COMMISSION
EUROPÉENNE

Bruxelles, le 13.3.2024
C(2024) 1519 final

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

du 13.3.2024

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

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

EXPOSÉ DES MOTIFS

1. CONTEXTE DE L'ACTE DÉLÉGUÉ

L'un des objectifs du règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier (DORA) est d'harmoniser et de rationaliser le régime de déclaration des incidents liés aux TIC par les entités financières de l'UE. À cette fin, il instaure des exigences cohérentes applicables aux entités financières en matière de gestion, de classification et de déclaration des incidents liés aux TIC.

À cet égard, l'article 18, paragraphe 3, du règlement DORA charge les autorités européennes de surveillance (AES) d'élaborer, par l'intermédiaire du comité mixte et en concertation avec la BCE et l'ENISA, des projets communs de normes techniques de réglementation précisant les éléments suivants:

(a) les critères énoncés à l'article 18, paragraphe 1, du règlement DORA sur la base desquels les entités financières doivent classer les incidents liés au TIC et déterminer leur incidence, notamment les seuils d'importance significative servant à déterminer les incidents majeurs liés aux TIC ou, le cas échéant, les incidents opérationnels ou de sécurité majeurs liés au paiement qui sont soumis à l'obligation de déclaration prévue à l'article 19, paragraphe 1, du règlement DORA;

(b) les critères que les autorités compétentes doivent appliquer pour évaluer si des incidents majeurs liés aux TIC ou, le cas échéant, des incidents opérationnels ou de sécurité majeurs liés au paiement, sont pertinents pour les autorités compétentes concernées des autres États membres, et les détails des rapports sur les incidents majeurs liés aux TIC ou, le cas échéant, les incidents opérationnels ou de sécurité majeurs liés au paiement, à partager avec les autres autorités compétentes conformément à l'article 19, paragraphes 6 et 7, du règlement DORA; et

(c) les critères permettant de classer les cybermenaces comme importantes, notamment les seuils d'importance significative élevés servant à identifier les cybermenaces importantes.

Le présent règlement délégué s'inscrit dans ce mandat et a été transmis à la Commission le 17 janvier 2024.

L'ENISA et la BCE ont fait partie du sous-comité sur la résilience opérationnelle numérique du comité mixte des AES (JC SC DOR).

2. CONSULTATION AVANT L'ADOPTION DE L'ACTE

Dans le cadre de l'élaboration des normes énoncées dans le présent projet de règlement, les AES ont publié le projet de normes techniques de réglementation le 19 juin 2023 pour une période de consultation de trois mois, qui s'est achevée le 11 septembre 2023. Elles ont reçu 105 réponses de divers acteurs du marché, dans l'ensemble du secteur financier. Leur rapport final donne un aperçu complet de ces réponses[1].

[1] Autorités européennes de surveillance (2024), «Final report on Draft Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554» (Rapport final sur les projets de normes techniques de réglementation précisant les critères de classification des incidents liés aux TIC, les seuils d'importance significative pour les incidents majeurs et les cybermenaces importantes au titre du règlement (UE) 2022/2554).

Les participants à la consultation publique ont formulé des observations sur tous les aspects du projet de normes techniques de réglementation proposé. Les principaux points qui ont été soulevés sont les suivants:

- **La méthode de classification des incidents majeurs:** De nombreux participants à la consultation publique ont estimé que la méthode de classification était trop complexe, et que le processus de déclaration poserait des difficultés aux établissements financiers lors du traitement des incidents. Certains d'entre eux ont en outre proposé que le poids de différents critères soit modifié d'une manière susceptible de mieux correspondre à leur secteur respectif (par exemple, de faire du critère «clients, contreparties financières et transactions touchés» un critère secondaire, et du critère «durée et interruptions de service» un critère primaire, etc.). Plusieurs participants ont également proposé que la méthode de classification prévue dans les normes techniques de réglementation repose plus directement sur l'incidence de l'incident;
- **Les critères de classification et leurs seuils d'importance significative:** Les critères de classification énoncés dans les normes techniques de réglementation correspondent à «clients, contreparties financières et transactions touchés», «atteinte à la réputation», «durée et interruptions de service», «répartition géographique», «pertes de données», «services critiques touchés» et «conséquences économiques». Les parties prenantes ont, , pour la plupart, demandé que des éclaircissements supplémentaires soient apportés (par exemple, sur la manière de calculer les seuils) et nombre d'entre elles ont demandé que les seuils d'importance significative soient relevés;
- **Incidents récurrents:** Plusieurs participants ont fait part de leurs préoccupations quant à la charge opérationnelle que représenterait l'analyse des similitudes entre les incidents, notamment le recours substantiel à des ressources internes que celle-ci nécessiterait et la difficulté que poserait l'évaluation des données. Certains ont également mentionné un problème de proportionnalité de cette exigence, car celle-ci pèserait de manière disproportionnée sur les petites entités.
- **Proportionnalité**: les parties prenantes ont également souligné qu'il importait de respecter le principe de proportionnalité. En outre, le comité consultatif mixte des AES sur la proportionnalité (ACP) a également fourni des conseils ad hoc sur la manière de renforcer la proportionnalité dans le projet de normes techniques de réglementation.

À la lumière des commentaires reçus, les AES ont apporté des modifications au projet de normes techniques de réglementation. Ces modifications concernaient la méthode de classification, la définition de certains critères de classification et de leurs seuils d'importance significative, ainsi que l'approche en matière d'incidents récurrents:

- en ce qui concerne la méthode de classification, les AES ont modifié le projet de normes techniques afin que les incidents soient classés comme majeurs par les entités financières si le critère «services critiques touchés» est rempli et si i) un accès malveillant non autorisé au réseau et aux systèmes d'information a été identifié dans le cadre du critère «pertes de données» ou ii) les seuils d'importance significative d'un des deux autres critères sont atteints;
- en ce qui concerne les critères de classification et leurs seuils, tout en maintenant une méthode de classification des incidents harmonisée pour toutes les entités financières relevant du champ d'application de DORA, les AES ont clarifié les différents aspects

de la classification pris en compte dans les critères et ont modifié les seuils pour les critères «clients, contreparties financières et transactions touchés» et «pertes de données» afin de les rendre plus proportionnés, de remédier à des problèmes spécifiques à certains secteurs et de faire en sorte que ces critères rendent compte des cyberincidents pertinents;

- enfin, pour répondre aux préoccupations concernant la charge déclarative qui pèserait sur les entités financières, les AES ont modifié la méthode de classification des incidents récurrents, laquelle cible désormais les incidents qui se sont produits au moins deux fois en six mois, qui ont la même cause originelle et qui, pris ensemble, rempliraient les critères de classification des incidents comme majeurs. L'évaluation du caractère récurrent doit être effectuée à une fréquence mensuelle.

3. ÉLÉMENTS JURIDIQUES DE L'ACTE DÉLÉGUÉ

Le chapitre I définit les critères de classification des incidents en fonction des clients, des contreparties financières et des transactions touchés (article 1er), de l'atteinte à la réputation (article 2), de la durée et des interruptions de service (article 3), de la répartition géographique (article 4), des pertes de données (article 5), de la criticité des services touchés (article 6) et des conséquences économiques (article 7).

Le chapitre II définit dans quelles conditions un incident est classé comme majeur et comment traiter les incidents récurrents (article 8), et il fixe à cet effet les seuils d'importance significative (article 9).

Le chapitre III traite des cybermenaces importantes et fixe les seuils d'importance significative permettant de déterminer si une cybermenace est importante (article 10).

Le chapitre IV fixe les règles à appliquer pour déterminer si un incident majeur est pertinent pour les autorités compétentes d'autres États membres (article 11) et comment partager les détails des incidents majeurs avec d'autres autorités compétentes (article 12).

Le chapitre V contient les dispositions finales relatives à l'entrée en vigueur (article 13).

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

du 13.3.2024

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

(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[2], et notamment son article 18, paragraphe 4, troisième alinéa,

considérant ce qui suit:

(1) Le règlement (UE) 2022/2554 vise à harmoniser et à rationaliser les obligations de déclaration des incidents liés aux TIC et des incidents opérationnels ou de sécurité liés au paiement concernant les établissements de crédit, les établissements de paiement, les prestataires de services d'information sur les comptes et les établissements de monnaie électronique (ci-après les «incidents»). Étant donné que ces obligations de déclaration concernent 20 types différents d'entités financières, les critères de classification et les seuils d'importance significative servant à identifier les incidents majeurs et les cybermenaces importantes devraient être précisés d'une manière simple, harmonisée et cohérente qui tienne compte des spécificités des services et activités de toutes les entités financières concernées.

(2) Dans un souci de proportionnalité, les critères de classification et les seuils d'importance significative devraient prendre en compte la taille des différentes entités financières, leur profil de risque général, ainsi que la nature, l'échelle et la complexité de leurs services. En outre, les critères et les seuils d'importance significative devraient être conçus de manière à s'appliquer de manière cohérente à toutes les entités financières, indépendamment de leur taille et de leur profil de risque, et à ne pas entraîner de charge déclarative disproportionnée pour les plus petites d'entre elles. Cependant, afin de tenir compte des situations où un incident ne dépasse pas le seuil applicable mais touche néanmoins un nombre significatif de clients, il convient de fixer un seuil absolu ciblant surtout les grandes entités financières.

(3) Il convient d'assurer aux entités financières une continuité par rapport aux cadres de notification des incidents qui préexistaient à l'entrée en vigueur du règlement (UE) 2022/2554. Par conséquent, les critères de classification et les seuils d'importance

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

significative devraient s'appuyer et s'aligner sur les orientations de l'ABE sur la notification des incidents majeurs au titre de la directive (UE) 2015/2366 du Parlement européen et du Conseil[3], les orientations sur l'information périodique et la notification des modifications importantes que les référentiels centraux doivent soumettre à l'AEMF, le dispositif BCE/MSU de déclaration des cyberincidents et d'autres orientations pertinentes. Il convient également de faire en sorte que les critères et seuils de classification soient adéquats pour les entités financières qui n'étaient pas soumises à des obligations de déclaration des incidents avant l'adoption du règlement (UE) 2022/2554.

(4) En ce qui concerne le critère de classification «volume et nombre de transactions touchées», la notion de transactions est large et couvre différentes activités et services dans les différents actes sectoriels applicables aux entités financières. Aux fins de ce critère de classification, les opérations de paiement et toutes les formes d'échange d'instruments financiers, de crypto-actifs, de matières premières ou de tout autre actif, également sous forme de marges, de sûretés ou de garanties, tant contre des espèces que contre tout autre actif, devraient être couvertes. Toutes les transactions impliquant des actifs dont la valeur peut être exprimée sous la forme d'un montant monétaire devraient être prises en considération aux fins de la classification.

(5) Les critères de classification devraient permettre de rendre compte de tous les types d'incidents majeurs pertinents. De nombreux critères de classification ne rendent pas nécessairement compte des cyberattaques liées à l'intrusion dans le réseau ou les systèmes d'information. Or celles-ci sont importantes car toute intrusion dans le réseau ou les systèmes d'information est susceptible de nuire à l'entité financière. En conséquence, les critères de classification «services critiques touchés» et «pertes de données» devraient être définis de manière à rendre compte de ces types d'incidents majeurs, en particulier des intrusions non autorisées qui, même si l'on n'en connaît pas immédiatement l'incidence, sont susceptibles d'entraîner de graves conséquences, notamment des violations de données et des fuites de données.

(6) Étant donné que les établissements de crédit sont soumis à la fois au cadre de classification des incidents prévu à l'article 18 du règlement (UE) 2022/2554 et au cadre relatif au risque opérationnel prévu par le règlement délégué (UE) 2018/959 de la Commission[4], les approches que prévoient respectivement ces deux cadres pour déterminer les conséquences économiques d'un incident sur la base du calcul des coûts et des pertes devraient, dans toute la mesure du possible, concorder, afin de ne pas donner lieu à des exigences incompatibles ou contradictoires.

(7) Le critère relatif à la répartition géographique d'un incident énoncé à l'article 18, paragraphe 1, point c), du règlement (UE) 2022/2554 devrait se concentrer sur l'incidence transfrontière de l'incident, puisque l'incidence d'un incident sur les

---

[3] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) nº 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

[4] Règlement délégué (UE) 2018/959 de la Commission du 14 mars 2018 complétant le règlement (UE) nº 575/2013 du Parlement européen et du Conseil par des normes techniques de réglementation précisant la méthode d'évaluation en vertu de laquelle les autorités compétentes autorisent les établissements à utiliser des approches par mesure avancée pour le risque opérationnel (JO L 169 du 6.7.2018, p. 1, ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

activités d'une entité financière au sein d'une même juridiction sera appréhendée par les autres critères énoncés dans cet article.

(8) Étant donné que les critères de classification sont interdépendants et liés entre eux, l'approche pour identifier les incidents majeurs qui doivent être déclarés en vertu de l'article 19, paragraphe 1, du règlement (UE) 2022/2554 devrait se fonder sur une combinaison de critères, qui donnerait à certains critères étroitement liés à la définition d'un incident lié aux TIC et à celle d'un incident majeur lié aux TIC données à l'article 3, paragraphes 8 et 10, du règlement (UE) 2022/2554 la prééminence sur les autres critères pour la classification d'un incident comme majeur.

(9) Afin que les rapports et notifications d'incidents majeurs reçus par les autorités compétentes en vertu de l'article 19, paragraphe 1, du règlement (UE) 2022/2554 soient utiles aussi bien à des fins de surveillance que pour la prévention de la contagion à l'ensemble du secteur financier, les seuils d'importance significative devraient permettre de rendre compte des incidents majeurs, en se concentrant, entre autres, sur l'incidence sur les services critiques propres à l'entité, sur les seuils absolus et relatifs spécifiques de clients ou de contreparties financières, sur les transactions qui indiquent une incidence significative sur l'entité financière, et sur l'importance de l'incidence dans d'autres États membres.

(10) Les incidents qui touchent des services TIC ou des réseaux et des systèmes d'information qui soutiennent des fonctions critiques ou importantes ou qui touchent des services financiers nécessitant une autorisation, ou les accès malveillants non autorisés aux réseaux et aux systèmes d'information qui soutiennent des fonctions critiques ou importantes, devraient être considérés comme des incidents touchant des services critiques des entités financières. L'accès malveillant non autorisé aux réseaux et aux systèmes d'information qui soutiennent des fonctions critiques ou importantes des entités financières comporte des risques graves pour l'entité financière et, étant donné qu'il peut toucher d'autres entités financières, devrait toujours être considéré comme un incident majeur à déclarer.

(11) Les incidents récurrents qui sont liés par une cause originelle apparente similaire et qui, pris isolément, ne constituent pas des incidents majeurs peuvent néanmoins être le signe de défaillances et de faiblesses importantes dans les procédures de gestion des risques et des incidents mises en place par l'entité financière. Par conséquent, les incidents récurrents devraient être collectivement considérés comme majeurs lorsqu'ils se produisent de manière répétée au cours d'une certaine période.

(12) Étant donné que les cybermenaces peuvent avoir une incidence négative sur l'entité financière et sur le secteur financier, toute notification de cybermenace importante effectuée par une entité financière devrait préciser la probabilité que cette menace se concrétise et la criticité de son incidence potentielle. En conséquence, afin de garantir une évaluation claire et cohérente de l'importance des cybermenaces, la classification d'une cybermenace comme importante devrait dépendre du type de cybermenace, des informations dont dispose l'entité financière, et de la probabilité que, si la cybermenace se concrétisait, elle remplirait les critères permettant de classer un incident comme majeur et atteindrait les seuils correspondants.

(13) Étant donné que les autorités compétentes d'autres États membres doivent être informées des incidents qui ont une incidence sur des entités financières et des clients sur leur territoire, l'évaluation de l'incidence dans un autre État membre conformément à l'article 19, paragraphe 7, du règlement (UE) 2022/2554 devrait se fonder sur la cause originelle de l'incident, sur les risques de contagion par

l'intermédiaire des prestataires tiers et des infrastructures des marchés financiers, ainsi que sur l'incidence de l'incident sur des groupes importants de clients ou de contreparties financières.

(14) Les processus de déclaration et de notification visés à l'article 19, paragraphes 6 et 7, du règlement (UE) 2022/2554 devraient permettre aux destinataires respectifs d'évaluer l'incidence des incidents. Par conséquent, les informations transmises devraient comporter tous les détails contenus dans les rapports d'incidents soumis par l'entité financière à l'autorité compétente.

(15) Lorsqu'un incident constitue une violation de données à caractère personnel au sens du règlement (UE) 2016/679 et de la directive 2002/58/CE, le présent règlement ne devrait pas influer sur les obligations en matière d'enregistrement et de notification des violations de données à caractère personnel qu'imposent ces actes de l'Union. Les autorités compétentes devraient coopérer avec les autorités visées dans le règlement (UE) 2016/679 et la directive 2002/58/CE et échanger avec elles des informations sur toutes les questions pertinentes.

(16) Le présent règlement se fonde sur les projets de normes techniques de réglementation soumis à la Commission par les autorités européennes de surveillance, après consultation de l'Agence de l'Union européenne pour la cybersécurité (ENISA) et de la Banque centrale européenne (BCE).

(17) Le comité mixte des autorités européennes de surveillance visé à l'article 54 du règlement (UE) nº 1093/2010 du Parlement européen et du Conseil[5], à l'article 54 du règlement (UE) nº 1094/2010 du Parlement européen et du Conseil[6] et à l'article 54 du règlement (UE) nº 1095/2010 du Parlement européen et du Conseil[7] a 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 entraînent et sollicité l'avis du groupe des parties intéressées au secteur bancaire institué en application de l'article 37 du règlement (UE) nº 1093/2010, du groupe des parties intéressées à l'assurance et la réassurance institué en application de l'article 37 du règlement (UE) nº 1094/2010 et du groupe des parties intéressées au secteur financier institué en application de l'article 37 du règlement (UE) nº 1095/2010.

(18) 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[8] et a rendu un avis le 24 janvier 2024,

---

5 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).

6 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).

7 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).

8 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

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Chapitre I
Critères de classification

Article premier
Clients, contreparties financières et transactions

1. Le nombre des clients touchés par l'incident, visé à l'article 18, paragraphe 1, point a), du règlement (UE) 2022/2554, comprend tous les clients touchés, qu'il s'agisse de personnes physiques ou morales, qui ne peuvent pas, ou n'ont pas pu, utiliser le service fourni par l'entité financière pendant la durée de l'incident, ou sur lesquels l'incident a eu une incidence préjudiciable. Ce nombre comprend également, en tant que bénéficiaires du service touché, les tiers explicitement couverts par l'accord contractuel conclu entre l'entité financière et le client.

2. Le nombre des contreparties financières touchées par l'incident, visé à l'article 18, paragraphe 1, point a), du règlement (UE) 2022/2554, comprend toutes les contreparties financières touchées qui ont conclu un accord contractuel avec l'entité financière.

3. En ce qui concerne l'importance des clients et des contreparties financières touchés par l'incident, visée à l'article 18, paragraphe 1, point a), du règlement (UE) 2022/2554, l'entité financière tient compte de la mesure dans laquelle l'incidence sur un client ou une contrepartie financière affectera la mise en œuvre de ses objectifs opérationnels, ainsi que de l'incidence potentielle de l'incident sur l'efficience du marché.

4. En ce qui concerne le volume ou le nombre des transactions touchées par l'incident, visé à l'article 18, paragraphe 1, point a), du règlement (UE) 2022/2554, l'entité financière tient compte de toutes les transactions touchées impliquant un montant monétaire qui sont au moins en partie effectuées dans l'Union.

5. Lorsque le nombre réel des clients ou des contreparties financières touchés, ou le nombre ou le volume réel des transactions touchées, ne peut pas être déterminé, l'entité financière estime ce nombre ou ce volume à partir des données disponibles portant sur des périodes de référence comparables.

Article 2
Atteinte à la réputation

1. Afin de déterminer l'incidence de l'incident sur la réputation, visée à l'article 18, paragraphe 1, point a), du règlement (UE) 2022/2554, les entités financières considèrent qu'il y a eu atteinte à la réputation lorsqu'au moins l'un des critères suivants est rempli:

   (a) l'incident a été relayé par les médias;

   (b) l'incident a donné lieu à des plaintes répétées de la part de différents clients ou contreparties financières concernant des services en contact direct avec la clientèle ou des relations commerciales critiques;

---

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).

(c) l'entité financière ne pourra pas satisfaire à certaines exigences réglementaires, ou il est probable qu'elle ne le pourra pas, en raison de l'incident;

(d) l'entité financière perdra, ou il est probable qu'elle perdra, des clients ou des contreparties financières en raison de l'incident, au grand détriment de son activité.

2. Lorsqu'elles évaluent l'incidence de l'incident sur la réputation, les entités financières tiennent compte du niveau de visibilité que l'incident a atteint, ou est susceptible d'atteindre, en ce qui concerne chaque critère énuméré au paragraphe 1.

Article 3
Durée et interruptions de service

1. Les entités financières mesurent la durée d'un incident, visée à l'article 18, paragraphe 1, point b), du règlement (UE) 2022/2554, à partir du moment où l'incident est survenu jusqu'au moment où il est résolu.

Lorsque les entités financières ne sont pas en mesure de déterminer le moment auquel l'incident est survenu, elles mesurent la durée de l'incident à partir du moment où il a été détecté. Lorsque les entités financières se rendent compte que la survenue de l'incident est antérieure à sa détection, elles mesurent la durée à partir du moment où l'incident est enregistré dans les journaux des réseaux ou des systèmes ou dans d'autres sources de données.

Lorsque les entités financières ne savent pas encore quand l'incident sera résolu ou ne sont pas en mesure de vérifier les enregistrements dans les journaux ou dans d'autres sources de données, elles appliquent des estimations.

2. Les entités financières mesurent les interruptions de service, visées à l'article 18, paragraphe 1, point b), du règlement (UE) 2022/2554, à partir du moment où le service est totalement ou partiellement indisponible pour les clients, les contreparties financières ou d'autres utilisateurs internes ou externes jusqu'au moment où les activités ou opérations régulières ont repris au niveau de service qui était fourni avant l'incident. Lorsque l'interruption de service provoque un retard dans la fourniture d'un service après la reprise des activités ou opérations régulières, l'interruption est mesurée à partir du début de l'incident jusqu'au moment où le service ayant subi un retard est intégralement fourni.

Lorsque les entités financières ne sont pas en mesure de déterminer le moment auquel l'interruption de service a commencé, elles mesurent l'interruption de service à partir du moment où celle-ci a été détectée.

Article 4
Répartition géographique

Afin de déterminer la répartition géographique en ce qui concerne les zones touchées par l'incident, visée à l'article 18, paragraphe 1, point c), du règlement (UE) 2022/2554, les entités financières évaluent si l'incident a ou a eu une incidence dans d'autres États membres, et évaluent notamment l'importance de cette incidence en ce qui concerne:

(a) les clients et les contreparties financières dans d'autres États membres;

(b) les succursales ou les autres entités financières du groupe qui exercent des activités dans d'autres États membres; ou

(c) les infrastructures des marchés financiers ou les prestataires tiers susceptibles d'affecter les entités financières établies dans d'autres États membres auxquelles ils fournissent des services, si ces informations sont disponibles.

Article 5
Pertes de données

Afin de déterminer les pertes de données occasionnées par l'incident, visées à l'article 18, paragraphe 1, point d), du règlement (UE) 2022/2554, les entités financières cherchent à savoir:

(a) en ce qui concerne la disponibilité des données, si l'incident a rendu temporairement ou durablement inaccessibles ou inutilisables les données sollicitées par l'entité financière, ses clients ou ses contreparties;

(b) en ce qui concerne l'authenticité des données, si l'incident a compromis la fiabilité de la source des données;

(c) en ce qui concerne l'intégrité des données, si l'incident a entraîné une modification non autorisée des données qui les a rendues inexactes ou incomplètes;

(d) en ce qui concerne la confidentialité des données, si l'incident a eu pour conséquence qu'une partie ou un système non autorisé a eu accès à des données ou que celles-ci lui ont été divulguées.

Article 6
Criticité des services touchés

Afin de déterminer la criticité des services touchés, visée à l'article 18, paragraphe 1, point e), du règlement (UE) 2022/2554, les entités financières évaluent si l'incident:

(a) touche ou a touché des services TIC ou des réseaux et des systèmes d'information qui soutiennent des fonctions critiques ou importantes de l'entité financière;

(b) touche ou a touché des services financiers fournis par l'entité financière qui nécessitent un agrément ou un enregistrement ou qui sont surveillés par les autorités compétentes;

(c) constitue ou a constitué un accès réussi, malveillant et non autorisé aux réseaux et aux systèmes d'information de l'entité financière.

Article 7
Conséquences économiques

1. Afin de déterminer les conséquences économiques de l'incident, visées à l'article 18, paragraphe 1, point f), du règlement (UE) 2022/2554, les entités financières, sans comptabiliser les recouvrements financiers, tiennent compte des types suivants de coûts et de pertes directs et indirects qu'elles ont supportés en raison de l'incident:

   (a) les fonds ou les actifs financiers expropriés dont elles sont responsables, y compris les actifs perdus à la suite d'un vol;

   (b) les coûts du remplacement ou du déplacement de logiciels, de matériel ou d'infrastructures;

   (c) les frais de personnel, y compris les coûts liés au remplacement ou au déménagement du personnel, au recrutement de personnel supplémentaire, à la

rémunération des heures supplémentaires et à la récupération des compétences perdues ou altérées;

(d) les frais dus au non-respect d'obligations contractuelles;

(e) les coûts de dédommagement et d'indemnisation des clients;

(f) les pertes dues aux recettes non perçues;

(g) les coûts liés à la communication interne et externe;

(h) les frais de conseil, y compris les coûts liés au conseil juridique, aux services d'analyse forensique et aux services de remédiation.

2. Les coûts et pertes visés au paragraphe 1 excluent les coûts nécessaires au fonctionnement quotidien de l'entreprise, en particulier:

(a) les coûts de maintenance générale des infrastructures, des équipements, du matériel et des logiciels, ainsi que les coûts d'actualisation des compétences du personnel;

(b) les coûts internes ou externes engagés pour renforcer l'activité après l'incident, notamment les mises à niveau, les améliorations et l'adoption de mesures d'évaluation des risques;

(c) les primes d'assurance.

3. Les entités financières calculent les montants des coûts et des pertes sur la base des données disponibles au moment de la déclaration. Lorsque les montants réels des coûts et des pertes ne peuvent pas être déterminés, les entités financières les estiment.

4. Lorsqu'elles évaluent les conséquences économiques de l'incident, les entités financières additionnent les coûts et les pertes visés au paragraphe 1.

Chapitre II
Incidents majeurs et seuils d'importance significative

Article 8
Incidents majeurs

1. Un incident est considéré comme un incident majeur aux fins de l'article 19, paragraphe 1, du règlement (UE) 2022/2554 lorsqu'il a touché des services critiques visés à l'article 6 et lorsque l'une des conditions suivantes est remplie:

(a) le seuil d'importance significative visé à l'article 9, paragraphe 5, point b), est atteint;

(b) au moins deux des autres seuils d'importance significative visés à l'article 9, paragraphes 1 à 6, sont atteints.

2. Les incidents récurrents qui, pris isolément, ne sont pas considérés comme un incident majeur au sens du paragraphe 1 sont considérés comme un incident majeur lorsqu'ils remplissent toutes les conditions suivantes:

(a) ils se sont produits au moins deux fois en six mois;

(b) ils ont la même cause originelle apparente, telle que visée à l'article 20, premier alinéa, point b) du règlement (UE) 2022/2554;

(c) ils remplissent collectivement les critères pour être considérés comme un incident majeur énoncés au paragraphe 1.

Les entités financières évaluent l'existence d'incidents récurrents chaque mois.

Le présent paragraphe ne s'applique pas aux microentreprises ni aux entités financières énumérées à l'article 16, paragraphe 1, du règlement (UE) 2022/2554.

Article 9

Seuils d'importance significative pour la détermination des incidents majeurs

1. Le seuil d'importance significative pour le critère «clients, contreparties financières et transactions» est atteint lorsque l'une des conditions suivantes est remplie:

   (a) le nombre des clients touchés dépasse 10 % de l'ensemble des clients qui utilisent le service touché;

   (b) le nombre des clients touchés qui utilisent le service touché dépasse 100 000;

   (c) le nombre des contreparties financières touchées dépasse 30 % de l'ensemble des contreparties financières qui exercent des activités liées à la fourniture du service touché;

   (d) le nombre des transactions touchées dépasse 10 % du nombre moyen journalier des transactions effectuées par l'entité financière liées au service touché;

   (e) le volume des transactions touchées dépasse 10 % de la valeur moyenne journalière des transactions effectuées par l'entité financière liées au service touché;

   (f) des clients ou des contreparties financières considérés comme importants en vertu de l'article 1er, paragraphe 3, ont été touchés.

   Lorsque le nombre réel des clients ou des contreparties financières touchés, ou le nombre ou le volume réel des transactions touchées, ne peut pas être déterminé, l'entité financière estime ce nombre ou ce volume à partir des données disponibles portant sur des périodes de référence comparables.

2. Le seuil d'importance significative pour le critère «atteinte à la réputation» est atteint lorsque l'une des conditions énoncées à l'article 2, points a) à d), est remplie.

3. Le seuil d'importance significative pour le critère «durée et interruptions de service» est atteint lorsque l'une des conditions suivantes est remplie:

   (a) la durée de l'incident dépasse 24 heures;

   (b) l'interruption de service dépasse 2 heures pour les services TIC qui soutiennent des fonctions critiques ou importantes.

4. Le seuil d'importance significative pour le critère «répartition géographique» est atteint lorsque l'incident a une incidence dans deux États membres ou plus, conformément à l'article 4.

5. Le seuil d'importance significative pour le critère «pertes de données» est atteint lorsque l'une des conditions suivantes est remplie:

   (a) l'incidence sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données, visée à l'article 5, nuit ou nuira à la mise en œuvre des objectifs opérationnels de l'entité financière ou à sa capacité de satisfaire aux exigences réglementaires;

(b) les réseaux et les systèmes d'information sont l'objet d'un accès réussi, malveillant et non autorisé non couvert par le point a) et susceptible d'entraîner des pertes de données.

6. Le seuil d'importance significative pour le critère «conséquences économiques» est atteint lorsque les coûts et les pertes supportés par l'entité financière en raison de l'incident ont dépassé, ou sont susceptibles de dépasser, 100 000 EUR.

Chapitre III
Cybermenaces importantes

Article 10

Seuils d'importance significative élevés pour la détermination des cybermenaces importantes

Aux fins de l'article 18, paragraphe 2, du règlement (UE) 2022/2554, une cybermenace est considérée comme importante lorsque toutes les conditions suivantes sont remplies:

(a) la cybermenace est ou était susceptible, en cas de matérialisation, de toucher des fonctions critiques ou importantes de l'entité financière, ou de toucher d'autres entités financières, prestataires tiers, clients ou contreparties financières, à en juger par les informations dont dispose l'entité financière;

(b) la probabilité que la cybermenace se matérialise au sein de l'entité financière ou d'autres entités financières est grande, compte tenu au moins des éléments suivants:

  i) les risques applicables liés à la cybermenace, visés au point a), y compris les vulnérabilités potentielles des systèmes de l'entité financière qui peuvent être exploitées;

  ii) les capacités et l'intention des acteurs de la menace, dans la mesure où l'entité financière en a connaissance;

  iii) la persistance de la menace et toute connaissance acquise sur les incidents qui ont eu une incidence sur l'entité financière ou son prestataire tiers, ses clients ou ses contreparties financières;

(c) Si elle se matérialisait, la cybermenace pourrait remplir ou atteindre l'un des critères ou seuils suivants:

  i) le critère de la criticité des services énoncé à l'article 18, paragraphe 1, point e), du règlement (UE) 2022/2554, tel qu'il est précisé à l'article 6 du présent règlement;

  ii) le seuil d'importance significative prévu à l'article 9, paragraphe 1;

  iii) le seuil d'importance significative prévu à l'article 9, paragraphe 4.

Lorsque, en fonction du type de cybermenace et des informations disponibles, l'entité financière conclut que les seuils d'importance significative prévus à l'article 9, paragraphes 2, 3, 5 et 6, pourraient être atteints, elle peut également prendre ces seuils en considération.

Chapitre IV
Pertinence des incidents majeurs pour les autorités compétentes d'autres États membres et détails des rapports à partager avec les autres autorités compétentes

Article 11
Pertinence des incidents majeurs pour les autorités compétentes d'autres États membres

L'évaluation visant à déterminer si un incident majeur est pertinent pour les autorités compétentes d'autres États membres, prévue par l'article 19, paragraphe 7, du règlement (UE) 2022/2554, est fondée sur le point de savoir si l'incident trouve son origine dans un autre État membre ou s'il a ou a eu une incidence importante dans un autre État membre en ce qui concerne:

(a) des clients ou des contreparties financières;

(b) une succursale de l'entité financière ou une autre entité financière du groupe;

(c) une infrastructure des marchés financiers ou un prestataire tiers susceptible d'affecter les entités financières auxquelles ils fournissent des services.

Article 12
Détails des incidents majeurs à partager avec les autres autorités compétentes

Les détails des incidents majeurs que les autorités compétentes communiquent aux autres autorités compétentes conformément à l'article 19, paragraphe 6, du règlement (UE) 2022/2554 et les notifications que l'ABE, l'AEMF ou l'AEAPP et la BCE soumettent aux autorités compétentes concernées des autres États membres conformément à l'article 19, paragraphe 7, dudit règlement contiennent le même niveau d'information, sans anonymisation, que celui des notifications et rapports d'incidents majeurs soumis par les entités financières conformément à l'article 19, paragraphe 4, du règlement (UE) 2022/2554.

Chapitre V
Dispositions finales

Article 13
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 13.3.2024

Par la Commission
La présidente
Ursula VON DER LEYEN