Commission de Surveillance
du Secteur Financier

Circulaire CSSF 25/893

sur la notification des incidents majeurs liés aux TIC et des cybermenaces importantes en vertu du règlement sur la résilience opérationnelle numérique (DORA)

Circulaire CSSF 25/893

sur la notification des incidents majeurs liés aux TIC et des cybermenaces importantes en vertu du règlement sur la résilience opérationnelle numérique (DORA)

À toutes les entités financières telles que définies à l'article 2, paragraphe 1, points a) à i), k) à m), p), r) et s), au sens de l'article 2, paragraphe 2, du règlement (UE) 2022/2554[1] sur la résilience opérationnelle numérique du secteur financier (ci-après le « règlement DORA ») et à tous les prestataires de services de paiement tels que définis à l'article 1er, paragraphe 37, de la loi du 10 novembre 2009 relative aux services de paiement (LSP)

Luxembourg, le 27 mai 2025

Mesdames, Messieurs,

Tel que défini à l'article 18, paragraphes 1 et 2, et à l'article 19, paragraphes 1 et 2, du règlement DORA, les entités financières soumises au règlement DORA sont tenues de se conformer aux obligations de classification et de notification des incidents majeurs liés aux TIC et, le cas échéant, des cybermenaces importantes. Les dispositions relatives à la classification et à la notification sont détaillées dans les normes techniques de réglementation (RTS) et les normes techniques d'exécution (ITS) suivantes :

- RTS sur la classification des incidents liés aux TIC et des cybermenaces[2] (ci-après « RTS sur la classification »), et
- RTS et ITS sur la notification des incidents et la notification volontaire des cybermenaces (ci-après « RTS sur la notification des incidents »[3] et « ITS sur la notification des incidents »[4])

[1] 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) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011

[2] Règlement délégué (UE) 2024/1772 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

[3] 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

[4] Règlement d'exécution (UE) 2025/302 de la Commission du 23 octobre 2023 définissant des normes techniques d'exécution pour l'application du règlement (UE) 2022/2554 du Parlement européen et du Conseil en ce qui concerne les formulaires, modèles et procédures types permettant aux entités financières de notifier un incident majeur lié aux TIC et de notifier une cybermenace importante

En outre, par la présente circulaire, la CSSF demande aux prestataires de services de paiement (PSP) qui n'entrent pas dans le champ d'application du règlement DORA de suivre les procédures de classification et de notification des incidents liés aux TIC et des cybermenaces prévues par le règlement DORA afin de remplir les obligations de notification énoncées à l'article 105-2 de la LSP. En clair, ces PSP doivent répondre aux exigences du règlement DORA pour tous les incidents liés aux TIC (à savoir, y compris, les incidents liés aux TIC qui ne sont pas liés aux services de paiement), afin d'éviter un double mécanisme de notification.

Dans ce contexte, la présente circulaire prévoit également les modalités pratiques selon lesquelles les entités financières entrant dans le champ d'application de cette circulaire sont tenues de notifier, à la CSSF, les incidents majeurs liés aux TIC ainsi que, le cas échéant, les cybermenaces importantes.

La présente circulaire est divisée en quatre chapitres :

- le chapitre 1 définit le champ d'application ;
- le chapitre 2 énumère les exigences relatives à la classification et à la notification des incidents et des cybermenaces pour les PSP qui ne relèvent pas du règlement DORA ;
- le chapitre 3 définit les modalités pratiques de notification des incidents majeurs liés aux TIC et des cybermenaces importantes ;
- le chapitre 4 prévoit l'entrée en vigueur de la présente circulaire.

TABLE DES MATIÈRES

Chapitre 1 : Champ d'application

1. Les entités suivantes sont à considérer comme des entités financières dans le cadre de la présente circulaire :

   a) établissements de crédit, entreprises d'investissement, opérateurs de marché exploitant une plate-forme de négociation et dispositifs de publication agréés (APA) avec une dérogation et mécanismes de déclaration agréés (ARM) avec une dérogation au sens de la loi du 5 avril 1993 relative au secteur financier (LSF) ;

   b) établissements de paiement, prestataires de services d'information sur les comptes et établissements de monnaie électronique au sens de la loi du 10 novembre 2009 relative aux services de paiement (LSP) ;

   c) prestataires de services sur crypto-actifs et émetteurs de jetons se référant à un ou des actifs au sens du règlement (UE) 2023/1114 ;

   d) dépositaires centraux de titres au sens de la loi du 6 juin 2018 relative aux dépositaires centraux de titres (Loi DCT) ;

   e) contreparties centrales au sens de la loi du 15 mars 2016 relative aux produits dérivés de gré à gré, aux contreparties centrales et aux référentiels centraux ;

   f) sociétés de gestion de droit luxembourgeois relevant du chapitre 15 ou de l'article 125-2 du chapitre 16 et succursales luxembourgeoises de gestionnaires de fonds d'investissement relevant du chapitre 17, et sociétés d'investissement qui n'ont pas désigné de société de gestion au sens de l'article 27 de la loi du 17 décembre 2010 concernant les organismes de placement collectif ;

   g) gestionnaires de fonds d'investissement alternatifs agréés au titre du chapitre 2 et fonds d'investissement alternatifs gérés de manière interne au sens de l'article 4, paragraphe 1, point b), de la loi du 12 juillet 2013 relative aux gestionnaires de fonds d'investissement alternatifs (Loi GFIA) ;

   h) institutions de retraite professionnelle agréées conformément à l'article 2, paragraphe 2, de la loi du 13 juillet 2005 relative aux institutions de retraite professionnelle sous forme de sepcav et assep ;

   i) administrateurs d'indices de référence d'importance critique au sens de l'article 20, paragraphe 1, point b), du règlement (UE) 2016/1011 ;

   j) prestataires de services de financement participatif au sens de la loi du 16 juillet 2019 relative à l'opérationnalisation de règlements européens dans le domaine des services financiers ;

   k) prestataires de services de paiement (PSP) tels que visés à l'article 1er, paragraphe 37, de la loi du 10 novembre 2009 relative aux services de paiement (LSP) tels que définis au point 1a) et b) ci-dessus, à savoir succursales luxembourgeoises de PSP ayant leur siège social dans un pays tiers, et POST Luxembourg.

2. Les dispositions du chapitre 2 de la présente circulaire s'appliquent uniquement aux entités entrant dans le champ d'application de la présente circulaire telles que définies au point k) ci-dessus, ci-après dénommées collectivement les « **PSP qui ne relèvent pas du règlement DORA** ».

3. Les dispositions du chapitre 3 de la présente circulaire s'appliquent à toutes les entités financières entrant dans le champ d'application de la présente circulaire, telles que définies au point 1a) à k) ci-dessus, ci-après dénommées collectivement « **Entités financières** » ou

individuellement « **Entité financière** », y compris leurs succursales telles que précisées dans les lois respectives.

4. Les succursales luxembourgeoises des Entités financières qui font partie d'une entité juridique dont le siège social est situé dans un autre État membre de l'Union européenne (succursales de l'UE) sont censées notifier leurs incidents majeurs liés aux TIC et leurs cybermenaces importantes en vertu du règlement DORA à l'autorité compétente de cet État membre (État membre d'origine) et sont donc exclues du champ d'application de la présente circulaire.

Chapitre 2 : Exigences relatives à la classification et à la notification des incidents et des cybermenaces pour les PSP qui ne relèvent pas du règlement DORA

5. Aux fins de la présente circulaire, les définitions suivantes sont reprises du règlement DORA et s'appliquent aux PSP qui ne relèvent pas du règlement DORA :

   a) « réseaux et systèmes d'information » :

      (1) un « réseau de communications électroniques » : les systèmes de transmission, qu'ils soient ou non fondés sur une infrastructure permanente ou une capacité d'administration centralisée et, le cas échéant, les équipements de commutation ou de routage et les autres ressources, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l'acheminement de signaux par câble, par la voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux fixes (avec commutation de circuits ou de paquets, y compris l'internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision, quel que soit le type d'information transmise.

      (2) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques; ou

      (3) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points 1 et 2 ci-dessus en vue de leur fonctionnement, utilisation, protection et maintenance ;

   b) « sécurité des réseaux et des systèmes d'information » : la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à tout événement susceptible de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, ou des services que ces réseaux et systèmes d'information offrent ou rendent accessibles ;

   c) « incident opérationnel ou de sécurité lié au paiement » : un événement ou une série d'événements liés entre eux que les entités financières n'ont pas prévu, lié ou non aux TIC, qui a une incidence négative sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données liées au paiement ou sur les services liés au paiement fournis par l'entité financière ;

   d) « incident lié aux TIC » : un événement ou une série d'événements liés entre eux que l'entité financière n'a pas prévu qui compromet la sécurité des réseaux et des systèmes

d'information, et a une incidence négative sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données ou sur les services fournis par l'entité financière. Cela comprend les incidents opérationnels ou de sécurité liés au paiement ;

e) « incident opérationnel ou de sécurité majeur lié au paiement » : un incident opérationnel ou de sécurité lié au paiement qui a une incidence négative élevée sur les services fournis liés au paiement ;

f) « incident majeur lié aux TIC » : un incident lié aux TIC qui a une incidence négative élevée sur les réseaux et les systèmes d'information qui soutiennent les fonctions critiques ou importantes de l'entité financière. Cela comprend les incidents opérationnels ou de sécurité majeur lié au paiement ;

g) « cybermenace » : toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes ;

h) « cybermenace importante » : une cybermenace dont les caractéristiques techniques indiquent qu'elle pourrait donner lieu à un incident majeur lié aux TIC ou à un incident opérationnel ou de sécurité majeur lié au paiement ;

i) « fonction critique ou importante » : une fonction dont la perturbation est susceptible de nuire sérieusement à la performance financière d'une entité financière, ou à la solidité ou à la continuité de ses services et activités, ou une interruption, une anomalie ou une défaillance de l'exécution de cette fonction qui est susceptible de nuire sérieusement à la capacité d'une entité financière de respecter en permanence les conditions et obligations de son agrément, ou ses autres obligations découlant des dispositions applicables des lois relatives aux services financiers.

6. Les PSP ne relevant pas du règlement DORA sont tenus de classer leurs incidents liés aux TIC et leurs cybermenaces selon les critères et les seuils d'importance définis dans les chapitres I, II et III des RTS sur la classification. Les chapitres IV et V des RTS sur la classification ne leur sont pas applicables.

7. Les PSP qui ne relèvent pas du règlement DORA sont en outre tenus de notifier les incidents majeurs liés aux TIC et, le cas échéant, les cybermenaces importantes, conformément aux RTS sur la notification des incidents et aux ITS sur la notification des incidents, qui s'appliquent intégralement à eux.

Chapitre 3 : Modalités pratiques pour la notification des incidents majeurs liés aux TIC et des cybermenaces importantes

8. Les notifications des incidents majeurs liés aux TIC ainsi que, le cas échéant, des cybermenaces importantes, doivent être soumises au moyen du formulaire correspondant, soit selon la procédure dédiée « DORA Major ICT-related Incident Notification » disponible sur le portail eDesk de la CSSF, soit via l'interface API (S3) fournie par la CSSF.

9. Les Entités financières doivent notifier la CSSF dans les délais prévus à l'article 5 des RTS sur la notification des incidents.

10. Les Entités financières doivent compléter la ou les sections pertinentes du formulaire de notification, en fonction de la phase dans laquelle elles se trouvent. La première section fait

référence à la notification initiale conformément à l'article 2 des RTS sur la notification des incidents, la deuxième section traite du rapport intermédiaire conformément à l'article 3 des RTS sur la notification des incidents et la troisième section renvoie au rapport final conformément à l'article 4 des RTS sur la notification des incidents. Le formulaire de notification contient des champs de données prévus aux annexes II et IV des ITS sur la notification des incidents.

11. L'article 7 des ITS sur la notification des incidents indique que la déclaration agrégée n'est possible que si les autorités compétentes en ont explicitement donné l'autorisation. À cet égard, la CSSF informe les Entités financières que, après avoir soigneusement évalué toutes les conditions des points a) à d) de l'article 7, paragraphe 1, ainsi que de l'article 7, paragraphe 2, des ITS sur la notification des incidents, aucun rapport agrégé n'est autorisé lorsqu'il s'agit de notifications d'incidents majeurs liés aux TIC.

12. Les Entités financières qui ont externalisé les obligations de notification restent pleinement responsables du respect des exigences en matière de notification des incidents liés aux TIC dans les délais applicables et de l'intégralité du contenu des notifications des incidents. Comme le précise l'article 6 des ITS sur la notification des incidents, les Entités financières doivent informer la CSSF dès que possible de l'externalisation des obligations de notification et, au plus tard, avant la première notification. À cet égard, les informations suivantes doivent être fournies à la CSSF (adresse électronique : ictrisksupervision@cssf.lu) :

    a) le nom, les coordonnées et un code d'identification du tiers qui soumettra les notifications pour le compte de l'Entité financière ;
    b) le nom, les coordonnées et la fonction connexe des personnes au sein du tiers à qui le rôle de notification d'incident connexe sera attribué dans la solution numérique de la CSSF.

Chapitre 4 : Date d'application

13. S'agissant des entités énumérées aux point 1a) à j) :

    a) cette circulaire s'applique avec effet immédiat et rend la circulaire CSSF 24/847 sur le cadre de notification des incidents liés aux TIC inapplicable ;
    b) la circulaire CSSF 21/787 concernant l'application des Orientations de l'EBA (EBA/GL/2021/03) sur la notification des incidents majeurs en vertu de la directive PSD2 ne leur est plus applicable.

14. S'agissant des entités énumérées au point 1k) :

    a) la présente circulaire s'applique six mois après sa date de publication ;
    b) pendant la période de transition, les critères de classification ainsi que les modalités de notification requises par les circulaires CSSF 24/847 sur le cadre de notification des incidents liés aux TIC et CSSF 21/787 sur l'application des Orientations de l'EBA (EBA/GL/2021/03) sur la notification des incidents majeurs en vertu de la directive PSD2 leur restent applicables.

15. Six mois après la date de publication de la présente circulaire, la circulaire CSSF 21/787 sur l'application des Orientations de l'EBA (EBA/GL/2021/03) sur la notification des incidents majeurs en vertu de la directive PSD2 sera abrogée.

Claude WAMPACH
Directeur

Marco ZWICK
Directeur

Jean-Pierre FABER
Directeur

Françoise KAUTHEN
Directeur

Claude MARX
Directeur général