



Conseil de
l'Union européenne

Bruxelles, le 29 mars 2022
(OR. en)

**Dossier interinstitutionnel:
2022/0084(COD)**

**7670/22
ADD 3**

**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 3
Objet:	ANNEXE 3 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 3.

p.j.: COM(2022) 119 final - Annexe 3



COMMISSION
EUROPÉENNE

Bruxelles, le 22.3.2022
COM(2022) 119 final

ANNEX 3

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 III

Mesures pour la protection physique des informations classifiées de l'Union européenne («ICUE»)

Équipement et mesures organisationnelles destinés à la protection physique des ICUE

1. Les zones administratives doivent satisfaire aux exigences suivantes:
 - a) avoir un périmètre défini de façon visible afin de permettre le contrôle des personnes et, dans la mesure du possible, des véhicules;
 - b) veiller à ce que les fenêtres susceptibles de permettre un accès visuel non autorisé aux ICUE présentes dans la zone soient rendues opaques ou équipées de stores, de rideaux ou d'autres formes de protections;
 - c) ne peuvent y pénétrer sans escorte que les personnes dûment autorisées par l'autorité de sécurité de l'institution ou de l'organe de l'Union concerné;
 - d) toutes les autres personnes sont escortées en permanence ou font l'objet de contrôles équivalents.
2. Outre les exigences énoncées au point 1, les zones sécurisées doivent satisfaire aux exigences suivantes:
 - a) avoir un périmètre défini et protégé de façon visible dont toutes les entrées et sorties sont contrôlées en permanence;
 - b) ne pas être équipées de lignes de communication, de téléphones ou d'autres dispositifs de communication ou matériels électriques ou électroniques qui ne sont pas autorisés;
 - c) être équipées d'un système de contrôle des accès, et de détection des intrusions (SDI) en temps réel auquel on associe du personnel de sécurité prêt à intervenir en cas d'incident;
 - d) faire l'objet d'une inspection après les heures normales de travail et à intervalles aléatoires en dehors de ces heures lorsqu'elles ne sont pas occupées vingt-quatre heures sur vingt-quatre par le personnel de service et lorsqu'aucun SDI en temps réel n'est en place;
 - e) être gérées par un personnel de sécurité formé, supervisé et dûment habilité;
 - f) disposer de procédures d'exploitation de sécurité incluant les aspects suivants:
 - i) le niveau de classification des ICUE traitées, discutées ou stockées dans la zone;
 - ii) les mesures de surveillance et de protection qu'il convient de mettre en place;
 - iii) les personnes autorisées à pénétrer dans la zone sans escorte grâce à leur autorisation d'accès aux ICUE et en raison de leur besoin d'en connaître;
 - iv) le cas échéant, les procédures applicables aux escortes ou à la protection des ICUE lorsque d'autres personnes sont autorisées à pénétrer dans la zone;
 - v) les autres mesures et procédures applicables.

3. Lorsque le fait de pénétrer dans une zone sécurisée équivaut à un accès direct aux informations classifiées qu'elle renferme, la zone doit être désignée comme zone de catégorie I, et, dans le cas contraire, elle doit être désignée comme zone de catégorie II.

Pour les deux catégories de zones de sécurité visées au premier alinéa, et en plus des exigences énoncées au point 2, le service/officier de sécurité de l'institution ou de l'organe de l'Union concerné doit indiquer clairement le niveau de classification le plus élevé qui s'applique aux informations conservées habituellement dans la zone et définir clairement un périmètre permettant le contrôle des personnes et, dans la mesure du possible, des véhicules.

Les institutions et organes de l'Union doivent veiller à ce que les personnes accédant à une zone sécurisée satisfassent aux critères suivants:

- a) disposer d'une autorisation spécifique pour pénétrer dans la zone;
 - b) être escortées en permanence;
 - c) disposer de l'habilitation de sécurité correspondante, sauf si des mesures sont prises pour empêcher l'accès aux ICUE.
4. Les zones sécurisées qui sont protégées contre les écoutes passives et actives doivent être qualifiées de zones sécurisées du point de vue technique. Ces zones doivent respecter les exigences suivantes, en plus de celles applicables aux zones sécurisées:
- a) être équipées d'un SDI, être verrouillées lorsqu'elles ne sont pas occupées et gardées lorsqu'elles sont occupées. Toutes les clés doivent être gérées conformément à l'article 29, paragraphe 3;
 - b) faire l'objet, à intervalles réguliers, d'inspections physiques ou techniques, ou les deux, réalisées par l'autorité de sécurité de l'institution ou l'organe de l'Union concerné. Ces inspections doivent également être effectuées après une entrée non autorisée, réelle ou présumée;
 - c) disposer d'une protection acoustique et TEMPEST appropriée.
5. Toutes les personnes qui pénètrent dans des zones sécurisées du point de vue technique doivent respecter les exigences énoncées au point 3.
6. Des zones sécurisées et des zones sécurisées du point de vue technique peuvent être temporairement établies dans une zone administrative en vue de la tenue d'une réunion classifiée ou à toute autre fin similaire.
7. Les chambres fortes doivent être installées dans des zones sécurisées. Une chambre forte est une pièce dont la construction physique a été renforcée et dont les murs, les planchers, les plafonds, les fenêtres et les portes verrouillables ont été approuvés par l'autorité de sécurité de l'institution ou de l'organe de l'Union concerné. Ces pièces doivent offrir une protection équivalant à celle d'un meuble de sécurité approuvé pour le stockage d'ICUE du même niveau de classification.

Mesures de protection physiques applicables au traitement et au stockage des ICUE

8. Les ICUE classifiées RESTREINT UE/EU RESTRICTED doivent être traitées et stockées dans l'une des zones suivantes:
- a) dans une zone sécurisée;

- b) dans une zone administrative à condition que les personnes non autorisées ne puissent avoir accès aux ICUE;
 - c) en dehors d'une zone sécurisée ou d'une zone administrative à condition que le détenteur se soit engagé à se conformer aux mesures compensatoires adoptées par l'autorité de sécurité de chaque institution ou organe de l'Union.
9. Les ICUE classifiées RESTREINT UE/EU RESTRICTED doivent être stockées dans un meuble de bureau fermé dans une zone administrative ou dans une zone sécurisée. Elles peuvent être temporairement stockées en dehors d'une zone administrative ou d'une zone sécurisée à condition que le détenteur se soit engagé à stocker les documents concernés dans un meuble de bureau adapté et fermé lorsqu'ils ne sont pas lus ou discutés.
10. Les institutions et organes de l'Union peuvent traiter et stocker des informations RESTREINT UE/EU RESTRICTED en dehors de leurs sites à condition que les informations pertinentes soient dûment protégées. À cet effet, les institutions et organes de l'Union doivent respecter les mesures énoncées au point 8 c).
11. Les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET doivent être traitées et stockées dans l'une des zones suivantes:
- a) dans une zone sécurisée;
 - b) dans une zone administrative à condition que les personnes non autorisées ne puissent avoir accès aux ICUE;
 - c) en dehors d'une zone sécurisée ou d'une zone administrative lorsque leur volume et la durée du traitement sont limités et à condition que le détenteur se soit engagé à se conformer aux mesures compensatoires adoptées par l'autorité de sécurité de l'institution ou de l'organe de l'Union concerné. En outre, le détenteur d'ICUE doit prendre les mesures suivantes:
 - i) informer le bureau d'ordre compétent du fait que des documents classifiés sont traités en dehors d'une zone protégée;
 - ii) conserver à tout moment le document sous leur contrôle.
12. Les informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET doivent être stockées dans une zone sécurisée agréée à ce niveau de classification par l'autorité d'homologation de sécurité compétente de l'institution ou de l'organe de l'Union concerné, soit dans un meuble de sécurité soit dans une chambre forte.
13. Les documents classifiés CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification plus élevé ne peuvent être copiés que par le bureau d'ordre compétent.
14. Les informations TRÈS SECRET UE/EU TOP SECRET doivent être traitées et stockées dans une zone sécurisée agréée à ce niveau de classification. À cette fin, les institutions et organes de l'Union peuvent conclure les arrangements nécessaires pour utiliser une zone sécurisée hébergée et agréée au niveau approprié par l'autorité d'homologation de sécurité (AHS) d'une autre institution ou d'un autre organe de l'Union.
15. Les informations TRÈS SECRET UE/EU TOP SECRET doivent être stockées dans une zone sécurisée agréée à ce niveau de classification par l'autorité d'homologation

de sécurité de l'institution ou de l'organe de l'Union compétent concerné, selon l'une des modalités suivantes:

- a) dans un meuble de sécurité agréé par l'autorité de sécurité de chaque institution ou organe de l'Union, moyennant un des contrôles supplémentaires suivants:
 - i) protection ou vérification en permanence par un membre habilité du personnel de sécurité ou du personnel de service;
 - ii) système de détection des intrusions approuvé auquel on associe du personnel de sécurité prêt à intervenir en cas d'incident;
- b) dans une chambre forte équipée d'un système de détection des intrusions à laquelle on associe du personnel de sécurité prêt à intervenir en cas d'incident.