Commission de Surveillance
du Secteur Financier

Circulaire CSSF 25/880

sur la gestion des relations avec les utilisateurs de services de paiement et l'évaluation des TIC des PSP

Circulaire CSSF 25/880

sur la gestion des relations avec les utilisateurs de services de paiement et l'évaluation des TIC des PSP

À tous les prestataires de services de paiement au sens de l'article 1er, point 37), de la loi du 10 novembre 2009 relative aux services de paiement

Luxembourg, le 9 avril 2025

Mesdames, Messieurs,

Depuis le 17 janvier 2025, les dispositions du règlement sur la résilience opérationnelle numérique[1] (« règlement DORA ») sont applicables aux entités financières, telles que définies dans le règlement DORA et surveillées par la CSSF. Le règlement DORA a introduit notamment des exigences harmonisées pour le cadre de gestion du risque lié aux technologies de l'information et de la communication (TIC).

Afin de réduire le chevauchement avec le règlement DORA, l'Autorité bancaire européenne (« EBA ») a procédé à une revue de ses orientations existantes sur la gestion des risques liés aux TIC et à la sécurité, EBA/GL/2019/04 (« Orientations de l'EBA »), qui reposent sur les dispositions de l'article 74 de la directive 2013/36/UE (« directive CRD »)[2] et de l'article 95, paragraphe 3, de la directive (UE) 2015/2366 (la directive concernant les services de paiement 2, « directive PSD2 »)[3]. Les Orientations de l'EBA sont mises en œuvre au Luxembourg par le biais de la circulaire CSSF 20/750 en matière de gestion des risques liés aux TIC et à la sécurité.

L'EBA est arrivée à la conclusion que le périmètre des entités soumises aux Orientations de l'EBA devrait être restreint et que le champ d'application des orientations devrait être réduit à l'Orientation 1.8[4] sur la gestion des relations avec les utilisateurs de services de paiement en rapport avec la prestation de services de paiement. À cette fin, l'EBA a émis les orientations EBA/GL/2025/02 modifiant les orientations EBA/GL/2019/04 sur la gestion des risques liés aux TIC et à la sécurité (« nouvelles Orientations de l'EBA »). L'EBA a, en outre, expliqué que les autorités nationales compétentes ont la possibilité de soumettre les prestataires de services de paiement (« PSP »), qui ne sont pas couverts par le règlement DORA, à des exigences nationales, indépendamment de l'existence d'orientations de l'EBA[5].

La présente circulaire met en œuvre les nouvelles Orientations de l'EBA qui s'appliqueront à tous les PSP, y compris aux succursales au Luxembourg de PSP ayant leur siège social dans un pays tiers, à POST Luxembourg, qui entrent dans le champ d'application de la loi du 10 novembre 2009 relative aux services de paiement (« LSP ») et qui sont surveillés par la CSSF. Par ailleurs, l'exigence

[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 (règlement DORA)

[2] https://eur-lex.europa.eu/eli/dir/2013/36/oj/fra

[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) n° 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35–127) (directive PSD2)

[4] Correspond à l'orientation 3.8 des Orientations de l'EBA en anglais.

[5] EBA/GL/2025/02 et communiqué de presse correspondant (uniquement en anglais)

nationale supplémentaire en vigueur pour le reporting annuel de l'évaluation des risques en relation avec les services de paiement (« évaluation des TIC des PSP »), qui faisait partie précédemment de la circulaire CSSF 20/750, a été intégrée dans la présente circulaire.

La présente circulaire est divisée en trois chapitres :

- Chapitre 1 met en œuvre les orientations de l'EBA EBA/GL/2025/02 modifiant les orientations EBA/GL/2019/04 sur la gestion des risques liés aux TIC et à la sécurité. La CSSF estime que le contenu de ces orientations reflète ses attentes concernant la gestion des relations avec les utilisateurs de services de paiement et les a, par le biais de la présente circulaire, intégré dans sa pratique administrative et dans son approche réglementaire ;
- Chapitre 2 énonce les exigences en matière d'évaluation des TIC des PSP, selon lesquelles les PSP sont invités à fournir à la CSSF une évaluation des TIC des PSP actualisée et exhaustive. Sur ce point, aucun changement n'intervient avec l'entrée en application du règlement DORA et les PSP sont tenus de continuer à respecter les exigences indiquées aux points 8 à 11 de la présente circulaire ;
- Chapitre 3 prévoit l'entrée en vigueur de la présente circulaire.

TABLE DES MATIÈRES

Chapitre 1. La gestion des relations avec les utilisateurs de services de paiement (« USP »)[6]

1. Les PSP devraient établir et mettre en œuvre des processus permettant de renforcer la sensibilisation des USP aux risques de sécurité liés aux services de paiement, en leur fournissant de l'assistance et des lignes directrices.

2. L'assistance et les lignes directrices fournies aux USP devraient être mises à jour en fonction des nouvelles menaces et vulnérabilités, et les changements devraient être communiqués aux USP.

3. Lorsque la fonctionnalité des produits le permet, les PSP devraient permettre aux USP de désactiver les fonctionnalités de paiement spécifiques aux services de paiement fournis par le PSP à l'USP.

4. Lorsque, conformément à l'article 82, paragraphe 1, de la LSP, un PSP a convenu avec le payeur des limites de dépenses pour les opérations de paiement exécutées au moyen d'instruments spécifiques de paiement, le PSP devrait donner au payeur la possibilité d'ajuster ces limites à hauteur de la limite maximale convenue.

5. Les PSP devraient offrir aux USP la possibilité de recevoir des alertes lors de tentatives initiées et/ou ratées d'initier des opérations de paiement, de manière à leur permettre de détecter toute utilisation frauduleuse ou malveillante de leurs comptes.

6. Les PSP devraient tenir les USP informés des mises à jour des procédures de sécurité ayant une incidence sur les USP s'agissant de la prestation de services de paiement.

7. Les PSP devraient fournir aux USP l'aide nécessaire pour toute question, demande de soutien et notification d'anomalies ou tout problème de sécurité relatifs aux services de paiement. Les USP devraient être correctement informés de la manière dont ils peuvent obtenir cette aide.

Chapitre 2. Évaluation des TIC des PSP (« PSP ICT Assessment »)

8. Conformément à l'article 105-1, paragraphe 2, de la LSP, les PSP ont l'obligation de fournir à la CSSF une évaluation des risques à jour et exhaustive en matière de services de paiement (ci-après « PSP ICT Assessment »). La CSSF a développé un formulaire standardisé pour le *PSP ICT Assessment* à utiliser par tous les PSP. L'objectif de ce formulaire standardisé du *PSP ICT Assessment* est de mettre à la disposition des PSP des lignes directrices sur les attentes de la CSSF par rapport aux informations à fournir par le biais du *PSP ICT Assessment*, et ainsi atteindre un certain degré d'harmonisation et de comparabilité entre les différents *PSP ICT Assessments*.

9. En ce qui concerne le champ d'application du *PSP ICT Assessment*, il est à noter que :

   a) Les établissements dont le modèle d'affaires n'inclut pas la prestation de services de paiement (tels que définis à l'article 1er, point 38), de la LSP), n'ont pas à fournir de *PSP ICT Assessment*. À partir du moment où le modèle d'affaires d'un établissement

[6] Tels que définis à l'article 1er, point 46), de la LSP

comprend la prestation de services de paiement, l'établissement doit soumettre à la CSSF, pour l'année civile en question, un *PSP ICT Assessment*.

b) Les succursales originaires d'un État membre de l'EEE établies au Luxembourg, qui offrent des services de paiement, n'ont pas à fournir de *PSP ICT Assessment* à la CSSF. Par contre, les PSP luxembourgeois qui ont établi des succursales dans d'autres pays de l'EEE et qui fournissent des services de paiement, doivent inclure ces succursales dans leur *PSP ICT Assessment*. Dans le cas de figure où l'évaluation des risques liés aux TIC et à la sécurité pour ces succursales s'écarte de celle du PSP, ceci est à préciser dans le *PSP ICT Assessment*[7].

10. Tous les PSP doivent soumettre le formulaire *PSP ICT Assessment*, dûment complété, à la CSSF sur une base annuelle, **au plus tard le 31 mars de chaque année et couvrant l'année civile précédente**.

11. Le formulaire *PSP ICT Assessment* est disponible sur le portail eDesk de la CSSF à l'adresse suivante :
https://edesk.apps.cssf.lu/.

    Le *PSP ICT Assessment* doit être validé par l'organe de direction du PSP, c'est-à-dire au moins par le membre de l'organe de direction responsable de la fonction TIC. Cette validation est à préciser dans la section du *PSP ICT Assessment* y relative.

    Le *PSP ICT Assessment*, dûment complété et validé, doit être soumis sur une base annuelle par un membre de l'organe de direction à la CSSF exclusivement par le portail eDesk de la CSSF.

Chapitre 3. Date d'application

12. La présente circulaire s'applique avec effet immédiat.

Claude WAMPACH
Directeur

Marco ZWICK
Directeur

Jean-Pierre FABER
Directeur

Françoise KAUTHEN
Directeur

Claude MARX
Directeur général

[7] Cf. Questions/réponses de l'EBA n° 2018_4176