Conseil de
l'Union européenne

Bruxelles, le 29 mars 2022
(OR. en)

Dossier interinstitutionnel:
2022/0084(COD)

7670/22
ADD 7

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

NOTE DE TRANSMISSION

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:	SWD(2022) 65 final
Objet:	DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION RÉSUMÉ DU RAPPORT D'ANALYSE D'IMPACT accompagnant le document: 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 SWD(2022) 65 final.

p.j.: SWD(2022) 65 final

COMMISSION
EUROPÉENNE

Bruxelles, le 22.3.2022
SWD(2022) 65 final

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

RÉSUMÉ DU RAPPORT D'ANALYSE D'IMPACT

accompagnant le document:

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

{COM(2022) 119 final} - {SWD(2022) 66 final}

Résumé de l'analyse d'impact

Analyse d'impact sur la sécurité de l'information dans les institutions, organes et organismes de l'Union

A. Contexte politique

Dans son programme stratégique 2019-2024, le Conseil européen engage les institutions à protéger les réseaux d'information et de communication de l'Union et ses processus décisionnels contre les activités malveillantes de tous types, y compris les cybermenaces et les menaces hybrides. En conséquence, le Conseil «Affaires générales» de décembre 2019 a conclu que les institutions et organes de l'Union devraient élaborer et mettre en œuvre un ensemble complet de mesures destinées à garantir la sécurité de leurs informations.

En juillet 2020, la Commission a adopté sa stratégie de l'UE pour l'union de la sécurité, par laquelle elle s'est engagée à compléter les efforts nationaux dans le domaine de la sécurité. Dans le cadre de cette stratégie, la Commission a proposé de créer un ensemble minimal de règles en matière de sécurité de l'information et de cybersécurité dans l'ensemble des institutions et organes de l'Union (IOU).

B. Quel est le problème?

Les principaux problèmes sont les suivants: i) la différence significative de niveau de sécurité entre les IOU liée à leurs règles internes en matière de sécurité de l'information et ii) le manque de coordination entre les institutions et organes de l'Union dans l'accomplissement de leurs tâches liées à la sécurité.

Actuellement, soit les institutions et organes de l'Union possèdent leurs propres règles en matière de sécurité de l'information, soit ils ne disposent d'aucune règle en la matière. La fragmentation du cadre juridique applicable a engendré différentes catégories d'informations non classifiées, différents marquages et différentes instructions de traitement dans tous les domaines. En ce qui concerne les informations classifiées de l'UE, l'interopérabilité des systèmes concernés reste limitée, ce qui empêche un transfert fluide des informations entre les institutions et organes et avec les États membres.

Cette situation accroît le risque que les auteurs d'attaques créent une faille de sécurité dans le maillon le plus faible et s'en servent comme point de départ pour de nouvelles attaques contre d'autres institutions et organes.

C. Quels sont les objectifs à atteindre?

L'objectif général de l'initiative est d'établir des règles en matière de sécurité de l'information pour l'ensemble des institutions et organes de l'Union dans le but d'assurer une protection renforcée et cohérente contre les menaces en constante évolution qui pèsent sur leurs informations.

L'objectif général se décline en quatre objectifs spécifiques:

- établir des catégories d'informations harmonisées et exhaustives;
- recenser les lacunes en matière de sécurité et mettre en œuvre les mesures requises;
- instaurer une coopération rationalisée dans le domaine de la sécurité de l'information entre les institutions et organes de l'Union;
- moderniser les politiques de sécurité de l'information en tenant compte de la transformation

numérique et du télétravail.

D. Quelles sont les positions des différentes parties prenantes?

Les parties prenantes consultées (institutions et organes de l'Union, autorités nationales de sécurité des États membres et experts chercheurs du JRC) sont convenues de la nécessité de normes communes en matière de sécurité de l'information pour l'ensemble des institutions et organes de l'Union, l'accent devant être mis sur les points suivants:

- la diversité des IOU et leur environnement opérationnel propre doivent être pris en considération et des solutions locales doivent être autorisées;
- si la majorité des institutions et organes sont prêts à coopérer avec leurs homologues au sein des organes communs pour les besoins de la sécurité de l'information, ils ne sont pas disposés à déléguer leurs pouvoirs décisionnels;
- le projet de règlement doit être élaboré dans le respect de l'accord intergouvernemental[1] conclu entre les États membres en ce qui concerne la protection des informations classifiées.

E. Quel est l'impact de la proposition?

Avantages

En créant une base de règles de référence en matière de sécurité de l'information pour l'ensemble des institutions et organes de l'Union, le projet de règlement augmentera le niveau global de sécurité de l'information tout en réduisant les divergences actuelles. Il devrait également contribuer à éliminer les éventuels maillons faibles tout en protégeant les informations partagées au sein de l'administration européenne.

Du point de vue de l'efficacité, le projet de règlement devrait permettre de tirer des bénéfices de l'exécution coordonnée des tâches communes en matière de sécurité de l'information (par exemple, habilitations, homologation des systèmes d'information et de communication) ainsi que de la création d'organes communs de gouvernance (par exemple, le groupe interinstitutionnel de coordination, les sous-groupes techniques).

Incidences économiques

Pour les institutions et organes de l'Union, les efforts nécessaires à la mise en œuvre de la nouvelle législation devraient être compensés par des gains d'efficacité, tandis que les coûts supplémentaires peuvent être couverts dans le cadre des programmes d'amélioration de la sécurité de l'information qui existent dans chaque organisation. À long terme, les institutions et organes de l'Union tireront profit de l'approche cohérente adoptée pour faire face aux menaces en constante évolution qui pèsent sur la sécurité de l'information.

La Commission européenne devrait assurer le secrétariat permanent du groupe interinstitutionnel de coordination et affecter des ressources humaines à cette tâche (un fonctionnaire AD et un fonctionnaire

[1] 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, 2011/C202/05.

AST).

Aucune incidence économique n'est attendue pour les administrations des États membres et le secteur privé.

F. Suivi

Quand la législation sera-t-elle réexaminée?

Une évaluation complète sera réalisée tous les 5 ans à partir de la date d'application afin d'évaluer les incidences et la mise en œuvre du projet de règlement. La Commission présentera un rapport contenant ses conclusions et le soumettra au Parlement européen et au Conseil.