



Conseil de
l'Union européenne

Bruxelles, le 29 mars 2022
(OR. en)

Dossier interinstitutionnel:
2022/0084(COD)

7670/22
ADD 1

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

PROPOSITION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	22 mars 2022
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	COM(2022) 119 final - Annexe 1
Objet:	ANNEXE de la proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à la sécurité de l'information dans les institutions, organes et organismes de l'Union

Les délégations trouveront ci-joint le document COM(2022) 119 final - Annexe 1.

p.j.: COM(2022) 119 final - Annexe 1



COMMISSION
EUROPÉENNE

Bruxelles, le 22.3.2022
COM(2022) 119 final

ANNEX 1

ANNEXE

de la

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

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

ANNEXE I

Mesures de protection applicables au traitement d'informations sensibles non classifiées

Marquage et traitement des informations sensibles non classifiées

1. Les documents contenant des informations sensibles non classifiées doivent se voir apposer un timbre de sécurité et, le cas échéant, un ou plusieurs timbres de diffusion ou timbres spécifiant le public cible, le cas échéant. Le timbre de sécurité standard est constitué du terme «SENSITIVE» en lettres majuscules, excepté dans les cas visés à l'article 15, paragraphe 2.
2. Les documents contenant des informations sensibles non classifiées ne doivent être accessibles qu'aux destinataires ayant un besoin d'en connaître à des fins officielles. Lorsque des timbres de diffusion sont utilisés, la permission de l'institution ou de l'organe de l'Union d'origine doit être demandée pour élargir la diffusion d'un document.
3. Toutes les personnes qui traitent des informations sensibles non classifiées doivent être informées des instructions de traitement.
4. Les documents marqués SENSITIVE sont déclassés au niveau EU NORMAL ou PUBLIC USE en supprimant ou en biffant les marquages.
5. Lorsque les institutions et organes de l'Union détruisent des documents contenant des informations sensibles non classifiées, elles doivent procéder de manière à ce que les documents ne puissent être aisément reconstitués. Les exemplaires papier doivent être déchiquetés et les exemplaires électroniques doivent faire l'objet d'un processus de réécriture sécurisé, être physiquement détruits ou être rendus irrécupérables d'une autre manière.

Protection des informations sensibles non classifiées lors du travail en dehors des sites des institutions et organes de l'Union

6. Les informations sensibles non classifiées doivent être protégées contre les écoutes et l'observation lors du télétravail et de missions en dehors du bureau, et elles ne peuvent pas être traitées ou stockées en public.
7. Les documents contenant des informations sensibles non classifiées ne peuvent être traités et stockés que sur du matériel ou dans des applications dûment sécurisés sous la responsabilité des institutions et organes de l'Union.
8. Les institutions et organes de l'Union doivent fournir des moyens permettant d'empêcher les personnes non autorisées, y compris les membres de la famille, d'accéder aux informations sensibles non classifiées traitées ou stockées avec l'équipement d'une institution ou d'un organe de l'Union, lors du travail en dehors du lieu d'affectation.
9. Les institutions et organes de l'Union doivent donner comme consigne à leur personnel:
 - a) de protéger l'équipement des institutions ou organes de l'Union utilisé pour traiter des informations sensibles non classifiées contre le vol, la perte et la détérioration et de signaler immédiatement tout incident de sécurité indésirable ayant une incidence sur leurs appareils ou les informations qui s'y trouvent;
 - b) de ne pas partager leurs appareils avec des personnes non autorisées;

- c) de ne pas utiliser l'équipement pour des activités sans lien avec le travail.
10. Les institutions et organes de l'Union doivent s'assurer que, dans la mesure du possible, le traitement et le stockage de tout document sensible non classifié au format électronique en dehors de leurs sites sont effectués au moyen de leur équipement ou de leurs applications dûment sécurisés. Il convient d'éviter de traiter des copies physiques de documents sensibles non classifiés en dehors du bureau.
 11. Lors de l'utilisation d'outils de téléconférence ou de vidéoconférence, les institutions et organes de l'Union doivent réduire au minimum le risque que des personnes non autorisées voient ou entendent les discussions en procédant à une authentification appropriée des participants et en utilisant des outils de communication chiffrés compatibles avec le besoin d'en connaître.
 12. Les institutions et organes de l'Union fournissent à l'ensemble de leur personnel travaillant à distance une formation sur le traitement des informations sensibles non classifiées lors du travail en dehors du bureau.

Informations sensibles non classifiées

13. Les documents contenant des informations sensibles non classifiées peuvent être partagés entre les institutions et organes de l'Union sans formalités supplémentaires.
14. Les institutions et organes de l'Union peuvent uniquement partager des documents contenant des informations sensibles non classifiées en dehors des institutions et organes de l'Union sur la base d'un engagement obligeant les parties à respecter les instructions de traitement.
15. Les institutions et organes de l'Union doivent informer les destinataires d'informations sensibles non classifiées de l'interdiction de partager ces informations avec des parties extérieures au public défini par les timbres de diffusion, sauf autorisation de l'autorité d'origine.
16. Les institutions et organes de l'Union doivent protéger les informations sensibles non classifiées qui leur sont fournies ou qui sont partagées par voie électronique en adoptant des mesures de sécurité appropriées, y compris un chiffrement des informations en transit au moyen de mécanismes cryptographiques appropriés.