Sécurité de l’information dans les institutions, organes et organismes de l’Union

2022/0084(COD) - 22/03/2022 - Document de base législatif

OBJECTIF : établir des règles en vue de parvenir à un niveau élevé commun de sécurité pour les informations classifiées de l’Union européenne et les informations non classifiées traitées et stockées par les institutions et organes de l’Union.

ACTE PROPOSÉ : Règlement du Parlement européen et du Conseil.

RÔLE DU PARLEMENT EUROPÉEN : le Parlement européen décide conformément à la procédure législative ordinaire et sur un pied d'égalité avec le Conseil.

CONTEXTE : en raison des volumes toujours plus importants d’informations sensibles non classifiées et d’informations classifiées de l’Union européenne (ICUE) que les institutions et organes de l’Union doivent se partager, et compte tenu de l’évolution spectaculaire des menaces, **l’administration européenne est exposée à des attaques dans tous ses domaines d’activité**. Les informations traitées par les institutions et organes de l’UE intéressent au plus haut point les acteurs malveillants, et elles doivent être correctement protégées, ce qui nécessite une action rapide afin d’améliorer leur protection.

Actuellement, soit les institutions et organes de l’Union possèdent leurs propres règles en matière de sécurité de l’information, fondées sur leur règlement de procédure ou leur acte fondateur, soit ils ne disposent d’aucune règle en la matière. **L’absence d’approche commune** entrave le déploiement d’outils communs fondés sur un ensemble concerté de règles tenant compte des besoins de sécurité des informations à protéger.

Dès lors, et afin d’accroître la protection des informations traitées par l’administration européenne, la présente initiative vise à **rationaliser les différents cadres juridiques des institutions et organes de l’ Union** dans ce domaine, grâce aux mesures suivantes:

- définir des catégories d’informations exhaustives et harmonisées, ainsi que des règles communes à toutes les institutions et tous les organes de l’Union en matière de traitement;

- établir un système rationalisé de coopération entre les institutions et organes de l’Union dans le domaine de la sécurité de l’information, capable de favoriser une culture de la sécurité de l’information dans l’ ensemble de l’administration européenne;

- moderniser les politiques en matière de sécurité de l’information à tous les niveaux de classification/de catégorisation, pour l’ensemble des institutions et organes de l’Union, en tenant compte de la transformation numérique et du développement du télétravail en tant que pratique structurelle.

La présente initiative fait partie de la stratégie de l’UE pour l’union de la sécurité adoptée par la Commission le 24 juillet 2020 et s’inscrit dans un vaste ensemble de politiques de l’Union dans le domaine de la sécurité et de la sécurité de l’information.

CONTENU : le règlement proposé est destiné à **créer un ensemble minimal de règles en matière de sécurité de l’information** applicables à l’ensemble des institutions et organes de l’Union. Il s’applique à

toutes les informations traitées et stockées par les institutions et organes de l'Union, y compris celles relatives aux activités de la Communauté européenne de l'énergie atomique, autres que les informations classifiées d'Euratom. Le règlement couvre à la fois les informations non classifiées et les ICUE.

Gouvernance et organisation de la sécurité

La proposition prévoit de créer un **groupe interinstitutionnel de coordination** dans lequel seront représentées les autorités de sécurité de l'ensemble des institutions et organes de l'Union. Le groupe de coordination aurait pour mission de **définir la politique commune** de ces institutions et organes dans le domaine de la sécurité de l'information. Il devrait améliorer la cohérence des politiques et contribuer à l' harmonisation des procédures et outils de sécurité de l'information dans l'ensemble des institutions et organes de l'Union.

Le groupe de coordination rédigerait des documents d'orientation et devrait créer des plateformes destinées au partage de bonnes pratiques et de connaissances sur les thèmes communs pertinents pour la sécurité de l'information ainsi qu'à la fourniture d'une assistance en cas d'incidents de sécurité de l' information. Il échangerait régulièrement avec les autorités nationales de sécurité des États membres, rassemblées au sein d'un **comité de sécurité de l'information.**

Cinq sous-groupes composés d'experts représentant différentes institutions et différents organes seraient créés en vue de rationaliser les procédures et les autres aspects pratiques liés à la sécurité de l'information.

Chaque institution ou organe de l'Union serait tenu de désigner une **autorité de sécurité**, responsable de la définition et de la mise en œuvre des politiques internes en matière de sécurité de l'information.

Assurance de l'information et systèmes d'information et de communication

Le règlement proposé établit un **sous-groupe** sur l'assurance de l'information ayant pour objectif d' améliorer la cohérence dans l'ensemble des institutions et organes de l'Union entre les règles relatives à la sécurité de l'information et la base de référence en cybersécurité définie par le règlement établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union.

Informations non classifiées

Le règlement prévoit **trois catégories d'informations** non classifiées: 1) les informations destinées à un usage public, 2) les informations ordinaires et 3) les informations sensibles non classifiées. Toutes les catégories sont définies, tandis que des marquages et des conditions de traitement sont établis afin de protéger ces informations.

La proposition établit un sous-groupe sur les informations non classifiées afin de coordonner les travaux sur les équivalences entre les catégories spécifiques établies par certaines institutions et certains organes de l'Union et les catégories communes prévues dans le règlement.

Informations classifiées (ICUE)

La proposition prévoit **quatre niveaux d'ICUE**: 1) TRÈS SECRET UE/EU TOP SECRET, 2) SECRET UE/EU SECRET, 3) CONFIDENTIEL UE/EU CONFIDENTIAL et 4) RESTREINT UE/EU RESTRICTED. Elle prévoit en outre l'obligation pour les institutions et organes de l'Union de prendre les mesures de sécurité nécessaires en fonction des résultats d'un processus de gestion des risques liés à la sécurité de l'information.

La proposition couvre également les aspects relatifs à la sécurité du personnel, à la sécurité physique, à la gestion des ICUE, à la protection dans les systèmes d'information et de communication, à la sécurité industrielle, au partage d'ICUE et à l'échange d'informations classifiées.

Le règlement proposé établit des sous-groupes sur l'assurance de l'information, sur les informations non classifiées, sur la sécurité physique, sur l'homologation des systèmes d'information et de communication traitant et stockant des ICUE ainsi que sur le partage d'ICUE et l'échange d'informations classifiées.