COUR DES COMPTES EUROPÉENNE

Décision n° 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)

LA COUR DES COMPTES EUROPÉENNE,

VU l'article 13 du traité sur l'Union européenne,

VU l'article 287 du traité sur le fonctionnement de l'Union européenne,

VU l'article 257 du 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,

VU l'article 1er, paragraphe 6, des modalités d'application du règlement intérieur de la Cour des comptes (décision de la Cour n° 21-2021),

VU les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne des autres institutions, agences et organes de l'UE,

VU la politique de sécurité de l'information de la Cour (DEC 127/15 FINAL) et sa politique de classification des informations (communication au personnel n° 123/2020),

CONSIDÉRANT qu'en vertu de l'article 287, paragraphe 3, du TFUE, la Cour des comptes a le droit d'accéder à tous les documents pertinents ou informations qu'elle estime nécessaires à l'accomplissement de sa mission, y compris aux informations classifiées de l'UE (ICUE), ce droit d'accès s'exerçant dans le plein respect du principe de coopération loyale entre les institutions et du principe d'attribution; et que ce droit d'accès aux ICUE, garanti par le TFUE, ne peut pas être remis en cause par l'autorité d'origine des ICUE, tandis qu'il peut être demandé à la Cour des comptes de mettre en place et de respecter certaines mesures de sécurité, comme cela est indiqué de façon détaillée ci-après;

CONSIDÉRANT que les Membres de la Cour des comptes, ainsi que ses fonctionnaires et autres agents sont tenus, même après la cessation de leurs fonctions, à une obligation de confidentialité au titre de l'article 339 du TFUE, de l'article 17 du statut, et d'autres actes adoptés en vertu de ceux-ci;

CONSIDÉRANT que compte tenu de leur nature sensible, le traitement des ICUE nécessite que le respect de l'obligation de confidentialité soit assuré au moyen de mesures de sécurité appropriées visant à garantir à ces informations un haut niveau de protection, équivalentes à celles arrêtées dans les règles en matière de protection des informations classifiées de l'Union européenne adoptées par les autres institutions, agences et organes de l'Union, étant entendu que, si la Cour des comptes estime que de telles mesures de sécurité ne sont pas

justifiées au regard de la nature et du type d'ICUE, elle se réserve le droit de soulever toute observation qu'elle jugerait appropriée, tout en respectant le niveau de classification des ICUE;

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 l'accès de la Cour des comptes aux informations classifiées est assuré dans le respect du principe du besoin d'en connaître aux fins de l'exécution des tâches qui lui sont confiées par les traités et par les actes juridiques adoptés sur la base des traités;

CONSIDÉRANT que compte tenu de la nature et du contenu sensible de certaines informations, il y a lieu d'établir une procédure spéciale pour le traitement, par la Cour des comptes, des documents contenant des ICUE;

CONSIDÉRANT que l'institution veille à la mise en œuvre de la présente décision dans le respect de toutes les règles applicables, notamment des dispositions en matière de protection des données à caractère personnel, de sécurité physique des personnes, des bâtiments et du système informatique, ainsi qu'en matière d'accès public aux documents,

DÉCIDE:

Article 1. **Objet et champ d'application**

1. La présente décision définit les principes de base et les normes de sécurité minimales pour la protection des informations classifiées traitées par la Cour des comptes dans l'exercice de son mandat.

2. Aux fins de la présente décision, on entend par «informations classifiées» l'un ou l'ensemble des types d'informations suivants:

   a) les «informations classifiées de l'UE» (ICUE) telles qu'elles sont définies dans les règles de sécurité des autres institutions, agences, organes ou organismes de l'Union et qui portent l'un des marquages de classification de sécurité suivants:

   - 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 européenne ou d'un ou de plusieurs de ses États membres;
   - SECRET UE/EU SECRET: informations et matériels dont la divulgation non autorisée pourrait nuire gravement aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres;
   - CONFIDENTIEL UE/EU CONFIDENTIAL: informations et matériels dont la divulgation non autorisée pourrait nuire aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres;
   - RESTREINT UE/EU RESTRICTED: informations et matériels dont la divulgation non autorisée pourrait être défavorable aux intérêts de l'Union européenne ou d'un ou de plusieurs de ses États membres.

b) les informations classifiées communiquées par des États membres et portant un marquage de classification de sécurité national équivalent à l'un des marquages de classification de sécurité utilisés pour les ICUE[1] énumérés au point a);

c) les informations classifiées communiquées à la Cour des comptes par des États tiers ou des organisations internationales et portant un marquage de classification de sécurité équivalent à l'un des marquages de classification de sécurité utilisés pour les ICUE énumérés au point a), conformément aux accords sur la sécurité des informations ou aux arrangements administratifs pertinents.

3. La Cour des comptes traite les informations de niveau RESTREINT UE/EU RESTRICTED dans ses locaux et prend toutes les mesures de protection nécessaires à cette fin. 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.

4. La présente décision s'applique à tous les services de la Cour des comptes et dans l'ensemble des locaux de celle-ci.

5. Nonobstant toute indication spécifique concernant des groupes particuliers de personnel, la présente décision s'applique aux Membres de la Cour des comptes, au personnel de la Cour des comptes couvert par le statut et par le régime applicable aux autres agents de l'Union européenne[2], aux experts nationaux détachés auprès de la Cour des comptes (END), aux prestataires de services et à leur personnel, aux stagiaires et à toute personne ayant accès aux bâtiments et autres propriétés de la Cour des comptes, ou à des informations gérées par la Cour des comptes.

6. Sauf indication contraire, les dispositions relatives aux ICUE s'appliquent de manière équivalente aux informations classifiées visées au paragraphe 2, point b) et c), du présent article.

Article 2. **Définitions**

Aux fins de la présente décision, on entend par:

a) «autorisation d'accès aux ICUE», une décision du directeur des Ressources humaines, finances et services généraux de la Cour des comptes prise en fonction d'une assurance donnée par une autorité compétente d'un État membre attestant qu'un fonctionnaire de la Cour des comptes, un autre agent ou un expert national détaché peut, pour autant que son besoin d'en connaître ait été établi et qu'il ait été correctement informé des responsabilités qui lui incombent en la matière, être autorisé à avoir accès aux ICUE jusqu'à un niveau de classification donné (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur) jusqu'à une date donnée; l'individu en question est alors «autorisé sécurité»;

b) «classification», l'attribution d'un niveau de classification à une information selon le degré de préjudice qui pourrait être causé par sa divulgation non autorisée;

c) «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;

---

[1] Voir 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 du 4 mai 2011 et son annexe (JO C 202 du 8 juillet 2011, p. 13).

[2] Règlement n° 31 (CEE) fixant le statut des fonctionnaires et le régime applicable aux autres agents, tel que modifié, JO 045 du 14.6.1962, p. 1385 (https://eur-lex.europa.eu/eli/reg/1962/31(1)/2020-01-01).

d) «déclassification», la suppression de toute classification de sécurité;

e) «document», toute information enregistrée, quelles qu'en soient la forme ou les caractéristiques physiques;

f) «déclassement», le passage à un niveau de classification de sécurité inférieur;

g) «habilitation de sécurité d'établissement», une décision administrative prise par une autorité de sécurité compétente selon laquelle, du point de vue de la sécurité, un établissement peut assurer un niveau suffisant de protection pour les ICUE d'un niveau de classification de sécurité déterminé;

h) «traitement» d'ICUE, l'ensemble des actions dont les ICUE sont susceptibles de faire l'objet tout au long de leur cycle de vie: création, enregistrement, traitement, transport, déclassement, déclassification et destruction. En ce qui concerne les systèmes d'information et de communication (SIC), sont en outre compris leur collecte, leur affichage, leur transmission et leur stockage;

i) «détenteur», une personne dûment autorisée qui, sur la base d'un besoin d'en connaître avéré, est en possession d'informations classifiées d'ICUE et à laquelle il incombe d'en assurer la protection;

j) «autorité de sécurité de l'information», le responsable de la sécurité de l'information à la Cour des comptes européenne, qui peut déléguer, en tout ou en partie, l'exécution des tâches prévues par la présente décision;

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

l) «matériel», tout média, support de données ou élément de machine ou d'équipement;

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

n) «habilitation de sécurité du personnel» (HSP), une déclaration émanant d'une autorité compétente d'un État membre établie à la suite d'une enquête de sécurité menée par les autorités compétentes d'un État membre et attestant qu'une personne peut, pour autant que son besoin d'en connaître ait été établi et qu'elle ait été correctement informée des responsabilités qui lui incombent en la matière, être autorisée à avoir accès aux ICUE jusqu'à un niveau de classification donné (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur) jusqu'à une date donnée;

o) «certificat d'habilitation de sécurité du personnel» (CHSP), un certificat délivré par la direction Ressources humaines, finances et services généraux de la Cour des comptes attestant qu'une personne détient une habilitation de sécurité valable ou une autorisation de sécurité, indiquant le niveau de classification des ICUE auquel l'intéressé peut se voir accorder l'accès (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur), la durée de validité de l'habilitation ou autorisation de sécurité correspondante et la date d'expiration du certificat;

p) «autorité de sécurité physique», le chef de la sécurité de la Cour des comptes, qui est responsable de la mise en œuvre des mesures et procédures de sécurité physique nécessaires à la protection des ICUE;

q) «bureau d'enregistrement», une entité administrée par le secrétariat de la Cour et située dans une zone administrative relevant de la responsabilité du directeur des Ressources humaines, finances et services généraux de la Cour. Il est responsable des entrées et des sorties des informations RESTREINT UE/EU RESTRICTED, ou équivalentes, échangées avec la Cour des comptes;

r) «bureau d'ordre pour les ICUE», une entité située au sein d'une zone sécurisée. Celui-ci est géré par l'agent contrôleur de la Cour des comptes, qui dispose d'une habilitation de sécurité et d'une autorisation d'accès aux ICUE. Ce bureau est responsable des entrées et des sorties des informations CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, ou équivalentes, échangées avec la Cour des comptes;

s) «autorité d'homologation de sécurité» (AHS), le directeur des Ressources humaines, finances et services généraux de la Cour des comptes.

Article 3. **Mesures de protection des ICUE**

1. La Cour des comptes assure la protection de toute information classifiée qui lui est transmise, d'une manière correspondant à son niveau de classification déterminé par l'autorité d'origine et selon les dispositions de la présente décision.

2. À cette fin, la Cour des comptes soumet le traitement de toutes les ICUE à des mesures de sécurité physique et, si nécessaire, de sécurité concernant le personnel, y compris à des autorisations d'accès pour les personnes identifiées et à des mesures de protection concernant les systèmes d'information et de communication. Ces mesures sont définies aux articles 4 à 6 et s'appliquent tout au long du cycle de vie des ICUE. Elles sont proportionnées au niveau de classification de sécurité, à la forme sous laquelle se présentent les informations ou les matériels ainsi qu'à leur volume, au lieu et à la construction des établissements où se trouvent les ICUE et à la menace, évaluée à l'échelle locale, que représentent les activités malveillantes et/ou criminelles, y compris l'espionnage, le sabotage et le terrorisme.

3. Les ICUE sont protégées par des mesures de sécurité physique; les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur seront en outre protégées par des mesures de sécurité concernant le personnel.

4. Les ICUE ne sont communiquées qu'aux personnes ayant un «besoin d'en connaître» au sein de l'institution. Il incombe au détenteur de tout élément d'ICUE de le protéger conformément à la présente décision.

5. Les ICUE ne font l'objet d'aucune divulgation écrite ou orale. Les observations préliminaires, les rapports, avis, communiqués de presse et autres produits de la Cour des comptes, ses sites internet et intranet, les interventions orales, les réponses aux demandes d'accès aux documents[3] ainsi que les enregistrements vocaux ou vidéo ne contiennent ni extrait ni référence à des ICUE. Cependant si l'autorité d'origine a publié des documents ou des informations contenant une référence à une ICUE, cette référence peut être mentionnée.

6. Nonobstant le paragraphe 5, la Cour des comptes et l'autorité d'origine peuvent convenir que pour un audit en particulier, la Cour des comptes soit autorisée à reproduire ou à utiliser des éléments d'ICUE dans un document. Dans ce cas, le document de la Cour des comptes concerné est dans un premier temps envoyé à l'autorité d'origine des ICUE concernées avant ou pendant la procédure contradictoire. La Cour des comptes et l'autorité d'origine s'entendent alors sur la nécessité de classifier ou non le document émis par la Cour des comptes. Lorsqu'un Membre rapporteur de la Cour des comptes estime nécessaire de transmettre un rapport d'audit ayant été classifié, en tout ou partie, à certains destinataires au sein du Parlement européen ou du Conseil - en tenant compte de toutes les mesures de sécurité de la présente décision -, le consentement de l'autorité d'origine de l'information classifiée est requis. Le cadre juridique et la procédure d'échange d'un tel document sont énoncés à l'article 7.

[3] En application de la décision n° 12-2005 de la Cour des comptes relative à l'accès du public aux documents de la Cour, modifiée par la décision n° 14-2009 de la Cour des comptes (JO C 67 du 20.3.2009, p. 1).

7. Lorsque la Cour, pour exercer son mandat, estime devoir partager plus largement certains éléments provenant d'un document ou d'informations classifiés, elle doit - en tenant dûment compte du marquage de classification de sécurité - consulter l'autorité d'origine avant de décider d'utiliser ces éléments ou informations, si elle est d'avis qu'il existe un intérêt public supérieur de ce faire. Les informations ne sont utilisées dans le rapport que de manière à ce que l'intérêt de l'autorité d'origine ne soit pas lésé. Cela peut être garanti de manière appropriée en invitant l'autorité d'origine à formuler des commentaires afin de parvenir à un accord sur la façon d'anonymiser les informations, de les condenser ou de les généraliser, etc., tout en respectant les intérêts des principaux concernés par les informations publiées.

8. La Cour des comptes ne transmet pas d'ICUE à une autre institution, agence, organe ou organisme de l'Union, à un État membre, à un État tiers ou à une organisation internationale sans consultation préalable ni autorisation écrite explicite de l'autorité d'origine.

9. À moins que l'autorité d'origine de documents classifiés SECRET UE/EU SECRET ou d'un niveau de classification inférieur ait imposé de restrictions à leur duplication ou à leur traduction, lesdits documents peuvent être dupliqués ou traduits à la demande du détenteur et conformément aux instructions pratiques de l'autorité de sécurité de l'information de la Cour des comptes. Les mesures de sécurité applicables au document original le sont aussi à ses copies et à ses traductions.

10. Si la Cour des comptes a besoin qu'un document classifié qui lui a été transmis, ou dont l'accès lui a été autorisé, soit déclassé ou déclassifié, elle doit consulter l'autorité d'origine pour lui demander si cette dernière peut lui fournir une version déclassée ou déclassifiée dudit document.

Article 4. Mesures de sécurité concernant le personnel

1. Les Membres de la Cour des comptes sont, en vertu de leurs fonctions, réputés autorisés à accéder aux ICUE et à participer aux réunions au cours desquelles des ICUE sont traitées. Les Membres de la Cour des comptes sont informés de leurs obligations en matière de sécurité en ce qui concerne la protection des ICUE et reconnaissent par écrit les responsabilités qui leur incombent en matière de protection de ces informations.

2. Un membre du personnel de la Cour des comptes soumis au statut ou au régime applicable aux autres agents ou un expert national détaché (END) ne peut se voir accorder l'accès aux ICUE qu'après:

   i. que son besoin d'en connaître a été établi;

   ii. avoir été informé des règles de sécurité applicables à la protection des ICUE ainsi que des normes et lignes directrices correspondantes en matière de sécurité, et avoir reconnu par écrit les responsabilités qui lui incombent en matière de protection de ces informations;

   iii. pour les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, s'être vu accorder une habilitation de sécurité et une autorisation d'accès.

3. La procédure ayant pour but de déterminer si un fonctionnaire ou un autre agent de la Cour des comptes, compte tenu de sa loyauté, de son intégrité et de sa fiabilité, peut être autorisé à accéder à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL après obtention de l'assurance par les autorités compétentes d'un État membre visée à l'article 2, point n), est précisée dans une décision déléguée prise en application de l'article 10, paragraphe 10. La décision d'accorder une autorisation d'accès est prise par le directeur des Ressources humaines, finances et services généraux de la Cour des comptes.

4. Le directeur des Ressources humaines, finances et services généraux de la Cour des comptes peut délivrer un CHSP précisant le niveau de classification des ICUE auquel l'intéressé peut se voir accorder l'accès (CONFIDENTIEL UE/EU CONFIDENTIAL ou un niveau supérieur), la durée de validité de l'autorisation d'accès à des ICUE correspondante et la date d'expiration du CHSP.

5. Seules les personnes disposant de l'autorisation visée au paragraphe 2, sous iii), du présent article et les Membres de la Cour des comptes, conformément au paragraphe 1 dudit article, peuvent être autorisés à participer à des réunions lors desquelles des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont traitées. La Cour des comptes et l'autorité d'origine conviennent, au cas par cas, des modalités pratiques relatives à ces réunions.

6. Les services de la Cour des comptes chargés de l'organisation des réunions lors desquelles des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont traitées informent l'autorité de sécurité de l'information de la Cour des comptes suffisamment à l'avance des dates, heures, lieux et participants de ces réunions.

7. Toute personne qui est en possession d'une ICUE sans y avoir été dûment autorisée et/ou en l'absence d'un besoin d'en connaître avéré est tenue de signaler la situation à l'autorité de sécurité de l'information dans les plus brefs délais et d'assurer la protection de l'ICUE conformément à la présente décision.

Article 5. Mesures de sécurité physique visant à protéger les informations classifiées

1. Par «sécurité physique», on entend l'utilisation de mesures physiques et techniques de protection pour empêcher l'accès non autorisé aux ICUE.

2. Les mesures de sécurité physique sont destinées à faire obstacle à toute intrusion par la ruse ou par la force, à avoir un effet dissuasif, à empêcher et détecter les actes non autorisés et permettre d'établir une distinction entre les membres du personnel au regard de l'accès aux ICUE conformément au principe du besoin d'en connaître. Ces mesures sont déterminées sur la base d'une procédure de gestion des risques, conformément à la présente décision.

3. Les zones dans lesquelles les ICUE sont traitées ou stockées font l'objet d'une inspection régulière par l'autorité de sécurité compétente de la Cour des comptes.

4. Seuls des équipements ou des dispositifs conformes aux règles applicables au sein des institutions, agences ou organes de l'UE en matière de protection des ICUE sont utilisés pour traiter et stocker les ICUE.

5. Le personnel de la Cour des comptes peut accéder aux ICUE classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, ou équivalent, dans des zones sécurisées situées en dehors des locaux de la Cour des comptes.

6. La Cour des comptes peut conclure un accord de service avec une autre institution de l'UE 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. Sauf accord spécifique de l'autorité d'origine, ces ICUE ne sont ni traitées ni stockées dans les locaux de la Cour des comptes et ne font l'objet d'aucune duplication ou traduction par la Cour des comptes.

7. Les informations RESTREINT UE/EU RESTRICTED reçues sont enregistrées par la Cour des comptes. La consultation d'informations classifiées CONFIDENTIEL UE/UE CONFIDENTIAL ou d'un niveau de classification supérieur, ou équivalent, en dehors des locaux de la Cour est enregistrée à des fins de sécurité.

8. Les ICUE RESTREINT UE/EU RESTRICTED peuvent être stockées dans un meuble de bureau adapté et fermé dans une zone administrative ou une zone sécurisée. Les ICUE classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET sont stockées en vertu d'un accord de service dans un meuble de sécurité situé dans une zone sécurisée d'une autre institution européenne au Luxembourg.

9. En dehors du bureau d'ordre, les ICUE sont transmises entre les services et les locaux selon les modalités suivantes:

   a) en règle générale, les ICUE sont transmises par voie électronique protégée par des produits cryptographiques agréés conformément à l'article 6, paragraphe 8;

   b) si la voie visée au point a) n'est pas utilisée, les ICUE sont transportées sur des supports électroniques (par exemple clé USB, CD, disque dur) protégés par des produits cryptographiques agréés conformément à l'article 6, paragraphe 8, ou en version papier dans une enveloppe opaque scellée.

10. Les informations RESTREINT UE/EU RESTRICTED peuvent être détruites par leur détenteur, selon les règles en matière d'archivage applicables à la Cour des comptes. La destruction d'informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur est effectuée uniquement par l'agent contrôleur, à la demande du détenteur ou d'une autorité compétente conformément aux règles en matière d'archivage applicables à la Cour des comptes. La destruction de documents classifiés SECRET UE/EU SECRET est effectuée en présence d'un témoin justifiant de l'habilitation de sécurité correspondant au moins au niveau de classification du document à détruire. L'agent contrôleur et le témoin, lorsque la présence de ce dernier est requise, signent un procès-verbal de destruction, qui est rempli dans le bureau d'ordre. L'agent contrôleur conserve les procès-verbaux de destruction des documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET pendant cinq ans au minimum.

11. L'autorité de sécurité physique et l'autorité de sécurité de l'information établissent un plan conjoint tenant compte des conditions locales pour assurer la sauvegarde des ICUE en temps de crise, y compris si nécessaire des plans de destruction et d'évacuation en cas d'urgence. Elles émettent les consignes qu'elles jugent appropriées pour éviter que des ICUE ne tombent entre les mains de personnes non autorisées.

12. En cas de transport des ICUE, la Cour des comptes se soumet aux mesures de protection exigées par l'autorité d'origine destinées à les protéger contre toute divulgation non autorisée durant le transport.

13. Les mesures de sécurité physique concernant les zones administratives dans lesquelles sont traitées et stockées des informations RESTREINT UE/EU RESTRICTED sont précisées dans l'annexe.

Article 6. **Protection des ICUE dans les systèmes d'information et de communication**

1. Aux fins du présent article, on entend par «système d'information et de communication» tout système permettant le traitement d'ICUE sous forme électronique. Un système d'information et de communication comprend l'ensemble des moyens nécessaires pour le faire fonctionner, y compris l'infrastructure, l'organisation, le personnel et les ressources d'information.

2. On entend par «utilisateur légitime» un Membre, un fonctionnaire, un autre agent ou un expert national détaché de la Cour des comptes qui a un besoin d'accès établi et reconnu à un système d'information spécifique.

3. La Cour des comptes fournit l'assurance que ses systèmes protégeront les informations qu'ils traitent et fonctionneront comme ils le doivent, quand ils le doivent, sous le contrôle d'utilisateurs légitimes. À cette fin, ils garantissent des niveaux appropriés:
   - d'«authenticité»: garantie que l'information est véridique et émane de sources dignes de foi;
   - de «disponibilité»: caractéristique de l'information selon laquelle elle est accessible et utilisable, à la demande d'une entité autorisée;
   - de «confidentialité»: propriété selon laquelle les informations ne sont pas divulguées à des personnes ou à des entités non autorisées et l'accès à ces informations n'est pas accordé à des processus non autorisés;
   - d'«intégrité»: propriété consistant à préserver l'exactitude et le caractère complet des informations et éléments;
   - de «non-répudiation»: la possibilité de prouver qu'une action ou un événement a eu lieu, de sorte qu'il ne peut être contesté par la suite.

   Cette assurance est fondée sur un processus de gestion des risques. On entend par «risque» la possibilité qu'une menace donnée se concrétise en tirant parti des vulnérabilités internes et externes d'une organisation ou d'un des systèmes qu'elle utilise et cause ainsi un préjudice à l'organisation ou à ses ressources matérielles ou immatérielles. Il se mesure en tenant compte à la fois de la probabilité de voir se concrétiser des menaces et de l'impact de celles-ci. Le processus de gestion des risques se compose des étapes suivantes: identification des menaces et des vulnérabilités, évaluation des risques, traitement des risques, acceptation des risques et communication des risques:

   - l'«évaluation des risques» consiste à déterminer les menaces et les vulnérabilités et à procéder à l'analyse des risques correspondants, c'est-à-dire à examiner leur probabilité et leur impact;
   - le «traitement des risques» consiste à atténuer, à éliminer, à réduire (par un ensemble approprié de mesures sur le plan technique, physique ou au niveau de l'organisation ou des procédures), à transférer ou à surveiller les risques;
   - l'«acceptation des risques» consiste à décider d'accepter qu'un risque résiduel subsiste au terme du traitement des risques;
   - on entend par «risque résiduel» le risque qui subsiste après que des mesures de sécurité ont été mises en œuvre, étant entendu qu'il est impossible de contrer toutes les menaces et d'éliminer toutes les vulnérabilités;
   - la «communication des risques» consiste à sensibiliser la communauté des utilisateurs d'un système d'information et de communication aux risques, à informer les autorités d'homologation de ces risques et à faire rapport à leur sujet aux autorités responsables de l'exploitation.

4. L'ensemble des dispositifs et équipements électroniques utilisés pour le traitement des ICUE sont conformes aux règles applicables en matière de protection des ICUE. La préférence est accordée aux dispositifs et équipements électroniques qui ont déjà été homologués par une autre institution, une autre agence ou un autre organe de l'UE. La sécurité des dispositifs est garantie tout au long de leur cycle de vie.

5. Le système d'information et de communication (SIC) de la Cour des comptes utilisé pour le traitement des ICUE est homologué par une autorité compétente. À cette fin, la Cour des comptes s'efforce de conclure un accord de service avec l'autorité d'homologation de sécurité d'une institution de l'UE ayant la capacité d'accorder une homologation à un SIC traitant des ICUE, en vue de la délivrance d'une déclaration d'homologation pour le traitement des informations RESTREINT UE/EU RESTRICTED par le SIC de la Cour des comptes, avec les modalités et les conditions de fonctionnement correspondantes. Cet accord de service fait également référence aux normes à appliquer à la procédure d'homologation et est conclu conformément à la procédure prévue à l'article 10, paragraphe 3.

6. Si la Cour des comptes doit mettre en place sa propre procédure d'homologation pour son SIC, une décision déléguée comme celle visée à l'article 10, paragraphe 10, de la présente décision établit la procédure conformément aux normes relatives à la procédure d'homologation pour les SIC traitant des ICUE dans les autres institutions, agences et organes de l'UE.

7. La responsabilité de la préparation des dossiers d'homologation et de la documentation conformément aux normes applicables incombe entièrement au détenteur du SIC.

8. Lorsque la protection des ICUE est assurée par des produits cryptographiques, la Cour des comptes donne la préférence à des produits agréés par le Conseil ou par le secrétaire général du Conseil en sa qualité d'autorité d'agrément cryptographique ou, à défaut, à ceux agréés par d'autres institutions, agences et organes de l'UE pour la protection des ICUE.

9. Les informations RESTREINT UE/EU RESTRICTED sont traitées uniquement sur des dispositifs électroniques (postes de travail, imprimantes, photocopieuses, etc.) situés dans une zone administrative ou une zone sécurisée. Les dispositifs électroniques qui traitent les informations RESTREINT UE/EU RESTRICTED sont séparés des autres réseaux informatiques et protégés par des mesures physiques ou techniques appropriées.

10. L'ensemble du personnel de la Cour des comptes participant à l'élaboration, au développement, aux essais, au fonctionnement, à la gestion ou à l'utilisation des SIC traitant des ICUE notifie au responsable de la sécurité de l'information toutes les faiblesses potentielles en matière de sécurité, les incidents, les infractions à la sécurité ou les compromissions susceptibles d'avoir un impact sur la protection du SIC et/ou des ICUE qu'il contient.

Article 7. **Procédure d'échange et d'autorisation d'accès aux informations classifiées**

1. Lorsqu'ils sont légalement tenus de le faire en vertu des traités ou des actes juridiques adoptés sur la base des traités, les institutions, agences, organes et organismes de l'UE ainsi que les autorités nationales fournissent à la Cour des comptes, de leur propre initiative ou à la demande écrite du président, du/des Membre(s) rapporteur(s) ou du secrétaire général, l'accès aux ICUE selon la procédure décrite ci-après.

2. Les demandes d'accès sont adressées aux institutions concernées par l'intermédiaire du bureau d'enregistrement de la Cour des comptes.

3. Pour autant que de besoin, la Cour des comptes conclut un arrangement administratif couvrant les modalités pratiques de l'échange d'ICUE ou d'informations équivalentes.

4. Aux fins de la conclusion de tels arrangements administratifs, la Cour des comptes fournit à l'autorité d'origine toutes les informations nécessaires relatives à son système de sécurité de l'information. Si nécessaire, une visite d'évaluation est organisée.

5. Ces arrangements administratifs sont conclus dans le plein respect des principes d'attribution et de coopération loyale énoncés à l'article 13 du traité sur l'Union européenne, et conformément à la procédure prévue à l'article 10, paragraphe 4.

6. En l'absence d'arrangement administratif avec une institution, un organe ou une agence de l'UE, un État tiers ou une organisation internationale concernant la transmission d'informations classifiées à la Cour des comptes, cette dernière signe une déclaration d'engagement visant à protéger les informations classifiées dont elle est destinataire.

Article 8. **Infraction à la sécurité, perte ou compromission d'informations classifiées**

1. Une infraction à la sécurité est un acte ou une omission commis par une personne qui est contraire aux règles de sécurité énoncées dans la présente décision et ses modalités d'application.

2. Il y a compromission lorsque, à la suite d'une infraction à la sécurité, des ICUE ont été divulguées en totalité ou en partie à des personnes non autorisées.

3. Toute infraction à la sécurité, réelle ou présumée, est immédiatement signalée à l'autorité de sécurité de l'information de la Cour des comptes.

4. Lorsqu'il est avéré ou qu'il existe des motifs raisonnables de supposer que des ICUE ont été compromises ou perdues, l'autorité de sécurité de l'information en informe le directeur des Ressources humaines, finances et services généraux ainsi que le secrétaire général de la Cour des comptes. Le directeur des Ressources humaines, finances et services généraux en informe immédiatement l'autorité de sécurité de l'autorité d'origine. Il procède à une enquête et informe le secrétaire général de la Cour des comptes et l'autorité de sécurité de l'autorité d'origine des résultats de cette enquête et des mesures prises pour éviter que les faits ne se reproduisent. Lorsqu'un Membre de la Cour des comptes est concerné, le président de la Cour des comptes est responsable de l'action à mener en collaboration avec le secrétaire général de la Cour.

5. Tout fonctionnaire ou agent de la Cour des comptes qui est responsable d'une infraction aux règles de sécurité énoncées dans la présente décision et dans ses modalités d'application est passible des sanctions prévues dans le statut des fonctionnaires de l'Union européenne et le régime applicable aux autres agents de l'Union européenne.

6. Tout Membre de la Cour des comptes responsable d'un manquement aux dispositions énoncées dans la présente décision est passible de mesures et de sanctions conformément à l'article 286, paragraphe 6, du traité.

7. Toute personne responsable de la perte ou de la compromission d'ICUE est passible de sanctions disciplinaires et/ou peut faire l'objet d'une action en justice conformément aux dispositions législatives et réglementaires applicables.

Article 9. **Sécurité en cas d'intervention externe**

1. La Cour des comptes peut confier la réalisation de tâches impliquant ou nécessitant, en vertu de leur contrat, l'accès à des ICUE à des contractants immatriculés dans un État membre, notamment dans le cadre de la maintenance de systèmes d'information et de communication et du réseau informatique.

2. En cas d'intervention externe, la Cour des comptes prend toutes les mesures de sécurité nécessaires énoncées au paragraphe 3 du présent article, y compris la demande d'une habilitation de sécurité d'établissement, visant à assurer la protection des ICUE par les candidats ou les soumissionnaires tout au long de la durée d'une procédure d'appel d'offres et de passation de marché, ainsi que par des contractants ou des sous-traitants tout au long du cycle de vie des contrats. Le pouvoir adjudicateur veille à ce que les normes minimales de sécurité prévues dans la présente décision soient mentionnées dans les contrats afin que les contractants soient tenus de les respecter.

3. Les règles de sécurité, les procédures de marché et les modèles pour les contrats et contrats de sous-traitance impliquant l'accès à des ICUE, les avis de marché, les documents d'orientation concernant les conditions dans lesquelles des habilitations de sécurité d'établissement et du personnel sont requises, les instructions de sécurité relatives à un programme/un projet, les annexes de sécurité, les visites, la transmission et le transport d'ICUE dans le cadre de ces contrats, sont conformes à ceux établis par la Commission européenne pour les contrats classifiés visés dans 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.

Article 10. **Mise en œuvre de la décision et responsabilités connexes**

1. Les services de la Cour des comptes prennent toutes les mesures nécessaires dans le cadre de leur responsabilité pour veiller à ce que, lors du traitement ou du stockage d'ICUE ou de toute autre information classifiée, la présente décision et les modalités d'application correspondantes soient appliquées.

2. Le secrétaire général est l'autorité investie du pouvoir de nomination et l'autorité habilitée à conclure les contrats d'engagement pour tous les fonctionnaires et autres agents. Il peut déléguer au directeur des Ressources humaines, finances et services généraux la responsabilité d'accorder aux fonctionnaires et autres agents l'autorisation d'accéder à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, d'exercer sa fonction d'autorité d'homologation de sécurité et de superviser le secrétariat de la Cour en ce qui concerne le traitement d'ICUE.

3. Le secrétaire général est compétent pour conclure des accords de service relatifs à l'homologation des équipements et systèmes d'information et de communication de la Cour des comptes, à l'utilisation d'une zone sécurisée dans une autre institution de l'UE et à la procédure de demande d'habilitation de sécurité du personnel pour accéder aux ICUE.

4. Le directeur des Ressources humaines, finances et services généraux est compétent pour conclure des arrangements administratifs avec les institutions, agences et autres organes de l'UE relatifs à l'échange d'ICUE dont la Cour des comptes a besoin pour accomplir son mandat. Il peut également conclure des arrangements administratifs avec des États tiers ou des organisations internationales relatifs à la protection des informations classifiées reçues.

5. Le directeur des Ressources humaines, finances et services généraux est compétent pour signer toute déclaration d'engagement à protéger les ICUE fournies dans le cadre d'une transmission ad hoc exceptionnelle.

6. Le responsable de la sécurité de l'information de la Cour des comptes fait office d'autorité de sécurité de l'information. Le responsable de la sécurité de l'information et les personnes à qui il délègue tout ou partie de ses tâches disposent d'une habilitation de sécurité appropriée. L'autorité de sécurité de l'information assume ses responsabilités en coopération étroite avec la direction Ressources humaines, finances et services généraux, la direction Information, environnement de travail et innovation, ainsi que la direction du comité chargé du contrôle qualité de l'audit (voir notamment les articles 4, 6 et 8). L'autorité de sécurité de l'information est également responsable des réunions de formation et de sensibilisation sur la sécurité de l'information ainsi que des inspections périodiques visant à vérifier le respect de la présente décision, y compris en cas d'intervention externe, et des éventuelles mesures à prendre pour assurer son respect.

7. Le chef de la sécurité physique est en charge des mesures de sécurité physique (voir notamment l'article 5).

8. Un bureau d'enregistrement créé au sein du secrétariat général de la Cour constitue le point d'entrée et de sortie des informations classifiées RESTREINT UE/EU RESTRICTED échangées entre la Cour des comptes et d'autres institutions, agences, organes et des États membres de l'UE. Il constitue également le point d'entrée et de sortie pour des informations équivalentes provenant d'États tiers et d'organisations internationales. Le bureau d'enregistrement est organisé conformément aux dispositions d'une décision déléguée. L'agent responsable du bureau d'enregistrement assume les principales responsabilités suivantes:

   a) enregistrement de l'entrée et de la sortie des informations classifiées RESTREINT UE/EU RESTRICTED;

   b) gestion des zones administratives dédiées à l'enregistrement du traitement, du stockage et de la consultation des ICUE classifiées RESTREINT UE/EU RESTRICTED.

9. Un bureau d'ordre est créé au titre d'un accord de service relatif à l'utilisation d'une zone sécurisée dans une autre institution de l'UE. Ce bureau d'ordre, mis en place par le secrétariat de la Cour et sous la responsabilité du directeur des Ressources humaines, finances et services généraux de la Cour des comptes, constitue le point d'entrée et de sortie des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL, ou d'un niveau de classification supérieur, échangées entre la Cour des comptes et d'autres institutions, agences, organes et des États membres de l'UE. Il constitue également le point d'entrée et de sortie des informations équivalentes provenant d'États tiers et d'organisations internationales. Il est équipé de coffres appropriés et autres équipements de sécurité adaptés à la protection d'informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL, ou d'un niveau de classification supérieur. Le bureau d'ordre est organisé conformément aux dispositions d'une décision déléguée. L'agent contrôleur dispose d'une habilitation de sécurité appropriée et assume les principales responsabilités suivantes:

   a) gestion des opérations relatives à l'enregistrement, la consultation, la conservation, la reproduction, la traduction, la transmission, l'expédition et, le cas échéant, la destruction des ICUE;

   b) exécution de toute autre tâche en relation avec la protection des ICUE définie dans la décision déléguée.

10. Le comité administratif adopte une décision déléguée fixant les modalités d'application de la présente décision. Le responsable de la sécurité de l'information établit les lignes directrices en matière de sécurité de l'information. Le comité chargé du contrôle qualité de l'audit définit les lignes directrices en matière d'audit.

Article 11. **Entrée en vigueur**

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

Fait à Luxembourg, le 3 juin 2021.

Par la Cour des comptes

Klaus-Heiner Lehne
Président

Annexe: MESURES DE SÉCURITÉ PHYSIQUE CONCERNANT LES ZONES ADMINISTRATIVES POUR ICUE

ANNEXE

MESURES DE SÉCURITÉ PHYSIQUE CONCERNANT LES ZONES ADMINISTRATIVES POUR ICUE

1. La présente annexe énonce les modalités d'application de l'article 5 de la décision. Il s'agit des règles minimales de protection physique des zones administratives pour les informations classifiées RESTREINT UE/EU RESTRICTED de la Cour des comptes, à savoir des zones dédiées à l'enregistrement, au stockage et à la consultation des informations classifiées RESTREINT UE/EU RESTRICTED.

2. Les mesures de sécurité physique pour les zones administratives sont destinées à prévenir l'accès non autorisé à ces zones, notamment:

   a) en établissant un périmètre défini de façon visible afin de permettre le contrôle des personnes;

   b) en octroyant l'accès sans escorte aux seules personnes dûment autorisées par l'autorité de sécurité de l'information de la Cour des comptes ou toute autre autorité compétente;

   c) en escortant en permanence toutes les autres personnes, ou en les soumettant à des contrôles équivalents.

3. L'autorité de sécurité de l'information de la Cour des comptes peut exceptionnellement délivrer une autorisation d'accès à des personnes non autorisées, y compris afin de travailler dans une zone administrative, sous réserve que l'accès à la zone administrative n'implique pas un accès à des ICUE, qui resteront protégées sous clé. L'accès de ces personnes ne peut se faire que si elles sont accompagnées et surveillées en permanence par l'autorité de sécurité de l'information de la Cour des comptes ou l'agent responsable du bureau d'enregistrement.

4. L'autorité de sécurité de l'information définit les procédures de gestion des clés et/ou des combinaisons pour toutes les zones administratives et les meubles de sécurité. Ces procédures visent à empêcher un accès non autorisé.

5. Les combinaisons doivent être mémorisées par le plus petit nombre possible de personnes qui ont besoin de les connaître. Les combinaisons des meubles de sécurité servant au stockage des informations RESTREINT UE/EU RESTRICTED doivent être changées:

   - à la réception d'un nouveau meuble de sécurité;
   - lors de tout changement du personnel connaissant la combinaison;
   - en cas de compromission, réelle ou présumée, de la combinaison;
   - si une serrure a fait l'objet d'un entretien ou d'une réparation;
   - au moins tous les 12 mois.

6. L'autorité de sécurité de l'information et le chef de la sécurité physique sont responsables du respect de ces règles.