Journal officiel
de l'Union européenne

FR
Série L

2024/1418

24.5.2024

Décision déléguée nº 19/2024 fixant les modalités d'application relatives au traitement des informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET

LE COMITÉ ADMINISTRATIF DE LA COUR DES COMPTES EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 287,

vu la décision nº 41/2021 de la Cour des comptes concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (ICUE) ([1]), ci-après la «décision nº 41/2021»,

vu la politique actuelle de sécurité de l'information de la Cour (DEC 127/15 FINAL) et sa politique de classification des informations (communication au personnel nº 123/20) ([2]),

vu les discussions du comité administratif lors de sa réunion du 18 mars 2024,

considérant que la décision nº 41/2021 s'applique à tous les services de la Cour des comptes et dans l'ensemble des locaux de celle-ci;

considérant que la décision nº 41/2021 dispose en son article 1er, paragraphe 3, que des arrangements seront conclus pour que les agents de la Cour des comptes devant accéder à des ICUE de niveaux de classification supérieurs puissent le faire dans des locaux appropriés d'autres institutions, agences ou organes de l'UE;

considérant que la décision nº 41/2021 dispose en son article 1er, paragraphe 3, et son article 5, paragraphe 6, que Cour des comptes peut conclure un accord de service avec une autre institution de l'Union au Luxembourg pour pouvoir traiter et stocker des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur dans une zone sécurisée de cette institution et qu'un protocole d'accord a été signé avec la direction générale des ressources humaines et de la sécurité de la Commission le 25 septembre 2023 concernant l'utilisation de la zone sécurisée de la DG à Luxembourg;

considérant que les mesures de sécurité pour la protection des informations classifiées de l'Union européenne (ICUE) tout au long de leur cycle de vie doivent être proportionnées, en particulier à leur classification de sécurité;

considérant que les mesures de sécurité visant à protéger la confidentialité, l'intégrité et la disponibilité des informations transmises à la Cour des comptes doivent être appropriées à la nature et au type d'informations concernés;

considérant que la décision nº 41/2021 dispose en son article 3, paragraphe 3, que l'ensemble des ICUE sont protégées par des mesures de sécurité physique et que les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont en outre protégées par des mesures de sécurité concernant le personnel;

considérant que la décision nº 41/2021 dispose en son article 10, paragraphe 10, que le comité administratif adopte une décision déléguée en fixant les modalités d'application; qu'en vertu des articles 8, paragraphe 1, et 10, paragraphe 1, de la décision nº 41/2021, ces modalités concernent des questions telles que le traitement et le stockage des ICUE ainsi que les infractions à la sécurité;

considérant que la Cour des comptes s'est assurée, par la décision nº 41/2021, que ses mesures de sécurité visant à garantir aux ICUE un haut niveau de protection sont équivalentes à celles arrêtées dans les règles en matière de protection de ces informations adoptées par les autres institutions, agences et organes de l'Union;

considérant qu'un arrangement administratif allégé entre la Cour des comptes et la Commission, le Conseil et le SEAE est entré en vigueur le 27 janvier 2023,

([1]) JO L 256 du 19.7.2021, p. 106.
([2]) Disponible sur la page https://www.eca.europa.eu/fr/Pages/LegalFramework.aspx.

DÉCIDE:

CHAPITRE 1

DISPOSITIONS GÉNÉRALES

Article premier

Objet et champ d'application

1. La présente décision établit les conditions de traitement des informations classifiées de l'Union européenne (ICUE) de niveau CONFIDENTIEL UE/EU CONFIDENTIAL ([3]) et SECRET UE/EU SECRET ([4]), conformément à la décision n° 41/2021 de la Cour des comptes.

2. La présente décision s'applique à tous les services de la Cour des comptes et dans l'ensemble des locaux de celle-ci. Elle s'applique également à ses chambres et comités, qui sont inclus dans le terme «services» aux fins de la présente décision.

Article 2

Critères d'accès aux informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET

1. L'accès aux informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET peut être accordé:

a) après avoir établi la nécessité pour une personne d'accéder à certaines informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET en vue d'exercer une fonction ou une tâche professionnelle pour la Cour des comptes;

b) après avoir informé la personne des règles ainsi que des normes et lignes directrices correspondantes en matière de sécurité pour la protection des informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET;

c) après que la personne a reconnu, par écrit, les responsabilités qui lui incombent en matière de protection des informations concernées;

d) après que la personne s'est vu accorder une habilitation de sécurité et une autorisation d'accès par le directeur des Ressources humaines, finances et services généraux de la Cour des comptes jusqu'au niveau correspondant et jusqu'à une date déterminée, conformément à l'article 4, paragraphe 4, de la décision n° 41/2021.

2. Il ne peut être confié aux stagiaires de la Cour des comptes des tâches qui leur imposent d'avoir accès aux informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

3. L'accès est refusé ou accordé aux autres catégories de personnel conformément au tableau figurant à l'annexe.

([3]) Conformément à l'article 1er, paragraphe 2, point a) de la décision n° 41/2021, on entend par informations CONFIDENTIEL UE/EU CONFIDENTIAL les «informations et matériels dont la divulgation non autorisée pourrait nuire aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres».

([4]) Conformément à l'article 1er, paragraphe 2, point a) de la décision n° 41/2021, on entend par informations SECRET UE/EU SECRET les «informations et matériels dont la divulgation non autorisée pourrait nuire gravement aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres».

CHAPITRE 2

CRÉATION D'INFORMATIONS CONFIDENTIEL UE/EU CONFIDENTIAL ET ECRET UE/EU SECRET

Article 3

Autorité d'origine

Bien que l'autorité d'origine au sens de l'article 2, point m), de la décision n° 41/2021 soit l'institution, l'organe ou l'agence de l'Union, l'État membre, l'État tiers ou l'organisation internationale sous l'autorité duquel/de laquelle les informations classifiées ont été créées et/ou introduites dans les structures de l'Union, elle ne correspond pas nécessairement au rédacteur des informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

Article 4

Attribution d'un niveau de classification

1. Un document est au moins classifié CONFIDENTIEL UE/EU CONFIDENTIAL si sa divulgation non autorisée peut, entre autres:

a) causer un préjudice important aux relations diplomatiques, c'est-à-dire donner lieu à des protestations officielles ou autres sanctions;

b) porter préjudice à la sécurité ou à la liberté des personnes;

c) nuire à l'efficacité opérationnelle ou à la sécurité du personnel déployé des États membres ou d'autres contributeurs, ou à l'efficacité d'opérations de sécurité ou de renseignement utiles;

d) fragiliser considérablement la viabilité financière d'organisations importantes;

e) entraver l'investigation d'une infraction grave ou en faciliter l'accomplissement;

f) desservir considérablement les intérêts financiers, monétaires, économiques et commerciaux de l'Union européenne ou des États membres;

g) entraver gravement l'élaboration ou le fonctionnement des principales politiques de l'Union européenne;

h) faire cesser ou perturber fortement d'une manière quelconque des activités importantes de l'Union européenne;

i) conduire à la découverte d'informations classifiées à un niveau supérieur.

2. Un document est au moins classifié SECRET UE/EU SECRET si sa divulgation non autorisée peut, entre autres:

a) provoquer des tensions internationales;

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

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

d) nuire gravement à l'efficacité opérationnelle ou à la sécurité du personnel déployé des États membres ou d'autres contributeurs, ou au maintien de l'efficacité d'opérations de sécurité ou de renseignement très utiles;

e) causer un préjudice matériel important aux intérêts financiers, monétaires, économiques et commerciaux de l'Union ou de l'un de ses États membres;

f) conduire à la découverte d'informations classifiées à un niveau supérieur.

3. Les autorités d'origine peuvent décider d'attribuer un niveau de classification standard aux catégories d'information qu'elles créent régulièrement. Cependant, elles veillent à ce que les différents éléments d'informations soient dotés du niveau de classification approprié.

Article 5

Traitement des projets

1. Les informations sont classifiées dès qu'elles sont produites. Les notes personnelles, les avant-projets ou les messages contenant des informations qui justifient une classification au niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET sont marqués comme tels dès le départ et sont produits et traités conformément à la présente décision.

2. Si le document final ne justifie plus le niveau de classification initial, il est déclassé ou déclassifié, après confirmation par l'autorité d'origine que cela ne présente pas de risque.

Article 6

Enregistrement des sources

Afin de permettre l'exercice du contrôle de l'autorité d'origine conformément à l'article 14 ci-dessous, les autorités d'origine des documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET tiennent un registre de toutes les sources classifiées utilisées pour produire des documents classifiés, y compris des informations sur les sources provenant d'États membres de l'Union européenne, 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 7

Classification de parties d'un document

1. Conformément au point 12 de la politique de classification des informations de la Cour des comptes européenne, le niveau général de classification d'un document est au moins égal à celui de sa partie portant la classification la plus élevée. Lorsqu'il rassemble des informations provenant de plusieurs sources, le document final agrégé est examiné pour en fixer le niveau général de classification de sécurité car il peut requérir un niveau de classification supérieur à celui de chacune des parties qui le composent.

2. Les documents contenant des parties classifiées et non classifiées sont structurés et marqués de manière que les éléments ayant des niveaux de classification et/ou de sensibilité différents puissent au besoin être aisément identifiés et séparés des autres. Chaque partie peut ainsi être traitée de manière appropriée lorsqu'elle est séparée des autres éléments.

Article 8

Marquage de classification en toutes lettres

1. Les informations qui justifient une classification sont marquées et traitées en tant que telles, quelle que soit leur forme physique. Le niveau de classification est clairement communiqué aux destinataires, soit par un marquage de classification si les informations sont transmises sous forme écrite (que ce soit en format papier, sur un support de données amovible ou dans un système d'information et de communication (SIC)), soit par une annonce si les informations sont transmises sous forme orale (par exemple dans une conversation ou une présentation). Les documents classifiés sont physiquement marqués de manière à faciliter l'identification de leur classification de sécurité.

2. Sur les documents, le marquage de classification en toutes lettres CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET est rédigé en français et en anglais (en français d'abord), en lettres capitales, conformément au paragraphe 3. Le marquage ne doit pas être traduit dans d'autres langues.

3. Le marquage de classification CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET est apposé de la manière suivante:

a) centré en haut et en bas de chaque page du document;

b) le marquage de classification complet sur une seule ligne, sans espace avant et après la barre oblique;

c) en lettres capitales, noir, police Times New Roman 16 (si possible, mais au moins 14), gras et entouré d'une bordure sur chaque côté.

4. Lors de la création d'un document CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET:

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

b) chaque page est numérotée;

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

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

e) la date de sa création est indiquée sur le document.

5. Si possible, le marquage SECRET UE/EU SECRET apparaît en rouge.

Article 9

Marquages de classification abrégés C-UE/EU-C et S-UE/EU-S

Les abréviations C-UE/EU-C et S-UE/EU-S peuvent être utilisées pour préciser le niveau de classification des différentes parties d'un document CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, respectivement, ou lorsque le marquage de classification en toutes lettres ne peut être apposé, par exemple sur un petit support de stockage amovible. Elles peuvent être utilisées dans le corps d'un texte où l'utilisation répétée du marquage de classification en toutes lettres serait fastidieuse. Les abréviations ne peuvent pas être utilisées à la place du marquage de classification en toutes lettres dans l'en-tête et le pied de page du document.

Article 10

Autres identifiants de sécurité

1. Les documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET peuvent porter d'autres marquages ou «identifiants de sécurité» qui précisent, par exemple, le domaine auquel le document se rapporte, ou indiquent une diffusion particulière en fonction du besoin d'en connaître. Exemple:

COMMUNICABLE AU LIECHTENSTEIN

2. Les documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET peuvent comporter une réserve de sécurité qui donne des instructions spécifiques concernant le traitement et la gestion des documents.

Dans la mesure du possible, les indications relatives à la déclassification sont apposées sur la première page du document lors de sa création. Le marquage suivant peut par exemple être utilisé:

SECRET UE/EU SECRET jusqu'au [jj.mm.aaaa] et RESTREINT UE/EU RESTRICTED ensuite

Article 11

Traitement électronique

1. Les documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET sont créés par voie électronique dans la mesure du possible.

2. Lors de la création d'informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, le personnel de la Cour des comptes utilise un SIC homologué pour le niveau de classification au moins correspondant. En cas de doute, des conseils supplémentaires peuvent être obtenus auprès du responsable de la sécurité de l'information de la Cour des comptes (ci-après «l'ISO»).

3. Les documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET, y compris les projets (voir article 5) ne doivent pas être envoyés au moyen de courriers électroniques, imprimés ou scannés sur des imprimantes ou des scanners standards ou traités sur les dispositifs personnels des membres du personnel. Seules les imprimantes ou photocopieuses connectées à des ordinateurs autonomes protégés des émissions électromagnétiques ou à un système agréé peuvent être utilisées pour imprimer les documents CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

Article 12

Enregistrement à des fins de sécurité

1. Les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET sont enregistrées à des fins de sécurité avant la diffusion et lors de leur réception. Elles sont enregistrées:

— lorsqu'elles arrivent dans la zone sécurisée de la Commission à Luxembourg, pour l'utilisation de laquelle la Cour des comptes a conclu un protocole d'accord, ou la quittent;

— lorsqu'elles arrivent dans un SIC ou le quittent.

2. Ces enregistrements peuvent être effectués sur papier ou dans des journaux de bord électroniques.

3. Si les informations sont traitées électroniquement dans un SIC, l'enregistrement peut également être mis en œuvre au moyen de processus internes au SIC lui-même. Dans ce cas, le SIC doit inclure des mesures permettant de garantir l'intégrité des enregistrements.

4. L'agent contrôleur tient un registre qui contient au moins les informations suivantes pour chaque document:

a) la date à laquelle le document classifié final a été enregistré;

b) le niveau de classification;

c) le cas échéant, la date d'expiration du niveau de classification;

d) le nom du service d'origine;

e) le(s) destinataire(s);

f) l'objet;

g) le numéro de référence attribué par le service d'origine au document;

h) le numéro d'enregistrement,

i) le nombre d'exemplaires diffusés;

j) si possible, le journal des sources utilisées pour la création du document;

k) la date de déclassement ou de déclassification du document;

l) des informations sur la destruction (lieu, date, méthode, supervision, certificat de destruction).

Article 13

Diffusion

L'expéditeur des documents CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET décide à qui il diffuse les informations, selon le besoin d'en connaître des destinataires. Une liste de diffusion est établie pour garantir que le principe du besoin d'en connaître est correctement appliqué.

CHAPITRE 3

TRAVAILLER AVEC DES INFORMATIONS CONFIDENTIEL UE/EU CONFIDENTIAL ET SECRET UE/EU SECRET EXISTANTES

Article 14

Contrôle de l'autorité d'origine

1. L'autorité d'origine exerce le «contrôle de l'autorité d'origine» sur les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET qu'elle a créées. 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) communiquées à un pays tiers ou à une organisation internationale;

d) divulguées à un tiers extérieur à la Cour des comptes, mais au sein de l'Union européenne.

2. L'accès aux informations classifiées a été accordé aux détenteurs d'informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET pour leur permettre d'exercer leurs fonctions. Ils ont la responsabilité du traitement, du stockage et de la protection adéquats de ces informations conformément à la décision n° 41/2021. Contrairement aux autorités d'origine des informations classifiées, les détenteurs ne sont pas autorisés à décider de déclasser, déclassifier ou communiquer ultérieurement les informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

3. Si l'autorité d'origine d'une information CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET ne peut être identifiée, le service de la Cour des comptes qui détient ces informations classifiées exerce le contrôle de l'autorité d'origine. Au cas où le détenteur estime nécessaire de communiquer des informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET à un pays tiers ou à une organisation internationale, la Cour des comptes sollicite l'avis de l'une des parties à un accord sur la sécurité de l'information conclu avec ce même pays tiers ou cette même organisation internationale ([5]).

Article 15

SIC conformes pour le traitement des informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET

Les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET sont traitées et transmises par voie électronique dans la mesure du possible. En application de l'article 6 de la décision n° 41/2021, seuls les SIC et les équipements homologués par une autre institution, une autre agence ou un autre organe de l'Union ou par la Cour des comptes peuvent être utilisés à cet effet.

Article 16

Mesures spécifiques pour les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET sur des supports de stockage amovibles

1. L'utilisation des supports de stockage amovibles, comme des clés USB, des CD, des DVD ou des cartes à mémoire (y compris des SSD ([6])) est strictement contrôlée et comptabilisée. Seuls les supports de stockage amovibles fournis par la Cour des comptes ou par une autre institution, une autre agence ou un autre organe de l'Union, qui sont approuvés par l'ISO et cryptés au moyen d'un produit approuvé par celui-ci peuvent être utilisés. Les supports de stockage amovibles personnels et ceux librement distribués lors de conférences, séminaires, etc. ne doivent pas être utilisés pour transférer des informations classifiées. Dans la mesure du possible, des supports de stockage amovibles protégés par la sécurité Tempest devraient être utilisés, conformément aux recommandations de l'ISO.

([5]) Voir article 35 pour plus de détails.
([6]) S'entend comme un dispositif à semi-conducteur, un dispositif d'état solide ou un disque statique.

2. Lorsqu'un document classifié est traité ou conservé électroniquement sur un support de stockage amovible, le marquage de classification est clairement visible dans les informations affichées, ainsi que dans le nom du fichier et sur le support de stockage amovible.

3. Le personnel garde à l'esprit que lorsque de grandes quantités d'informations classifiées sont conservées sur des supports de stockage amovibles, il peut s'avérer nécessaire de conférer un niveau de classification supérieur aux dispositifs.

4. Seuls les SIC dûment homologués peuvent être utilisés pour transférer des informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET sur des supports de stockage amovibles ou à partir de ceux-ci.

5. Avant que ces informations ne soient téléchargées sur un support de stockage amovible, il convient de veiller particulièrement à ce que ce support ne contienne pas de virus ou de logiciels malveillants.

6. Le cas échéant, les supports de stockage amovibles sont traités conformément aux procédures d'exploitation de sécurité relatives au système de cryptage utilisé.

7. Les documents présents sur les supports de stockage amovibles qui ne sont plus nécessaires ou qui ont été transférés sur un SIC approprié sont supprimés ou effacés en toute sécurité au moyen de produits ou de méthodes agréés. À moins d'être stockés dans un coffre-fort verrouillé, les supports de stockage amovibles sont détruits lorsqu'ils ne sont plus nécessaires. Toute destruction ou suppression est réalisée conformément aux règles de sécurité de la Cour des comptes. Un inventaire des supports de stockage amovibles est conservé et leur destruction est enregistrée.

Article 17

Traitement et stockage des informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET

1. Conformément à l'article 5, paragraphes 5 et 6, de la décision n° 41/2021, les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET sont traitées dans une zone sécurisée ([7]). Le personnel de la Cour de comptes peut également accéder à ces informations dans des zones sécurisées d'une autre institution de l'UE.

2. Conformément à l'article 5, paragraphe 6, de la décision n° 41/2021, et si l'autorité d'origine en convient expressément, ces informations peuvent exceptionnellement être traitées dans une zone administrative ([8]) de la Cour des comptes, à condition que les personnes non autorisées ne puissent pas avoir accès aux ICUE.

3. En temps de crise ou en cas d'urgence, ces informations peuvent être traitées en dehors d'une zone sécurisée ou administrative à condition que le détenteur se soit engagé à se conformer aux mesures compensatoires, qui incluent au moins ce qui suit:

— les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET ne doivent pas être lues dans des lieux publics;

— les ICUE restent à tout moment sous le contrôle personnel du détenteur;

— si les documents sont au format papier, le détenteur a avisé le bureau d'ordre pour les ICUE, dans les meilleurs délais et en fonction de la nature de la crise ou de la situation d'urgence, du traitement des documents classifiés en dehors d'une zone sécurisée ou d'une zone administrative;

— les documents sont rangés dans un coffre-fort approprié lorsqu'ils ne sont pas lus ou discutés;

— les portes de la salle sont fermées lorsque les documents sont lus ou discutés;

— le contenu des documents n'est pas abordé au téléphone sur une ligne non sécurisée ou dans un courrier électronique;

— le détenteur ne photocopie ou ne scanne pas les documents. Seul le bureau d'ordre pour les ICUE peut fournir des exemplaires supplémentaires;

([7]) Voir définition à l'article 18 de la décision (UE, Euratom) 2015/444 de la Commission du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 72 du 17.3.2015, p. 53).

([8]) Voir définition à l'annexe de la décision n° 41/2021.

— les documents ne peuvent être traités et temporairement conservés en dehors d'une zone administrative ou sécurisée que pendant le temps strictement nécessaire, à l'issue duquel ils doivent être restitués au bureau d'ordre pour les ICUE;

— Les documents doivent être soumis à signature lors de leur restitution;

— le détenteur ne doit ni jeter ni détruire les documents classifiés.

4. Les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET sont stockées dans une zone sécurisée, soit dans un meuble de sécurité soit une chambre forte.

5. Des conseils supplémentaires peuvent être obtenus auprès de l'ISO.

6. Tout incident de sécurité réel ou suspecté impliquant un document est signalé dès que possible à l'ISO.

Article 18

Duplication et traduction d'informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET

1. Les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET peuvent être dupliquées ou traduites sur instruction du détenteur si l'autorité d'origine en a expressément convenu et n'a pas imposé de restrictions. Cependant, le nombre de copies ne doit pas dépasser ce qui est strictement nécessaire. La Cour des comptes peut également demander à l'autorité d'origine de fournir une copie traduite en anglais.

2. Lorsque seule une partie d'un document classifié est reproduite, les conditions qui s'appliquent sont les mêmes que pour la duplication de l'intégralité du document. Les extraits sont également classifiés au même niveau, sauf si l'autorité d'origine les a classifiés à un niveau inférieur ou a apposé un marquage spécifique indiquant qu'ils ne sont pas classifiés.

3. Les mesures de sécurité applicables aux informations originales s'appliquent également aux copies et traductions de celles-ci.

Article 19

Principes généraux applicables au transport d'informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET

1. Dans la mesure du possible, les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET devant être transportées en dehors d'une zone sécurisée ou d'une zone administrative conformément à l'article 17, paragraphe 2, sont envoyées par voie électronique à l'aide de moyens dûment homologués et/ou de produits cryptographiques agréés.

2. Selon les moyens disponibles ou les circonstances particulières, les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET peuvent être physiquement transportées en personne sur support papier ou sur des supports de stockage amovibles. L'utilisation de supports de stockage amovibles est préférable à l'envoi de documents papier pour le transfert d'informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET.

3. Conformément à l'article 6, paragraphe 8, de la décision n° 41/2021, le support de stockage amovible est crypté au moyen d'un produit agréé pour la protection des ICUE par le Conseil ou par le secrétaire général du Conseil en sa qualité d'autorité d'agrément cryptographique ou par une autre institution, une autre agence ou un autre organe de l'UE. Les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET sur des supports de stockage amovibles non protégés par un produit de cryptage agréé de la sorte sont traitées de la même manière qu'une copie papier.

4. Un envoi peut contenir plusieurs ICUE dès lors que le principe du besoin d'en connaître est respecté.

5. L'emballage utilisé garantit que le contenu n'est pas visible. Les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET sont transportées sous double emballage opaque, tel qu'une enveloppe, un classeur opaque ou une mallette. L'emballage extérieur est scellé et ne doit porter aucune indication sur la nature ou le niveau de classification de son contenu. L'emballage intérieur porte la mention CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET. Les deux emballages indiquent le nom, la fonction et l'adresse du destinataire prévu ainsi qu'une adresse de retour si la livraison ne peut être effectuée.

6. Les membres du personnel ou les transporteurs qui acheminent en personne les informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET disposent d'une autorisation de sécurité et d'un certificat de courrier.

7. Les enveloppes ou emballages ne doivent pas être ouverts pendant le transport. L'autorisation de sécurité délivrée au transporteur ne l'autorise pas à accéder aux informations classifiées constituant l'envoi.

8. En vertu de l'article 5, paragraphe 12, de la décision n° 41/2021, l'autorité d'origine peut également imposer des mesures de sécurité physique supplémentaires visant à protéger les informations classifiées contre toute divulgation non autorisée durant le transport.

9. Tout incident de sécurité réel ou suspecté impliquant des informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET transportées par le personnel ou par des transporteurs est signalé dès que possible à l'ISO en vue d'une enquête ultérieure.

Article 20

Transport par porteur des supports de stockage amovibles

1. Les supports de stockage amovibles utilisés pour transporter les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET sont accompagnés d'une déclaration d'expédition donnant des détails sur les supports et tous les fichiers qui y figurent, afin de permettre au destinataire d'effectuer les vérifications nécessaires et d'en accuser réception.

2. Les dispositifs ne contiennent que les ICUE transportées. Toutes les informations classifiées stockées sur un dispositif donné doivent avoir le même destinataire. Les expéditeurs gardent à l'esprit que le stockage de grandes quantités d'informations classifiées sur un seul dispositif peut requérir un niveau de classification plus élevé pour le dispositif dans son ensemble.

3. Seuls les supports de stockage amovibles portant le marquage de classification approprié sont utilisés pour transporter des informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

4. Toutes les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET sauvegardées sur un support de stockage amovible sont enregistrées à des fins de sécurité.

Article 21

Transport de documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET au sein des services et dans les locaux de la Cour des comptes

1. Le personnel disposant d'une autorisation de sécurité peut transporter des documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET au sein des services et dans les locaux de la Cour des comptes, pour autant que le porteur ne se sépare pas des documents et que ceux-ci ne soient pas lus en public.

2. Les documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET ne sont pas envoyés par courrier interne.

Article 22

Transport de documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET au sein de l'Union européenne

1. Les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET peuvent être transportées par le personnel ou les transporteurs de la Cour des comptes ou de l'institution, l'agence ou l'organe de l'UE d'origine partout dans l'Union dès lors qu'ils respectent les instructions suivantes:

a) des enveloppes ou des emballages doubles opaques sont utilisés pour transmettre les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET. L'emballage extérieur est scellé et ne doit porter aucune indication sur la nature ou le niveau de classification de son contenu;

b) le porteur ne se sépare pas des informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET;

c) l'enveloppe ou l'emballage ne doivent pas être ouverts pendant le transport et les informations ne doivent pas être lues dans des lieux publics.

2. Le personnel du bureau d'ordre pour les ICUE qui souhaite envoyer des informations CONFIDENTIEL UE/EU CONFIDENTIAL vers d'autres sites de l'Union peut faire en sorte qu'elles soient transmises par l'un des moyens suivants:

a) par des services postaux nationaux qui suivent l'envoi ou certains services de courrier commercial qui garantissent le transport par porteur personnel, dès lors qu'ils respectent les exigences établies à l'article 24 de la présente décision;

b) par courrier militaire, gouvernemental ou diplomatique, en coordination avec le personnel du bureau d'enregistrement.

3. Les membres du personnel qui souhaitent envoyer des informations SECRET UE/EU SECRET à d'autres États membres de l'Union européenne peuvent uniquement s'adresser à l'agent contrôleur pour qu'elles soient transmises par courrier militaire, gouvernemental ou diplomatique, et non par les services postaux ou les courriers commerciaux.

4. Les membres du personnel ou les transporteurs officiels de la Cour des comptes transportant les informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET sont munis d'un certificat de courrier pour chaque envoi. Le certificat est délivré par l'agent contrôleur et indique que le porteur est autorisé à transporter l'envoi.

Article 23

Transport d'informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET vers le territoire d'un pays tiers, ou en provenance de celui-ci

1. Les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET peuvent être transportées en personne par le personnel de la Cour des comptes ou de l'institution, l'agence ou l'organe de l'UE d'origine entre le territoire de l'Union et le territoire d'un pays tiers.

2. Le personnel du bureau d'ordre pour les ICUE peut organiser un transport par courrier militaire ou diplomatique.

3. Lorsque le personnel transporte en personne des documents papier ou des supports de stockage amovibles classifiés CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, il respecte toutes les mesures supplémentaires suivantes:

— lorsqu'il utilise les transports publics, les informations classifiées sont placées dans une mallette ou un sac qui reste sous la garde personnelle du porteur. Elles ne peuvent être consignées dans une soute à bagages;

— l'emballage intérieur porte un scellé officiel indiquant qu'il s'agit d'un envoi officiel qui ne doit pas faire l'objet de contrôles de sécurité;

— le porteur est muni d'un certificat de courrier, délivré par l'agent contrôleur, qui certifie qu'il est autorisé à transporter l'envoi CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

Article 24

Transport par des courriers commerciaux

1. Aux fins de la présente décision, les «courriers commerciaux» incluent les services postaux nationaux et les sociétés de courrier commercial qui proposent un service où les informations sont livrées contre paiement et sont soit transportées en personne, soit soumises à un suivi.

2. Les courriers commerciaux peuvent transmettre des informations CONFIDENTIEL UE/EU CONFIDENTIAL au sein d'un État membre de l'UE ou entre deux États membres. Les courriers commerciaux peuvent transmettre des informations SECRET UE/EU SECRET au sein d'un État membre mais pas à l'étranger.

3. Les services de courrier commercial sont informés qu'ils ne doivent livrer les envois CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET qu'à l'agent contrôleur, à son remplaçant dûment autorisé ou au destinataire prévu.

4. Les courriers commerciaux peuvent avoir recours aux services d'un sous-traitant. Cependant, la responsabilité de respecter la présente décision incombe à la société de courrier.

Article 25

Préparation des ICUE pour le transport par des services de courrier commercial

1. Lors de la préparation d'envois classifiés, les expéditeurs gardent à l'esprit que les services de courrier commercial ne peuvent livrer les envois CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET qu'à l'agent contrôleur, à son remplaçant dûment autorisé ou au destinataire prévu.

2. Lorsque les informations sont envoyées par un service de courrier commercial agréé, l'envoi est préparé et emballé de la manière suivante:

a) les informations sont placées dans une enveloppe double opaque (l'enveloppe intérieure étant conçue de telle sorte que toute tentative de l'ouvrir sera évidente) ou un autre matériel d'emballage suffisamment sécurisé;

b) le niveau de classification est clairement indiqué sur l'enveloppe ou l'emballage intérieur(e);

c) l'emballage extérieur est scellé et ne doit porter aucun marquage de classification;

d) les enveloppes ou les emballages tant intérieurs qu'extérieurs sont clairement adressés à une personne désignée chez le destinataire prévu et comportent une adresse de retour;

e) un formulaire de récépissé d'enregistrement est placé dans l'enveloppe ou l'emballage intérieur(e) et doit être rempli et renvoyé par le destinataire. Le récépissé d'enregistrement, qui n'est pas lui-même classifié, indique le numéro de référence, la date et le numéro d'exemplaire du document, mais pas l'objet;

f) l'enveloppe ou l'emballage extérieur(e) doit contenir un récépissé de livraison. Le récépissé de livraison, qui n'est pas lui-même classifié, indique le numéro de référence, la date et le numéro d'exemplaire du document, mais pas l'objet;

g) le service de courrier doit obtenir, et fournir à l'expéditeur, une preuve de livraison de l'envoi sur le bordereau de livraison, ou obtenir des reçus ou des numéros de colis.

3. Avant l'expédition de l'envoi, l'expéditeur convient avec le destinataire désigné d'une date et d'une heure de livraison appropriées.

4. L'expéditeur est le seul responsable des envois expédiés par un service de courrier commercial. En cas de perte ou de livraison tardive d'un envoi, l'expéditeur en informe l'ISO et l'agent contrôleur, qui assureront le suivi de l'incident de sécurité.

Article 26

Autres conditions de traitement spécifiques

1. Toutes les conditions de transport supplémentaires définies dans un accord sur la sécurité de l'information ou dans des arrangements administratifs doivent être respectées. En cas de doute, les membres du personnel consultent l'ISO ou l'agent contrôleur.

2. L'exigence du double emballage peut être levée pour les informations classifiées protégées au moyen de produits cryptographiques agréés. Cependant, à des fins d'adressage, et du fait que les supports de stockage amovibles portent un marquage de classification de sécurité explicite, les supports sont transportés au minimum dans une enveloppe opaque scellée, mais des mesures de protection physiques supplémentaires peuvent s'avérer nécessaires, telles qu'une enveloppe en papier bulle.

CHAPITRE 4

RÉUNIONS CLASSIFIÉES

Article 27

Préparation d'une réunion CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET

1. Les réunions au cours desquelles des informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET seront examinées sont uniquement tenues dans une salle de réunion agréée au niveau approprié ou à un niveau supérieur. La Cour des comptes peut utiliser des salles de réunion situées dans une zone sécurisée d'une autre institution européenne. Lorsque ces salles ne sont pas disponibles, le personnel sollicite l'avis de l'ISO.

2. En règle générale, les ordres du jour des réunions ne sont pas classifiés. Si l'ordre du jour d'une réunion mentionne des documents classifiés, l'ordre du jour lui-même n'est pas automatiquement classifié. Les points de l'ordre du jour sont formulés de façon à éviter de compromettre les intérêts de l'Union ou de ses États membres.

3. Les organisateurs de la réunion rappellent aux participants que les éventuels commentaires concernant un point de l'ordre du jour CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET ne doivent pas être envoyés au moyen de courriers électroniques ou par d'autres moyens qui n'ont pas été dûment agréés conformément à l'article 11 de la présente décision.

4. Ils s'efforcent de regrouper les points CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET dans l'ordre du jour afin de faciliter le bon déroulement de la réunion. Seules les personnes qui ont un besoin d'en connaître, qui disposent d'une habilitation de sécurité du niveau approprié et qui y ont été dûment autorisées peuvent être présentes aux discussions des points classifiés.

5. L'invitation à la réunion doit prévenir les participants que des sujets classifiés figureront à l'ordre du jour et que les mesures de sécurité correspondantes s'appliqueront.

6. Les organisateurs de la réunion rappellent aux participants que les appareils électroniques portables doivent être laissés à l'extérieur de la salle de réunion pendant la discussion des points CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

7. Ils établissent une liste complète des participants avant la réunion. Conformément à l'article 4, paragraphe 6, de la décision n° 41/2021, ils précisent également en temps utile à l'ISO les date, heure, lieu de la réunion et lui transmettent la liste des participants.

Article 28

Accès des participants à une réunion CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET

1. Les organisateurs de la réunion informent l'ISO et l'agent contrôleur de la participation de tout visiteur extérieur à une réunion CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET organisée dans les locaux de la Cour des comptes.

2. Les participants devront prouver qu'ils détiennent une habilitation de sécurité du personnel valable au niveau approprié pour pouvoir assister à la discussion des points de l'ordre du jour CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

Article 29

Équipements électroniques dans les salles de réunion CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET

Seuls les systèmes informatiques agréés conformément à l'article 11 de la présente décision peuvent être utilisés lorsque des informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET sont transmises, par exemple dans le cadre d'une présentation ou d'une visioconférence.

Article 30

Procédures à suivre au cours d'une réunion CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET

1. Au début d'une discussion classifiée, le président annonce aux participants que la réunion passe en mode classifié. Les portes sont fermées.

2. Seul le nombre nécessaire de documents est soumis à signature et distribué aux participants et aux interprètes, le cas échéant, au début de la discussion.

3. Les documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET ne sont pas laissés sans surveillance pendant les pauses de la réunion.

4. À la fin de la réunion, il est rappelé aux participants et aux interprètes de ne laisser aucun document classifié ni aucune note classifiée qu'ils auraient pu prendre sans surveillance dans la salle. Les documents CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET dont les participants n'ont pas besoin à la fin de la réunion, et tous ceux utilisés par les interprètes, sont soumis à signature et restitués à l'agent contrôleur pour qu'ils soient détruits dans des déchiqueteuses agréées ([9]).

5. La liste des participants est établie au cours de la réunion, ainsi qu'un résumé des informations classifiées partagées avec les États membres et communiquées oralement à des pays tiers ou à des organisations internationales, en vue d'être consignés dans les résultats des travaux.

Article 31

Interprètes et traducteurs

Seuls les interprètes et traducteurs habilités et autorisés, soumis au statut des fonctionnaires ou au régime applicable aux autres agents de l'Union européenne ([10]) ou qui ont un lien contractuel avec la Cour des comptes ou une autre institution de l'UE, ont accès aux informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

([9]) Voir article 42, paragraphe 6, de la présente décision pour plus de détails.

([10]) Règlement n° 31 (CEE) fixant le statut des fonctionnaires et le régime applicable aux autres agents, tel que modifié (JO 45 du 14.6.1962, p. 1385/62) (ELI: http://data.europa.eu/eli/reg/1962/31(1)/2023-01-01).

CHAPITRE 5

PARTAGE ET ÉCHANGE D'INFORMATIONS CONFIDENTIEL UE/EU CONFIDENTIAL ET SECRET UE/EU SECRET

Article 32

Consentement de l'autorité d'origine

Si la Cour des comptes n'est pas l'autorité d'origine des informations classifiées à communiquer ou partager, ou des sources qu'elles peuvent contenir, le service de la Cour des comptes qui détient les informations classifiées demande au préalable le consentement écrit de l'autorité d'origine. Si l'autorité d'origine ne peut être identifiée, le service de la Cour des comptes qui détient les informations classifiées exerce le contrôle de l'autorité d'origine.

Article 33

Partage d'informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET avec d'autres entités de l'Union

1. Les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET ne sont partagées avec une autre institution, une autre agence, un autre organe ou un autre organisme de l'UE que si le destinataire a un besoin d'en connaître et si cette entité a un arrangement légal correspondant avec la Cour des comptes.

2. À la Cour des comptes, le bureau d'ordre pour les ICUE représente, en règle générale, le principal point d'entrée et de sortie des échanges d'informations classifiées avec d'autres institutions, agences, organes et organismes de l'UE.

Article 34

Échange d'informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET avec des États membres

1. Les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET peuvent être partagées avec d'autres États membres si le destinataire a un besoin d'en connaître et qu'il a reçu une habilitation de sécurité.

2. Les informations classifiées des États membres qui portent un marquage de classification national ([11]) équivalent et qui ont été fournies à la Cour des comptes bénéficient du même niveau de protection que les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET.

Article 35

Échange d'informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET avec des pays tiers et des organisations internationales

1. Les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET ne sont communiquées à un pays tiers ou à une organisation internationale que si le destinataire a un besoin d'en connaître et que le pays ou l'organisation internationale dispose d'un cadre juridique ou administratif approprié, par exemple un accord sur la sécurité de l'information ou un arrangement administratif avec la Cour des comptes. Les dispositions d'un tel accord ou d'un tel arrangement prévalent sur les dispositions de la présente décision.

2. Le bureau d'ordre pour les ICUE représente, en règle générale, le principal point d'entrée et de sortie de toutes les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET échangées entre la Cour des comptes et des États tiers ou des organisations internationales.

([11]) Le tableau d'équivalence pour les marquages des États membres est établi à l'annexe I de la décision (UE, Euratom) 2015/444.

3. Toutes les informations classifiées reçues d'un pays tiers ou d'une organisation internationale sont enregistrées à des fins de sécurité. Le personnel contacte alors le bureau d'ordre pour les ICUE s'il reçoit des informations classifiées ne provenant pas du circuit habituel de celui-ci.

4. Afin de garantir la traçabilité, les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET sont enregistrées:

— lorsqu'elles arrivent dans la zone sécurisée ou la quittent;

— lorsqu'elles arrivent dans un SIC ou le quittent.

5. Ces enregistrements peuvent être effectués sur papier ou dans des journaux de bord électroniques.

6. Les procédures d'enregistrement des informations classifiées traitées dans un SIC homologué peuvent être mises en œuvre au moyen de processus intervenant au sein du SIC même. Dans ce cas, le SIC inclut des mesures permettant de garantir l'intégrité des journaux de bord.

7. Les informations classifiées reçues d'un pays tiers ou d'une organisation internationale bénéficient du même niveau de protection que les ICUE portant un marquage de classification équivalent, conformément à l'accord sur la sécurité de l'information ou l'arrangement administratif applicable.

Article 36

Communication *ad hoc* exceptionnelle d'informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET

1. Lorsque la Cour des comptes ou l'un de ses services estime qu'il est nécessaire, à titre exceptionnel, de communiquer des informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET à un pays tiers, une organisation internationale ou une entité de l'Union européenne, mais qu'il n'existe aucun accord sur la sécurité de l'information ou arrangement administratif, la procédure de communication *ad hoc* exceptionnelle s'applique.

2. Les services de la Cour des comptes contactent l'ISO et l'autorité d'origine. La Cour des comptes sollicite l'avis de l'une des parties à un accord sur la sécurité de l'information conclu avec ce même pays tiers, cette même organisation internationale ou cette même entité de l'UE.

3. À l'issue de cette consultation, le collège de la Cour peut, sur proposition du secrétaire général, autoriser la communication des informations concernées.

CHAPITRE 6

FIN DE VIE DES INFORMATIONS CONFIDENTIEL UE/EU CONFIDENTIAL ET SECRET UE/EU SECRET

Article 37

Quand déclasser ou déclassifier

1. Les informations ne restent classifiées que tant qu'elles nécessitent une protection. Le déclassement signifie le passage à un niveau de classification de sécurité inférieur. La déclassification signifie que les informations ne sont plus considérées comme classifiées. Au moment de la création du document classifié, l'autorité d'origine indique, si possible, si les ICUE qui y figurent peuvent ou non être déclassées ou déclassifiées à une date donnée ou après un événement spécifique. À défaut, l'autorité d'origine examine les informations et évalue les risques tous les cinq ans au moins en vue de déterminer si le niveau de classification original est toujours approprié.

2. Les documents de la Cour des comptes peuvent également être déclassés ou déclassifiés sur une base *ad hoc*, par exemple à la suite d'une demande d'accès du public.

Article 38

Responsabilité en matière de déclassement ou de déclassification

1. Les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET ne sont pas déclassées ou déclassifiées sans la permission de l'autorité d'origine.

2. Le service de la Cour des comptes qui a créé un document classifié est responsable de la décision relative à son déclassement ou à sa déclassification. À la Cour des comptes, toutes les demandes de déclassement et de déclassification font l'objet d'une consultation du chef de service ou du directeur responsable du service d'origine, ou du chef de mission. Si le service a compilé des informations classifiées à partir de diverses sources, il sollicite tout d'abord le consentement de toutes les autres parties ayant fourni des sources, y compris les États membres, les autres organes de l'Union européenne, les pays tiers ou les organisations internationales.

3. Lorsque le service d'origine de la Cour n'existe plus et que ses responsabilités ont été reprises par un autre service, la décision de déclasser ou de déclassifier est prise par ce dernier. Lorsque le service d'origine n'existe plus et que ses responsabilités n'ont pas été reprises par un autre service, la décision de déclasser ou de déclassifier est prise conjointement par les directeurs de la Cour des comptes.

4. Le service responsable du déclassement ou de la déclassification collabore avec le bureau d'ordre pour les ICUE sur les modalités pratiques du déclassement ou de la déclassification.

Article 39

Informations sensibles non classifiées

Lorsque l'examen d'un document entraîne une décision de déclassifier, il convient d'examiner si le document doit porter un marquage «informations sensibles non classifiées» au sens du point 16 de la politique de classification des informations de la Cour des comptes européenne ([12]) et du point 4 des lignes directrices sur la classification et le traitement des informations non classifiées de l'Union européenne.

Article 40

Comment indiquer qu'un document a été déclassé ou déclassifié

1. Le marquage de classification d'origine figurant en haut et en bas de chaque page est biffé de manière visible (et non supprimé) en utilisant la fonction «strikethrough» pour les formats électroniques, ou biffé manuellement pour les impressions.

2. La première 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.

3. Les destinataires initiaux des informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET sont informés du déclassement ou de la déclassification. Il incombe aux destinataires initiaux d'en informer tous les destinataires successifs auxquels ils ont fait suivre l'original ou une copie des informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

4. Le service des archives de la Cour des comptes est informé de toutes les décisions de déclassification.

5. Toutes les traductions des informations classifiées sont soumises aux mêmes procédures de déclassement ou de déclassification que la version linguistique originale.

([12]) Disponible sur la page https://www.eca.europa.eu/fr/Pages/LegalFramework.aspx.

Article 41

Déclassement partiel ou déclassification partielle des informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET

1. Un déclassement partiel ou une déclassification partielle est également possible (par exemple, les annexes, quelques paragraphes seulement, etc.). La procédure est identique à celle du déclassement ou de la déclassification d'un document complet.

2. Le déclassement partiel ou la déclassification partielle d'informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET donne lieu à la production d'un extrait déclassifié.

3. Dans l'extrait déclassifié, les parties qui restent classifiées sont remplacées par:

PARTIE À NE PAS DÉCLASSIFIER

soit dans le corps du texte, si la partie qui reste classifiée fait partie d'un paragraphe, soit en tant que paragraphe, si la partie qui reste classifiée constitue un paragraphe ou plus d'un paragraphe complet.

4. Une mention spécifique est ajoutée dans le texte si une annexe complète ne peut être déclassifiée et a, pour cette raison, été retirée de l'extrait.

Article 42

Destruction et suppression régulières d'informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET

1. La Cour des comptes ne doit pas accumuler de grandes quantités d'informations classifiées.

2. Les services d'origine examinent les documents tous les cinq ans au moins en vue de leur destruction ou suppression. Cette disposition s'applique à intervalles réguliers tant pour les informations sur support papier que pour les informations stockées dans les SIC.

3. Le personnel ne détruit pas les exemplaires papier des documents CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET dont il n'a plus besoin, mais demande à l'agent contrôleur de le faire, sous réserve des exigences d'archivage applicables au document d'origine.

4. Les membres du personnel ne sont pas tenus d'informer l'autorité d'origine s'ils suppriment des copies des documents CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET.

5. Les projets de documents contenant des informations classifiées sont soumis aux mêmes méthodes d'élimination que les documents classifiés définitifs.

6. Seules les déchiqueteuses agréées sont utilisées pour détruire les documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET. Les déchiqueteuses de niveau 5 de la norme DIN 66399 sont conformes pour détruire les documents CONFIDENTIEL UE/EU CONFIDENTIAL. Les déchiqueteuses de niveau 6 de la norme DIN 66399 sont conformes pour détruire les documents SECRET UE/EU SECRET.

7. Les bandes des déchiqueteuses agréées peuvent être éliminées comme des déchets de bureau normaux.

8. L'agent contrôleur crée des certificats de destruction et actualise en conséquence les cahiers d'enregistrement et les autres informations relatives aux enregistrements.

9. Tous les supports et dispositifs contenant des informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET sont correctement nettoyés au terme de leur durée de vie. Les données électroniques sont détruites ou supprimées des ressources informatiques et des supports de stockage associés de façon à garantir raisonnablement que les informations sont irrécupérables. Le nettoyage implique de supprimer toutes les données des dispositifs de stockage ainsi que toutes les étiquettes, tous les marquages et tous les journaux d'activités.

10. Les supports de stockage informatique sont donnés à l'ISO pour qu'ils soient détruits et éliminés après que l'agent contrôleur en a été informé.

Article 43

Évacuation et destruction d'informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET en cas d'urgence

1. En vertu du protocole d'accord signé entre la Cour des comptes et la direction générale des ressources humaines et de la sécurité de la Commission concernant l'utilisation de sa zone sécurisée, la procédure d'urgence établie par la Commission pour assurer la sauvegarde des informations classifiées s'applique. Le cas échéant, le responsable local de sécurité de la direction «Sécurité» de la Commission au Luxembourg aura accès au coffre-fort de la Cour des comptes afin de mettre en œuvre la procédure d'urgence établie par la Commission et d'activer les plans d'évacuation et de destruction d'urgence pour assurer la sauvegarde des ICUE qui présentent un risque significatif de tomber entre les mains de personnes non autorisées en temps de crise. Par ordre d'importance, et selon la nature de l'urgence, il convient:

i) de déplacer les ICUE vers un autre lieu sûr, si possible une zone sécurisée au sein du même bâtiment;

ii) d'évacuer les ICUE vers un autre lieu sûr, si possible une zone sécurisée dans un bâtiment différent, de préférence d'une institution de l'UE;

iii) de détruire les ICUE, si possible par des moyens de destruction agréés.

2. Si les plans d'urgence ont été activés, les informations SECRET UE/EU SECRET sont déplacées ou détruites en priorité, les informations CONFIDENTIEL UE/EU CONFIDENTIAL suivent.

3. Les modalités opérationnelles des plans d'évacuation et de destruction d'urgence sont elles-mêmes classifiées RESTREINT UE/EU RESTRICTED. Un exemplaire est conservé dans chaque coffre-fort qui est utilisé pour stocker les informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET de manière à ce qu'il soit accessible en cas d'urgence.

Article 44

Archivage

1. Les décisions déterminant s'il y a lieu d'archiver et, dans ce cas, à quel moment, ainsi que les mesures pratiques correspondantes à prendre, sont conformes à la politique de sécurité de l'information, à la politique de classification des informations et à la politique d'archivage de la Cour des comptes.

2. Les documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET ne doivent pas être envoyés aux archives historiques de l'Union européenne à Florence.

CHAPITRE 7

DISPOSITIONS FINALES

Article 45

Transparence

La présente décision est portée à la connaissance du personnel de la Cour de comptes et de toutes les autres personnes auxquelles elle s'applique, et est publiée au Journal officiel de l'Union européenne.

Article 46

Entrée en vigueur

La présente décision, après avoir été adoptée par le comité administratif, entrera en vigueur le lendemain de sa publication au Journal officiel de l'Union européenne.

Fait à Luxembourg, le 19 mars 2024.

Par le comité administratif de la Cour des comptes
Le président
Tony MURPHY

ANNEXE

Catégories de personnel qui peuvent avoir accès aux informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET si nécessaire pour l'exercice de leurs fonctions

Catégories de personnel de la Cour des comptes	Accès aux informations CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET	Conditions
Membres	Oui	réunion d'information + reconnaissance des responsabilités
Fonctionnaires	Oui	Enquête + réunion d'information + reconnaissance des responsabilités + autorisation + besoin d'en connaître
Agents temporaires	Oui	Enquête + réunion d'information + reconnaissance des responsabilités + autorisation + besoin d'en connaître
Agents contractuels	Oui	Enquête + réunion d'information + reconnaissance des responsabilités + autorisation + besoin d'en connaître
Experts nationaux détachés par les États membres de l'UE	Oui	Uniquement s'ils ont reçu une habilitation des États membres d'origine avant de prendre leurs fonctions + réunion d'information par la Cour des comptes + reconnaissance des responsabilités + autorisation de la Cour des comptes + besoin d'en connaître
Stagiaires	Non	Aucune exception possible
Toute autre catégorie de personnel (intérimaires, externes intra-muros, etc.)	Non	Aucune exception possible