Journal officiel
de l'Union européenne

FR
Série L

2025/301

20.2.2025

RÈGLEMENT DÉLÉGUÉ (UE) 2025/301 DE LA COMMISSION

du 23 octobre 2024

complétant le règlement (UE) 2022/2554 du Parlement européen et du Conseil par des normes techniques de réglementation précisant le contenu et les délais pour la notification initiale des incidents majeurs liés aux TIC, et pour les rapports intermédiaire et final y afférents, et le contenu de la notification volontaire en ce qui concerne les cybermenaces importantes

(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) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011 ([1]), et notamment son article 20, troisième alinéa,

considérant ce qui suit:

(1) Afin de garantir l'harmonisation et la simplification des exigences en matière de notification et de déclaration des incidents majeurs liés aux TIC visées à l'article 19, paragraphe 4, du règlement (UE) 2022/2554, les délais de notification des incidents majeurs liés aux TIC devraient suivre une approche cohérente pour tous les types d'entités financières. Pour ces raisons, les délais devraient également, dans toute la mesure du possible, suivre une approche cohérente avec les exigences énoncées dans la directive (UE) 2022/2555 du Parlement européen et du Conseil ([2]), et avoir au moins un effet équivalent à celles-ci.

(2) Afin d'éviter d'imposer une charge de déclaration excessive aux entités financières lorsqu'elles traitent l'incident lié aux TIC, le contenu de la notification initiale devrait être limité aux informations les plus importantes. Pour pouvoir prendre des mesures de surveillance appropriées, les autorités compétentes doivent recevoir des informations sur les incidents majeurs liés aux TIC le plus rapidement possible après que l'entité financière a classé un incident lié aux TIC comme majeur. Par conséquent, le délai de soumission d'une notification initiale visée à l'article 19, paragraphe 4, point a), du règlement (UE) 2022/2554 devrait être aussi court que possible après qu'un incident lié aux TIC a été classé comme majeur, tout en permettant une certaine souplesse, en particulier pour les modèles commerciaux de services qui ne sont pas particulièrement limités dans le temps, si les entités financières ont besoin de plus de temps pour traiter l'incident lié aux TIC après en avoir pris connaissance.

(3) Après avoir reçu la notification initiale, les autorités compétentes devraient recevoir des informations plus détaillées sur l'incident lié aux TIC dans le rapport intermédiaire et toutes les informations pertinentes dans le rapport final. Les informations contenues dans ces rapports devraient permettre aux autorités compétentes d'évaluer plus avant l'incident lié aux TIC et d'évaluer les mesures de surveillance qu'elles pourraient souhaiter prendre.

(4) Les délais de notification visés à l'article 20, premier alinéa, point a), ii), du règlement (UE) 2022/2554 devraient donc établir un équilibre entre la nécessité pour les autorités compétentes de recevoir rapidement les informations et la nécessité d'accorder aux entités financières suffisamment de temps pour obtenir des informations complètes et exactes.

(5) Compte tenu des critères énoncés à l'article 20, premier alinéa, point a), du règlement (UE) 2022/2554, les délais de notification ne devraient pas représenter une charge disproportionnée pour les microentreprises et les autres entités financières qui ne sont pas importantes. En outre, les délais de notification devraient tenir compte des weekends et jours fériés, afin d'éviter de faire supporter une charge disproportionnée aux entités financières.

([1]) JO L 333 du 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) 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, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(6) Étant donné que les cybermenaces importantes doivent être notifiées sur une base volontaire, le contenu de ces notifications ne devrait pas imposer de charge aux entités financières et devrait être plus limité que les informations demandées pour les incidents majeurs liés aux TIC.

(7) Le présent règlement se fonde sur le projet de normes techniques de réglementation soumis à la Commission par les autorités européennes de surveillance.

(8) Les autorités européennes de surveillance ont procédé à des consultations publiques ouvertes sur les projets de normes techniques de réglementation sur lesquels se fonde le présent règlement, analysé les coûts et avantages potentiels qu'ils impliquent et sollicité l'avis du groupe des parties intéressées institué en application de l'article 37 des règlements (UE) nº 1093/2010 ([3]), (UE) nº 1094/2010 ([4]) et (UE) nº 1095/2010 ([5]) du Parlement européen et du Conseil.

(9) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([6]) et a rendu un avis positif le 22 juillet 2024. Tout traitement de données à caractère personnel relevant du champ d'application du présent règlement devrait être effectué conformément aux principes applicables en matière de protection des données et aux dispositions du règlement (UE) 2018/1725.

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Informations générales à fournir dans les notifications initiales et les rapports intermédiaire et final sur les incidents majeurs liés aux TIC

Les entités financières incluent dans la notification initiale, le rapport intermédiaire et le rapport final, visés à l'article 19, paragraphe 4, du règlement (UE) 2022/2554, les informations générales suivantes:

a) le type de soumission (notification initiale, rapport intermédiaire ou rapport final);

b) le nom de l'entité financière, son code LEI et le type d'entité financière visé à l'article 2, paragraphe 1, du règlement (UE) 2022/2554;

c) le nom et le code d'identification de l'entité qui soumet la notification initiale, ou le rapport intermédiaire ou final, pour l'entité financière;

d) le cas échéant, les noms et codes LEI de toutes les entités financières couvertes par la notification initiale agrégée ou le rapport intermédiaire ou final;

e) les coordonnées des personnes chargées de communiquer avec l'autorité compétente au sujet de l'incident majeur lié aux TIC;

f) le cas échéant, l'identification de l'entreprise mère du groupe auquel l'entité financière appartient;

g) en cas d'incidence sur la situation monétaire, la monnaie dans laquelle les montants sont calculés.

([3]) Règlement (UE) nº 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission (JO L 331 du 15.12.2010, p. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Règlement (UE) nº 1094/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/79/CE de la Commission (JO L 331 du 15.12.2010, p. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Règlement (UE) nº 1095/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des marchés financiers), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/77/CE de la Commission (JO L 331 du 15.12.2010, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 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, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Article 2

Informations spécifiques à fournir dans les notifications initiales

Les notifications initiales visées à l'article 19, paragraphe 4, point a), du règlement (UE) 2022/2554 contiennent au moins toutes les informations spécifiques suivantes:

a) le code de référence de l'incident attribué par l'entité financière;

b) la date et l'heure de détection de l'incident et sa classification conformément à l'article 8 du règlement délégué (UE) 2024/1772 de la Commission ([7]);

c) une description de l'incident lié aux TIC;

d) les critères énoncés aux articles 1er à 8 du règlement délégué (UE) 2024/1772, sur la base desquels l'entité financière a classé l'incident lié aux TIC comme majeur;

e) les États membres touchés par l'incident lié aux TIC;

f) des informations sur la manière dont l'incident lié aux TIC a été détecté;

g) le cas échéant, des informations sur l'origine de l'incident lié aux TIC;

h) des informations indiquant si l'entité financière a activé un plan de continuité des activités;

i) le cas échéant, des informations sur le reclassement de l'incident lié aux TIC de majeur à non majeur;

j) le cas échéant, toute autre information pertinente.

Article 3

Informations spécifiques à fournir dans les rapports intermédiaires

Les rapports intermédiaires visés à l'article 19, paragraphe 4, point b), du règlement (UE) 2022/2554 contiennent au moins toutes les informations spécifiques suivantes:

a) le cas échéant, le code de référence de l'incident attribué par l'autorité compétente;

b) la date et l'heure auxquelles l'incident lié aux TIC est survenu;

c) le cas échéant, la date et l'heure auxquelles l'entité financière a repris ses activités régulières;

d) des informations sur la manière dont les critères énoncés aux articles 1er à 8 du règlement délégué (UE) 2024/1772 ont été remplis, sur la base desquels l'entité financière a classé l'incident lié aux TIC comme majeur;

e) le type d'incident lié aux TIC;

f) le cas échéant, les menaces et les techniques utilisées par l'acteur de la menace;

g) les domaines fonctionnels et les processus opérationnels concernés;

h) les composants d'infrastructure concernés soutenant les processus opérationnels;

i) l'incidence sur les intérêts financiers des clients;

j) des informations sur la notification de l'incident lié aux TIC à d'autres autorités;

k) les actions ou mesures temporaires prises ou prévues par l'entité financière pour se rétablir à la suite de l'incident lié aux TIC;

l) le cas échéant, des informations sur les indicateurs de compromis.

([7]) Règlement délégué (UE) 2024/1772 de la Commission du 13 mars 2024 complétant le règlement (UE) 2022/2554 du Parlement européen et du Conseil par des normes techniques de réglementation précisant les critères de classification des incidents liés aux TIC et des cybermenaces, fixant des seuils d'importance significative et précisant les détails des rapports d'incidents majeurs (JO L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

Article 4

Informations spécifiques à fournir dans les rapports finaux

Les rapports finaux visés à l'article 19, paragraphe 4, point c), du règlement (UE) 2022/2554 contiennent toutes les informations spécifiques suivantes:

a) des informations sur les causes originelles de l'incident lié aux TIC;

b) les dates et heures auxquelles l'incident lié aux TIC a été résolu et la ou les causes originelles ont été traitées;

c) des informations sur la résolution de l'incident lié aux TIC;

d) le cas échéant, les informations pertinentes pour les autorités de résolution;

e) des informations sur les coûts et pertes directs et indirects découlant de l'incident lié aux TIC et des informations sur les recouvrements financiers;

f) le cas échéant, des informations sur les incidents récurrents liés aux TIC.

Article 5

Délais pour la notification initiale et pour les rapports intermédiaire et final

1. Les entités financières soumettent la notification initiale et les rapports intermédiaire et final visés à l'article 19, paragraphe 4, points a), b) et c), du règlement (UE) 2022/2554 dans les délais suivants:

a) pour le rapport initial: le plus tôt possible, mais en tout état de cause, dans un délai de quatre heures à compter de la classification de l'incident lié aux TIC comme majeur et au plus tard 24 heures à compter du moment où l'entité financière en a eu connaissance;

b) pour le rapport intermédiaire: au plus tard dans un délai de 72 heures à compter de la soumission de la notification initiale, même si la situation ou le traitement de l'incident n'ont pas changé conformément à l'article 19, paragraphe 4, point b), du règlement (UE) 2022/2554. Les entités financières soumettent sans retard injustifié un rapport intermédiaire actualisé et, en tout état de cause, lorsque les activités régulières ont repris;

c) pour le rapport final: au plus tard un mois après la soumission du rapport intermédiaire ou, le cas échéant, après la dernière mise à jour du rapport intermédiaire.

2. Lorsque l'entité financière n'a pas classé un incident lié aux TIC comme majeur dans un délai de 24 heures à compter du moment où elle en a eu connaissance, mais qu'elle classe cet incident comme majeur à un stade ultérieur, elle soumet la notification initiale dans un délai de quatre heures à compter de la classification de l'incident lié aux TIC comme majeur.

3. Les entités financières qui ne sont pas en mesure de soumettre la notification initiale, le rapport intermédiaire ou le rapport final dans les délais fixés au paragraphe 1 en informent l'autorité compétente dans les meilleurs délais, mais au plus tard dans les délais respectifs pour la soumission de la notification ou du rapport, et en expliquent les raisons.

4. Lorsque le délai de soumission d'une notification initiale, d'un rapport intermédiaire ou d'un rapport final expire un jour de week-end ou un jour férié dans l'État membre de l'entité financière déclarante, l'entité financière peut soumettre la notification initiale, le rapport intermédiaire ou le rapport final au plus tard à midi le jour ouvrable suivant.

5. Le paragraphe 4 ne s'applique pas à la soumission d'une notification initiale ou d'un rapport intermédiaire par les établissements de crédit, les contreparties centrales, les opérateurs de plates-formes de négociation et d'autres entités financières considérées comme des entités essentielles ou importantes conformément à l'article 3 de la directive (UE) 2022/2555.

6. Les autorités compétentes peuvent décider que le paragraphe 4 ne s'applique pas à la soumission d'une notification initiale ou d'un rapport intermédiaire par les entités financières, autres que celles visées au paragraphe 5, qui sont classées comme importantes ou présentent un caractère systémique pour le secteur financier au niveau national ou de l'Union. Les autorités compétentes notifient leur décision aux entités financières concernées. La décision de l'autorité compétente ne s'applique qu'en ce qui concerne les incidents déclarés après la date de la notification de la décision par l'autorité compétente aux entités financières concernées.

Article 6

Contenu de la notification volontaire des cybermenaces importantes

Le contenu de la notification volontaire en ce qui concerne les cybermenaces importantes visée à l'article 19, paragraphe 2, du règlement (UE) 2022/2554 couvre l'ensemble des éléments suivants:

a) des informations générales sur l'entité financière notifiante, conformément à l'article 1er;

b) la date et l'heure de détection de la cybermenace importante et de tout autre horodatage pertinent lié à cette dernière;

c) une description de la cybermenace importante;

d) des informations sur l'incidence potentielle de la cybermenace importante sur l'entité financière, ses clients ou ses contreparties financières;

e) les critères de classification susceptibles d'avoir été à l'origine d'un rapport d'incident majeur prévus aux articles 1er à 8 du règlement délégué (UE) 2024/1772 en cas de matérialisation de la cybermenace;

f) des informations sur la situation de la cybermenace importante et sur tout changement dans l'activité de la menace;

g) le cas échéant, une description des mesures prises par l'entité financière pour empêcher la matérialisation des cybermenaces importantes;

h) des informations sur toute notification de la cybermenace importante à d'autres entités ou autorités financières;

i) le cas échéant, des informations sur les indicateurs de compromis;

j) le cas échéant, toute autre information pertinente.

Article 7

Entrée en vigueur

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 23 octobre 2024.

Par la Commission
La présidente
Ursula VON DER LEYEN