Informations de base

2022/0085(COD) COD - Procédure législative ordinaire (ex-procedure codécision) Règlement	Procédure terminée
Un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union **Subject** 2.80 Coopération et simplification administratives 3.30.06 Technologies de l'information et de la communication, technologies numériques 3.30.07 Cybersécurité, politique cyberespace 3.30.25 Réseaux mondiaux et société de l'information, internet 8.40 Institutions de l'Union 8.40.08 Agences et organes de l'Union	

Acteurs principaux

Parlement européen

Commission au fond	Rapporteur(e)	Date de nomination
ITRE Industrie, recherche et énergie	VIRKKUNEN Henna (EPP)	18/05/2022
	Rapporteur(e) fictif/fictive KUMPULA-NATRI Miapetra (S&D) BILBAO BARANDICA Izaskun (Renew) PEKSA Mikuláš (Greens /EFA) TOŠENOVSKÝ Evžen (ECR) BUCHHEIT Markus (ID) BOTENGA Marc (The Left)	

Commission pour avis	Rapporteur(e) pour avis	Date de nomination
BUDG Budgets	UŠAKOVS Nils (S&D)	22/04/2022
LIBE Libertés civiles, justice et affaires intérieures (Commission associée)	TOBÉ Tomas (EPP)	12/12/2022
AFCO Affaires constitutionnelles	GREGOROVÁ Markéta (Greens/EFA)	20/06/2022

Conseil de l'Union européenne	
Commission européenne	DG de la Commission: Services numériques Commissaire: HAHN Johannes

Evénements clés

Date	Evénement	Référence	Résumé
22/03/2022	Publication de la proposition législative	COM(2022)0122	Résumé
04/04/2022	Annonce en plénière de la saisine de la commission, 1ère lecture		
15/09/2022	Annonce en plénière de la saisine des commissions associées		
09/03/2023	Vote en commission,1ère lecture		
09/03/2023	Décision de la commission parlementaire d'ouvrir des négociations interinstitutionnelles à travers d'un rapport adopté en commission		
10/03/2023	Dépôt du rapport de la commission, 1ère lecture	A9-0064/2023	Résumé
13/03/2023	Décision de la commission parlementaire d'engager des négociations interinstitutionnelles annoncée en plénière (Article 71)		
15/03/2023	Décision de la commission parlementaire d'engager des négociations interinstitutionnelles confirmée par la plénière (Article 71)		
19/09/2023	Approbation en commission du texte adopté en négociations interinstitutionnelles de la 1ère lecture	PE753.446 GEDA/A/(2023)005465	
21/11/2023	Décision du Parlement, 1ère lecture	T9-0398/2023	Résumé
21/11/2023	Résultat du vote au parlement		
08/12/2023	Adoption de l'acte par le Conseil après la 1ère lecture du Parlement		
13/12/2023	Signature de l'acte final		
18/12/2023	Publication de l'acte final au Journal officiel		

Informations techniques

Référence de la procédure	2022/0085(COD)
Type de procédure	COD - Procédure législative ordinaire (ex-procedure codécision)
Sous-type de procédure	Note thématique
Instrument législatif	Règlement
Base juridique	Traité Euratom A 106a-pa Règlement du Parlement EP 57_o Traité sur le fonctionnement de l'Union européenne TFEU 298-p2
Autre base juridique	Règlement du Parlement EP 165
État de la procédure	Procédure terminée

Dossier de la commission	ITRE/9/08708

Portail de documentation

Parlement Européen

Type de document	Commission	Référence	Date	Résumé
Avis de la commission	BUDG	PE732.682	13/07/2022	
Projet de rapport de la commission		PE737.231	07/10/2022	
Amendements déposés en commission		PE738.403	27/10/2022	
Avis de la commission	AFCO	PE730.184	01/02/2023	
Avis de la commission	LIBE	PE739.801	01/03/2023	
Rapport déposé de la commission, 1ère lecture/lecture unique		A9-0064/2023	10/03/2023	Résumé
Texte convenu lors de négociations interinstitutionnelles		PE753.446	15/09/2023	
Texte adopté du Parlement, 1ère lecture/lecture unique		T9-0398/2023	21/11/2023	Résumé

Conseil de l'Union

Type de document	Référence	Date	Résumé
Lettre de la Coreper confirmant l'accord interinstitutionnel	GEDA/A/(2023)005465	15/09/2023	
Projet d'acte final	00057/2023/LEX	13/12/2023	

Commission Européenne

Type de document	Référence	Date	Résumé
Document de base législatif	COM(2022)0122	22/03/2022	Résumé
Document annexé à la procédure	SWD(2022)0067	22/03/2022	
Document annexé à la procédure	SWD(2022)0068	22/03/2022	
Réaction de la Commission sur le texte adopté en plénière	SP(2024)109	23/02/2024	

Autres Institutions et organes

Institution/organe	Type de document	Référence	Date	Résumé
EDPS	Document annexé à la procédure	N9-0039/2022 JO C 258 05.07.2022, p. 0010	17/05/2022	

Informations complémentaires

Source	Document	Date

Service de recherche du PE	Briefing	02/09/2022
Commission européenne	EUR-Lex	

Réunions avec des représentant(e)s d'intérêts, publiées conformément au règlement intérieur

Rapporteur(e)s, rapporteur(e)s fictifs/fictives et président(e)s des commissions

Transparence

Nom	Rôle	Commission	Date	Représentant(e)s d'intérêts
VIRKKUNEN Henna	Rapporteur(e)	ITRE	25/01/2023	European Central Bank
GREGOROVÁ Markéta	Rapporteur(e)	AFCO	07/12/2022	Representatives of Nemec+Chvatal representatives of S.ICZ
VIRKKUNEN Henna	Rapporteur(e)	ITRE	29/09/2022	Finnish Transport and Communications Agency Traficom Finnish Ministry of Transport and Communications
VIRKKUNEN Henna	Rapporteur(e)	ITRE	22/09/2022	European Central Bank
VIRKKUNEN Henna	Rapporteur(e)	ITRE	12/09/2022	ECSO Policy Task Force
VIRKKUNEN Henna	Rapporteur(e)	ITRE	07/09/2022	Finnish Ministry of Transport and Communications

Acte final

Règlement 2023/2841
JO L 000 18.12.2023, p. 0000

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

2022/0085(COD) - 22/03/2022 - Document de base législatif

OBJECTIF : établir des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes 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 : l'évolution de la technologie ainsi que la complexité et l'interdépendance croissantes des systèmes numériques amplifient les risques de cybersécurité et **rendent l'administration de l'Union plus vulnérable aux cybermenaces et aux incidents**.

Les institutions, organes et organismes de l'Union sont devenus des cibles très attrayantes pour les cyberattaques sophistiquées. Entre 2019 et 2021, le nombre d'incidents importants touchant des institutions, organes et organismes de l'Union et perpétrés par des acteurs de menaces persistantes avancées a considérablement augmenté. Au cours du premier semestre de 2021, on a enregistré autant d'incidents importants que sur l'ensemble de l'année 2020.

Le Centre pour la cybersécurité des institutions, organes et organismes de l'Union (CERT-UE) a évalué les principales cybermenaces auxquelles les institutions, organes et organismes de l'Union sont actuellement exposés ou sont susceptibles de l'être dans un avenir prévisible. L'analyse a examiné l'influence des grands changements en cours sur la façon dont les institutions de l'Union gèrent et utilisent leurs infrastructures et services informatiques. Parmi ces changements figurent l'augmentation du télétravail, la migration des systèmes vers le nuage et l'externalisation accrue des services informatiques.

L'analyse des vingt institutions, organes et organismes de l'Union concernés fait apparaître **des disparités considérables** en ce qui concerne leur gouvernance, leur hygiène informatique, leurs capacités globales et leur maturité. Par conséquent, pour remédier à cette hétérogénéité des niveaux de maturité en matière de cybersécurité, il est nécessaire que les institutions, organes et organismes de l'Union atteignent **un niveau élevé commun de cybersécurité** grâce à une base de référence en cybersécurité, à l'échange d'informations et à la collaboration.

La présente proposition s'appuie sur la stratégie de l'UE pour l'union de la sécurité et sur la stratégie de cybersécurité de l'UE pour la décennie numérique.

CONTENU : la présente proposition établit **un cadre destiné à assurer des règles et des mesures communes en matière de cybersécurité au sein des institutions, organes et organismes de l'Union** afin de leur permettre d'accomplir leurs missions respectives de manière ouverte, efficace et indépendante. Elle vise à améliorer la résilience de toutes les entités ainsi que leurs capacités de réaction aux incidents.

Le règlement proposé :

- oblige les institutions, organes et organismes de l'Union à i) établir **un cadre interne** pour la gestion, la gouvernance et le contrôle des risques de cybersécurité, garantissant une gestion efficace et prudente de tous ces risques, ii) adopter une **base de référence** en cybersécurité pour faire face aux risques identifiés au moyen de ce cadre, iii) procéder, au moins tous les trois ans, à une **évaluation de la maturité** en matière de cybersécurité portant sur l'ensemble des éléments de son environnement informatique et iv) à adopter un **plan de cybersécurité**;

- institue un **conseil interinstitutionnel de cybersécurité** chargé de suivre la mise en œuvre du présent règlement par les institutions, organes et organismes de l'Union, ainsi que de surveiller la mise en œuvre des priorités et des objectifs généraux par le CERT-UE et de fournir à ce dernier des orientations stratégiques;

- **définit la tâche et les missions du CERT-UE**, centre interinstitutionnel autonome de cybersécurité au service de l'ensemble des institutions, organes et organismes de l'Union. Le CERT-UE contribuera à la sécurité de l'environnement informatique de l'ensemble des institutions, organes et organismes de l'Union en les conseillant, en les aidant à prévenir, à détecter et à limiter les incidents, ainsi qu'à y répondre, et en faisant office de plateforme d'échange d'informations et de coordination des réponses aux incidents dans le domaine de la cybersécurité;

- **garantit la coopération et l'échange d'informations entre le CERT-UE et les institutions, organes et organismes de l'Union** afin de renforcer la confiance. À cette fin, le CERT-UE pourrait demander aux institutions, organes et organismes de l'Union de lui fournir des informations pertinentes et il pourrait échanger des informations spécifiques à un incident avec les institutions, organes et organismes de l'Union afin de faciliter la détection des cybermenaces ou incidents similaires sans le consentement de la partie concernée. Le CERT-UE ne pourrait échanger des informations spécifiques à un incident qui révèlent l'identité de la cible de l'incident de cybersécurité qu'avec le consentement de la partie concernée;

- oblige l'ensemble des institutions, organes et organismes de l'Union à **notifier au CERT-UE** les cybermenaces importantes, les vulnérabilités importantes et les incidents importants dans les plus brefs délais et, en tout état de cause, au plus tard 24 heures après en avoir eu connaissance.

INCIDENCE BUDGÉTAIRE : d'après les études, les dépenses directes en matière de cybersécurité représentent généralement entre 4 et 7% du total des dépenses informatiques des organisations. Toutefois, l'analyse des menaces menée par la CERT-UE indique que les organisations politiques et organismes internationaux sont confrontés à des risques accrus et qu'il semblerait plus approprié de consacrer **10%** des dépenses informatiques à la cybersécurité.

Le coût exact de ces efforts est impossible à déterminer en raison du manque d'informations détaillées sur les dépenses informatiques des institutions, organes et organismes de l'Union et sur la part que représentent les dépenses de cybersécurité.

Le CERT-UE aura besoin de ressources supplémentaires pour mener à bien sa mission élargie et ces ressources devraient être réaffectées à partir des institutions, organes et organismes de l'UE bénéficiant des services du CERT-UE.

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.

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

2022/0085(COD) - 10/03/2023 - Rapport déposé de la commission, 1ère lecture/lecture unique

La commission de l'industrie, de la recherche et de l'énergie a adopté le rapport d'Henna VIRKUNEN (PPE, FI) 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 commission compétente a recommandé que la position du Parlement européen adoptée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

Objet

Le règlement devrait établir des mesures qui ont pour but d'obtenir un niveau élevé commun de cybersécurité au sein des entités de l'Union. À cette fin, le règlement fixerait:

- les obligations qui imposent aux entités de l'Union de mettre en place un cadre de gestion des risques, de traitement des incidents, de gouvernance et de contrôle des risques de cybersécurité;

- les obligations incombant aux entités de l'Union en ce qui concerne la gestion des risques de cybersécurité et la communication d'informations;

- les règles sous-jacentes aux obligations de partage d'informations et à la facilitation des modalités de partage volontaire d'informations pour les entités de l'Union;

- les règles relatives à l'organisation, aux missions et au fonctionnement du centre de cybersécurité des entités de l'Union (CERT-UE) et à l' organisation et au fonctionnement du conseil interinstitutionnel de cybersécurité (IICB).

Cadre de gestion des risques, de traitement des incidents, de gouvernance et de contrôle des risques

Sur la base d'un audit de cybersécurité exhaustif, **chaque entité de l'Union** devrait établir son propre cadre de gestion des risques, de traitement des incidents, de gouvernance et de contrôle des risques de cybersécurité. L'établissement de ce cadre devrait être placé sous la supervision du **niveau hiérarchique le plus élevé** de l'entité de l'Union et se trouver sous sa responsabilité.

Le cadre de gestion des risques devrait i) définir les objectifs stratégiques permettant d'assurer un niveau élevé de cybersécurité au sein des entités de l'Union; ii) définir des mesures de cybersécurité pour la sécurité des réseaux et des systèmes d'information englobant la totalité de l'environnement TIC et déterminer les rôles et les responsabilités du personnel des entités de l'Union chargé d'assurer la bonne mise en œuvre du règlement; iii) comporter les indicateurs de performance clés (IPC).

Le cadre devrait être **réexaminé régulièrement** et au moins tous les trois ans.

Mesures de gestion des risques de cybersécurité de gestion des risques

Les mesures de gestion des risques devraient garantir, pour les réseaux et les systèmes d'information de la **totalité de l'environnement TIC**, un niveau de sécurité adapté aux risques identifiés dans le cadre de gestion des risques en tenant compte de l'état des connaissances et, s'il y a lieu, des normes européennes et internationales applicables ou des certificats de cybersécurité européens disponibles.

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

Évaluations de la maturité en matière de cybersécurité

Chaque entité de l'Union devrait procéder, au plus tard 18 mois après la date d'entrée en vigueur du règlement, puis au moins tous les deux ans par la suite, à une évaluation de la maturité en matière de cybersécurité portant sur l'ensemble des éléments de son environnement TIC. Les petites entités de l'Union dont les tâches ou la structure sont similaires pourraient effectuer une évaluation combinée de la maturité en matière de cybersécurité.

Compte tenu des conclusions tirées de l'évaluation de la maturité en matière de cybersécurité et des risques identifiés, le niveau hiérarchique le plus élevé de chaque entité de l'Union devrait approuver un **plan de cybersécurité** dans les meilleurs délais après l'établissement du cadre et l'adoption des mesures de gestion des risques de cybersécurité.

Conseil interinstitutionnel de cybersécurité - IICB

L'IICB a pour but d'aider les entités à améliorer leurs postures de cybersécurité respectives grâce à la mise en œuvre du règlement. Afin d'aider les entités de l'Union, l'IICB devrait i) adopter les **orientations et les recommandations** requises pour les évaluations de la maturité en matière de cybersécurité et les plans de cybersécurité des entités de l'Union, ii) réexaminer les interconnexions éventuelles entre les environnements TIC des entités de l'Union et iii) soutenir la mise en place d'un **groupe de responsables de la cybersécurité** relevant de l'ENISA, comprenant les responsables locaux de la cybersécurité de toutes les entités de l'Union, avec pour objectif de faciliter le partage de bonnes pratiques et d'expériences découlant de la mise en œuvre du règlement.

Lorsque l'IICB considère qu'une entité de l'Union n'a pas appliqué ou mis en œuvre le règlement avec efficacité, il pourrait i) demander la documentation pertinente et disponible portant sur la bonne mise en œuvre des dispositions du règlement, ii) faire part de son **avis motivé** relatif aux lacunes observées dans la mise en œuvre du règlement, iii) inviter l'entité de l'Union concernée à fournir une auto-évaluation de son avis motivé et iv) publier, en coopération avec le CERT-UE, des **orientations** destinées à rendre conformes au règlement son cadre de gestion, de gouvernance et de contrôle des risques, ses mesures de gestion des risques de cybersécurité, ses plans de cybersécurité et ses obligations de communication d' information.

Mission et tâches du CERT-UE

La mission du CERT-UE, centre interinstitutionnel autonome de cybersécurité au service de l'ensemble des entités de l'Union serait de contribuer à la sécurité de l'environnement TIC non classifié de l'ensemble des entités de l'Union et de leur fournir des conseils concernant la cybersécurité, en les aidant à prévenir, à détecter et à traiter les incidents, ainsi qu'à en atténuer les effets, à y répondre et à s'en remettre. Le CERT-UE serait un fournisseur interinstitutionnel autonome de services destinés à l'ensemble des entités de l'Union. Il serait intégré à la structure administrative d'une direction générale de la Commission, afin de bénéficier des structures d'appui de la Commission en matière administrative, financière, de gestion et de comptabilité.

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 devraient informer le CERT-UE de tout incident ayant un impact important. Un incident est considéré comme important si: a) il a causé ou est susceptible de causer une perturbation opérationnelle grave du service ou des pertes financières pour l'entité concernée; b) 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 devraient notifier, entre autres, toute information qui permet au CERT-UE de déterminer toute conséquence inter-entités, transfrontière ou pour l'État membre hôte de l'incident important. L'ensemble des entités de l'Union devraient transmettre au CERT-EU:

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 si l'on suspecte l'incident important d'avoir été causé par des actes illicites ou malveillants ou s'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, un rapport d'incident.

Le CERT-UE devrait coordonner le traitement des **incidents majeurs** entre les entités de l'Union.