Un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l’Union

2022/0085(COD) - 21/11/2023 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 557 voix pour, 0 contre et 27 abstentions, une résolution législative sur la proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l’Union.

La position du Parlement européen arrêtée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

Objet

Le règlement établit des mesures visant à **parvenir à un niveau élevé commun de cybersécurité** au sein des entités de l’Union en ce qui concerne:

- l’établissement par chaque entité de l’Union d’un cadre interne de gestion, de gouvernance et de contrôle des risques de cybersécurité;

- la gestion des risques de cybersécurité, la communication et le partage d’informations;

- l’organisation, le fonctionnement et la gestion du conseil interinstitutionnel de cybersécurité (IICB) institué par le règlement ainsi que l’organisation, le fonctionnement et la gestion du service de cybersécurité pour les institutions, organes et organismes de l’Union (CERT-UE);

- le suivi de la mise en œuvre du règlement.

Cadre de gestion, de gouvernance et de contrôle des risques de cybersécurité

Chaque entité de l’Union devra établir, après avoir procédé à un examen initial de la cybersécurité, tel qu’ un audit, un cadre interne de gestion, de gouvernance et de contrôle des risques de cybersécurité. L’ établissement du cadre sera placé sous la **supervision et la responsabilité du niveau hiérarchique le plus élevé** de l’entité de l’Union. Le cadre sera fondé sur une approche «tous risques». Il garantira un niveau élevé de cybersécurité et fera régulièrement l’objet d’une révision au moins tous les quatre ans.

Chaque entité de l’Union désignera un **responsable local de la cybersécurité** ou une fonction équivalente qui fera office de point de contact unique pour tous les aspects liés à la cybersécurité. Le responsable local de la cybersécurité facilitera la mise en œuvre du règlement et rendra directement et régulièrement compte au niveau hiérarchique le plus élevé de l’état d’avancement de la mise en œuvre.

Mesures de gestion des risques de cybersécurité

Dans les meilleurs délais et en tout état de cause au plus tard 20 mois à compter de la date d’entrée en vigueur du règlement, chaque entité de l’Union devra prendre des **mesures techniques, opérationnelles et organisationnelles** appropriées et proportionnées afin de gérer les risques de cybersécurité identifiés dans le cadre et de prévenir et réduire les conséquences des incidents. Ces mesures doivent garantir, pour les réseaux et les systèmes d’information de la totalité de l’environnement TIC, un niveau de sécurité adapté aux risques de cybersécurité encourus, en tenant compte de l’état des connaissances et, s’il y a lieu, des normes européennes et internationales applicables

Lors de l'évaluation de la proportionnalité de ces mesures, il sera tenu compte du degré d'exposition de l' entité de l'Union aux risques de cybersécurité, de sa taille et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales, économiques et interinstitutionnelles.

Plans de cybersécurité

Compte tenu de la conclusion de l'évaluation de la maturité en matière de cybersécurité effectuée conformément au règlement et des risques de cybersécurité identifiés dans le cadre, ainsi que des mesures prise en matière de gestion des risques de cybersécurité, le niveau hiérarchique le plus élevé de chaque entité de l'Union approuvera un plan de cybersécurité au plus tard 24 mois à compter de la date d'entrée en vigueur du règlement.

Conseil interinstitutionnel de cybersécurité

Le règlement institue le conseil interinstitutionnel de cybersécurité (IICB), en vue de faciliter l' instauration d'un niveau élevé commun de cybersécurité parmi les entités de l'Union. L'IICB jouera un rôle exclusif pour surveiller et soutenir la mise en œuvre du règlement par les entités de l'Union, superviser la mise en œuvre des priorités et des objectifs généraux du CERT-UE et fournir des orientations stratégiques au CERT-UE.

Afin d'aider les entités de l'Union, l'IICB devra fournir des orientations au chef du CERT-UE, adopter une stratégie pluriannuelle visant à relever le niveau de cybersécurité dans les entités de l'Union, mettre au point la méthode et les autres aspects relatifs aux évaluations volontaires par les pairs, et faciliter la création d'un groupe informel de responsables locaux de la cybersécurité, soutenu par l'Agence de l' Union européenne pour la cybersécurité (ENISA), afin d'échanger de bonnes pratiques et des informations relatives à la mise en œuvre du règlement.

Le **CERT-UE** devra recueillir, gérer, analyser et partager avec les entités de l'Union des informations sur les cybermenaces, les vulnérabilités et les incidents relatifs aux infrastructures TIC non classifiées. Il coordonnera les réponses aux incidents au niveau interinstitutionnel et au niveau des entités de l'Union, y compris en assurant ou en coordonnant la fourniture d'une assistance opérationnelle spécialisée.

Obligations en matière de communication d'informations

Le règlement définit une approche de la notification des incidents importants en plusieurs étapes. L' ensemble des entités de l'Union devront **informer le CERT-UE de tout incident ayant un impact important**. Un incident est considéré comme important : a) s'il a causé ou est susceptible de causer une perturbation opérationnelle grave du service ou des pertes financières pour l'entité concernée; b) s'il a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

Les entités de l'Union devront transmettre au CERT-UE:

a) sans retard injustifié et en tout état de cause **dans les 24 heures** après avoir eu connaissance de l' incident important, une alerte précoce qui, le cas échéant, indique que l'on suspecte l'incident important d' avoir été causé par des actes illicites ou malveillants ou qu'il pourrait avoir un impact inter-entités ou transfrontière;

b) sans retard injustifié et en tout état de cause **dans les 72 heures** après avoir eu connaissance de l' incident important, une notification d'incident qui, le cas échéant, fournit une évaluation initiale de l' incident important, y compris de sa gravité et de son impact, ainsi que des indicateurs de compromission, lorsqu'ils sont disponibles;

c) un rapport final **au plus tard un mois** après la présentation de la notification d'incident comprenant: i) une description détaillée de l'incident, y compris de sa gravité et de son impact; ii) le type de menace ou la cause profonde qui a probablement déclenché l'incident; iii) les mesures d'atténuation appliquées et en cours; iv) le cas échéant, l'impact transfrontière ou inter-entités de l'incident.

Une entité de l'Union devra informer, sans retard injustifié et en tout état de cause **dans les 24 heures** après avoir eu connaissance d'un incident important, tous les homologues des États membres concernés dans l'État membre dans lequel il est situé qu'un incident important est survenu.

Le texte amendé précise que le traitement, par le CERT-UE, le conseil interinstitutionnel de cybersécurité et les entités de l'Union, de **données à caractère personnel** au titre du règlement doit être effectué conformément au règlement (UE) 2018/1725 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.