphe 8, au sujet du rapport;

c) envoyer le rapport pour suivi à l'autorité de sécurité de l'institution ou de l'organe de l'Union ayant fait l'objet de la visite.

4. Lorsque le rapport propose une mesure corrective ou formule des recommandations, une visite de suivi est organisée afin de vérifier si la mesure a été prise ou si les recommandations ont été suivies.

Article 54

Partage d'ICUE

1. Une institution ou un organe de l'Union peut partager des ICUE avec une autre institution ou un autre organe de l'Union lorsque les conditions suivantes sont réunies:

   a) la nécessité de l'échange a été démontrée;

   b) une visite d'évaluation a été effectuée auprès de l'institution ou de l'organe de l'Union concerné, conformément à l'article 53, et les résultats de cette visite attestent de la capacité de ladite institution ou dudit organe à traiter et stocker un niveau donné d'ICUE;

   c) l'autorité de sécurité de l'institution ou de l'organe de l'Union concerné décide que cette institution ou cet organe peut partager des informations classifiées jusqu'à un niveau déterminé avec d'autres institutions et organes de l'Union ayant été certifiés de la même manière.

2. Le secrétariat du groupe de coordination établit une liste des niveaux d'ICUE qui peuvent être traités et stockés par chaque institution ou organe de l'Union répondant aux conditions visées au paragraphe 1, points b) et c). Il met régulièrement cette liste à jour.

Article 55

Accords sur la sécurité des informations

1. Lorsqu'un échange à long terme d'informations classifiées avec un pays tiers ou une organisation internationale est nécessaire, l'institution ou l'organe de l'Union compétent cherche à négocier et conclure un accord sur la sécurité des informations, conformément à l'article 218 du traité sur le fonctionnement de l'Union européenne.

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

3. Les accords sur la sécurité des informations prévoient des modalités techniques d'application qui doivent être arrêtées d'un commun accord entre les autorités de sécurité compétentes des institutions et organes de l'Union concernés et l'autorité de sécurité compétente du pays tiers ou de l'organisation internationale concerné(e).

4. Préalablement à l'approbation des modalités techniques d'application, visées au paragraphe 3, le sous-groupe sur le partage d'ICUE et l'échange d'informations classifiées procède à une visite d'évaluation conformément à l'article 57.

Article 56

Coopération avec des pays tiers et des organisations internationales

1. Lorsque leurs règlements intérieurs ou leurs actes fondateurs prévoient une telle possibilité, les institutions et organes de l'Union peuvent conclure un arrangement administratif avec leurs homologues de pays tiers ou d'organisations internationales, après en avoir informé le sous-groupe sur le partage d'ICUE et l'échange d'informations classifiées, lorsque les conditions suivantes sont remplies:

   a) l'institution ou l'organe de l'Union concerné doit échanger de manière durable des informations classifiées qui, en général, ne dépassent pas le niveau RESTREINT UE/EU RESTRICTED avec son homologue d'un pays tiers ou d'une organisation internationale;

b) l'institution ou l'organe de l'Union concerné satisfait aux conditions énoncées à l'article 54, paragraphe 1;

c) le rapport de la visite d'évaluation, visé à l'article 57, atteste que l'homologue concerné du pays tiers ou de l'organisation internationale concerné(e) a la capacité de traiter et de stocker un niveau donné d'ICUE.

2. Avant de conclure un arrangement administratif, une visite d'évaluation est effectuée conformément aux principes établis à l'article 57. L'institution ou l'organe de l'Union qui sollicite l'arrangement administratif peut demander au sous-groupe sur le partage d'ICUE de procéder à la visite d'évaluation pour son compte ou de participer à la visite.

3. L'autorité de sécurité de l'institution ou de l'organe de l'Union sollicitant l'arrangement administratif détermine les conditions particulières régissant l'échange ainsi que le niveau maximal de classification des ICUE qui peuvent être échangées. Ce niveau ne doit pas dépasser celui établi pour le partage d'ICUE avec d'autres institutions et organes de l'Union, conformément à l'article 54, et, le cas échéant, ne devrait pas être supérieur à celui prévu dans le cadre d'un accord sur la sécurité des informations conclu avec le même pays tiers ou la même organisation internationale.

Article 57

Visites d'évaluation pour l'échange d'informations classifiées avec des pays tiers et des organisations internationales

1. Une visite d'évaluation dans un pays tiers ou une organisation internationale est effectuée afin de déterminer si une institution ou un organe de l'Union peut échanger des informations classifiées avec le pays tiers ou l'organisation internationale concerné(e).

2. L'objectif de la visite d'évaluation est d'évaluer l'efficacité des règles et procédures de sécurité dans le pays tiers ou l'organisation internationale concerné(e) pour ce qui est de la protection des ICUE au niveau requis. La visite d'évaluation est effectuée d'un commun accord avec le pays tiers ou l'organisation internationale concerné(e).

3. Les visites d'évaluation portent au moins sur les aspects suivants:

a) le cadre réglementaire applicable à la protection des informations classifiées et son adéquation pour la protection des ICUE au niveau requis;

b) tous les aspects spécifiques de la politique de sécurité et du mode d'organisation de la sécurité dans le pays tiers ou l'organisation internationale susceptibles d'avoir une incidence sur le niveau des informations classifiées qui peuvent être échangées;

c) les mesures et les procédures de sécurité effectivement en place;

d) les procédures d'habilitation de sécurité relatives au niveau d'ICUE à communiquer.

4. Le comité de sécurité de l'information visé à l'article 6, paragraphe 8, reçoit un rapport sur les conclusions de ces visites avant que les ICUE soient effectivement transmises au pays tiers ou à l'organisation internationale concerné(e). Le cas échéant, le rapport est également communiqué à l'institution ou à l'organe de l'Union concerné.

5. Les autorités de sécurité compétentes de l'institution ou de l'organe de l'Union concerné notifient au pays tiers ou à l'organisation internationale la date à compter de laquelle l'institution ou l'organe sera en mesure d'échanger des ICUE ainsi que le niveau maximal de classification des ICUE qui peuvent faire l'objet d'un échange sur support papier ou par voie électronique.

6. Des visites de suivi sont organisées lorsque les conditions suivantes sont réunies:

   a) il est nécessaire de relever le niveau des ICUE pouvant être échangées;

   b) l'institution ou l'organe de l'Union concerné a été informé de modifications fondamentales des dispositions de sécurité du pays tiers ou de l'organisation internationale susceptibles d'avoir un effet sur la manière dont les ICUE sont protégées;

   c) un incident grave pour la sécurité de l'information a eu lieu, impliquant la divulgation non autorisée d'ICUE.

Article 58

Communication ad hoc exceptionnelle d'ICUE

1. En l'absence d'accord sur la sécurité des informations ou d'arrangement administratif, lorsqu'une institution ou un organe de l'Union décide qu'il est nécessaire, à titre exceptionnel, de communiquer des ICUE à une autre institution ou un autre organe de l'Union ou à un pays tiers ou une organisation internationale, ou

   lorsqu'un accord sur la sécurité des informations ou un arrangement administratif a été conclu et qu'une institution ou un organe de l'Union décide qu'il est nécessaire, à titre exceptionnel, de communiquer des ICUE d'un niveau supérieur à celui déjà déterminé dans l'accord ou l'arrangement, l'institution ou l'organe de l'Union fournissant des ICUE prend les mesures suivantes:

   a) dans la mesure du possible, elle ou il vérifie auprès des autorités de sécurité du pays tiers, de l'organisation internationale ou de l'institution ou de l'organe de l'Union destinataire que leurs règles, structures et procédures de sécurité sont à même de garantir la protection des ICUE communiquées conformément à des normes qui ne sont pas moins strictes que celles prévues dans le présent règlement;

   b) elle ou il demande un avis du comité de sécurité de l'information, visé à l'article 6, paragraphe 8, sur la base de la vérification effectuée conformément au point a), à moins que des circonstances opérationnelles ne nécessitent une communication ad hoc immédiate, auquel cas le comité de sécurité de l'information est informé ultérieurement.

2. Tous les documents communiqués conformément au présent article portent un timbre d'autorisation de divulgation indiquant le pays tiers, l'organisation internationale ou l'institution ou l'organe de l'Union auquel ils ont été communiqués.

3. Avant la communication effective ou au moment de celle-ci, l'institution ou l'organe de l'Union fournissant des ICUE demande à la partie destinataire de s'engager par écrit à protéger les ICUE qui lui sont transmises. Le cas échéant, le destinataire est invité à s'engager à protéger les ICUE conformément aux principes de base et aux normes minimales énoncés dans le présent règlement.

Chapitre 6
Dispositions finales

Article 59

Mise en œuvre

1. Le groupe de coordination élabore des orientations sur la sécurité de l'information aux fins de la mise en œuvre du présent règlement.

2. En fonction de leurs besoins particuliers, les institutions et organes de l'Union peuvent adopter des règles internes aux fins de la mise en œuvre du présent règlement, conformément à l'article 8, paragraphe 2.

Article 60

Dispositions transitoires

1. Les règles internes en matière de sécurité de l'information adoptées par une institution ou un organe de l'Union donné avant le [jj/mm/aaaa date d'application] sont révisées au plus tard [trois ans après l'entrée en vigueur du présent règlement].

2. L'ensemble des institutions et organes de l'Union ayant fait l'objet d'une évaluation de la Commission, du Conseil ou du SEAE avant le [jj/mm/aaaa date d'applicabilité] ayant débouché sur la constatation de leur capacité à traiter et à stocker des ICUE sont réputés remplir les conditions visées à l'article 19, paragraphe 1.

3. Tout arrangement administratif conclu par les institutions et organes de l'Union avec des pays tiers et des organisations internationales avant le [jj/mm/aaaa date d'application] demeure valable.

4. Lorsque les États membres sur le territoire desquels les bénéficiaires de la convention de subvention de la Commission au titre du programme européen de développement industriel dans le domaine de la défense ont décidé de mettre en place un cadre de sécurité spécifique pour la protection et le traitement d'informations classifiées nationales relatives à la convention de subvention concernée, la Commission, au moment d'appliquer les procédures de sécurité industrielle établies dans le présent règlement, respecte ledit cadre de sécurité jusqu'à la fin du cycle de vie de la convention de subvention.

Article 61

Suivi et évaluation

1. Au plus tard pour le [jj/mm/aaaa, trois ans après la date d'application], la Commission présente un rapport sur la mise en œuvre du présent règlement au Parlement européen et au Conseil.

2. Au plus tôt [cinq ans après la date d'application], puis tous les cinq ans par la suite, la Commission procède à une évaluation du présent règlement et présente un rapport sur ses principales conclusions au Parlement européen et au Conseil.

Article 62

Entrée en vigueur et application

1. Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

2. Il est applicable à partir du [date: le premier jour du mois suivant la période de deux ans à compter de sa date d'entrée en vigueur].

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président*
[...]	*[...]*

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

1.2. Domaine(s) politique(s) concerné(s)

1.3. La proposition/l'initiative est relative à:

1.4. Objectif(s)

1.4.1. Objectif général/objectifs généraux

1.4.2. Objectif(s) spécifique(s)

1.4.3. Résultat(s) et incidence(s) attendus

1.4.4. Indicateurs de performance

1.5. Justifications de la proposition/de l'initiative

1.5.1. Besoin(s) à satisfaire à court ou à long terme, assorti(s) d'un calendrier détaillé pour la mise en œuvre de l'initiative

1.5.2. Valeur ajoutée de l'intervention de l'Union (celle-ci peut résulter de différents facteurs, par exemple gains de coordination, sécurité juridique, efficacité accrue, complémentarités, etc.). Aux fins du présent point, on entend par «valeur ajoutée de l'intervention de l'Union» la valeur découlant de l'intervention de l'Union qui vient s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres.

1.5.3. Leçons tirées d'expériences similaires

1.5.4. Compatibilité avec le cadre financier pluriannuel et synergies éventuelles avec d'autres instruments appropriés

1.5.5. Évaluation des différentes possibilités de financement disponibles, y compris des possibilités de redéploiement

1.6. Durée et incidence financière de la proposition/de l'initiative

1.7. Mode(s) de gestion prévu(s)

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

2.2. Système(s) de gestion et de contrôle

2.2.1. Justification du (des) mode(s) de gestion, du (des) mécanisme(s) de mise en œuvre des financements, des modalités de paiement et de la stratégie de contrôle proposée

2.2.2. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer

2.2.3. Estimation et justification du rapport coût/efficacité des contrôles (rapport «coûts du contrôle ÷ valeur des fonds gérés concernés»), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)

2.3. Mesures de prévention des fraudes et irrégularités

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

3.2. Incidence financière estimée de la proposition sur les crédits

3.2.1. Synthèse de l'incidence estimée sur les crédits opérationnels

3.2.2. Estimation des réalisations financées avec des crédits opérationnels

3.2.3. Synthèse de l'incidence estimée sur les crédits administratifs

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

3.2.5. Participation de tiers au financement

3.3. Incidence estimée sur les recettes

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à la sécurité de l'information dans les institutions, organes et organismes de l'Union

1.2. Domaine(s) politique(s) concerné(s)

Administration publique européenne

Les règles des institutions et organes de l'Union en matière de sécurité de l'information devraient, dans leur ensemble, constituer un cadre général complet et cohérent au niveau de l'administration européenne, ayant pour objet d'assurer la protection des informations et l'équivalence des principes de base et normes minimales. Le niveau de protection des informations devrait également être équivalent dans toutes les institutions et tous les organes de l'Union.

1.3. La proposition/l'initiative est relative à:

☑une action nouvelle

☐ une action nouvelle suite à un projet pilote/une action préparatoire[32]

☐ la prolongation d'une action existante

☐ une fusion ou une réorientation d'une ou de plusieurs actions vers une autre action/une action nouvelle

1.4. Objectif(s)

1.4.1. Objectif général/objectifs généraux

L'objectif général de l'initiative est de créer des règles en matière de sécurité de l'information pour l'ensemble des institutions et des organes de l'Union dans le but d'assurer une protection renforcée et cohérente contre l'évolution des menaces qui pèsent sur leurs informations.

1.4.2. Objectif(s) spécifique(s)

• OS 1: définir des catégories d'informations exhaustives et harmonisées, ainsi que des exigences en matière de traitement communes à toutes les informations traitées par l'administration européenne, et faciliter des échanges d'informations sécurisés entre les institutions et organes de l'Union, tout en réduisant au minimum l'incidence sur les États membres.

• OS 2: veiller à ce que toutes les institutions et tous les organes de l'Union détectent les éventuelles failles de sécurité dans leurs processus et mettent en œuvre les mesures nécessaires pour assurer des conditions équitables en matière de sécurité de l'information.

• OS 3: établir un système rationalisé de coopération entre les institutions et organes de l'Union dans le domaine de la sécurité de l'information, capable de favoriser une

[32] Tel(le) que visé(e) à l'article 58, paragraphe 2, point a) ou b), du règlement financier.

culture cohérente de la sécurité de l'information dans l'ensemble de l'administration européenne.

• OS 4: moderniser les politiques en matière de sécurité de l'information à tous les niveaux de classification/de catégorisation, pour l'ensemble des institutions et organes de l'Union, en tenant compte de la transition numérique et du développement du télétravail en tant que pratique structurelle.

1.4.3. Résultat(s) et incidence(s) attendus

Préciser les effets que la proposition/l'initiative devrait avoir sur les bénéficiaires/la population visée.

La proposition aura les effets suivants sur les institutions et organes de l'Union:

– révision de leurs règles et procédures internes afin de les adapter au règlement;

– catégorisation de toutes les informations traitées conformément au système établi par le règlement;

– garantie que leurs systèmes d'information et de communication soient conformes aux exigences établies dans le règlement;

– participation au groupe de coordination interinstitutionnelle de la sécurité de l'information (ci-après le «groupe de coordination»).

Les États membres bénéficieront du présent règlement étant donné que la coopération avec les institutions et organes de l'Union dans tous les domaines pertinents (sécurité du personnel, sécurité industrielle ou partage d'informations) reposera sur les mêmes notions, règles et procédures.

1.4.4. Indicateurs de performance

Préciser les indicateurs permettant de suivre l'avancement et les réalisations.

Indicateurs pertinents pour l'objectif spécifique nº 1

– Adoption de lignes directrices appropriées

– Application de nouveaux marquages

– Publication d'instructions de traitement mises à jour pour toutes les catégories d'informations

– Mise en œuvre de systèmes communs traitant des informations sensibles non classifiées et des ICUE

Indicateurs pertinents pour l'objectif spécifique nº 2

– Nombre de recommandations formulées/mises en œuvre

– Nombre de fuites d'informations dans les institutions et organes

Indicateurs pertinents pour l'objectif spécifique nº 3

– Statistiques sur les marchés centralisés par rapport aux marchés locaux

– Rapports d'inspection

– Nombre de demandes traitées par le secrétariat du groupe de coordination de la sécurité de l'information

Indicateurs pertinents pour l'objectif spécifique nº 4

– Nombre d'utilisateurs suivant une formation

– Niveau de connaissance des règles en matière de sécurité de l'information par le personnel

– Pourcentage du personnel autorisé à travailler avec du matériel de télétravail sécurisé

1.5. Justifications de la proposition/de l'initiative

1.5.1. Besoin(s) à satisfaire à court ou à long terme, assorti(s) d'un calendrier détaillé pour la mise en œuvre de l'initiative

La mise en œuvre de la présente initiative sera effectuée selon une approche progressive, comme suit:

– 2022/2023: adoption du règlement, entrée en vigueur

– 2024/2025: révision par l'ensemble des institutions et organes de l'Union de leurs règles internes en matière de sécurité de l'information en vue de les adapter au règlement

– 2025: travail organisationnel en vue de la création du groupe de coordination et de son secrétariat, ainsi que des sous-groupes techniques

– 2024/2025: entrée en application du règlement

– 2025/2026: adoption du règlement intérieur du groupe de coordination et des sous-groupes techniques

– 2026/2028: travaux en vue d'élaborer des documents d'orientation destinés à faciliter la mise en œuvre du règlement, échange de bonnes pratiques entre les institutions et organes

– 2029/2030: préparation de la première évaluation du règlement (tous les cinq ans à partir de la date d'entrée en application)

– 2030: première évaluation du règlement

1.5.2. Valeur ajoutée de l'intervention de l'Union (celle-ci peut résulter de différents facteurs, par exemple gains de coordination, sécurité juridique, efficacité accrue, complémentarités, etc.). Aux fins du présent point, on entend par «valeur ajoutée de l'intervention de l'Union» la valeur découlant de l'intervention de l'Union qui vient s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres.

L'initiative contribue à garantir que les institutions et organes de l'Union soient assistés dans l'exercice de leur mission par une administration ouverte, efficace et indépendante.

Elle vient s'ajouter aux efforts généraux déployés au niveau national par les États membres dans le domaine de la sécurité de l'Union en protégeant les institutions et organes contre les ingérences extérieures et les activités d'espionnage.

1.5.3. Leçons tirées d'expériences similaires

s.o.

1.5.4. Compatibilité avec le cadre financier pluriannuel et synergies éventuelles avec d'autres instruments appropriés

Le projet nécessite la réaffectation/l'affectation de deux ETP au secrétariat du groupe de coordination de la sécurité de l'information.

D’autres projets, tels que l’élaboration d’outils communs et la centralisation de certaines activités, sont déjà partiellement en cours et couverts par des accords de niveau de service et des contrats-cadres.

1.5.5. Évaluation des différentes possibilités de financement disponibles, y compris des possibilités de redéploiement

Veuillez vous référer à la question précédente.

1.6. Durée et incidence financière de la proposition/de l'initiative

☐ **durée limitée**

– ☐ en vigueur à partir du [JJ/MM]AAAA jusqu'en/au [JJ/MM]AAAA

– ☐ Incidence financière de AAAA jusqu'en AAAA pour les crédits d'engagement et de AAAA jusqu'en AAAA pour les crédits de paiement.

– ☑ **durée illimitée**

1.7. Mode(s) de gestion prévu(s)[33]

☑ **Gestion directe** par la Commission et par chaque institution et organe de l'Union

– ☑ dans ses services, y compris par l'intermédiaire de son personnel dans les délégations de l'Union;

– ☐ par les agences exécutives

☐ **Gestion partagée** avec les États membres

☐ **Gestion indirecte** en confiant des tâches d'exécution budgétaire:

– ☐ à des pays tiers ou aux organismes qu'ils ont désignés;

– ☐ à des organisations internationales et à leurs agences (à préciser);

– ☐ à la BEI et au Fonds européen d'investissement;

– ☐ aux organismes visés aux articles 70 et 71 du règlement financier;

– ☐ à des organismes de droit public;

– ☐ à des organismes de droit privé investis d'une mission de service public, pour autant qu'ils présentent les garanties financières suffisantes;

– ☐ à des entités de droit privé d'un État membre qui sont chargées de la mise en œuvre d'un partenariat public-privé et dotées de garanties financières suffisantes;

– ☐ à des personnes chargées de l'exécution d'actions spécifiques relevant de la PESC, en vertu du titre V du traité sur l'Union européenne, identifiées dans l'acte de base concerné.

– *Si plusieurs modes de gestion sont indiqués, veuillez donner des précisions dans la partie «Remarques».*

Remarques

[33] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Préciser la fréquence et les conditions de ces dispositions.

Le règlement fera l'objet d'une évaluation tous les cinq ans et la Commission rendra compte de ses conclusions au Conseil et au Parlement européen.

2.2. Système(s) de gestion et de contrôle

2.2.1. Justification du (des) mode(s) de gestion, du (des) mécanisme(s) de mise en œuvre des financements, des modalités de paiement et de la stratégie de contrôle proposée

Le règlement établit des règles en matière de sécurité de l'information applicables à l'ensemble des institutions et des organes de l'Union. Le suivi de sa mise en œuvre adéquate sera effectué au moyen d'un groupe de coordination auquel participeront toutes les autorités de sécurité des institutions et organes.

La sécurité continue à relever de la pleine responsabilité de l'autorité de sécurité de chaque institution ou organe, et est soumise au cadre de contrôle interne existant au sein de chaque institution ou organe.

2.2.2. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer

Le règlement créera une base de règles en matière de sécurité de l'information et assurera la transparence des mesures de sécurité adoptées pour les échanges d'informations entre les institutions et organes de l'Union; ce faisant, il réduira les risques liés à la sécurité de l'information à tous les niveaux.

Le règlement est conforme aux standards de contrôle interne et inclut une approche de l'élaboration des politiques fondée sur les risques.

2.2.3. Estimation et justification du rapport coût/efficacité des contrôles (rapport «coûts du contrôle ÷ valeur des fonds gérés concernés»), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)

Les mécanismes de contrôle existants pour les institutions et organes seront applicables. La conformité avec le règlement et les risques liés à la sécurité de l'information devraient être indiqués dans les rapports annuels des institutions et des organes sur les risques.

2.3. Mesures de prévention des fraudes et irrégularités

Préciser les mesures de prévention et de protection existantes ou envisagées, au titre de la stratégie antifraude par exemple.

S.O.

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

- Lignes budgétaires existantes

Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Type de dépense	Participation			
	Numéro	CD/CND[34]	de pays AELE[35]	de pays candidats[36]	de pays tiers	au sens de l'article 21, paragraphe 2, point b), du règlement financier
H7	20 01 02 01	CND	S.O.	S.O.	S.O.	S.O.

- Nouvelles lignes budgétaires, dont la création est demandée

Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Type de dépense	Participation			
	Numéro	CD/CND	de pays AELE	de pays candidats	de pays tiers	au sens de l'article 21, paragraphe 2, point b), du règlement financier
	Néant		OUI/NON	OUI/NON	OUI/NON	OUI/NON

34 CD = crédits dissociés/CND = crédits non dissociés.
35 AELE: Association européenne de libre-échange.
36 Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

3.2. Incidence financière estimée de la proposition sur les crédits

3.2.1. Synthèse de l'incidence estimée sur les crédits opérationnels

– ☑ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

– ☐ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

Rubrique du cadre financier pluriannuel	Numéro	

DG: <…….>			Année **N**[37]	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (voir point 1.6)			**TOTAL**
• Crédits opérationnels										
Ligne budgétaire[38]	Engagements	1a								
	Paiements	2a								
Ligne budgétaire	Engagements	1b								
	Paiements	2b								
Crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques[39]										
Ligne budgétaire		3)								
TOTAL des crédits TOTAL DG <…….>	Engagements	=1a+1b +3								
	Paiements	=2a+2b +3								

37 L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative. Veuillez remplacer «N» par la première année de mise en œuvre prévue (par exemple: 2021). Procédez de la même façon pour les années suivantes.

38 Selon la nomenclature budgétaire officielle.

39 Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

• TOTAL des crédits opérationnels	Engagements	4)								
	Paiements	5)								
• TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques		6)								
TOTAL des crédits pour la RUBRIQUE <….> du cadre financier pluriannuel	Engagements	=4+ 6								
	Paiements	=5+ 6								

Si plusieurs rubriques opérationnelles sont concernées par la proposition/l'initiative, dupliquer la section qui précède:

• TOTAL des crédits opérationnels (toutes les rubriques opérationnelles)	Engagements	4)								
	Paiements	5)								
TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques (toutes les rubriques opérationnelles)		6)								
TOTAL des crédits pour les RUBRIQUES 1 à 6 du cadre financier pluriannuel (montant de référence)	Engagements	=4+ 6								
	Paiements	=5+ 6								

Rubrique du cadre financier pluriannuel	7	«Dépenses administratives»

Cette partie est à compléter en utilisant les «données budgétaires de nature administrative», à introduire d'abord dans l'annexe de la fiche financière législative (annexe V des règles internes), à charger dans DECIDE pour les besoins de la consultation interservices.

En Mio EUR (à la 3e décimale)

		Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
DG: HR							
• Ressources humaines		0,314	0,314	0,314	0,314	0,314	**1,570**
• Autres dépenses administratives							
TOTAL DG <…….>	Crédits	0,314	0,314	0,314	0,314	0,314	**1,570**

TOTAL des crédits pour la RUBRIQUE 7 du cadre financier pluriannuel	(Total engagements = Total paiements)	0,314	0,314	0,314	0,314	0,314	**1,570**

En EUR (à la 3e décimale)

		Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
TOTAL des crédits pour les RUBRIQUES 1 à 7 du cadre financier pluriannuel	Engagements	0,314	0,314	0,314	0,314	0,314	**1,570**
	Paiements	0,314	0,314	0,314	0,314	0,314	**1,570**

3.2.2. Estimation des réalisations financées avec des crédits opérationnels

Crédits d'engagement en Mio EUR (à la 3e décimale)

Indiquer les objectifs et les réalisations ⇩			Année **N**		Année **N+1**		Année **N+2**		Année **N+3**		Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (voir point 1.6)						**TOTAL**	
	RÉALISATIONS																	
	Type[40]	Coût moyen	N°	Coût	N°	Coût	N°	Coût	N°	Coût	N°	Coût	N°	Coût	N°	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 1[41]...																		
- Réalisation																		
- Réalisation																		
- Réalisation																		
Sous-total objectif spécifique nº 1																		
OBJECTIF SPÉCIFIQUE nº 2…																		
- Réalisation																		
Sous-total objectif spécifique nº 2																		
TOTAUX																		

[40] Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

[41] Tel que décrit au point 1.4.2. «Objectif(s) spécifique(s)…»

3.2.3. *Synthèse de l'incidence estimée sur les crédits administratifs*

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

– ☑ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
RUBRIQUE 7 du cadre financier pluriannuel						
Ressources humaines	0,314	0,314	0,314	0,314	0,314	**1,570**
Autres dépenses administratives						
Sous-total RUBRIQUE 7 du cadre financier pluriannuel	0,314	0,314	0,314	0,314	0,314	**1,570**

Hors RUBRIQUE 7[42] du cadre financier pluriannuel						
Ressources humaines						
Autres dépenses de nature administrative						
Sous-total hors RUBRIQUE 7 du cadre financier pluriannuel						

TOTAL	0,314	0,314	0,314	0,314	0,314	**1,570**

Les besoins en crédits pour les ressources humaines et les autres dépenses de nature administrative seront couverts par les crédits de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

[42] Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

3.2.3.1. Besoins estimés en ressources humaines

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

– ☑ La proposition/l'initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après:

Estimation à exprimer en équivalents temps plein

		Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**
20 01 02 01 (au siège et dans les bureaux de représentation de la Commission)		2	2	2	2	2
20 01 02 03 (en délégation)						
01 01 01 01 (recherche indirecte)						
01 01 01 11 (recherche directe)						
Autres lignes budgétaires (à spécifier)						
20 02 01 (AC, END, INT de l'enveloppe globale)						
20 02 03 (AC, AL, END, INT et JPD dans les délégations)						
XX 01 xx **yy zz** [43]	- au siège					
	- en délégation					
01 01 01 02 (AC, END, INT sur recherche indirecte)						
01 01 01 12 (AC, END, INT sur recherche directe)						
Autres lignes budgétaires (à spécifier)						
TOTAL		**2**	**2**	**2**	**2**	**2**

XX est le domaine politique ou le titre concerné.

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

Description des tâches à effectuer:

Fonctionnaires et agents temporaires	Secrétariat du groupe de coordination de la sécurité de l'information: 1 fonctionnaire AD + 1 fonctionnaire AST
Personnel externe	

[43] Sous-plafond de personnel externe financé sur crédits opérationnels (anciennes lignes «BA»).

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

La proposition/l'initiative:

– ☑ peut être intégralement financée par voie de redéploiement au sein de la rubrique concernée du cadre financier pluriannuel (CFP).

La proposition nécessite l'allocation de deux membres du personnel au secrétariat permanent du groupe de coordination interinstitutionnellle, établi au sein de l'unité HR.DS.

– ☐ nécessite l'utilisation de la marge non allouée sous la rubrique correspondante du CFP et/ou le recours aux instruments spéciaux comme le prévoit le règlement CFP.

Expliquez le besoin, en précisant les rubriques et lignes budgétaires concernées, les montants correspondants et les instruments dont le recours est proposé.

– ☐ nécessite une révision du CFP.

Expliquez le besoin, en précisant les rubriques et lignes budgétaires concernées et les montants correspondants.

3.2.5. Participation de tiers au financement

La proposition/l'initiative:

– ☑ ne prévoit pas de cofinancement par des tierces parties

– ☐ prévoit le cofinancement par des tierces parties estimé ci-après:

Crédits en Mio EUR (à la 3e décimale)

	Année **N**[44]	Année **N+1**	Année **N+2**	Année **N+3**	Total
Préciser l'organisme de cofinancement					
TOTAL crédits cofinancés					

Remarque: la proposition intensifiera les coopérations actuelles en matière de sécurité de l'information au moyen d'accords de niveau de service.

[44] L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative. Veuillez remplacer «N» par la première année de mise en œuvre prévue (par exemple: 2021). Procédez de la même façon pour les années suivantes.

3.3. Incidence estimée sur les recettes

– ☑ La proposition/l'initiative est sans incidence financière sur les recettes.

– ☐ La proposition/l'initiative a une incidence financière décrite ci-après:

☐ sur les ressources propres

☐ sur les autres recettes

veuillez indiquer si les recettes sont affectées à des lignes de dépenses☐

En Mio EUR (à la 3e décimale)

Ligne budgétaire de recettes:	Montants inscrits pour l'exercice en cours	Incidence de la proposition/de l'initiative[45]			
		Année **N**	Année **N+1**	Année **N+2**	Année **N+3**

Pour les recettes affectées, préciser la (les) ligne(s) budgétaire(s) de dépenses concernée(s).

Autres remarques (relatives, par exemple, à la méthode/formule utilisée pour le calcul de l'incidence sur les recettes ou toute autre information).

[45] En ce qui concerne les ressources propres traditionnelles (droits de douane et cotisations sur le sucre), les montants indiqués doivent être des montants nets, c'est-à-dire des montants bruts après déduction de 20 % de frais de perception.