Politique de classification des informations de la Cour des comptes européenne

Objectif

01 La présente politique a pour objet d'établir le cadre réglementaire selon lequel la Cour des comptes européenne (ci-après «la Cour») entend procéder à l'évaluation, à la classification, à la protection et au traitement de ses propres informations ainsi que de celles de tiers, en fonction de leur degré de sensibilité et de confidentialité. Elle vise à garantir que ces informations soient classées et traitées correctement et à réduire le risque de fuites, de modifications non autorisées ou de pertes.

02 La présente politique régit la classification et la gestion des informations «non classifiées de l'UE» à tous les échelons de la Cour, en vue d'appliquer et de maintenir un niveau de confidentialité approprié tout au long du cycle de vie des informations, à savoir de leur création ou réception à leur destruction en passant par leur enregistrement, leur partage ou échange, leur stockage et leur archivage. Elle fait également référence aux informations «classifiées de l'UE» et aux quatre catégories de confidentialité correspondantes.

03 La présente politique complète la politique de sécurité de l'information de la Cour[1]. Elle annule et remplace la politique de classification des informations précédente[2]. L'application de la présente politique s'appuie sur des lignes directrices générales en matière de classification des informations ainsi que sur des lignes directrices relatives à des activités spécifiques de la Cour[3].

Champ d'application

04 La présente politique s'applique à toutes les informations créées, détenues et gérées par la Cour, y compris les documents papier et les informations numériques stockées sur quelque type de support que ce soit. Elle définit les rôles et les responsabilités de toutes les personnes participant à la gestion de la classification des informations, qu'il s'agisse des membres de la Cour, des agents de la Cour ou de prestataires externes à la Cour.

05 Le présent règlement s'applique sans préjudice:

a) du règlement (UE) 2018/1725[4] du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données;

---

1 https://intranet.eca.eu/documentcenter/DEC/DEC%20 127 %2015/DFS066 064FR02-15MD-DEC127-15-information_security_policy-TRAN-s.pdf

2 https://ecanet.eca.eu/fr/secgen/sg3/ECADocuments/DFS070 432FR01-15PP-CP-68-TRs.pdf

3 Ces lignes directrices sont actuellement en cours d'élaboration.

4 https://eur-lex.europa.eu/eli/reg/2018/1725/oj

b) de la décision n° 12-2005[5] de la Cour des comptes européenne relative à l'accès du public aux documents de la Cour, modifiée par la décision n° 14-2009[6];

c) de la décision n° 6-2019[7] de la Cour des comptes européenne sur la politique d'ouverture des données et la réutilisation des documents;

d) du règlement (CEE, Euratom) n° 354/83[8] du Conseil du 1er février 1983 concernant l'ouverture au public des archives de la Communauté économique européenne et de la Communauté européenne de l'énergie atomique, modifié par le règlement (CE, Euratom) n° 1700/2003[9] du Conseil du 22 septembre 2003 et par le règlement (UE) 2015/496[10] du Conseil du 17 mars 2015.

Définitions

06 Aux fins de la présente politique, on entend par:

a) «processus automatisés»: l'utilisation de la technologie numérique pour des processus destinés à exécuter des séquences de tâches et des fonctions;

b) «disponibilité»: le fait d'être accessible et utilisable, à la demande d'une entité autorisée;

c) «RAA»: le régime applicable aux autres agents de l'Union européenne, tel qu'il a été défini dans le règlement n° 31 (CEE)[11], tel que modifié;

d) «classification»: l'attribution d'un niveau de confidentialité aux informations sur la base du caractère confidentiel de leur contenu;

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

f) «prestataire externe à la Cour»: les stagiaires, les prestataires de services qui travaillent dans les locaux de la Cour (intra-muros) et/ou dans leurs propres locaux (extra-muros);

g) «agents de la Cour»: les fonctionnaires, les agents temporaires et contractuels, ainsi que les experts nationaux détachés;

---

5 https://intranet.eca.eu/documentcenter/Decisions/Decision%20 012 %2005/012fr_FR.pdf

6 https://documentcenter.eca.eu/officialdocuments/Decisions/Decision%20 014 %2009/014fr_FR.pdf

7 https://documentcenter.eca.eu/officialdocuments/Decisions/Decision%20 006 %2019/SGL108 714FR02-19MD-D-006-2019-TRs.pdf

8 http://data.europa.eu/eli/reg/1983/354/oj

9 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32 003R1700

10 https://eur-lex.europa.eu/eli/reg/2015/496/oj

11 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:01 962R0031-20 200 101

h) «information classifiée de l'Union européenne» (ICUE): toute information ou tout matériel auxquels s'applique une classification de sécurité de l'UE;

i) «information»: toute information écrite ou orale, quel qu'en soit le support ou l'auteur. L'information peut être créée par la Cour et/ou fournie par des tiers;

j) «violation d'informations»: toute action ou omission ayant pour effet la divulgation partielle ou totale d'informations non publiques à des personnes non autorisées, ou la perte de telles informations;

k) «autorité d'origine de l'information»: tout tiers ayant transmis des informations à la Cour. Dans le cas des informations d'audit, il s'agit de l'organisme (ou de la personne) qui les a communiquées;

l) «système d'information»: un système qui stocke et gère l'information sous une forme numérisée;

m) «intégrité»: la propriété consistant à préserver l'exactitude et le caractère complet des informations et éléments;

n) «information non classifiée de l'Union européenne»: toute information qui n'est pas une ICUE. La Cour classifie ces informations en trois catégories: «Sensible», «Utilisation par la Cour» et «Public» (ci-après le «niveau de confidentialité à la Cour»);

o) «locaux»: tous les biens et possessions immeubles et assimilés de la Cour;

p) «accord de niveau de service»: un engagement contractuel conclu entre la Cour et un prestataire de services et précisant les aspects particuliers du service à fournir, y compris les dispositions en matière de sécurité des informations communiquées par la Cour ou la concernant;

q) «statut»: le régime applicable aux fonctionnaires de l'Union européenne, tel qu'il a été défini dans le règlement n° 31 (CEE), tel que modifié;

r) «tiers»: toute personne physique ou morale ou entité extérieure à la Cour, y compris les États membres, les autres institutions et organes de l'Union ou ceux extérieurs à celle-ci, et les pays tiers.

Principes

07 La sécurité de l'information impose de prendre toutes les mesures raisonnables pour protéger l'information contre tout accès, toute utilisation, toute divulgation, toute modification ou toute destruction non autorisés.

08 La présente politique est régie par les principes ci-après. Il en ira de même pour toute future ligne directrice dans ce domaine.

I. Discrétion professionnelle

09 Les règles et les lignes directrices définies dans la présente politique s'appuient sur l'obligation, pour les agents de la Cour, de s'abstenir de toute divulgation non autorisée d'informations portées à leur connaissance dans l'exercice de leurs fonctions conformément aux dispositions de l'article 17 du statut[12] et du cadre éthique[13] de la Cour.

II. Besoin d'en connaître

10 L'échange d'informations non publiques entre les membres de la Cour, les agents de la Cour et les prestataires externes à la Cour devrait se limiter aux seules informations nécessaires à l'exercice de leurs obligations professionnelles. Les droits d'accès octroyés aux utilisateurs des systèmes d'information de la Cour et aux processus automatisés doivent se limiter à ceux nécessaires pour la réalisation des tâches concernées.

Politique

11 Les informations non classifiées de l'Union européenne sont évaluées en fonction du préjudice que leur divulgation et/ou modification non autorisée peut causer aux intérêts de la Cour, à ceux de ses membres et de ses agents, ainsi qu'à ceux des autres institutions ou organes de l'UE ou de tout autre tiers. Le résultat de cette analyse détermine le niveau de confidentialité à la Cour.

12 Lorsque des informations agrégées contiennent des éléments présentant différents niveaux de confidentialité, le plus élevé d'entre eux doit s'appliquer.

13 Les informations reçues d'autres institutions de l'UE ou de tiers doivent conserver leur niveau de confidentialité d'origine, celui que la Cour attribuera devant être au moins équivalent.

---

[12] Cet article s'applique par analogie aux agents temporaires et contractuels (voir article 11, paragraphe 1, et article 81 du RAA).

[13] https://www.eca.europa.eu/fr/Pages/Ethics.aspx

14 Notre institution traitera et conservera toujours les informations avec le plus grand soin afin d'en préserver l'intégrité tout en garantissant un degré de disponibilité approprié.

15 Si un protocole d'accord relatif à l'échange de données est signé avec d'autres organismes officiels, il devra contenir un tableau de concordance entre les niveaux de classification de la Cour et les leurs.

16 Sur la base de ces principes, toute information créée, collectée ou reçue par la Cour se voit attribuer l'un des niveaux de confidentialité ci-après (le niveau de confidentialité par défaut est «UTILISATION PAR LA COUR», sauf pour les ICUE ou les informations auxquelles un autre niveau de confidentialité spécifique a été attribué).

I. PUBLIC

Information créée, collectée ou reçue par la Cour et susceptible, de par son contenu, d'être rendue accessible au monde extérieur sans préjudice. Il peut s'agir d'une information collectée auprès d'une source publique ou reçue d'une telle source, ou d'une information résultant des activités opérationnelles et administratives de la Cour, que celle-ci décide de rendre publique, notamment sous la forme de documents publiés.

II. UTILISATION PAR LA COUR (niveau par défaut)

Information de travail non publique créée, collectée ou reçue par la Cour dans le cadre de ses activités opérationnelles et administratives, à laquelle s'appliquent le principe général de discrétion professionnelle visé à l'article 17 du statut[14] et le cadre éthique de l'institution, et qui ne requiert pas de niveau de confidentialité supérieur.

L'accès aux informations du niveau «UTILISATION PAR LA COUR» est accordé aux agents de la Cour et aux prestataires externes à la Cour sur la base du besoin d'en connaître, selon les différentes étapes du processus d'audit ou dans le cadre d'autres activités de traitement de l'information qui leur sont confiées.

[14] Cet article s'applique par analogie aux agents temporaires et contractuels (voir article 11, paragraphe 1, et article 81 du RAA).

III. SENSIBLE

Information que la Cour est tenue de protéger en vertu d'obligations légales énoncées dans les traités ou d'autres actes juridiques, en vue de préserver les droits et les intérêts des institutions de l'UE ainsi que des personnes physiques ou morales concernées.

La Cour est tenue de respecter strictement le principe de non-divulgation des informations SENSIBLES aux personnes non autorisées en recourant à des procédures spécifiques de traitement et de stockage de ce type d'informations.

L'accès à une information SENSIBLE est soumis à l'accord explicite de son propriétaire.

IV. CLASSIFIÉ UE

Toute «information classifiée de l'Union européenne» (ICUE) à laquelle une institution de l'UE ou un État membre a attribué l'un des niveaux suivants:

RESTREINT UE / EU RESTRICTED – niveau de classification de sécurité de l'UE appliqué aux 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;

CONFIDENTIEL UE / EU CONFIDENTIAL – niveau de classification de sécurité de l'UE appliqué aux 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;

SECRET UE / EU SECRET – niveau de classification de sécurité de l'UE appliqué aux 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;

TRÈS SECRET UE/EU TOP SECRET – niveau de classification de sécurité de l'UE appliqué aux 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.

Rôles et responsabilités

17 Le **propriétaire de l'information** peut être le président, un membre, le secrétaire général, un directeur, le président d'une commission ou d'un comité de la Cour, ou tout autre agent de celle-ci chargé d'une procédure par ou pour laquelle des informations sont créées, collectées et/ou reçues. Il est tenu de veiller à ce que les informations dont

il est responsable soient classifiées et gérées dans le respect de la présente politique et de ses lignes directrices.

18 Dans le cas des informations liées à une activité d'audit, le propriétaire de l'information est le membre rapporteur. Il peut désigner un gestionnaire de l'information (en l'occurrence un directeur, un manager principal ou un chef de mission) et lui déléguer ses tâches.

19 Le **gestionnaire de l'information** est chargé de superviser le traitement, la gestion et la protection des informations pour le compte du propriétaire de l'information et de faire rapport à ce propos.

20 L'**utilisateur de l'information** désigne tout membre de la Cour, tout agent de la Cour ou tout prestataire externe à la Cour qui interagit avec l'information.

a) Tous les agents de la Cour sont tenus par un devoir de confidentialité et s'engagent à respecter toutes leurs obligations en matière de confidentialité et de non-divulgation découlant de l'article 17 du statut[15].

b) L'ensemble des prestataires externes à la Cour sont tenus de se conformer aux règles de confidentialité et de non-divulgation dans le cadre de leurs obligations contractuelles à l'égard de l'institution.

c) L'ensemble des agents de la Cour et des prestataires externes à la Cour sont tenus de traiter l'information dans le respect du niveau de classification à la Cour que son propriétaire lui a attribué.

d) L'ensemble des agents de la Cour et des prestataires externes à la Cour doivent signaler les incidents liés à l'application de la présente politique au gestionnaire de l'information.

21 **Dépositaires de l'information** – En ce qui concerne les données stockées dans les systèmes d'information: il s'agit des «administrateurs IT» de la Cour chargés de gérer les systèmes, les bases de données et les serveurs utilisés pour le stockage des informations de l'institution, d'en assurer la maintenance et de prendre les mesures de sauvegarde appropriées.

22 Les **dépositaires de l'information par contrat** sont des entités ou sociétés externes avec lesquelles la Cour a conclu un contrat portant sur la mise en œuvre et la maintenance des systèmes, des bases de données et des serveurs utilisés pour le stockage des informations de l'institution, ainsi que sur la prise de mesures de

[15] Cet article s'applique par analogie aux agents temporaires et contractuels (voir article 11, paragraphe 1, et article 81 du RAA).

sauvegarde appropriées. Les mesures de sécurité applicables sont définies dans un accord de niveau de service entre la Cour et les contractants.

23 Le **responsable de la sécurité de l'information** est en charge de la sécurité de toutes les informations.

24 Le **délégué à la protection des données (DPD)** est responsable de la protection des données à caractère personnel détenues et/ou traitées par la Cour.

25 Le **chef de la sécurité** est responsable de la mise en œuvre des mesures et procédures de sécurité physique nécessaires à la protection de l'information.

26 Les lignes directrices de la Cour en matière de classification des informations ainsi que d'autres lignes directrices spécifiques précisent les rôles et les responsabilités des divers acteurs susmentionnés, dans le but de garantir et de faciliter l'application de la présente politique.

Traitement des violations d'informations

27 Tout agent de la Cour ou tout prestataire externe à la Cour qui aurait connaissance d'une violation avérée ou présumée de la sécurité doit la signaler immédiatement au responsable de la sécurité de l'information.

28 Toute personne responsable de la compromission ou de la perte des informations classifiées de l'UE ou d'informations sensibles est passible de sanctions disciplinaires conformément au statut. De telles sanctions disciplinaires s'appliquent sans préjudice d'autres actions en justice ou procédures pénales intentées par les autorités nationales compétentes des États membres conformément à leurs lois et règlements[16].

29 Toutes les mesures appropriées doivent être prises pour:

a) informer l'autorité d'origine de l'information (lorsque celle-ci a été reçue d'un tiers);

b) garantir que le cas soit examiné par du personnel qui n'est pas directement concerné par la violation afin d'établir les faits;

c) évaluer l'éventuel préjudice causé;

d) prendre les mesures qui s'imposent pour éviter que l'incident ne se reproduise.

[16] Voir articles 86 et suivants du statut ainsi que l'article 6 et l'article 7, paragraphe 1, du code de conduite des membres de la Cour.

30 Si une faille ou une violation est constatée dans la protection des informations dans un système informatique, elle doit être signalée au responsable de la sécurité de l'information.

31 Si une faille ou une violation est constatée dans la protection des informations stockées physiquement, elle doit être signalée au chef de la sécurité.

32 Si des données à caractère personnel sont concernées, le DPD doit en être informé.

33 Si des informations classifiées de l'Union européenne sont également concernées, il est nécessaire de suivre la procédure relative aux règles de sécurité en matière de protection des informations classifiées de l'UE[17].

[17] Décision n° 16-2020 de la Cour des comptes européenne concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (en cours d'élaboration).