Conseil de
l'Union européenne

Bruxelles, le 17 décembre 2025
(OR. en)

16960/25

CYBER 389
JAI 1924
DATAPROTECT 345
TELECOM 485
MI 1075
CSC 693
CSCI 284
DELACT 198

NOTE DE TRANSMISSION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	11 décembre 2025
Destinataire:	Madame Thérèse BLANCHET, secrétaire générale du Conseil de l'Union européenne
N° doc. Cion:	C(2025) 8407 final
Objet:	RÈGLEMENT DÉLÉGUÉ (UE) …/... DE LA COMMISSION du 11.12.2025 complétant le règlement (UE) 2024/2847 du Parlement européen et du Conseil en précisant les conditions d'application des motifs ayant trait à la cybersécurité en ce qui concerne le report de la diffusion des notifications

Les délégations trouveront ci-joint le document C(2025) 8407 final.

p.j.: C(2025) 8407 final

COMMISSION
EUROPÉENNE

Bruxelles, le 11.12.2025
C(2025) 8407 final

RÈGLEMENT DÉLÉGUÉ (UE) …/... DE LA COMMISSION

du 11.12.2025

complétant le règlement (UE) 2024/2847 du Parlement européen et du Conseil en précisant les conditions d'application des motifs ayant trait à la cybersécurité en ce qui concerne le report de la diffusion des notifications

(Texte présentant de l'intérêt pour l'EEE)

EXPOSÉ DES MOTIFS

1. CONTEXTE DE L'ACTE DÉLÉGUÉ

Le règlement (UE) 2024/2847 du Parlement européen et du Conseil (ci-après le «règlement sur la cyberrésilience») impose aux fabricants de produits comportant des éléments numériques de notifier, par l'intermédiaire d'une plateforme unique de signalement, toute vulnérabilité activement exploitée ou tout incident grave ayant des répercussions sur la sécurité d'un de ces produits. Conformément à l'article 16, paragraphe 2, dudit règlement, le centre de réponse aux incidents de sécurité informatique (CSIRT) désigné par l'État membre comme coordinateur qui reçoit initialement la notification peut, dans des circonstances exceptionnelles et pour des motifs justifiés ayant trait à la cybersécurité, retarder la diffusion de la notification aux CSIRT d'autres États membres dans lesquels le produit comportant des éléments numériques a été mis à disposition.

Le présent acte délégué vise donc à compléter le règlement sur la cyberrésilience en précisant les conditions d'application des motifs ayant trait à la cybersécurité pour retarder la diffusion des notifications. Pour ce faire, il distingue trois types de raisons pour lesquelles le CSIRT recevant initialement la notification peut décider qu'il est nécessaire de retarder la diffusion à d'autres CSIRT. Cette décision peut être prise dans trois cas:

- à la lumière d'une évaluation de la nature des informations notifiées;
- si le CSIRT qui reçoit la notification n'est pas en mesure de garantir la confidentialité de ces informations;
- si la plateforme unique de signalement a été compromise ou n'est temporairement pas opérationnelle.

Les obligations en matière de communication d'informations énoncées à l'article 14 du règlement (UE) 2024/2847 devraient s'appliquer à partir du 11 septembre 2026.

2. CONSULTATION AVANT L'ADOPTION DE L'ACTE

Différents projets du présent acte ont été soumis pour consultation au réseau des CSIRT et à l'Agence de l'Union européenne pour la cybersécurité (ENISA). Un débat préliminaire comportant des questions d'orientation a eu lieu le 26 mars 2025, avec la possibilité de fournir des contributions écrites au plus tard le 11 avril 2025. Une première version de projet du présent acte a été communiquée au réseau des CSIRT et à l'ENISA le 16 mai 2025 et une discussion a eu lieu le 6 juin 2025, avec la possibilité de fournir des contributions écrites au plus tard le 27 juin 2025. Une deuxième version de ce projet a été communiquée au réseau des CSIRT et à l'ENISA le 23 juillet 2025, avec la possibilité de fournir des contributions écrites au plus tard le 1er septembre 2025. Une troisième version de ce projet a été communiquée au réseau des CSIRT et à l'ENISA le 25 septembre 2025 et une discussion a eu lieu le 9 octobre 2025, avec la possibilité de fournir des contributions écrites au plus tard le 27 octobre 2025.

Le projet d'acte a fait l'objet d'une consultation publique entre le 16 octobre 2025 et le 13 novembre 2025, dans le cadre de laquelle ont été reçues 34 réponses de 31 répondants uniques (ce qui tient compte du fait qu'un même répondant s'est exprimé au moyen de 4 contributions différentes). Parmi ces réponses, 29,41 % émanaient d'associations professionnelles, 26,47 % d'entreprises, 17,65 % de citoyens de l'UE, 14,71 % d'autorités publiques, 5,88 %

d'organisations non gouvernementales (ONG) et 5,88 % d'établissements universitaires/de recherche[1].

Le 22 octobre, le projet a également été examiné avec le groupe d'experts sur la cybersécurité des produits comportant des éléments numériques (E03967), dont les membres comprennent des autorités des États membres, l'ENISA, des experts individuels nommés à titre personnel et des organisations au sens large (par exemple, des entreprises, des associations, des ONG).

3. ÉLÉMENTS JURIDIQUES DE L'ACTE DÉLÉGUÉ

L'habilitation à adopter des actes délégués est prévue à l'article 14, paragraphe 9, du règlement sur la cyberrésilience, qui impose à la Commission de préciser les conditions d'application des motifs ayant trait à la cybersécurité en ce qui concerne le report de la diffusion des notifications au plus tard le 11 décembre 2025.

[1] Ces pourcentages ne tiennent pas compte du fait qu'un même répondant s'est exprimé au moyen de 4 contributions différentes.

RÈGLEMENT DÉLÉGUÉ (UE) …/... DE LA COMMISSION

du 11.12.2025

complétant le règlement (UE) 2024/2847 du Parlement européen et du Conseil en précisant les conditions d'application des motifs ayant trait à la cybersécurité en ce qui concerne le report de la diffusion des notifications

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) nº 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience)[2], et en particulier son article 14, paragraphe 9,

considérant ce qui suit:

(1) Dans des circonstances exceptionnelles et, en particulier, à la demande du fabricant et compte tenu du degré de sensibilité des informations notifiées, et pour des motifs justifiés ayant trait à la cybersécurité, le centre de réponse aux incidents de sécurité informatique (CSIRT) désigné comme coordinateur qui reçoit initialement la notification d'une vulnérabilité activement exploitée ou d'un incident grave ayant des répercussions sur la sécurité d'un produit comportant des éléments numériques (ci-après le «CSIRT recevant initialement la notification») peut décider de retarder, pour la durée strictement nécessaire, la diffusion de la notification via la plateforme unique de signalement aux CSIRT désignés comme coordinateurs sur le territoire desquels le fabricant soumettant la notification a indiqué que le produit comportant des éléments numériques a été mis à disposition (ci-après les «CSIRT concernés»). Par conséquent, il est nécessaire de définir les conditions d'application de ces motifs. Lorsque de tels motifs s'appliquent, le CSIRT recevant initialement la notification est autorisé à retarder la diffusion auprès des CSIRT concernés pour la durée strictement nécessaire, mais n'est pas tenu de le faire. En vertu de l'article 16, paragraphe 2, du règlement (UE) 2024/2847, lorsqu'un CSIRT recevant initialement la notification décide d'invoquer de tels motifs, il devrait immédiatement informer l'Agence de l'Union européenne pour la cybersécurité (ENISA) de sa décision de reporter la notification, ainsi que des raisons qui la motivent, et lui indiquer la date à laquelle il a l'intention de diffuser la notification.

(2) Conformément à l'article 16, paragraphe 2, deuxième alinéa, du règlement (UE) 2024/2847, les conditions d'application des motifs ayant trait à la cybersécurité énoncées dans le présent règlement ne s'appliquent pas à l'accès de l'ENISA aux informations notifiées. L'accès de l'ENISA aux informations notifiées ne peut être restreint que dans des circonstances particulièrement exceptionnelles: lorsque le

[2] JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

fabricant indique dans sa notification que l'une des trois conditions visées à l'article 16, paragraphe 2, troisième alinéa, points a), b) ou c), du règlement (UE) 2024/2847 est remplie, et uniquement en ce qui concerne la notification de vulnérabilité soumise dans les 72 heures visée à l'article 14, paragraphe 2, point b), du règlement (UE) 2024/2847. Dans de tels cas, les seules informations qui doivent être mises simultanément à la disposition de l'ENISA sont l'information qu'une notification a été effectuée par un fabricant, des informations générales sur le produit comportant des éléments numériques, des informations sur la nature générale du code d'exploitation et l'information indiquant que des motifs liés à la sécurité ont été invoqués.

(3) L'accès aux informations notifiées permet aux CSIRT d'avoir une vue d'ensemble de l'environnement de sécurité sur leur territoire et de mettre en place des mesures d'atténuation, ce qui relève le niveau global de cybersécurité dans l'Union. Par conséquent, il ne devrait être possible de restreindre davantage la diffusion des notifications eu égard à la nature des informations notifiées que dans les cas où, compte tenu de la sensibilité des informations notifiées, les risques en matière de cybersécurité découlant d'une diffusion plus large l'emportent sur les avantages en matière de sécurité pour l'Union, et où ces risques ne peuvent être atténués de manière adéquate en imposant des restrictions au traitement et à la diffusion plus large de la notification au moyen de protocoles appropriés utilisés au sein du réseau des CSIRT, tels que les protocoles TLP ou PAP. Tel peut être le cas, par exemple, lorsqu'un fabricant a informé le CSIRT recevant initialement la notification qu'il prévoit de fournir prochainement une mesure d'atténuation (telle qu'un correctif). Cela peut également se produire lorsque le CSIRT recevant initialement la notification décide de ne partager que certaines parties d'une notification, et que ces parties sont néanmoins suffisantes pour permettre aux CSIRT concernés de s'assurer qu'ils sont en mesure de mettre en place des mesures adéquates d'atténuation des risques. En outre, et afin d'encourager la coopération en matière d'identification et de divulgation des vulnérabilités entre les fabricants, les CSIRT et les spécialistes de la recherche sur la sécurité, cela peut aussi être le cas lorsque le CSIRT fait office d'intermédiaire de confiance pour une procédure de divulgation coordonnée des vulnérabilités (DCV) en cours, telle que mentionnée à l'article 12, paragraphe 1, de la directive (UE) 2022/2555 du Parlement européen et du Conseil[3]. Dans un tel cas, lorsque le CSIRT décide de retarder la diffusion d'une notification, et conformément à l'article 16, paragraphe 6, du règlement (UE) 2024/2847, il doit la reporter pour une durée qui n'excède pas ce qui est strictement nécessaire et jusqu'à ce que les parties concernées par la DCV aient donné leur consentement à la divulgation.

(4) Les informations figurant dans la notification aideront les CSIRT à s'acquitter de leurs tâches dans le cadre de l'atténuation des risques et de la gestion des incidents. Toutefois, dans de rares cas, ces informations pourraient être suffisantes pour permettre, même à des acteurs disposant de compétences et de ressources limitées, de créer une technique d'exploitation sans recherche supplémentaire. Si ces informations devenaient accessibles à des acteurs malveillants, les répercussions sur la cybersécurité de l'Union seraient lourdes, compte tenu de la facilité d'exploitation. Cela pourrait se

[3] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

produire, par exemple, lorsque la version vulnérable d'un logiciel ne diffère que de manière marginale des versions antérieures non vulnérables. En pareil cas, si le CSIRT recevant initialement la notification juge impossible d'atténuer de manière adéquate les risques de cybersécurité découlant d'une diffusion plus large en imposant des restrictions en matière de traitement et de diffusion plus large, il peut décider de retarder la diffusion jusqu'à ce qu'une mesure efficace d'atténuation des risques, telle qu'une mise à jour de sécurité ou des orientations à l'intention des utilisateurs, soit disponible.

(5) Si un CSIRT concerné n'est pas en mesure de protéger de manière adéquate les informations notifiées, des acteurs malveillants pourraient accéder à des informations sensibles et des codes d'exploitation pourraient être mis en place dans l'ensemble du marché unique. Par conséquent, lorsqu'il existe de sérieuses réserves quant à la capacité d'un CSIRT concerné à garantir la confidentialité des informations notifiées, le CSIRT recevant initialement la notification peut décider de reporter la diffusion d'une notification uniquement à ce CSIRT concerné jusqu'à ce que ces réserves aient été levées. Tel peut être le cas lorsqu'un CSIRT concerné a été touché par un incident de cybersécurité affectant sa capacité à fonctionner en toute sécurité, ou lorsqu'il existe des preuves ou des informations indiquant que des lacunes importantes dans les capacités de ce CSIRT ont été détectées, telles que de fortes contraintes en matière de ressources compromettant sa capacité à exercer ses fonctions, ou l'utilisation de logiciels obsolètes ou vulnérables.

(6) Afin d'empêcher des acteurs malveillants d'accéder à des informations sensibles, lorsque la plateforme unique de signalement établie en vertu de l'article 16 du règlement (UE) 2024/2847 a été compromise par un incident de cybersécurité, le CSIRT recevant initialement la notification devrait retarder la diffusion via la plateforme unique de signalement jusqu'à ce que la capacité de cette plateforme à garantir la confidentialité des informations notifiées ait été rétablie.

(7) Conformément à l'article 16, paragraphe 2, premier alinéa, du règlement (UE) 2024/2847, le CSIRT recevant initialement la notification n'est pas tenu de diffuser une notification à tout autre CSIRT concerné si le fabricant indique que le produit comportant des éléments numériques n'est mis à disposition que sur le marché de l'État membre du CSIRT recevant initialement la notification.

(8) La Commission a consulté et sollicité l'avis des parties prenantes concernées lors de l'élaboration du projet d'acte délégué et a consulté le groupe d'experts sur la cybersécurité des produits comportant des éléments numériques.

(9) Conformément à l'article 14, paragraphe 9, du règlement (UE) 2024/2847, la Commission a coopéré étroitement avec le réseau des CSIRT établi en vertu de l'article 15 de la directive (UE) 2022/2555 et avec l'ENISA lors de l'élaboration du projet d'acte délégué,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Objet

Le présent règlement précise les conditions d'application des motifs ayant trait à la cybersécurité visés à l'article 16, paragraphe 2, du règlement (UE) 2024/2847, qui permettent au CSIRT désigné comme coordinateur recevant initialement une notification conformément à l'article 14, paragraphes 1 et 3, et à l'article 15, paragraphes 1 et 2, dudit règlement de

retarder la diffusion de la notification aux CSIRT désignés comme coordinateurs sur le territoire desquels le fabricant a indiqué que le produit comportant des éléments numériques a été mis à disposition.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

(1) «CSIRT recevant initialement la notification»: le CSIRT désigné comme coordinateur qui reçoit initialement la notification conformément à l'article 14, paragraphes 1 et 3, et à l'article 15, paragraphes 1 et 2, du règlement (UE) 2024/2847;

(2) «CSIRT concerné»: le CSIRT désigné comme coordinateur sur le territoire duquel le fabricant a indiqué que le produit comportant des éléments numériques a été mis à disposition.

Article 3

Conditions d'application des motifs ayant trait à la cybersécurité découlant de la nature des informations déclarées

Le CSIRT recevant initialement la notification peut décider de retarder, pendant une période limitée à ce qui est strictement nécessaire, la diffusion des notifications ou de parties de celles-ci aux CSIRT concernés dans les cas où, compte tenu de la sensibilité des informations notifiées, les risques en matière de cybersécurité liés à la diffusion l'emportent sur les avantages en matière de sécurité qu'elle procure, et où il est impossible d'atténuer ces risques en imposant des restrictions au traitement ou à la diffusion plus large de la notification au moyen de protocoles appropriés, tels que les protocoles «Traffic Light Protocol» (TLP) ou «Permissible Actions Protocol» (PAP), et lorsqu'au moins une des conditions suivantes est remplie:

(a) le fabricant a informé le CSIRT recevant initialement la notification qu'une mesure efficace d'atténuation des risques, telle qu'une mise à jour de sécurité ou des orientations à l'intention des utilisateurs, devrait être mise à disposition dans un délai de 72 heures; si aucune mesure efficace d'atténuation des risques n'est mise à disposition dans ce délai, le CSIRT recevant initialement la notification diffuse la notification aux CSIRT concernés;

(b) les informations figurant dans la notification sont jugées suffisantes, compte tenu de la nature de la vulnérabilité activement exploitée notifiée, pour créer une technique d'exploitation, en particulier lorsque la vulnérabilité peut être facilement identifiée et exploitée par des acteurs disposant de compétences et de ressources limitées; dès lors qu'une mesure efficace d'atténuation des risques, telle qu'une mise à jour de sécurité ou des orientations à l'intention des utilisateurs, est mise à disposition, le CSIRT recevant initialement la notification diffuse la notification aux CSIRT concernés;

(c) le CSIRT recevant initialement la notification est en mesure de partager avec les CSIRT concernés des informations suffisantes pour faire en sorte que les CSIRT concernés puissent mettre en place des mesures adéquates d'atténuation des risques; dès lors qu'une mesure efficace d'atténuation des risques, telle qu'une mise à jour de sécurité ou des orientations à l'intention des utilisateurs, est mise à disposition, le

CSIRT recevant initialement la notification diffuse la notification complète aux CSIRT concernés;

(d) le CSIRT recevant initialement la notification de la vulnérabilité activement exploitée en a été informé dans le cadre d'une divulgation coordonnée des vulnérabilités (DCV) pour laquelle il fait office d'intermédiaire de confiance conformément à l'article 12, paragraphe 1, de la directive (UE) 2022/2555; dans ce cas, et conformément à l'article 16, paragraphe 6, du règlement (UE) 2024/2847, le CSIRT recevant initialement la notification la diffuse aux CSIRT concernés lorsqu'il n'est plus strictement nécessaire d'en reporter la diffusion et que les parties concernées par la DCV ont donné leur consentement à la divulgation.

Article 4

Conditions d'application des motifs ayant trait à la cybersécurité en ce qui concerne un CSIRT particulier

Le CSIRT recevant initialement la notification peut décider de retarder pour une période limitée à ce qui est strictement nécessaire la diffusion des notifications ou de parties de celles-ci à un CSIRT concerné particulier dans les cas où:

(a) le CSIRT concerné a été touché par un incident de cybersécurité remettant en cause sa capacité à garantir la confidentialité des informations notifiées;

(b) il a des raisons suffisantes de penser que les capacités du CSIRT concerné sont insuffisantes pour garantir la confidentialité des informations notifiées.

Dans les cas visés au premier alinéa, point a), le CSIRT recevant initialement la notification peut retarder la diffusion jusqu'à ce que le CSIRT concerné ait informé le réseau des CSIRT mentionné à l'article 15 de la directive 2022/2555 que sa capacité à garantir la confidentialité des notifications a été rétablie.

Dans les cas visés au premier alinéa, point b), le CSIRT recevant initialement la notification peut retarder la diffusion au CSIRT concerné jusqu'à ce que ce dernier ait fourni la preuve qu'il a remédié aux lacunes constatées.

Article 5

Conditions d'application des motifs ayant trait à la cybersécurité en ce qui concerne la plateforme unique de signalement

Le CSIRT recevant initialement la notification peut décider de retarder la diffusion des notifications via la plateforme unique de signalement établie par l'article 16 du règlement (UE) 2024/2847 lorsque l'ENISA a informé le réseau des CSIRT, conformément à l'article 16, paragraphe 4, dudit règlement, que la plateforme unique de signalement a été touchée par un incident de cybersécurité remettant en cause sa capacité à garantir la confidentialité des informations notifiées. Dans un tel cas, le CSIRT recevant initialement la notification peut retarder la diffusion via la plateforme unique de signalement jusqu'à ce que l'ENISA ait informé le réseau des CSIRT que la capacité de la plateforme à garantir la confidentialité des notifications a été rétablie.

Article 6

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 11.12.2025

Par la Commission
La présidente
Ursula VON DER LEYEN