COM(2023) 367 FINAL

ASSEMBLÉE NATIONALE **SÉNAT**

Reçu à la Présidence de l'Assemblée nationale
le 07 septembre 2023

Enregistré à la Présidence du Sénat
le 07 septembre 2023

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,
À L'ASSEMBLÉE NATIONALE ET AU SÉNAT.

Proposition de règlement du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur et modifiant le règlement (UE) nº 1093/2010

E18087

Conseil de
l'Union européenne

Bruxelles, le 5 juillet 2023
(OR. en)

11222/23

Dossier interinstitutionnel:
2023/0210 (COD)

EF 200
ECOFIN 694
CODEC 1237

NOTE DE TRANSMISSION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	29 juin 2023
Destinataire:	Madame Thérèse BLANCHET, secrétaire générale du Conseil de l'Union européenne
N° doc. Cion:	COM(2023) 367 final
Objet:	Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL concernant les services de paiement dans le marché intérieur et modifiant le règlement (UE) nº 1093/2010

Les délégations trouveront ci-joint le document COM(2023) 367 final.

p.j.: COM(2023) 367 final

COMMISSION
EUROPÉENNE

Bruxelles, le 28.6.2023
COM(2023) 367 final

2023/0210 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

concernant les services de paiement dans le marché intérieur et modifiant le règlement (UE) nº 1093/2010

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

{COM(2023) 366 final} - {SEC(2023) 256 final} - {SWD(2023) 231 final} - {SWD(2023) 232 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

La deuxième directive sur les services de paiement (DSP2[1]) fournit un cadre juridique pour tous les paiements de détail dans l'UE, tant en euros que dans d'autres monnaies, et tant nationaux que transfrontières. La première directive sur les services de paiement (DSP1[2]), adoptée en 2007, avait établi un cadre juridique harmonisé pour la création d'un marché européen intégré des paiements. S'appuyant sur la DSP1, la DSP2 a permis de lever les obstacles à de nouveaux types de services de paiement et d'améliorer le niveau de protection et de sécurité des consommateurs. La plupart des règles énoncées dans la DSP2 sont applicables depuis janvier 2018, mais certaines, telles que celles relatives à l'authentification forte du client, ne s'appliquent que depuis septembre 2019.

La DSP2 contient des règles relatives à la prestation de services de paiement et des règles relatives à l'agrément et à la surveillance d'une catégorie de prestataires de services de paiement, à savoir les établissements de paiement. Parmi les autres catégories de prestataires de services de paiement figurent les établissements de crédit, qui sont réglementés par la législation bancaire de l'UE[3], et les établissements de monnaie électronique, qui sont régis par la directive sur la monnaie électronique[4].

Dans sa communication de 2020 sur une stratégie en matière de paiements de détail pour l'UE[5], la Commission a défini ses priorités dans le domaine des paiements de détail pour le mandat de l'actuel collège des commissaires (2019-2024). Cette communication était accompagnée d'une stratégie en matière de finance numérique, qui définissait des priorités pour la stratégie numérique dans le secteur financier hors secteur des paiements. Dans cette stratégie, il était annoncé que «*[f]in 2021, la Commission lancera[it] une évaluation complète de l'application et de l'incidence de la DSP2*». Cette évaluation a été dûment réalisée, essentiellement en 2022, et a conduit la Commission à décider de proposer des modifications législatives de la DSP2 afin d'en améliorer le fonctionnement. Ces modifications sont présentées dans deux propositions, à savoir la présente proposition de règlement concernant les services de paiement dans l'UE et une proposition de directive concernant les services de paiement et les services de monnaie électronique, axée sur l'agrément et la surveillance des établissements de paiement (et modifiant certaines autres directives).

La proposition de révision de la DSP2 figure dans le programme de travail de la Commission pour 2023, parallèlement à une initiative législative prévue sur un cadre régissant l'accès aux données financières, qui étend l'accès aux données financières et l'utilisation de celles-ci au-delà des comptes de paiement à un plus grand nombre de services financiers.

---

1 Directive (UE) 2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

2 Directive 2007/64/CE du 13 novembre 2007 concernant les services de paiement dans le marché intérieur.

3 Le règlement (UE) nº 575/2013 concernant les exigences prudentielles applicables aux établissements de crédit, ainsi que la directive 2013/36/UE concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit.

4 Directive 2009/110/CE concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements.

5 COM(2020) 592 final du 24 septembre 2020.

- **Cohérence avec les dispositions existantes dans le domaine d'action**

Parmi les dispositions existantes présentant un intérêt pour la présente initiative figurent d'autres actes législatifs dans le domaine des paiements, d'autres actes législatifs relatifs aux services financiers qui portent également sur les prestataires de services de paiement ainsi que la législation de l'UE d'application horizontale qui a une incidence sur le domaine des paiements. La Commission a veillé, lors de l'élaboration de la présente proposition, à assurer la cohérence avec ces dispositions.

Le règlement de 2012 relatif à l'espace unique de paiement en euros (SEPA), qui harmonise les exigences techniques applicables aux virements et aux prélèvements en euros, constitue une autre législation dans le domaine des paiements de détail[6]. Le 26 octobre 2022, la Commission a proposé une modification du règlement SEPA afin d'accélérer et de faciliter l'utilisation des paiements instantanés en euros dans l'UE[7]; cette proposition prévoit l'obligation pour les prestataires de services de paiement proposant des paiements instantanés en euros d'offrir aux utilisateurs un «service de vérification du nom et du numéro IBAN», obligation que la présente proposition étend aux prestataires de services de paiement qui proposent tout virement dans n'importe quelle monnaie de l'UE. Le règlement concernant les paiements transfrontaliers uniformise la tarification des virements nationaux et transfrontaliers en euros[8]. Le règlement relatif aux commissions d'interchange fixe des plafonds pour ces commissions[9]. La présente proposition est cohérente par rapport à l'objectif d'améliorer l'accès aux espèces, en ce qu'elle autorise les commerçants à proposer, dans les magasins physiques, des services de fourniture d'espèces même en l'absence d'achat par un client. Les travaux sur l'accès aux espèces doivent également être considérés dans le contexte de la stratégie en matière de paiements de détail de la Commission, dont l'un des objectifs est que les espèces restent largement accessibles.

Parmi les autres actes législatifs pertinents relatifs aux services financiers figure la directive concernant le caractère définitif du règlement (DCDR)[10], à laquelle une modification ciblée est apportée dans la proposition de directive accompagnant la présente proposition. Parmi les autres instruments législatifs pertinents, on peut citer le règlement sur les marchés de crypto-actifs (MiCA)[11], le règlement sur la résilience opérationnelle numérique concernant la cybersécurité (DORA)[12] ainsi que la directive anti-blanchiment, pour laquelle un ensemble de propositions de modifications est actuellement examiné par les colégislateurs[13].

La présente initiative est pleinement cohérente par rapport aux autres initiatives de la Commission exposées dans sa stratégie en matière de finance numérique pour l'Europe[14], qui a été adoptée en même temps que la stratégie en matière de paiements de détail et qui vise à promouvoir la transformation numérique de la finance et de l'économie de l'UE et à remédier à la fragmentation du marché unique numérique.

---

6 Règlement (UE) nº 260/2012 du 14 mars 2012.

7 COM(2022) 546 final.

8 Règlement (UE) 2021/1230 du 14 juillet 2021 concernant les paiements transfrontaliers dans l'Union.

9 Règlement (UE) 2015/751 du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte.

10 Directive 98/26/CE du 19 mai 1998 concernant le caractère définitif du règlement dans les systèmes de paiement et de règlement des opérations sur titres.

11 Règlement (UE) 2023/1114 du 31 mai 2023 sur les marchés de crypto-actifs.

12 Règlement (UE) 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier.

13 Les prestataires de services de paiement sont des entités assujetties au sens de la législation anti-blanchiment de l'UE.

14 COM(2020) 591 final du 24 septembre 2020.

- **Cohérence avec les autres politiques de l'UE**

La présente initiative est cohérente par rapport à la communication de la Commission de 2021 intitulée «Système économique et financier européen: favoriser l'ouverture, la solidité et la résilience»[15], qui rappelait l'importance de sa stratégie en matière de paiements de détail et de l'innovation numérique dans le secteur financier pour renforcer le marché intérieur des services financiers. Dans la même communication, la Commission a confirmé que ses services et ceux de la Banque centrale européenne examineraient conjointement, au niveau technique, un large éventail de questions de politique et de questions juridiques et techniques découlant de l'introduction éventuelle d'un euro numérique, en tenant compte de leurs mandats respectifs prévus dans les traités de l'Union européenne.

La Commission présente actuellement, en liaison avec les propositions de modification de la DSP2, une proposition de cadre juridique de l'Union pour l'accès aux données d'information financière (FIDA); cette proposition porte sur l'accès aux données financières autres que les données relatives aux comptes de paiement, lesquelles restent régies par la législation sur les paiements.

Parmi les législations pertinentes de l'UE d'un caractère plus général figurent le RGPD[16], l'acte législatif européen sur l'accessibilité[17] et la proposition de règlement sur les données, pertinente pour la banque ouverte[18]. En particulier, les chapitres III et IV de la proposition de règlement sur les données établissent un cadre horizontal de droits et d'obligations en ce qui concerne les conditions de la mise à disposition des données dans les relations interentreprises.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

- **Base juridique**

La base juridique de la DSP2 est l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE), qui charge les institutions de l'UE d'arrêter des dispositions en vue d'établir le marché intérieur et d'en assurer le bon fonctionnement conformément à l'article 26 dudit traité.

- **Subsidiarité (en cas de compétence non exclusive)**

Les prestataires de services de paiement peuvent également fournir des services de paiement transfrontières au sein du marché intérieur des services de paiement. Les prestataires de services de paiement font largement usage de la libre prestation de services et de la liberté d'établissement. Afin de garantir des conditions harmonieuses ainsi que des conditions de concurrence équitables au sein du marché intérieur des services de paiement de détail, il est

15 COM(2021)32 final du 19 janvier 2021.

16 Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Voir également ci-dessous le paragraphe consacré aux«Droits fondamentaux».

17 Directive (UE) 2019/882 du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services. Cela est pertinent pour les mesures visant à améliorer l'accès à l'authentification forte du client, qui sont conçues pour être compatibles avec ladite directive.

18 Proposition de règlement fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), COM(2022) 68 final. La proposition de règlement sur les données prévoit des règles horizontales régissant l'accès aux données et l'utilisation des données. Dans ce contexte, des règles sectorielles d'accès aux données peuvent être adoptées, s'il y a lieu, y compris en ce qui concerne les règles relatives à la banque ouverte.

nécessaire de légiférer au niveau de l'Union. Cette motivation sous-tend les première et deuxième directives sur les services de paiement et continue de s'appliquer à la présente proposition.

- **Proportionnalité**

La proposition contient des mesures de proportionnalité ciblées, telles que la possibilité, dans le domaine de la banque ouverte, pour un prestataire de services de paiement gestionnaire de comptes d'obtenir de son autorité compétente nationale une dérogation à l'obligation de disposer d'une interface spécifique d'accès aux données.

- **Choix de l'instrument**

La DSP2 est actuellement une directive qui est appliquée par l'intermédiaire des législations de transposition des États membres. Toutefois, dans divers domaines de la législation de l'UE sur les services financiers[19], il a été jugé approprié d'adopter des règles applicables aux entreprises financières sous la forme d'un règlement directement applicable afin de renforcer la cohérence de la mise en œuvre dans les États membres. À l'issue du réexamen de la DSP2, il a été conclu que cette approche serait également appropriée pour la législation sur les paiements, ce qui a conduit à ce que les propositions de modification de la DSP2 figurent dans deux actes législatifs distincts: la présente proposition de règlement, qui contient des règles applicables aux prestataires de services de paiement et aux consommateurs, et une proposition de directive, qui prévoit notamment des règles relatives à l'agrément et à la surveillance des établissements de paiement.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

- **Évaluations ex post/bilans de qualité de la législation existante**

La DSP2 a fait l'objet d'une évaluation en 2022. Les contributions à l'évaluation comprenaient un rapport établi par un contractant indépendant ainsi que les avis des parties intéressées exprimés lors de diverses consultations publiques. Le rapport d'évaluation est publié en annexe de l'analyse d'impact accompagnant la présente proposition[20].

Il est conclu dans le rapport d'évaluation que la DSP2 a atteint ses objectifs à des degrés divers. L'un des domaines dans lesquels l'incidence a été positive est la prévention de la fraude, grâce à l'introduction de l'authentification forte du client; bien qu'elle soit plus difficile à mettre en œuvre que prévu, l'authentification forte du client a déjà eu une incidence notable en matière de réduction de la fraude. La DSP2 a également été particulièrement efficace en ce qui concerne son objectif d'accroître l'efficience, la transparence et le choix des instruments de paiement pour les utilisateurs de services de paiement. Toutefois, l'efficacité de la DSP2 pour parvenir à des conditions de concurrence équitables est limitée, compte tenu notamment du déséquilibre persistant entre prestataires de services de paiement bancaires et prestataires de services de paiement non bancaires en raison du manque d'accès direct de ces derniers à certains systèmes de paiement clés. L'adoption de la banque ouverte a connu un succès mitigé, avec des problèmes liés aux interfaces d'accès aux données pour les prestataires de services de banque ouverte, malgré les coûts de mise en œuvre des dispositions de la DSP2 relatives à la banque ouverte. Concernant l'objectif d'achèvement du marché

[19] Par exemple, les règles prudentielles applicables aux banques ou les règles régissant les marchés de titres.

[20] SWD(2023) 231 final.

intérieur, alors que la prestation transfrontière de services de paiement augmente, de nombreux systèmes de paiement (en particulier les systèmes de cartes de débit) restent nationaux. Les baisses de coûts escomptées pour les commerçants grâce à de nouveaux moyens de paiement moins chers ne se sont pas encore pleinement concrétisées. Dans l'ensemble, il est conclu dans l'évaluation que, malgré certaines lacunes, le cadre actuel de la DSP2 a permis de progresser dans la réalisation de ses objectifs, tout en étant relativement efficient au regard de ses coûts et en apportant une valeur ajoutée européenne.

- **Consultation des parties intéressées**

Afin que la proposition de la Commission tienne compte des points de vue de toutes les parties intéressées, la stratégie de consultation mise en place pour cette initiative a inclus:

– une consultation publique ouverte, menée du 10 mai au 2 août 2022[21];

– une consultation ciblée (mais néanmoins publique et ouverte), avec des questions plus détaillées que celles de la consultation publique, menée du 10 mai au 5 juillet 2022[22];

– un appel à contributions, ouvert du 10 mai au 2 août 2022[23];

– une consultation ciblée sur la directive concernant le caractère définitif du règlement, menée du 12 février au 7 mai 2021;

– une consultation des parties intéressées au sein du groupe d'experts du marché des systèmes de paiement de la Commission;

– des contacts ad hoc avec différentes parties intéressées, à l'initiative de ces dernières ou de la Commission;

– la consultation des experts des États membres au sein du groupe d'experts de la Commission sur la banque, les paiements et l'assurance.

Le résultat de ces consultations est résumé à l'annexe 2 de l'analyse d'impact accompagnant la présente proposition.

- **Obtention et utilisation d'expertise**

Un certain nombre de contributions et de sources d'expertise ont été utilisées lors de la préparation de la présente initiative, parmi lesquelles:

– les contributions fournies à la faveur des différentes consultations énumérées ci-dessus ou d'une manière ponctuelle par les parties intéressées;

– les contributions fournies par l'Autorité bancaire européenne dans son avis[24];

– une étude réalisée par un contractant, Valdani Vicari & Associati Consulting, remise en septembre 2022 et intitulée «A study on the application and the impact of Directive (EU) 2015/2366 on Payment Services (PSD2)»[25];

---

21 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules/public-consultation_fr

22 https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-psd2-review_en

23 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules_fr

24 EBA/Op/2022/06 du 23 juin 2022. Référence du contrat: FISMA/2021/OP/0002.

25 Disponible via ce lien: https://data.europa.eu/doi/10.2874/996945.

– des données obtenues auprès d'opérateurs du secteur privé, par exemple dans le domaine de la banque ouverte, et auprès d'organisations de consommateurs.

• **Analyse d'impact**

Ces deux propositions sont accompagnées d'une analyse d'impact qui a été examinée le 1er mars 2023 par le comité d'examen de la réglementation (CER). Le comité a rendu, le 3 mars 2023, un avis favorable assorti de réserves.

L'analyse d'impact a révélé l'existence de quatre grands problèmes sur le marché des paiements de l'UE, malgré les résultats obtenus avec la DSP2:

– les consommateurs sont exposés au risque de fraude et manquent de confiance dans les paiements;

– le cadre de la banque ouverte fonctionne de manière imparfaite;

– les autorités de surveillance de l'UE sont titulaires de pouvoirs et d'obligations incohérents;

– les conditions de concurrence entre les banques et les prestataires de services de paiement non bancaires ne sont pas équitables.

Ces problèmes entraînent notamment les conséquences suivantes:

– les utilisateurs (en particulier les consommateurs, les commerçants et les PME) continuent d'être exposés à des risques de fraude;

– les prestataires de services de banque ouverte sont confrontés à des obstacles lorsqu'il s'agit de proposer des services de banque ouverte de base et éprouvent davantage de difficultés à innover et à concurrencer les acteurs historiques tels que les schémas de cartes;

– les prestataires de services de paiement ne sont pas au clair sur leurs obligations et les prestataires de services de paiement non bancaires se trouvent dans une situation concurrentielle désavantageuse par rapport aux banques;

– les opérations commerciales sont inefficaces sur le plan économique et affichent des coûts plus élevés, ce qui a une incidence négative sur la compétitivité de l'UE;

– le marché intérieur des paiements est fragmenté et marqué par un phénomène de juridiction la plus favorable.

L'initiative poursuit quatre objectifs spécifiques, qui correspondent aux problèmes recensés:

1. renforcer la protection des utilisateurs et la confiance dans les paiements;
2. améliorer la compétitivité des services de banque ouverte;
3. améliorer le contrôle de l'application et la mise en œuvre dans les États membres;
4. améliorer l'accès (direct ou indirect) aux systèmes de paiement et aux comptes bancaires pour les prestataires de services de paiement non bancaires.

L'analyse d'impact présente un ensemble d'options privilégiées visant à atteindre les objectifs spécifiques (la liste ci-dessous comprend tant les mesures figurant dans le présent règlement que celles énoncées dans la directive qui l'accompagne):

– en ce qui concerne l'objectif spécifique nº 1, des améliorations dans la mise en œuvre de l'authentification forte du client, une base juridique pour l'échange d'informations sur la fraude et l'obligation de sensibiliser les clients aux risques de fraude, l'extension de la vérification du code IBAN à l'ensemble des virements, et le

renversement conditionnel de la responsabilité en cas de fraude au paiement par autorisation; l'obligation pour les prestataires de services de paiement d'améliorer l'accessibilité de l'authentification forte du client pour les utilisateurs handicapés, les personnes âgées et les autres personnes rencontrant des difficultés dans l'utilisation de l'authentification forte du client; des mesures visant à améliorer la disponibilité des espèces; des améliorations concernant les droits et l'information des utilisateurs;

– en ce qui concerne l'objectif spécifique nº 2, l'obligation pour les prestataires de services de paiement gestionnaires de comptes de mettre en place une interface spécifique d'accès aux données; des «tableaux de bord des permissions» permettant aux utilisateurs de gérer les permissions d'accès à la banque ouverte qu'ils ont accordées; des spécifications plus détaillées pour les exigences minimales applicables aux interfaces de données de banque ouverte;

– en ce qui concerne l'objectif spécifique nº 3, remplacer la majeure partie de la DSP2 par un règlement directement applicable clarifiant les aspects de la DSP2 qui sont peu clairs ou ambigus; renforcer les dispositions en matière de sanctions; intégrer les régimes d'agrément pour les établissements de paiement et les établissements de monnaie électronique;

– en ce qui concerne l'objectif spécifique nº 4, renforcer le droit à un compte bancaire pour les établissements de paiement et les établissements de monnaie électronique; accorder la possibilité d'une participation directe des établissements de paiement et des établissements de monnaie électronique à tous les systèmes de paiement, y compris ceux désignés par les États membres en vertu de la DCDR, avec des précisions supplémentaires sur les procédures d'admission et d'évaluation des risques.

Plusieurs options ont été rejetées dans l'analyse d'impact en raison de coûts de mise en œuvre élevés et d'incertitudes quant aux avantages. Les coûts des options retenues sont principalement des coûts ponctuels qui pèsent en grande partie sur les prestataires de services de paiement gestionnaires de comptes (essentiellement des banques). Dans la banque ouverte, les coûts sont compensés par les économies réalisées (telles que la suppression de l'obligation de maintenir en permanence une interface de secours et de la procédure d'exemption correspondante) et par l'adoption de mesures de proportionnalité (dérogations possibles pour les prestataires de services de paiement gestionnaires de comptes de niche). Le coût pour les États membres de l'amélioration du contrôle de l'application et de la mise en œuvre sera limité. Les coûts de l'accès direct aux systèmes de paiement clés pour les établissements de paiement seront limités, et seront pris en charge par les systèmes de paiement en question. Par ailleurs, les avantages profiteront à un large éventail de parties intéressées, dont les utilisateurs de services de paiement (consommateurs, entreprises, commerçants et administrations publiques) et les prestataires de services de paiement eux-mêmes (en particulier les prestataires de services de paiement qui sont des entreprises de technologie financière non bancaires). Les avantages seront récurrents, tandis que les coûts seront principalement des coûts d'ajustement ponctuels; par conséquent, les avantages cumulés devraient, avec le temps, dépasser les coûts totaux.

- **Réglementation affûtée et simplification**

La présente initiative n'est pas une initiative s'inscrivant dans le cadre du programme pour une réglementation affûtée et performante (REFIT). Néanmoins, des possibilités de simplification administrative ont été recherchées à la faveur du processus d'évaluation et de réexamen. La clarification des règles relatives à l'authentification forte du client et d'autres

clarifications, ainsi que la suppression des divergences liées à la transposition nationale d'une directive, contribueront à cette simplification.

- **Droits fondamentaux**

La présente initiative concerne tout particulièrement le droit fondamental à la protection des données à caractère personnel. Dans la mesure où le traitement de données à caractère personnel est nécessaire pour se conformer à la présente initiative, il est proportionné pour garantir le bon fonctionnement du marché intérieur des paiements numériques. Dans le cadre de la présente initiative, le traitement des données à caractère personnel doit être conforme au règlement général sur la protection des données (RGPD), lequel s'applique directement à tous les services de paiement concernés par la présente proposition.

- **Application du principe «un ajout, un retrait»**

La présente initiative n'engendre pas de coûts administratifs pour les entreprises ou les consommateurs, étant donné qu'elle n'entraînera pas d'augmentation de la supervision ou de la surveillance des prestataires de services de paiement, ni de nouvelles obligations de déclaration spéciales qui ne figureraient pas déjà dans la DSP2. L'initiative ne fait pas non plus naître de frais ou de charges réglementaires. Aussi la Commission considère-t-elle que la présente initiative ne génère pas de coûts administratifs qui nécessiteraient une compensation en application du principe «un ajout, un retrait», bien qu'elle entre en ligne de compte pour l'application de ce principe dans la mesure où elle engendre des coûts de mise en œuvre. Le regroupement des régimes législatifs applicables respectivement aux établissements de monnaie électronique et aux établissements de paiement permettra de réduire les coûts administratifs, par exemple en supprimant l'obligation d'obtenir un nouvel agrément dans certaines circonstances.

- **Climat et durabilité**

Aucune incidence négative sur le climat n'a été relevée pour la présente initiative. L'initiative contribuera à la réalisation de la cible 8.2 des objectifs de développement durable des Nations unies: «*Parvenir à un niveau élevé de productivité économique par la diversification, la modernisation technologique et l'innovation, notamment en mettant l'accent sur les secteurs à forte valeur ajoutée et à forte intensité de main-d'œuvre*».

4. INCIDENCE BUDGÉTAIRE

La présente proposition n'a pas d'incidence sur le budget de l'Union.

5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

L'initiative prévoira la réalisation d'un réexamen cinq ans après la date d'application. Dans le cadre de ce réexamen, il conviendra d'accorder une attention particulière aux dispositions concernant les règles relatives à la banque ouverte, les frais et les charges pour les services de paiement, ainsi que les règles relatives à la responsabilité et à la réparation des opérations frauduleuses.

- **Explication détaillée de certaines dispositions de la proposition**

Objet, champ d'application et définitions

La proposition énonce des règles applicables aux prestataires de services de paiement en matière de paiements. Elle ne modifie pas la liste des services de paiement établie par la DSP2. La liste des exclusions est pratiquement inchangée. La proposition inclut une liste de définitions, qui est élargie par rapport à celle figurant dans la DSP2 et qui contient davantage de termes et des précisions sur certains termes. Des définitions des opérations initiées par les commerçants et des ordres de paiement passés par courrier ou par téléphone sont introduites. La définition de l'«opération de paiement à distance» au sens de la DSP2 est simplifiée afin de permettre une délimitation plus claire des notions d'«initiation d'une opération de paiement» et d'«initiation à distance d'une opération de paiement».

Systèmes de paiement et accès aux comptes détenus auprès d'établissements de crédit

En ce qui concerne les opérateurs de systèmes de paiement, l'obligation de disposer de règles et de procédures d'accès qui soient proportionnées, objectives et non discriminatoires est également étendue aux systèmes de paiement désignés par un État membre en vertu de la directive 98/26/CE (directive concernant le caractère définitif du règlement[26]). Les opérateurs de systèmes de paiement sont tenus de procéder à une évaluation des risques pertinents lorsqu'ils examinent une demande de participation émanant d'un prestataire de services de paiement. La décision rendue sur une demande doit être communiquée par écrit et un droit de recours est instauré. Les autorités compétentes doivent être désignées par les États membres lorsqu'il n'existe pas de surveillance par le système européen de banques centrales; lorsqu'il existe une surveillance du système européen de banques centrales, il est possible de s'appuyer sur elle pour remédier aux insuffisances des règles et procédures d'admission des systèmes de paiement.

Les règles relatives à l'accès (ouverture et clôture) d'un établissement de paiement à un compte ouvert auprès d'un établissement de crédit sont renforcées par rapport à celles prévues dans la DSP2. Elles s'appliquent également aux demandeurs d'un agrément en tant qu'établissement de paiement (compte tenu de l'importance pour eux de disposer d'un compte bancaire pour obtenir leur agrément), ainsi qu'aux agents et aux distributeurs des établissements de paiement. Tout refus ou retrait d'accès doit être fondé sur des motifs sérieux, par exemple sur des soupçons raisonnables d'activité illégale ou de risque pour l'établissement de crédit. Les motifs du refus ou du retrait de l'accès doivent être communiqués par écrit et motivés de manière circonstanciée compte tenu de la situation propre à l'établissement de paiement en question.

Transparence des conditions et exigences en matière d'informations en ce qui concerne les services de paiement

Pour ce qui est de la dérogation aux exigences en matière d'informations pour les instruments de paiement relatifs à des montants de faible valeur et la monnaie électronique pour les opérations de paiement nationales, la faculté laissée aux États membres d'ajuster les montants des limites de dépenses est supprimée.

Par souci de cohérence interne, l'obligation d'informer l'utilisateur de services de paiement des procédures de règlement extrajudiciaire des litiges dans les contrats-cadres est étendue aux opérations de paiement isolées.

---

[26] Cette modification doit être examinée conjointement avec une modification ciblée de la DCDR figurant dans la proposition de directive sur les services de paiement qui l'accompagne.

Des éclaircissements sont apportés afin que les prestataires de services de paiement insèrent dans les relevés de compte de paiement les informations nécessaires pour permettre l'identification certaine du bénéficiaire, y compris une référence à sa dénomination commerciale.

Des éclaircissements sont apportés afin que, lorsque des services de paiement sont proposés conjointement avec des services techniques soutenant la prestation de services de paiement et fournis par le prestataire de services de paiement ou par un tiers avec lequel il a noué un partenariat, ces services techniques soient soumis aux mêmes exigences relatives aux frais de résiliation que le contrat-cadre.

Des exigences supplémentaires en matière d'information pour les retraits aux distributeurs automatiques de billets (DAB) nationaux sont introduites dans différentes hypothèses.

En ce qui concerne les virements et les transmissions de fonds de l'UE vers un pays tiers, les prestataires de services de paiement sont tenus de communiquer à l'utilisateur de services de paiement le délai estimé de réception des fonds par les prestataires de services de paiement du bénéficiaire situé en dehors de l'UE. Pour permettre une meilleure comparabilité, les frais de conversion monétaire estimés de telles opérations internationales doivent être exprimés de la même manière que pour les virements au sein de l'UE, à savoir en marge de pourcentage sur les derniers taux de change de référence de l'euro disponibles émis par la BCE.

Droits et obligations liés à la prestation et à l'utilisation de services de paiement

Dispositions communes

En vertu de la DSP2, l'interdiction de la surfacturation, qui englobe les services de paiement auxquels s'applique le règlement relatif aux commissions d'interchange[27], est limitée aux virements et prélèvements libellés en euros, et non dans d'autres monnaies de l'UE. Des modifications sont introduites pour étendre l'interdiction de la surfacturation aux virements et aux prélèvements dans toutes les monnaies de l'UE.

Les règles applicables aux opérations initiées par les commerçants et aux prélèvements sont harmonisées et les mêmes mesures de protection des consommateurs, telles que les remboursements, s'appliquent aux prélèvements et aux opérations initiées par les commerçants, étant donné que ces deux types d'opération sont initiés par le bénéficiaire.

Banque ouverte (services d'information sur les comptes et services d'initiation de paiement)

Les dispositions relatives à la banque ouverte prévoient une série de modifications par rapport à la DSP2 et intègrent certaines dispositions figurant actuellement dans une norme technique de réglementation[28]. Les principales modifications comprennent l'obligation, sauf dans des circonstances exceptionnelles, de disposer d'une interface spécifique pour l'accès aux données nécessaires à la banque ouverte et la suppression, sauf circonstances exceptionnelles autorisées, de l'obligation incombant aux prestataires de services de paiement gestionnaires de comptes de maintenir en permanence une interface de secours. Des exigences supplémentaires concernant les interfaces spécifiques sont introduites en ce qui concerne les performances et les fonctionnalités. Afin que les utilisateurs de services de banque ouverte

[27] Règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte.

[28] Règlement délégué (UE) 2018/389 de la Commission complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication.

puissent gérer d'une manière pratique les permissions qu'ils ont accordées en matière de banque ouverte, les prestataires de services de paiement gestionnaires de comptes sont tenus de leur proposer un «tableau de bord» permettant de retirer les droits d'accès aux données à tout prestataire de services de banque ouverte.

Il n'y a pas eu de forte demande du marché pour un service spécial de confirmation de la disponibilité des fonds, qui faisait l'objet de l'article 65 de la DSP2 en tant que service de banque ouverte parallèlement aux services d'information sur les comptes et d'initiation de paiement. Très peu de modèles commerciaux, voire aucun, ont été élaborés à partir de ce service, le marché s'appuyant sur l'utilisation du service d'information sur les comptes comme autre moyen de vérifier la disponibilité des fonds. Cette disposition a donc été supprimée en tant que service de banque ouverte autonome.

Autorisation des opérations de paiement

Le prestataire de services de paiement du bénéficiaire est tenu de fournir à son utilisateur de services de paiement, sur demande, un service permettant de vérifier la concordance entre l'identifiant unique du bénéficiaire et le nom du bénéficiaire fourni par le payeur et d'informer le prestataire de services de paiement du payeur de toute divergence détectée. Si l'identifiant unique du bénéficiaire et le nom du bénéficiaire ne concordent pas, le prestataire de services de paiement notifie cette divergence et le degré détecté de cette divergence au payeur. La proposition de la Commission sur les paiements instantanés modifiant le règlement SEPA[29], actuellement examinée par les colégislateurs, prévoit une disposition similaire concernant les divergences entre le nom d'un bénéficiaire et son identifiant unique pour les virements instantanés libellés en euros. Afin d'établir un cadre cohérent pour l'ensemble des virements, la disposition de la présente proposition s'applique aux virements autres que les virements instantanés dans toutes les monnaies de l'Union et aux virements instantanés libellés dans des monnaies autres que l'euro. La notification doit être faite avant que le payeur ne finalise l'ordre de paiement et avant que le prestataire de services de paiement n'exécute le virement. Dans tous les cas, l'utilisateur conserve toute latitude pour décider de soumettre ou non l'ordre de paiement pour le virement.

En ce qui concerne la disposition relative aux limites pour l'utilisation d'un instrument de paiement, il est précisé que les prestataires de services de paiement ne doivent pas augmenter unilatéralement les limites de dépenses convenues avec leurs utilisateurs de services de paiement.

Une précision est apportée à la disposition relative à la responsabilité du prestataire de services de paiement pour les opérations de paiement non autorisées, selon laquelle seuls des motifs raisonnables de soupçonner une fraude de la part du payeur peuvent conduire à un refus de remboursement de la part du prestataire de services de paiement. Dans ce cas, le prestataire de services de paiement doit justifier le refus du remboursement et indiquer les instances que le payeur peut saisir.

Le prestataire de services de paiement du payeur doit être tenu pour responsable du montant total du virement s'il n'a pas notifié au payeur une divergence détectée entre l'identifiant unique du bénéficiaire et le nom de celui-ci fourni par le payeur. Un prestataire de services de paiement est tenu pour responsable lorsqu'un consommateur a été manipulé, pour qu'il autorise une opération de paiement, par un tiers se faisant passer, par des mensonges ou par imposture, pour un employé du prestataire de services de paiement de ce consommateur. Les

[29] Proposition COM(2022) 546 final du 26 octobre 2022, modifiant le règlement (UE) nº 260/2012.

fournisseurs de services de communications électroniques sont désormais tenus de coopérer avec les prestataires de services de paiement en vue de prévenir une telle fraude.

Lorsque la responsabilité est imputable au prestataire de services de paiement du bénéficiaire, ce dernier prestataire doit rembourser le préjudice financier subi par le prestataire de services de paiement du payeur. Les dispositions relatives à la notification et à la rectification des opérations de paiement non autorisées ou mal exécutées, aux exigences en matière d'information et au droit de recours (action récursoire) sont mises à jour afin de tenir compte de la nouvelle disposition relative à la responsabilité en cas d'application incorrecte du service de vérification de la concordance.

De nouvelles dispositions relatives à la responsabilité pour les prestataires de services techniques et les opérateurs de schémas de paiement sont incluses en ce qui concerne le défaut de soutien à l'authentification forte du client; en effet, l'évaluation de la DSP2 a mis en évidence des problèmes concernant la mise en œuvre de l'authentification forte du client liés au rôle joué par ces parties prenantes dans le déploiement de l'authentification forte du client, ce qui a même contribué au report de l'application de l'authentification forte du client de 2018 à 2020.

Il est désormais précisé que le payeur ne supporte aucune perte financière lorsque le prestataire de services de paiement du payeur ou celui du bénéficiaire applique une dérogation à l'utilisation de l'authentification forte du client.

En ce qui concerne les opérations de paiement pour lesquelles le montant de l'opération n'est pas connu à l'avance et pour lesquelles les fonds sont bloqués sur un instrument de paiement, la présente proposition introduit, à l'endroit du bénéficiaire, l'obligation légale d'informer le prestataire de services de paiement du montant exact de l'opération de paiement immédiatement après la livraison du service ou des biens au payeur, ainsi que l'exigence que le montant des fonds bloqués soit proportionné au montant de la future opération de paiement pouvant être raisonnablement prévu au moment du blocage des fonds.

Exécution des opérations de paiement

Lorsqu'un prestataire de services d'initiation de paiement fournit un identifiant unique inexact de bénéficiaire, il est tenu pour responsable du montant de l'opération.

Protection des données

Une nouvelle disposition est insérée afin de définir explicitement un intérêt public important pour lequel le traitement de catégories particulières de données à caractère personnel pourrait être nécessaire dans le cadre de la présente proposition de règlement.

Risques opérationnels et de sécurité et authentification

Une nouvelle disposition est ajoutée pour exiger des prestataires de services de paiement qu'ils disposent de mécanismes de contrôle des opérations afin de prévoir l'application d'une authentification forte du client et d'améliorer la prévention et la détection des opérations frauduleuses. Cette disposition clarifie la notion d'«inhérence», en précisant que ces mécanismes de contrôle des opérations doivent être fondés sur l'analyse d'opérations de paiement et tenir compte d'éléments qui sont propres à l'utilisateur de services de paiement dans des conditions d'utilisation normale des données de sécurité personnalisées, notamment des caractéristiques environnementales et comportementales telles que celles liées à la localisation de l'utilisateur de services de paiement, à l'heure de l'opération, au dispositif utilisé, aux habitudes de dépense et au magasin en ligne où l'achat est effectué.

Aux fins du contrôle des opérations, des dispositions ont été ajoutées qui permettent aux prestataires de services de paiement d'échanger, sur une base volontaire, des données à

caractère personnel telles que les identifiants uniques de bénéficiaires dans le cadre de dispositifs de partage d'informations. Ces dispositifs de partage d'informations doivent définir les modalités détaillées de participation et les éléments opérationnels, y compris l'utilisation de plates-formes informatiques spécifiques. Avant de participer à de tels dispositifs, les prestataires de services de paiement doivent effectuer une analyse d'impact relative à la protection des données et, si nécessaire, consulter préalablement l'autorité de contrôle, conformément au règlement (UE) 2016/679.

En ce qui concerne l'application de l'authentification forte du client dans le cas des opérations de paiement initiées par un commerçant, il est précisé qu'il faut appliquer une authentification forte du client lors de l'établissement du mandat, mais sans qu'il soit nécessaire de l'appliquer aux opérations de paiement ultérieures initiées par un commerçant. En ce qui concerne l'application de l'authentification forte du client dans le cas des ordres de paiement passés par courrier ou par téléphone, il est précisé qu'il suffit que l'initiation d'une opération de paiement ne soit pas numérique pour que cette opération ne soit pas concernée par les obligations d'authentification forte du client. Toutefois, les opérations de paiement fondées sur des ordres de paiement passés par le payeur sur support papier, par courrier ou par téléphone devraient être soumises par le prestataire de services de paiement du payeur à des normes de sécurité et à des vérifications permettant l'authentification de l'opération de paiement afin d'éviter un contournement abusif des exigences relatives à l'authentification forte. En outre, le champ d'application de la dérogation à l'authentification forte du client a été restreint dans le cas des opérations de paiement pour lesquelles le bénéficiaire passe des ordres de paiement en vertu d'un mandat donné par le payeur (prélèvements), tandis qu'une obligation d'imposer l'authentification forte du client a été introduite lorsqu'un mandat est conféré grâce à un moyen de communication à distance avec l'intervention directe d'un prestataire de services de paiement.

L'authentification forte du client n'est requise que pour les services d'information sur les comptes lors du premier accès aux données; toutefois, les prestataires de services d'information sur les comptes doivent exiger l'authentification forte du client au moins tous les 180 jours lorsque leurs clients accèdent aux données agrégées de leurs comptes dans le domaine du prestataire de services d'information sur les comptes.

Des dispositions ont été ajoutées pour améliorer l'accessibilité de l'authentification forte du client, notamment pour que tous les clients, y compris les personnes handicapées, les personnes âgées, les personnes ayant de faibles compétences numériques et celles qui n'ont pas accès à des canaux numériques ou à un téléphone intelligent, disposent d'au moins un moyen leur permettant de procéder à une authentification forte du client.

En ce qui concerne l'obligation pour les prestataires de services de paiement d'appliquer aux «paiements à distance» une authentification forte du client qui comprenne des éléments permettant d'établir un lien dynamique entre l'opération, d'une part, et un montant et un bénéficiaire donnés, d'autre part, il est précisé que cette obligation s'applique aux opérations de paiement électronique pour lesquelles un ordre de paiement est passé au moyen d'un dispositif du payeur utilisant la technologie de proximité pour l'échange d'informations avec l'infrastructure du bénéficiaire, et pour lesquelles la réalisation d'une authentification forte du client nécessite l'utilisation de l'internet sur le dispositif du payeur.

Une disposition impose aux prestataires de services de paiement et aux prestataires de services techniques de conclure des accords d'externalisation dans les cas où les prestataires de services techniques fournissent et vérifient les éléments d'authentification forte du client.

Pouvoirs d'intervention de l'Autorité bancaire européenne sur les produits

La présente proposition confère à l'ABE des pouvoirs d'intervention sur les produits conformément à l'article 9, paragraphe 5, du règlement (UE) nº 1093/2010. Cela permettra à l'ABE, sur la base de certains critères, d'interdire temporairement la vente de certains produits de paiement qui présenteraient certains risques.

Autres dispositions

Des habilitations sont prévues pour des normes techniques de réglementation élaborées par l'ABE, y compris des normes techniques de réglementation existantes et, dans certains cas, de nouvelles normes de ce type. L'ABE peut modifier les normes techniques de réglementation existantes, mais si elle ne le fait pas, celles-ci resteront en vigueur.

Le règlement proposé entrera en vigueur le vingtième jour suivant celui de sa publication au Journal officiel et entrera en application 18 mois plus tard[30]. Un tableau de correspondance entre les articles du règlement proposé et ceux de la DSP2 et de la DME 2 figure en annexe.

[30] Cette date est alignée sur le délai de transposition de la directive sur les services de paiement qui accompagne la présente proposition.

2023/0210 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

concernant les services de paiement dans le marché intérieur et modifiant le règlement (UE) nº 1093/2010

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

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen[31],

vu l'avis de la Banque centrale européenne[32],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) Depuis l'adoption de la directive (UE) 2015/2366 du Parlement européen et du Conseil[33], le marché des services de paiement de détail a connu des changements importants, en grande partie liés à l'utilisation croissante des cartes et des moyens de paiement numériques, à la diminution de l'utilisation des espèces et à la présence grandissante de nouveaux acteurs et services, notamment les portefeuilles numériques et les paiements sans contact. La pandémie de COVID-19 et les transformations qu'elle a apportées aux pratiques de consommation et de paiement ont accru l'importance de disposer de paiements sécurisés et efficaces.

(2) Dans sa communication sur une stratégie en matière de paiements de détail pour l'UE[34], la Commission a annoncé le lancement d'un réexamen complet de l'application et de l'incidence de la directive (UE) 2015/2366, «*qui devrait inclure une évaluation globale de sa pertinence, eu égard à l'évolution du marché*».

(3) La directive (UE) 2015/2366 visait à lever les obstacles à de nouveaux types de services de paiement et à améliorer le niveau de protection et de sécurité des consommateurs. L'évaluation par la Commission de l'incidence et de l'application de la directive (UE) 2015/2366 a permis non seulement de constater que la directive (UE) 2015/2366 était largement couronnée de succès quant à la réalisation de bon nombre

---

31 JO C du , p. .

32 JO C du , p. .

33 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).

34 COM(2020) 592 final.

de ses objectifs, mais également de recenser certains domaines dans lesquels les objectifs de ladite directive n'étaient pas pleinement atteints. Par exemple, l'évaluation a mis en évidence l'augmentation de nouveaux types de fraude en tant que sujet de préoccupation à l'égard des objectifs de protection des consommateurs. Des lacunes ont également été relevées en ce qui concerne l'objectif consistant à améliorer la concurrence sur le marché grâce aux «services de banque ouverte» (services d'information sur les comptes et services d'initiation de paiement) en réduisant les obstacles auxquels sont confrontés les prestataires tiers sur le marché. Les progrès accomplis dans la réalisation de l'objectif consistant à améliorer la prestation de services de paiement transfrontières ont également été limités, en grande partie en raison d'incohérences dans les pratiques de surveillance et dans le contrôle de l'application des règles dans les différents pays de l'Union. L'évaluation a également mis en évidence des facteurs qui freinent les progrès en ce qui concerne l'objectif d'instauration de conditions de concurrence équitables entre tous les prestataires de services de paiement.

(4) L'évaluation a également recensé des problèmes liés à des divergences dans la mise en œuvre et le contrôle de l'application de la directive (UE) 2015/2366 qui ont une incidence directe sur la concurrence entre les prestataires de services de paiement et qui se sont traduits par des conditions réglementaires différentes selon les États membres, ce qui a encouragé l'arbitrage réglementaire. Il ne devrait pas y avoir de place pour le «forum shopping» dans le contexte duquel les prestataires de services de paiement pourraient choisir, comme pays d'origine, les États membres dans lesquels l'application des règles de l'Union relatives aux services de paiement leur est plus avantageuse, alors qu'ils fournissent des services transfrontières dans d'autres États membres qui adoptent une interprétation plus stricte des règles ou appliquent des politiques plus actives de contrôle de leur respect aux prestataires de services de paiement qui y sont établis. Une telle pratique fausse la concurrence. Il convient donc d'harmoniser davantage les règles de l'Union relatives aux services de paiement, en intégrant dans un règlement les règles régissant la conduite de l'activité des services de paiement, notamment les droits et obligations des parties concernées. Ces règles, à l'exclusion des règles relatives à l'agrément et à la surveillance des établissements de paiement, qui devraient rester dans une directive, devraient être précisées et plus détaillées afin de réduire au minimum les marges d'interprétation.

(5) Même si l'émission de monnaie électronique est régie par la directive 2009/110/CE du Parlement européen et du Conseil[35], l'utilisation de la monnaie électronique pour financer des opérations de paiement est, dans une très large mesure, régie par la directive (UE) 2015/2366. Dès lors, le cadre juridique applicable aux établissements de monnaie électronique et aux établissements de paiement, notamment en ce qui concerne les règles de conduite, est déjà en grande partie harmonisé. Pour résoudre les problèmes de cohérence externe et étant donné que les services de monnaie électronique et les services de paiement sont de plus en plus difficiles à distinguer, il convient de rapprocher les cadres législatifs concernant les établissements de monnaie électronique et les établissements de paiement. Toutefois, les exigences en matière d'agrément, en particulier en ce qui concerne le capital initial et les fonds propres,

[35] Directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE (JO L 267 du 10.10.2009, p. 7).

ainsi que certains concepts de base essentiels régissant les activités de monnaie électronique, tels que l'émission, la distribution et le remboursement de monnaie électronique, sont distincts des services fournis par les établissements de paiement. Il y a donc lieu de préserver ces spécificités lors de la fusion des dispositions de la directive (UE) 2015/2366 et de la directive 2009/110/CE. Étant donné que la directive 2009/110/CE est abrogée par la directive (UE) XXXX [DSP3], ses règles, à l'exception des règles relatives à l'agrément et à la surveillance, qui ont été intégrées dans la directive (UE) XXX [DSP3], devraient être reprises dans un cadre unifié au sein du présent règlement, moyennant les adaptations appropriées.

(6) Pour garantir la sécurité juridique et un champ d'application clair des règles applicables à l'exercice de l'activité de prestation de services de paiement et de services de monnaie électronique, il est nécessaire de préciser les catégories de prestataires de services de paiement qui sont soumises aux obligations concernant l'exercice de l'activité de prestation de services de paiement et de services de monnaie électronique dans l'ensemble de l'Union.

(7) Il existe plusieurs catégories de prestataires de services de paiement. Les établissements de crédit reçoivent des dépôts d'utilisateurs qui peuvent être utilisés pour exécuter des opérations de paiement. Ils sont agréés conformément à la directive 2013/36/UE du Parlement européen et du Conseil[36]. Les établissements de paiement ne reçoivent pas de dépôts. Ils peuvent détenir des fonds des utilisateurs et émettre de la monnaie électronique qui peut être utilisée pour exécuter des opérations de paiement. Ils sont agréés en application de la directive (UE) XXX [DSP3]. Les offices de chèques postaux qui sont habilités à le faire par leur droit national peuvent également fournir des services de monnaie électronique et de paiement. Parmi les autres catégories de prestataires de services de paiement figurent la Banque centrale européenne (BCE) et les banques centrales nationales lorsqu'elles n'agissent pas en qualité d'autorités monétaires ou d'autres autorités publiques, ainsi que les États membres ou leurs autorités régionales ou locales lorsqu'ils n'agissent pas en qualité d'autorités publiques.

(8) Il convient de dissocier, d'une part, le service permettant le retrait d'espèces d'un compte de paiement et, d'autre part, l'activité de gestion d'un compte de paiement, car il se peut que les prestataires de services de retrait d'espèces ne gèrent pas de comptes de paiement. Les services d'émission d'instruments de paiement et d'acquisition d'opérations de paiement, qui étaient mentionnés ensemble au point 5 de l'annexe de la directive (UE) 2015/2366 comme si l'un ne pouvait être proposé sans l'autre, devraient être présentés comme deux services de paiement différents. La mention séparée des services d'émission et des services d'acquisition, conjuguée à des définitions distinctes pour chaque service, devrait permettre de rendre plus clair que les services d'émission et les services d'acquisition peuvent être proposés séparément par les prestataires de services de paiement.

(9) L'exclusion du champ d'application de la directive (UE) 2015/2366 de certaines catégories d'opérateurs de distributeurs automatiques de billets (DAB) s'est révélée difficile à mettre en pratique. Il conviendrait, par conséquent, de remplacer la catégorie

[36] Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (Texte présentant de l'intérêt pour l'EEE) (JO L 176 du 27.6.2013, p. 338).

d'opérateurs de DAB qui étaient exclus de l'obligation d'être agréés en tant que prestataires de services de paiement en vertu de la directive (UE) 2015/2366 par une nouvelle catégorie d'opérateurs de DAB qui ne gèrent pas de comptes de paiement. Bien que ces opérateurs ne soient pas soumis aux obligations pour l'agrément au titre de la directive (UE) XXX [DSP3], ils devraient être soumis à des exigences en matière de transparence des frais dans les cas où ces opérateurs en perçoivent pour les retraits d'espèces.

(10) Afin d'améliorer encore l'accès aux espèces, lequel constitue une priorité de la Commission, les commerçants devraient être autorisés à proposer, dans les magasins physiques, des services de fourniture d'espèces, même en l'absence d'achat par un client, sans devoir obtenir d'agrément en tant que prestataire de services de paiement et sans devoir être un agent d'un établissement de paiement. Ces services de fourniture d'espèces devraient toutefois être soumis à l'obligation de communication des frais facturés au client, le cas échéant. Les détaillants devraient fournir ces services sur une base volontaire et en fonction des espèces dont ils disposent.

(11) L'exclusion du champ d'application de la directive (UE) 2015/2366 des opérations de paiement allant du payeur au bénéficiaire, par l'intermédiaire d'un agent commercial agissant pour le compte du payeur ou du bénéficiaire, a fait l'objet d'une application très divergente selon les États membres. La notion d'agent commercial étant généralement définie dans le droit civil national, elle peut varier d'un État membre à l'autre, ce qui conduit à des incohérences dans le traitement réservé aux mêmes services dans les différents pays. Il convient donc d'harmoniser et de clarifier la notion d'agent commercial aux fins de cette exclusion en faisant référence à la définition des agents commerciaux figurant dans la directive 86/653/CEE du Conseil[37]. En outre, il convient de préciser davantage les conditions dans lesquelles les opérations de paiement allant du payeur au bénéficiaire par l'intermédiaire d'agents commerciaux peuvent être exclues du champ d'application du présent règlement. À cet effet, il convient d'exiger que les agents soient habilités, par contrat avec le payeur ou le bénéficiaire, à négocier ou à conclure la vente ou l'achat de biens ou de services pour le compte du seul payeur ou du seul bénéficiaire, mais pas des deux, que l'agent commercial soit ou non en possession des fonds du client. Les plates-formes de commerce électronique qui agissent en tant qu'agents commerciaux pour le compte aussi bien d'acheteurs que de vendeurs individuels sans que ni les uns ni les autres ne disposent d'une marge d'autonomie réelle pour négocier ou conclure la vente ou l'achat de biens ou de services ne devraient pas être exclues du champ d'application du présent règlement. L'Autorité bancaire européenne (ABE) devrait élaborer des orientations sur l'exclusion des opérations de paiement allant du payeur au bénéficiaire par l'intermédiaire d'un agent commercial, afin d'apporter davantage de clarté et de convergence entre les autorités compétentes. Ces orientations peuvent inclure un référentiel des cas d'utilisation qui relèvent généralement de l'exclusion applicable aux agents commerciaux.

(12) L'exclusion des instruments à finalité spécifique du champ d'application de la directive (UE) 2015/2366 a été appliquée différemment d'un État membre à l'autre, bien que les prestataires de services dont les instruments relevaient de cette exclusion aient été tenus de notifier leur activité aux autorités compétentes. L'ABE a fourni des orientations supplémentaires dans ses «*Guidelines on the limited network exclusion*

[37] Directive 86/653/CEE du Conseil du 18 décembre 1986 relative à la coordination des droits des États membres concernant les agents commerciaux indépendants (JO L 382 du 31.12.1986, p. 17).

under PSD2» («Orientations sur l'exclusion relative aux "réseaux limités" au titre de la DSP2», en anglais) du 24 février 2022[38]. Malgré ces tentatives visant à clarifier l'application de l'exclusion relative aux instruments à finalité spécifique, il subsiste des prestataires de services qui essaient de bénéficier de cette exclusion alors qu'ils fournissent des services portant sur des volumes de paiement importants et sur une variété de produits proposés à un grand nombre de clients. En pareils cas, les consommateurs ne bénéficient pas des garanties nécessaires et les services concernés ne devraient pas bénéficier de l'exclusion relative aux instruments à finalité spécifique. Il est par conséquent nécessaire de préciser qu'il ne devrait pas être possible d'utiliser le même instrument à finalité spécifique pour effectuer des opérations de paiement en vue d'acquérir des biens et des services au sein de plus d'un réseau limité ou d'acquérir un éventail illimité de biens ou de services.

(13) Pour déterminer si un réseau limité devrait être exclu du champ d'application, il convient de prendre en considération la localisation géographique des points d'acceptation de ce réseau ainsi que le nombre de points d'acceptation. Les instruments à finalité spécifique devraient permettre au détenteur d'acquérir des biens ou des services uniquement dans les locaux physiques de l'émetteur, tandis que l'utilisation dans un environnement de magasin en ligne ne devrait pas relever de la notion de locaux de l'émetteur. Les instruments à finalité spécifique devraient comprendre, selon le régime contractuel applicable dans chaque cas, les cartes qui ne peuvent être utilisées que dans une chaîne de magasins déterminée ou dans un centre commercial particulier, les cartes de carburant, les cartes de membre, les cartes de transports en commun, les billets de parking, les titres-repas ou les titres-services, qui peuvent relever d'un cadre juridique particulier en matière fiscale ou de droit du travail, destiné à encourager le recours à ces instruments pour atteindre les objectifs fixés dans la législation sociale, tels que des titres de services pour la garde d'enfant ou des bons écologiques. Les instruments à finalité spécifique devraient également inclure les instruments fondés sur la monnaie électronique lorsqu'ils satisfont aux critères de cette exclusion. Il n'y a pas lieu d'exclure les instruments de paiement pouvant être utilisés pour réaliser des achats auprès de commerçants enregistrés dans une liste, lesdits instruments étant conçus, en principe, pour un réseau de prestataires de services qui ne cesse de s'étendre.

(14) L'exclusion relative à certaines opérations de paiement au moyen d'un système informatique ou de télécommunications devrait concerner plus particulièrement les micropaiements effectués pour l'achat de contenus numériques et de services vocaux. Une référence claire aux opérations de paiement effectuées pour l'achat de billets électroniques devrait être conservée afin que les clients puissent encore aisément réserver, payer, obtenir et valider des billets électroniques n'importe où et n'importe quand au moyen de téléphones mobiles ou d'autres dispositifs. Les billets électroniques permettent et facilitent la livraison de services pour lesquels les consommateurs pourraient, à défaut, acheter des billets sur support papier, et concernent les transports, les loisirs, le parking et l'accès à des monuments/manifestations, mais pas les biens physiques. Les opérations de paiement exécutées par un fournisseur déterminé de réseaux de communications électroniques depuis ou au moyen d'un dispositif électronique et imputées sur la facture correspondante pour recueillir des dons en faveur d'organismes caritatifs devraient

[38] Autorité bancaire européenne, EBA/GL/2022/02.

également être exclues. L'exclusion ne devrait s'appliquer que lorsque la valeur des opérations de paiement est inférieure à un seuil déterminé.

(15) L'espace unique de paiements en euros (SEPA) a facilité la mise en place de centres de paiement et de centres d'encaissement à travers l'Union, ce qui a permis une centralisation des opérations de paiement d'un même groupe. À cet égard, les opérations de paiement entre une entreprise mère et sa filiale, ou entre filiales d'une même entreprise mère, qui sont effectuées par un prestataire de services de paiement faisant partie du même groupe devraient être exclues du champ d'application du présent règlement. La centralisation des ordres de paiement pour le compte d'un groupe par une entreprise mère ou sa filiale pour transmission ultérieure à un autre prestataire de services de paiement ne devrait pas être considérée comme un service de paiement.

(16) La prestation de services de paiement nécessite le soutien de services techniques. Ces services techniques comprennent le traitement et le stockage de données, les services de portail de paiement, les services de confiance et de protection de la vie privée, l'authentification des données et des entités, la fourniture de technologies de l'information et de réseaux de communication, la fourniture et la maintenance d'interfaces destinées aux consommateurs qui sont utilisées pour la collecte des informations sur les paiements, y compris les terminaux et dispositifs utilisés aux fins des services de paiement. Les services d'initiation de paiement et les services d'information sur les comptes ne sont pas des services techniques.

(17) Les services techniques ne sont pas des services de paiement en tant que tels car les prestataires de services techniques n'entrent à aucun moment en possession des fonds à transférer. C'est pourquoi ils devraient être exclus de la définition des services de paiement. Ces services devraient toutefois être soumis à certaines obligations, telles que celles relatives à la responsabilité pour défaut de soutien à l'application d'une authentification forte du client, ou à l'obligation de conclure des accords d'externalisation avec des prestataires de services de paiement dans le cas où les prestataires de services techniques devraient fournir et vérifier les éléments d'authentification forte du client. Il conviendrait également de prévoir certaines obligations relatives aux frais de résiliation des contrats-cadres lorsque des services de paiement sont proposés conjointement avec des services techniques.

(18) Compte tenu de l'évolution rapide du marché des paiements de détail et de l'apparition de nouveaux services de paiement et de nouvelles solutions de paiement, il convient d'adapter certaines des définitions figurant dans la directive (UE) 2015/2366 aux réalités du marché afin que la législation de l'Union continue de répondre aux objectifs poursuivis et reste neutre sur le plan technologique.

(19) La clarification du processus et des différentes étapes devant être suivies pour l'exécution d'une opération de paiement revêt une importance considérable pour les droits et obligations des parties à une opération de paiement et pour l'application d'une authentification forte du client. Le processus conduisant à l'exécution d'une opération de paiement est initié soit par le payeur ou pour le compte de celui-ci, soit par le bénéficiaire. Le payeur initie l'opération de paiement en passant un ordre de paiement. Une fois l'ordre de paiement passé, le prestataire de services de paiement vérifie si l'opération a été autorisée et authentifiée, y compris, s'il y a lieu, en appliquant une authentification forte du client, puis le prestataire de services de paiement valide l'ordre de paiement. Le prestataire de services de paiement prend

ensuite les mesures nécessaires pour exécuter l'opération de paiement, dont le transfert de fonds.

(20) Compte tenu des divergences de vues relevées par la Commission dans le cadre de son réexamen de la mise en œuvre de la directive (UE) 2015/2366 et soulignées par l'Autorité bancaire européenne (ABE) dans son avis du 23 juin 2022 sur le réexamen de la directive (UE) 2015/2366, il est nécessaire de clarifier la définition d'un compte de paiement. Le critère déterminant pour qu'un compte soit qualifié de compte de paiement réside dans la faculté d'effectuer quotidiennement des opérations de paiement à partir de ce compte. La possibilité d'effectuer des opérations de paiement à destination d'un tiers depuis un compte ou de bénéficier de telles opérations effectuées par un tiers est une caractéristique essentielle de la notion de compte de paiement. Un compte de paiement devrait donc être défini comme étant un compte utilisé pour envoyer et recevoir des fonds à destination et en provenance de tiers. Tout compte qui présente ces caractéristiques devrait être considéré comme un compte de paiement et être accessible pour la prestation de services d'initiation de paiement et d'information sur les comptes. Les situations dans lesquelles un autre compte intermédiaire est nécessaire pour l'exécution des opérations de paiement en provenance ou à destination de tiers ne devraient pas relever de la définition d'un compte de paiement. Les comptes d'épargne ne sont pas utilisés pour envoyer ou recevoir des fonds à destination ou en provenance d'un tiers, ce qui les exclut par conséquent de la définition d'un compte de paiement.

(21) Compte tenu de l'apparition de nouveaux types d'instruments de paiement et des incertitudes qui existent sur le marché quant à leur qualification juridique, il convient de préciser davantage la définition d'un «instrument de paiement» en fournissant quelques exemples afin d'illustrer ce qui constitue ou non un instrument de paiement, en tenant compte du principe de neutralité technologique.

(22) Bien que la communication en champ proche (NFC) permette l'initiation d'une opération de paiement, la considérer comme un «instrument de paiement» à part entière créerait quelques difficultés, par exemple en ce qui concerne l'application d'une authentification forte du client pour les paiements sans contact au point de vente et l'application du régime de responsabilité du prestataire de services de paiement. Aussi la communication en champ proche devrait-elle être plutôt considérée comme une fonctionnalité d'un instrument de paiement et non comme un instrument de paiement en tant que tel.

(23) La définition de l'«instrument de paiement» au sens de la directive (UE) 2015/2366 faisait référence à un «dispositif personnalisé». Étant donné qu'il existe des cartes prépayées sur lesquelles le nom du détenteur de l'instrument n'est pas imprimé, l'utilisation de cette référence pourrait exclure ces types de cartes du champ d'application de la définition d'un instrument de paiement. La définition d'un «instrument de paiement» devrait donc être modifiée de manière à faire référence à des dispositifs «individualisés», plutôt qu'à des dispositifs «personnalisés», et préciser que les cartes prépayées sur lesquelles le nom du détenteur de l'instrument n'est pas imprimé relèvent du champ d'application du présent règlement.

(24) Les portefeuilles numériques de type «pass-through» (portefeuilles à transfert direct), qui impliquent la tokenisation d'un instrument de paiement existant, par exemple d'une carte de paiement, doivent être considérés comme des services techniques et devraient, dès lors, être exclus de la définition de l'instrument de paiement car, selon la Commission, un jeton ne saurait être considéré, en tant que tel, comme un

instrument de paiement, mais plutôt comme une «application de paiement» au sens de l'article 2, point 21), du règlement (UE) 2015/751 du Parlement européen et du Conseil[39]. Toutefois, d'autres catégories de portefeuilles numériques, à savoir les portefeuilles électroniques prépayés tels que les «staged-wallets» (portefeuilles fonctionnant par étapes) , sur lesquels les utilisateurs peuvent stocker de l'argent en vue de futures opérations en ligne, devraient être considérées comme un instrument de paiement et leur émission comme un service de paiement.

(25) Les évolutions technologiques survenues depuis l'adoption de la directive (UE) 2015/2366 ont transformé la manière dont les services d'information sur les comptes sont fournis. Les entreprises qui proposent ces services fournissent aux utilisateurs de services de paiement des informations agrégées en ligne concernant un ou plusieurs comptes de paiement dont ils sont titulaires auprès d'un ou de plusieurs prestataires de services de paiement et qui sont accessibles via des interfaces en ligne du prestataire de services de paiement gestionnaire du compte. Les utilisateurs de services de paiement sont donc en mesure d'avoir une vue globale et structurée de leurs comptes de paiement immédiatement et à tout moment.

(26) Le réexamen auquel la Commission a procédé a mis en évidence le fait que les prestataires agréés de services d'information sur les comptes fournissent parfois des données relatives aux comptes de paiement qu'ils ont agrégées, non pas au consommateur dont ils ont reçu la permission d'accéder aux données et de les agréger, mais à une autre partie, afin de permettre à cette dernière de fournir d'autres services au consommateur en utilisant ces données. Il existe toutefois des divergences de vues quant à la question de savoir si cette activité relève du service d'information sur les comptes qui est réglementé. La Commission considère que cette évolution du modèle économique de la «banque ouverte» vers une «licence en tant que service» peut constituer une source de services innovants fondés sur les données, dans l'intérêt ultime des utilisateurs finaux. En effet, ce modèle économique permet aux utilisateurs finaux de donner accès aux données de leurs comptes de paiement afin de recevoir des services, autres que les services de paiement, tels que des prêts, des services de comptabilité et d'évaluation de la solvabilité. Il est toutefois essentiel que les utilisateurs de services de paiement sachent précisément qui a accès aux données relatives à leurs comptes de paiement, sur quelles bases juridiques et à quelle fin. Les utilisateurs de services de paiement devraient être dûment informés de la transmission de leurs données à une autre entreprise et autoriser cette transmission. Ce nouveau modèle économique fondé sur la banque ouverte nécessite une modification de la définition des services d'information sur les comptes, afin qu'il soit précisé que les informations agrégées par le prestataire agréé de services d'information sur les comptes sont susceptibles d'être transmises à un tiers pour permettre à ce tiers de fournir un autre service à l'utilisateur final, avec la permission de ce dernier. Afin de procurer aux consommateurs une protection adéquate des données relatives à leurs comptes de paiement et la sécurité juridique concernant le statut des entités ayant accès à leurs données, le service d'agrégation des données à partir de comptes de paiement devrait toujours être fourni par une entité réglementée sur le fondement d'un agrément, même lorsque les données sont finalement transmises à un autre prestataire de services.

[39] Règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte (JO L 123 du 19.5.2015, p. 1).

(27) La transmission de fonds est un service de paiement qui repose généralement sur des espèces fournies par un payeur à un prestataire de services de paiement, sans création de compte de paiement au nom du payeur ou du bénéficiaire, qui consiste à transmettre le montant correspondant à un bénéficiaire ou à un autre prestataire de services de paiement agissant pour le compte du bénéficiaire. Dans certains États membres, les supermarchés, les commerçants et autres détaillants fournissent au public un service lui permettant de régler des factures de services d'utilité publique et d'autres factures régulières du ménage. Ces services de paiement de factures devraient être traités comme une transmission de fonds.

(28) La définition de «fonds» devrait couvrir toutes les formes de monnaie de banque centrale émises pour une utilisation de détail, y compris les billets de banque et les pièces, ainsi que toute monnaie numérique de banque centrale, toute monnaie électronique et toute monnaie de banque commerciale susceptible d'être émise à l'avenir. La monnaie de banque centrale émise en vue d'une utilisation entre la banque centrale et des banques commerciales, c'est-à-dire pour une utilisation en gros, ne devrait pas relever de la définition.

(29) Le règlement (UE) 2023/1114 du 31 mai 2023 sur les marchés de crypto-actifs prévoit que les jetons de monnaie électronique sont réputés être de la monnaie électronique. Ces jetons sont donc inclus, en tant que monnaie électronique, dans la définition de «fonds» figurant dans le présent règlement.

(30) Afin de préserver la confiance des détenteurs de monnaie électronique, il est nécessaire que la monnaie électronique soit remboursable. La possibilité de remboursement n'implique pas, en soi, que les fonds reçus en échange de monnaie électronique soient considérés comme des dépôts ou d'autres fonds remboursables aux fins de la directive 2013/36/UE[40]. Le remboursement devrait être possible à tout moment, à la valeur nominale et sans qu'il soit possible de convenir d'un seuil minimal de remboursement. Le remboursement devrait, en règle générale, être gratuit. Toutefois, il devrait être possible de demander un défraiement proportionné et déterminé en fonction des coûts, sans préjudice de la législation nationale en matière fiscale ou sociale et de toutes obligations imposées à l'émetteur de monnaie électronique par d'autres législations de l'Union ou des États membres applicables, y compris les réglementations en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, ainsi que toute mesure visant le gel des fonds ou toute autre mesure particulière liée à la prévention des infractions et aux enquêtes en la matière.

(31) Les prestataires de services de paiement ont besoin d'avoir accès à des systèmes de paiement pour fournir des services de paiement aux utilisateurs. En général, ces systèmes de paiement comprennent des schémas de cartes faisant intervenir quatre parties, ainsi que les principaux systèmes permettant de traiter des virements et des prélèvements. Pour garantir, dans toute l'Union, l'égalité de traitement des différentes catégories de prestataires de services de paiement agréés, il convient de clarifier les règles régissant l'accès aux systèmes de paiement. Cet accès peut être direct ou indirect par l'intermédiaire d'un autre participant à ce système de paiement. Cet accès

[40] Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (JO L 176 du 27.6.2013, p. 338).

devrait être soumis à des exigences qui garantissent l'intégrité et la stabilité de ces systèmes de paiement. À cette fin, l'opérateur de système de paiement devrait procéder à une évaluation des risques d'un prestataire de services de paiement qui introduit une demande de participation directe; cette évaluation des risques devrait porter sur tous les risques pertinents, y compris, s'il y a lieu, le risque de règlement, le risque opérationnel, le risque de crédit, le risque de liquidité et le risque d'entreprise. Chaque prestataire de services de paiement candidat à une participation à un système de paiement devrait supporter le risque lié à son propre choix de système et apporter la preuve au système de paiement que son organisation interne est suffisamment solide pour faire face à ces types de risques. Les opérateurs de systèmes de paiement ne devraient rejeter la candidature à une participation directe déposée par un prestataire de services de paiement que si ce dernier n'est pas en mesure de respecter les règles du système ou présente un niveau de risque inacceptable.

(32) Les opérateurs de systèmes de paiement devraient avoir mis en place des règles et procédures d'accès proportionnées, objectives, non discriminatoires et transparentes. Les opérateurs de systèmes de paiement ne devraient pas opérer de discrimination à l'égard des établissements de paiement en ce qui concerne leur participation dès lors que les règles du système peuvent être respectées et qu'il n'y a pas de risque inacceptable pour le système. Ces systèmes comprennent, entre autres, ceux désignés au titre de la directive 98/26/CE du Parlement européen et du Conseil[41]. Dans les cas où le système de paiement considéré fait déjà l'objet d'une surveillance par le système européen de banques centrales en vertu du règlement (UE) nº 795/2014 de la Banque centrale européenne[42], la ou les banques centrales qui exercent cette surveillance devraient contrôler le respect de ces règles dans le cadre de leur surveillance. Dans le cas d'autres systèmes de paiement, les États membres devraient désigner des autorités compétentes nationales chargées de veiller à ce que les opérateurs de l'infrastructure des systèmes de paiement respectent ces exigences.

(33) Pour garantir une concurrence équitable entre prestataires de services de paiement, un participant à un système de paiement qui fournit des services liés à un tel système à un prestataire de services de paiement agréé ou enregistré devrait aussi, sur demande, donner accès à ces services, de manière objective, proportionnée et non discriminatoire, à tout autre prestataire de services de paiement agréé ou enregistré.

(34) Les dispositions relatives à l'accès aux systèmes de paiement ne devraient pas s'appliquer aux systèmes dont un seul prestataire de services de paiement assure la mise en œuvre et le fonctionnement. Ces systèmes de paiement peuvent fonctionner soit en concurrence directe avec d'autres systèmes de paiement, soit, de manière plus courante, dans une niche du marché qui n'est pas couverte par d'autres systèmes de paiement. Ils couvrent les schémas faisant intervenir trois parties, tels que les schémas de cartes tripartites, dans la mesure où ils ne fonctionnent jamais comme des schémas de cartes de facto quadripartites, notamment en faisant appel à des titulaires de licence, à des agents ou à des partenaires de comarquage. Ces systèmes couvrent aussi en général les services de paiement proposés par des opérateurs de télécommunications,

---

41 Directive 98/26/CE du Parlement européen et du Conseil du 19 mai 1998 concernant le caractère définitif du règlement dans les systèmes de paiement et de règlement des opérations sur titres (JO L 166 du 11.6.1998, p. 45).

42 Règlement (UE) nº 795/2014 de la Banque centrale européenne du 3 juillet 2014 concernant les exigences de surveillance applicables aux systèmes de paiement d'importance systémique (JO L 217 du 23.7.2014, p. 16).

pour lesquels le gestionnaire du système est à la fois le prestataire de services de paiement du payeur et du bénéficiaire, ainsi que les systèmes internes des groupes bancaires. Pour stimuler la concurrence que ces systèmes de paiement fermés peuvent apporter par rapport aux systèmes de paiement ordinaires en place, il conviendrait de ne pas accorder à des tiers l'accès à ces systèmes de paiement fermés exclusifs. Néanmoins, ces systèmes fermés devraient continuer d'être soumis aux règles nationales et de l'Union en matière de concurrence, ce qui peut obliger à accorder l'accès à ces systèmes pour maintenir une concurrence effective sur les marchés de paiement.

(35) Les établissements de paiement doivent être en mesure d'ouvrir et de gérer un compte auprès d'un établissement de crédit afin de satisfaire à leurs obligations pour l'agrément en ce qui concerne la protection des fonds de la clientèle. Toutefois, comme l'a notamment montré l'ABE dans son avis du 5 janvier 2022[43], malgré les dispositions relatives aux comptes des établissements de paiement auprès d'une banque commerciale figurant dans la directive (UE) 2015/2366, certains établissements de paiement ou entreprises qui introduisent une demande d'agrément en tant qu'établissement de paiement sont toujours confrontés à des pratiques de certains établissements de crédit qui soit refusent de leur ouvrir un compte, soit clôturent leur compte lorsqu'il en existe un, en invoquant un risque perçu comme plus élevé de blanchiment de capitaux ou de financement du terrorisme. Ces pratiques dites de «réduction des risques» créent d'importantes difficultés en matière de concurrence pour les établissements de paiement.

(36) Les établissements de crédit devraient donc fournir un compte de paiement aux établissements de paiement et aux demandeurs d'un agrément en tant qu'établissement de paiement, ainsi qu'à leurs agents et distributeurs, sauf dans des cas exceptionnels où il existe des motifs sérieux de refuser l'accès. Il est nécessaire d'inclure dans cette disposition les demandeurs d'un agrément en tant qu'établissement de paiement, étant donné qu'un compte bancaire sur lequel les fonds des clients peuvent être protégés est une condition préalable à l'obtention d'un agrément d'établissement de paiement. Les motifs de refus devraient être des motifs sérieux de soupçon d'activités illégales exercées par l'établissement de paiement ou par son intermédiaire, ou un modèle économique ou un profil de risque entraînant des risques graves ou des coûts de mise en conformité excessifs pour l'établissement de crédit. Par exemple, les modèles économiques dans lesquels les établissements de paiement recourent à un vaste réseau d'agents peuvent engendrer des coûts de mise en conformité importants en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme (LBC/FT). Un établissement de paiement devrait avoir le droit de former un recours contre un refus d'un établissement de crédit auprès d'une autorité compétente désignée par un État membre. Afin de faciliter l'exercice de ce droit de recours, les établissements de crédit devraient motiver par écrit et de manière détaillée tout refus de fournir un compte ou toute clôture ultérieure d'un compte. Cette motivation devrait faire mention d'éléments particuliers relatifs à l'établissement de paiement concerné, et non de considérations générales ou génériques. Afin de faciliter le traitement par les autorités compétentes des recours formés contre un refus d'ouverture de compte ou une clôture de compte et contre la motivation de l'une ou de l'autre décision, l'ABE devrait élaborer des normes techniques d'exécution harmonisant la présentation de ces motivations.

---

[43] Autorité bancaire européenne EBA/Op/2022/01.

(37) Afin de faire des choix éclairés et de pouvoir choisir facilement leur prestataire de services de paiement au sein de l'Union, les utilisateurs de services de paiement devraient recevoir des informations comparables et claires sur les services de paiement. Afin que les utilisateurs de services de paiement reçoivent les informations nécessaires, suffisantes et compréhensibles relatives tant au contrat de services de paiement qu'aux opérations de paiement elles-mêmes, il convient de préciser et d'harmoniser les obligations des prestataires de services de paiement en ce qui concerne la fourniture d'informations aux utilisateurs de services de paiement.

(38) Lorsqu'ils fournissent les informations requises aux utilisateurs de services de paiement, les prestataires de services de paiement devraient tenir compte des besoins des utilisateurs de services de paiement ainsi que des aspects pratiques et du rapport coût-efficacité en fonction du contrat de services de paiement concerné. Les prestataires de services de paiement devraient soit communiquer activement les informations au moment opportun, sans autre sollicitation de la part de l'utilisateur de services de paiement, soit mettre ces informations à la disposition des utilisateurs de services de paiement à leur demande. Dans la seconde situation, les utilisateurs de services de paiement devraient prendre activement des mesures afin d'obtenir les informations, notamment en les réclamant explicitement aux prestataires de services de paiement, en consultant leur compte bancaire en ligne ou en introduisant leur carte bancaire dans un appareil imprimant les extraits de comptes bancaires. À ces fins, les prestataires de services de paiement devraient veiller à ce qu'il soit possible d'avoir accès aux informations et à ce que ces informations soient mises à la disposition des utilisateurs de services de paiement.

(39) Ne se trouvant pas dans la même situation de vulnérabilité, consommateurs et entreprises n'ont pas besoin du même niveau de protection. Alors qu'il importe de garantir les droits des consommateurs au moyen de dispositions auxquelles il n'est pas possible de déroger par contrat, il est judicieux de laisser les entreprises et les organisations en décider autrement lorsqu'elles n'ont pas affaire à des consommateurs. Les microentreprises, au sens de la recommandation 2003/361/CE de la Commission[44], peuvent être traitées de la même manière que les consommateurs. Certaines règles devraient toujours s'appliquer, quel que soit le statut de l'utilisateur.

(40) Afin de maintenir un niveau élevé de protection des consommateurs, ceux-ci devraient avoir le droit de recevoir gratuitement des informations sur les conditions et les prix des services avant d'être liés par un quelconque contrat de services de paiement. Afin de permettre aux consommateurs de comparer les services et les conditions proposés par les prestataires de services de paiement et, en cas de litige, de vérifier leurs droits et obligations contractuels, les consommateurs devraient être en mesure de demander ces informations et le contrat-cadre sur support papier, sans frais et à tout moment au cours de la relation contractuelle.

(41) Afin d'accroître le niveau de transparence, les prestataires de services de paiement devraient communiquer au consommateur des informations de base sur les opérations de paiement effectuées, sans frais supplémentaires. Dans le cas d'une opération de paiement isolée, le prestataire de services de paiement ne devrait pas facturer ces informations séparément. De même, les prestataires de services de paiement devraient fournir gratuitement et mensuellement les informations ultérieures relatives aux opérations de paiement au titre d'un contrat-cadre. Cependant, compte tenu de

44 JO L 124 du 20.5.2003, p. 36.

l'importance que revêt la transparence en matière de tarification et des besoins différents des clients, les parties contractantes devraient pouvoir, d'un commun accord, fixer les frais qu'entraînerait la communication d'informations supplémentaires ou plus fréquentes.

(42) Les instruments de paiement relatifs à des montants de faible valeur devraient constituer un moyen simple et bon marché de régler des biens et des services de faible prix et ne devraient pas être soumis à des exigences excessives. Les exigences d'information et les règles relatives à l'exécution qui leur sont applicables devraient donc être limitées aux informations essentielles, compte tenu également des capacités techniques que l'on est en droit d'attendre d'instruments spécialisés dans les paiements de faible valeur. Malgré ce régime allégé, les utilisateurs de services de paiement devraient bénéficier d'une protection adéquate étant donné les risques limités que présentent ces instruments de paiement, en particulier en ce qui concerne les instruments de paiement prépayés.

(43) Pour les opérations de paiement isolées, les informations essentielles devraient toujours être communiquées à l'initiative des prestataires de services de paiement. Comme les payeurs sont en général présents lorsqu'ils donnent l'ordre de paiement, il ne devrait pas être nécessaire que les informations soient toujours fournies sur support papier ou sur un autre support durable. Les prestataires de services de paiement devraient pouvoir communiquer les informations verbalement ou les rendre aisément accessibles d'une autre manière, y compris en affichant les conditions sur un panneau d'information dans leurs locaux. Il conviendrait également d'indiquer où il est possible de trouver d'autres informations plus détaillées, notamment sur le site internet. Toutefois, lorsque le consommateur en fait la demande, les prestataires de services de paiement devraient également fournir les informations essentielles sur support papier ou sur un autre support durable.

(44) Les informations requises devraient être proportionnées aux besoins des utilisateurs. Les exigences d'information applicables à une opération de paiement isolée devraient être différentes de celles applicables à un contrat-cadre prévoyant une série d'opérations de paiement.

(45) Pour pouvoir choisir en connaissance de cause, les utilisateurs de services de paiement devraient être en mesure de comparer les frais des distributeurs automatiques de billets (DAB) avec ceux pratiqués par d'autres prestataires. Afin d'accroître la transparence des frais de DAB facturés aux utilisateurs de services de paiement, les prestataires de services de paiement devraient fournir à ces utilisateurs des informations sur tous les frais applicables aux retraits effectués aux DAB nationaux dans différentes situations, en fonction du DAB auquel les utilisateurs de services de paiement retirent des espèces.

(46) Les contrats-cadres et les opérations de paiement auxquels ils s'appliquent sont plus courants et plus importants du point de vue économique que les opérations de paiement isolées. S'il existe un compte de paiement ou un instrument de paiement spécifique, un contrat-cadre s'impose. Dès lors, les exigences relatives aux informations préalables sur les contrats-cadres devraient être détaillées, et ces informations devraient toujours être fournies sur support papier ou sur un autre support durable. Toutefois, les prestataires de services de paiement et les utilisateurs de services de paiement devraient pouvoir arrêter, dans le contrat-cadre, les modalités de la transmission des informations fournies par la suite sur les opérations de paiement effectuées.

(47) Les dispositions contractuelles ne devraient pas introduire de discriminations en raison de la nationalité ou du lieu de résidence à l'égard de consommateurs qui résident légalement dans l'Union. Lorsqu'un contrat-cadre prévoit le droit de bloquer un instrument de paiement pour des raisons objectivement motivées, le prestataire de services de paiement ne devrait pas pouvoir invoquer ce droit simplement parce que l'utilisateur de services de paiement a changé de lieu de résidence dans l'Union.

(48) Afin de garantir un niveau élevé de protection des consommateurs, les États membres devraient être en mesure, dans l'intérêt du consommateur, d'introduire ou de maintenir des restrictions ou des interdictions concernant les modifications unilatérales des termes d'un contrat-cadre, par exemple lorsqu'une modification n'est pas justifiée.

(49) Afin de faciliter la mobilité des utilisateurs de services de paiement, ces derniers devraient pouvoir résilier sans frais un contrat-cadre. Cependant, pour les contrats résiliés par les utilisateurs de services de paiement moins de six mois après leur entrée en vigueur, les prestataires de services de paiement devraient être autorisés à imputer des frais en fonction des coûts dus à la résiliation du contrat-cadre par l'utilisateur. Lorsque, en vertu d'un contrat-cadre, des services de paiement sont proposés conjointement avec des services techniques qui soutiennent la prestation de services de paiement, tels que la location de terminaux utilisés pour les services de paiement, les utilisateurs de services de paiement ne devraient pas être prisonniers de leur prestataire de services de paiement au moyen de conditions plus onéreuses fixées dans les clauses contractuelles régissant les services techniques. Afin de préserver la concurrence, ces clauses contractuelles devraient être soumises aux mêmes exigences relatives aux frais de résiliation que le contrat-cadre. Pour les consommateurs, le délai de préavis convenu ne devrait pas être supérieur à un mois et, pour les prestataires de services de paiement, ce délai ne devrait pas être inférieur à deux mois. Ces règles devraient être sans préjudice de l'obligation qui est faite au prestataire de services de paiement de résilier le contrat de services de paiement dans des situations exceptionnelles en application d'une autre législation du droit de l'Union ou de droit national pertinente, telle que les législations relatives à la lutte contre le blanchiment de capitaux ou le financement du terrorisme, ou toute action visant au gel de fonds, ou toute mesure particulière liée à la prévention d'infractions ou aux enquêtes en la matière.

(50) Pour permettre la comparabilité, les frais de conversion monétaire estimés pour les virements et les transmissions de fonds effectués au sein de l'Union et de l'Union vers un pays tiers devraient être exprimés de la même manière, à savoir en marge de pourcentage sur les derniers taux de change de référence de l'euro disponibles émis par la Banque centrale européenne (BCE). Lorsqu'il est fait référence aux «frais» dans le présent règlement, cela devrait également englober, s'il y a lieu, les frais de «conversion monétaire».

(51) L'expérience a montré que le partage des frais entre payeur et bénéficiaire constituait la solution la plus efficiente, car elle facilite le traitement entièrement automatisé des paiements. Il conviendrait donc de prévoir que les frais sont directement prélevés sur le payeur et le bénéficiaire par leurs prestataires de services de paiement respectifs. Le montant des frais prélevé peut aussi être nul car les règles appliquées ne devraient pas avoir d'incidence sur la pratique selon laquelle un prestataire de services de paiement ne facture pas aux consommateurs le fait de créditer leur compte. De même, selon les clauses du contrat, un prestataire de services de paiement peut ne facturer l'utilisation du service de paiement qu'au bénéficiaire, auquel cas aucun frais n'est imputé au payeur. Il est possible que les systèmes de paiement imposent des frais au moyen d'une cotisation d'abonnement. Les dispositions concernant le montant transféré ou

les frais prélevés n'ont aucun effet direct sur les tarifs appliqués entre les prestataires de services de paiement ou les autres intermédiaires.

(52) La surfacturation consiste en des frais que les commerçants facturent aux consommateurs en plus du prix demandé pour les biens et les services lorsque les consommateurs utilisent un certain mode de paiement. L'une des raisons de la surfacturation est d'orienter les consommateurs vers des instruments de paiement moins chers ou plus efficaces, favorisant ainsi la concurrence entre différents modes de paiement. Dans le cadre du régime instauré par la directive (UE) 2015/2366, les bénéficiaires ont été empêchés d'appliquer des frais pour l'utilisation d'instruments de paiement pour lesquels les commissions d'interchange sont régies par le chapitre II du règlement (UE) 2015/751, c'est-à-dire pour les cartes de débit et de crédit des consommateurs émises dans le cadre de schémas de cartes quadripartites, et pour les services de paiement auxquels s'applique le règlement (UE) nº 260/2012 du Parlement européen et du Conseil[45], c'est-à-dire pour les opérations de virement et de prélèvement libellées en euros au sein de l'Union. Les États membres étaient autorisés par la directive (UE) 2015/2366 à continuer d'interdire ou de limiter le droit du bénéficiaire d'appliquer des frais compte tenu de la nécessité d'encourager la concurrence et de favoriser l'utilisation de moyens de paiement efficaces.

(53) Les éléments recueillis lors de du réexamen de la directive (UE) 2015/2366 montrent que les règles actuelles relatives aux frais sont appropriées et ont eu une incidence positive. Il n'existe pas de besoin impérieux de poursuivre l'harmonisation des pratiques tarifaires entre les États membres, étant donné que l'interdiction actuelle de surfacturation s'applique déjà à une très grande partie des paiements dans l'Union. On estime en effet que 95 % des paiements par carte sont soumis à ladite interdiction. En outre, lorsqu'une surfacturation est appliquée, elle est plafonnée au coût réel supporté par le commerçant. Toutefois, lors de son réexamen de la directive (UE) 2015/2366, la Commission a constaté des interprétations divergentes concernant les instruments de paiement soumis à l'interdiction de surfacturation. Il est donc nécessaire d'étendre explicitement l'interdiction de surfacturation à tous les virements et prélèvements, et pas seulement à ceux auxquels s'applique le règlement (UE) nº 260/2012, comme c'était le cas dans le cadre de la directive (UE) 2015/2366.

(54) Les services d'information sur les comptes et les services d'initiation de paiement, souvent dénommés collectivement «services de banque ouverte», sont des services de paiement qui supposent l'accès aux données d'un utilisateur de services de paiement de la part de prestataires de services de paiement qui ne détiennent pas les fonds du titulaire du compte ni ne gèrent de comptes de paiement. Les services d'information sur les comptes permettent, à la demande d'un utilisateur de services de paiement, d'agréger en un seul endroit les données de ce dernier provenant de différents prestataires de services de paiement gestionnaires de comptes. Les services d'initiation de paiement permettent d'initier un paiement à partir du compte de l'utilisateur, tel qu'un virement ou un prélèvement, d'une manière pratique pour l'utilisateur et le bénéficiaire, sans recourir à un instrument tel qu'une carte de paiement.

(55) Les prestataires de services de paiement gestionnaires de comptes devraient permettre aux prestataires de services d'information sur les comptes et de services d'initiation de

[45] Règlement (UE) nº 260/2012 du Parlement européen et du Conseil du 14 mars 2012 établissant des exigences techniques et commerciales pour les virements et les prélèvements en euros et modifiant le règlement (CE) nº 924/2009 (JO L 94 du 30.3.2012, p. 22).

paiement d'avoir accès aux données relatives aux comptes de paiement si l'utilisateur de services de paiement peut accéder au compte de paiement en ligne et qu'il a accordé une permission pour cet accès. La directive (UE) 2015/2366 était fondée sur le principe de l'accès aux données relatives aux comptes de paiement sans qu'il soit nécessaire d'établir une relation contractuelle entre le prestataire de services de paiement gestionnaire du compte et les prestataires de services d'information sur les comptes et de services d'initiation de paiement, ce qui a eu pour effet d'empêcher, dans la pratique, la facturation de l'accès aux données. Depuis l'application de la directive (UE) 2015/2366, l'accès aux données dans le cadre de la banque ouverte s'effectue sur une telle base non contractuelle et sans frais. Si les services réglementés d'accès aux données devaient être soumis à des frais, alors qu'il n'y avait pas de frais jusqu'à présent, l'incidence sur la poursuite de la prestation de ces services, partant sur la concurrence et l'innovation sur les marchés des paiements, pourrait être très importante. Ce principe devrait dès lors être maintenu. Le maintien de cette approche est conforme aux chapitres III et IV de la proposition de règlement fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données)[46], en particulier à l'article 9, paragraphe 3, de ladite proposition sur la compensation, que le présent règlement ne remet pas en cause. La proposition de règlement de la Commission sur l'accès aux données financières (FIDA) prévoit une possibilité de compensation pour l'accès aux données relevant du règlement FIDA. Ce régime serait donc différent de celui réglé par le présent règlement. Cette différence de traitement est justifiée par le fait que, contrairement à l'accès aux données relatives aux comptes de paiement, qui est réglementé par le droit de l'Union depuis l'entrée en vigueur de la directive (UE) 2015/2366, l'accès aux autres données financières n'est pas encore soumis à la réglementation de l'Union. Il n'y a donc pas de risque de perturbation car, contrairement à l'accès aux données relatives aux comptes de paiement, il s'agit d'un marché émergent, qui sera réglementé pour la première fois par le règlement FIDA.

(56) Les prestataires de services de paiement gestionnaires de comptes et les prestataires de services d'information sur les comptes et de services d'initiation de paiement peuvent établir une relation contractuelle, y compris dans le cadre d'un accord contractuel multilatéral (par exemple un schéma), avec possibilité de compensation, pour encadrer l'accès aux données relatives aux comptes de paiement et la prestation de services de banque ouverte autres que ceux requis par le présent règlement. Un exemple de ces services à valeur ajoutée proposés au moyen d'interfaces de programmation d'applications (API) dites «premium» est la possibilité de programmer des paiements récurrents variables futurs. Toute compensation pour ces services devrait être conforme aux chapitres III et IV de la proposition de règlement sur les données une fois que ce texte sera entré en application, notamment en ce qui concerne l'article 9, paragraphes 1 et 2, sur la compensation. Il devrait toujours être possible, pour les prestataires de services d'information sur les comptes et de services d'initiation de paiement, d'avoir accès aux données relatives aux comptes de paiement régies par le présent règlement sans obligation de relation contractuelle, et dès lors sans frais, même dans les cas où un accord contractuel multilatéral (par exemple un schéma) existe et où les mêmes données sont également disponibles dans le cadre dudit accord.

[46] Proposition de règlement fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données). COM(2022) 68 final.

(57) Afin de garantir un niveau élevé de sécurité en matière d'accès aux données et d'échange de données, l'accès aux comptes de paiement et aux données qu'ils contiennent devrait, sauf circonstances particulières, être accordé aux prestataires de services d'information sur les comptes et de services d'initiation de paiement par l'intermédiaire d'une interface conçue et spécifique à des fins de banque ouverte, telle qu'une API. À cette fin, le prestataire de services de paiement gestionnaire du compte devrait établir une communication sécurisée avec les prestataires de services d'information sur les comptes et de services d'initiation de paiement. Afin d'éviter toute incertitude concernant l'identité des personnes qui ont accès aux données de l'utilisateur de services de paiement, l'interface spécifique devrait permettre aux prestataires de services d'information sur les comptes et de services d'initiation de paiement de s'identifier auprès du prestataire de services de paiement gestionnaire du compte et de recourir à toutes les procédures d'authentification que le prestataire de services de paiement gestionnaire du compte propose à l'utilisateur de services de paiement. Les prestataires de services d'information sur les comptes et de services d'initiation de paiement devraient, en règle générale, utiliser l'interface spécifique pour accéder aux données et ne devraient donc pas utiliser l'interface client d'un prestataire de services de paiement gestionnaire du compte pour accéder à ces données, sauf en cas de défaillance ou d'indisponibilité de l'interface spécifique dans les conditions énoncées dans le présent règlement. En pareilles circonstances, la continuité de leurs activités serait compromise par leur incapacité à accéder aux données pour lesquelles ils ont obtenu une permission. Il est indispensable que les prestataires de services d'information sur les comptes et de services d'initiation de paiement soient à tout moment en mesure d'accéder aux données dont ils ont impérativement besoin pour offrir des services à leurs clients.

(58) Afin de faciliter la bonne utilisation de l'interface spécifique, ses spécifications techniques devraient être dûment documentées et un résumé devrait être mis à la disposition du public par le prestataire de services de paiement gestionnaire du compte. Afin de permettre aux prestataires de services de banque ouverte de préparer correctement leur accès futur et de résoudre tout problème technique éventuel, le prestataire de services de paiement gestionnaire du compte devrait permettre aux prestataires de services d'information sur les comptes et de services d'initiation de paiement de tester une interface avant la date d'activation de cette interface. Seuls les prestataires agréés de services d'information sur les comptes et de services d'initiation de paiement devraient avoir accès aux données relatives aux comptes de paiement au moyen de cette interface, mais les demandeurs d'agrément en tant que prestataires de services d'information sur les comptes et de prestataires de services d'initiation de paiement devraient pouvoir consulter les spécifications techniques. Afin de garantir l'interopérabilité des différentes solutions de communication technologiques, l'interface devrait utiliser des normes de communication mises au point par des organisations européennes ou internationales de normalisation telles que le Comité européen de normalisation (CEN) ou l'Organisation internationale de normalisation (ISO).

(59) Pour que les prestataires de services d'information sur les comptes et de services d'initiation de paiement assurent à tout moment la continuité de leurs activités et puissent fournir des services de haute qualité à leurs clients, l'interface spécifique qu'ils sont censés utiliser doit satisfaire à des exigences élevées sur le plan des performances et des fonctionnalités. Elle devrait au minimum garantir la «parité des données» avec l'interface client que le prestataire de services de paiement gestionnaire de comptes fournit à ses utilisateurs et, par conséquent, inclure les données relatives

aux comptes de paiement qui sont également à la disposition des utilisateurs de services de paiement dans l'interface qui leur est fournie par le prestataire de services de paiement gestionnaire de comptes. En ce qui concerne les services d'initiation de paiement, l'interface spécifique devrait permettre non seulement l'initiation de paiements isolés, mais aussi d'ordres permanents et de prélèvements. Des exigences plus détaillées relatives aux interfaces spécifiques devraient être définies dans les normes techniques de réglementation élaborées par l'ABE.

(60) Compte tenu de l'incidence catastrophique qu'une indisponibilité prolongée d'une interface spécifique aurait sur la continuité des activités des prestataires de services d'information sur les comptes et de services d'initiation de paiement, les prestataires de services de paiement gestionnaires de comptes devraient remédier à une telle indisponibilité sans tarder. Les prestataires de services de paiement gestionnaires de comptes devraient informer, dans les plus brefs délais, les prestataires de services d'information sur les comptes et de services d'initiation de paiement de toute indisponibilité de leur interface spécifique et des mesures prises pour y remédier. En cas d'indisponibilité d'une interface spécifique et lorsque le prestataire de services de paiement gestionnaire du compte ne propose aucune autre solution efficace, les prestataires de services d'information sur les comptes et de services d'initiation de paiement devraient être en mesure de préserver la continuité de leurs activités. Ils devraient être autorisés à demander à leur autorité compétente nationale de pouvoir utiliser l'interface que le prestataire de services de paiement gestionnaire de comptes fournit à ses utilisateurs jusqu'à ce que l'interface spécifique soit à nouveau disponible. L'autorité compétente devrait prendre sa décision sans tarder après réception de la demande. Dans l'attente de la décision de l'autorité, les prestataires de services d'information sur les comptes et de services d'initiation de paiement dont émane la demande devraient être autorisés à utiliser temporairement l'interface que le prestataire de services de paiement gestionnaire de comptes fournit à ses utilisateurs. L'autorité compétente concernée devrait fixer un délai au prestataire de services de paiement gestionnaire de comptes pour qu'il rétablisse le bon fonctionnement de l'interface spécifique et prévoir la possibilité de sanctions en cas de non-respect de ce délai. Tous les prestataires de services d'information sur les comptes et de services d'initiation de paiement, et pas seulement ceux qui ont introduit la demande, devraient être autorisés à avoir accès aux données dont ils ont besoin pour assurer la continuité de leurs activités.

(61) Un tel accès direct temporaire ne devrait pas avoir d'effet négatif sur les consommateurs. Aussi les prestataires de services d'information sur les comptes et de services d'initiation de paiement devraient-ils toujours dûment s'identifier et respecter toutes leurs obligations, telles que les limites de la permission qui leur a été accordée, et ne devraient notamment accéder qu'aux données dont ils ont besoin pour satisfaire à leurs obligations contractuelles et fournir le service réglementé. Il ne devrait jamais être possible d'avoir accès aux données relatives aux comptes de paiement sans identification correcte (c'est-à-dire en pratiquant ce que l'on appelle la «capture de données d'écran» ou le «screen scraping»).

(62) Étant donné que la mise en place d'une interface spécifique pourrait, pour certains prestataires de services de paiement gestionnaires de comptes, être considérée comme une charge disproportionnée, une autorité compétente nationale devrait être en mesure d'exempter un prestataire de services de paiement gestionnaire de comptes, à sa demande, de l'obligation de disposer d'une interface spécifique d'accès aux données, et de l'autoriser soit à ne proposer un accès aux données de paiement que par

l'intermédiaire de son «interface client», soit à ne proposer aucune interface d'accès aux données de banque ouverte. L'accès aux données par l'intermédiaire de l'interface client (sans interface spécifique) peut être approprié dans le cas d'un prestataire de services de paiement gestionnaire de comptes de très petite taille, pour lequel une interface spécifique représenterait une charge financière et une charge en ressources importantes. Le fait d'être exempté de l'obligation de maintenir une interface d'accès aux données nécessaires à la banque ouverte peut se justifier lorsque le prestataire de services de paiement gestionnaire de comptes a un modèle économique particulier, dans le cadre duquel, par exemple, les services de banque ouverte ne présenteraient pas d'intérêt pour ses clients. Des critères détaillés concernant l'octroi de ces différents types de décisions d'exemption devraient être définis dans les normes techniques de réglementation élaborées par l'ABE.

(63) Pour exploiter pleinement le potentiel de la banque ouverte dans l'Union, il est essentiel d'empêcher tout traitement discriminatoire des prestataires de services d'information sur les comptes et de services d'initiation de paiement par les prestataires de services de paiement gestionnaires de comptes. Lorsque l'utilisateur de services de paiement décide d'avoir recours aux services d'un prestataire de services d'information sur les comptes ou d'un prestataire de services d'initiation de paiement, le prestataire de services de paiement gestionnaire du compte devrait traiter cet ordre de la même manière qu'il traiterait une telle demande si elle était faite directement par l'utilisateur de services de paiement dans son «interface client», à moins que le prestataire de services de paiement gestionnaire du compte n'ait des raisons objectives de traiter différemment cette demande d'accès au compte, notamment des soupçons sérieux de fraude.

(64) En ce qui concerne la prestation de services d'initiation de paiement, le prestataire de services de paiement gestionnaire du compte devrait fournir au prestataire de services d'initiation de paiement toutes les informations dont il dispose sur l'exécution de l'opération de paiement immédiatement après la réception de l'ordre de paiement. Il arrive parfois que le prestataire de services de paiement gestionnaire du compte prenne connaissance d'informations supplémentaires après avoir reçu l'ordre de paiement, mais avant d'avoir exécuté l'opération de paiement. Lorsque ces informations supplémentaires présentent un intérêt pour l'ordre de paiement et pour l'exécution de l'opération de paiement, le prestataire de services de paiement gestionnaire du compte devrait les communiquer au prestataire de services d'initiation de paiement. Le prestataire de services d'initiation de paiement devrait bénéficier des informations nécessaires pour évaluer les risques de non-exécution de l'opération initiée. Ces informations sont indispensables pour permettre au prestataire de services d'initiation de paiement d'offrir au bénéficiaire pour le compte duquel il initie l'opération un service dont la qualité puisse concurrencer d'autres moyens de paiement électronique mis à la disposition du bénéficiaire, dont les cartes de paiement.

(65) Pour renforcer la confiance dans la banque ouverte, il est essentiel que les utilisateurs de services de paiement qui utilisent les services d'information sur les comptes et d'initiation de paiement aient la pleine maîtrise de leurs données et aient accès à des informations claires sur les permissions d'accès aux données qu'ils ont accordées aux prestataires de services de paiement, notamment la finalité de la permission et les catégories de données relatives aux comptes de paiement qui sont concernées, telles que les données d'identité du compte, l'opération et le solde du compte. Les prestataires de services de paiement gestionnaires de comptes devraient par conséquent mettre à la disposition des utilisateurs de services de paiement qui

recourent à ces services un «tableau de bord» pour qu'ils puissent contrôler et retirer ou rétablir l'accès aux données qu'ils ont accordé aux prestataires de services de «banque ouverte». Les permissions d'initiation de paiements isolés ne devraient pas figurer sur ce tableau de bord. Un tableau de bord peut ne pas permettre à un utilisateur de services de paiement d'établir de nouvelles permissions d'accès aux données en faveur d'un prestataire de services d'information sur les comptes ou de services d'initiation de paiement auquel aucun accès aux données n'a été accordé antérieurement. Les prestataires de services de paiement gestionnaires de comptes devraient informer rapidement les prestataires de services d'information sur les comptes et de services d'initiation de paiement de tout retrait de leur accès aux données. Les prestataires de services d'information sur les comptes et de services d'initiation de paiement devraient informer rapidement les prestataires de services de paiement gestionnaires de comptes des permissions d'accès aux données, nouvelles ou rétablies, accordées par les utilisateurs de services de paiement, y compris de la durée de validité de la permission et de la finalité de celle-ci (en particulier si les données sont consolidées dans l'intérêt de l'utilisateur ou en vue de leur transmission à un tiers). Un prestataire de services de paiement gestionnaire du compte ne devrait, en aucune façon, encourager un utilisateur de services de paiement à retirer les permissions qu'il a accordées à des prestataires de services d'information sur les comptes et de services d'initiation de paiement. Le tableau de bord devrait avertir l'utilisateur de services de paiement par une formule type du risque d'éventuelles conséquences contractuelles en cas de retrait de l'accès aux données accordé à un prestataire de services de banque ouverte, étant donné que le tableau de bord ne gère pas la relation contractuelle entre l'utilisateur et un prestataire de services de banque ouverte mais qu'il appartient à l'utilisateur de services de paiement de vérifier ce risque. Un tableau de bord des permissions devrait donner aux clients les moyens de gérer, de manière éclairée et impartiale, les permissions qu'ils accordent et donner aux clients un haut niveau de maîtrise de la manière dont leurs données à caractère personnel et non personnel sont utilisées. Un tableau de bord des permissions devrait tenir compte, s'il y a lieu, des exigences en matière d'accessibilité prévues par la directive (UE) 2019/882 du Parlement européen et du Conseil.

(66) Le réexamen de la directive (UE) 2015/2366 a révélé que les prestataires de services d'information sur les comptes et de services d'initiation de paiement étaient toujours exposés à de nombreux obstacles injustifiés, malgré le niveau d'harmonisation atteint et l'interdiction de ces obstacles imposée par l'article 32, paragraphe 3, du règlement délégué (UE) 2018/389 de la Commission[47]. Ces obstacles entravent encore considérablement l'exploitation du plein potentiel de la banque ouverte dans l'Union. Ils sont régulièrement signalés par les prestataires de services d'information sur les comptes et de services d'initiation de paiement aux autorités de surveillance et de régulation et à la Commission. Ils ont été analysés par l'ABE dans son avis de juin 2020 sur «*les entraves au sens de l'article 32, paragraphe 3, des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication*». Malgré les efforts de clarification entrepris, de nombreuses incertitudes subsistent, tant sur le marché qu'au sein des autorités de surveillance, sur ce qui constitue une «entrave interdite» aux services de

[47] Règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication (JO L 69 du 13.3.2018, p. 23).

banque ouverte réglementés. Il est donc indispensable de fournir une liste claire et non exhaustive de ces entraves interdites à la banque ouverte, en s'appuyant notamment sur les travaux menés par l'ABE.

(67) L'obligation de préserver la sécurité des données de sécurité personnalisées est cruciale pour protéger les fonds de l'utilisateur de services de paiement et pour limiter les risques liés à la fraude et à l'accès non autorisé aux comptes de paiement. Cependant, les conditions et autres obligations imposées aux utilisateurs de services de paiement par les prestataires de services de paiement pour ce qui est de préserver la sécurité des données de sécurité personnalisées ne devraient pas être libellées de telle façon que les utilisateurs de services de paiement seraient empêchés de profiter des services proposés par d'autres prestataires de services de paiement, y compris des services d'initiation de paiement et des services d'information sur les comptes. Les conditions en question ne devraient contenir aucune disposition qui compliquerait d'une quelconque façon l'utilisation des services de paiement d'autres prestataires de services de paiement agréés ou enregistrés en vertu de la directive (UE) XXX (DSP3). Il convient en outre de préciser qu'en ce qui concerne les activités des prestataires de services d'initiation de paiement et des prestataires de services d'information sur les comptes, le nom du titulaire du compte et le numéro de compte ne constituent pas des données de paiement sensibles.

(68) Pour atteindre entièrement ses objectifs, la «banque ouverte» nécessite un contrôle rigoureux et effectif du respect des règles qui régissent cette activité. Étant donné qu'il n'existe pas d'autorité unique au niveau de l'Union pour faire respecter les droits et obligations liés à la «banque ouverte», les autorités compétentes nationales sont le premier niveau de contrôle du respect des règles en matière de banque ouverte. Il est donc essentiel que les autorités compétentes nationales veillent de manière proactive et rigoureuse au respect du cadre réglementé de l'Union en matière de «banque ouverte». Un contrôle insuffisant par les autorités compétentes du respect de ces règles est régulièrement présenté par les opérateurs de banque ouverte comme l'une des raisons de son adoption encore limitée dans l'Union. Les autorités compétentes nationales devraient disposer des ressources appropriées pour s'acquitter de manière efficace et efficiente de leurs tâches de contrôle du respect. Les autorités compétentes nationales devraient promouvoir et faciliter un dialogue fluide et régulier entre les différents acteurs de l'écosystème de la «banque ouverte». Les prestataires de services de paiement gestionnaires de comptes et les prestataires de services d'information sur les comptes et de services d'initiation de paiement qui ne respectent pas leurs obligations devraient faire l'objet de sanctions appropriées. La surveillance régulière du marché de la «banque ouverte» dans l'Union par les autorités compétentes, coordonnées par l'ABE, devrait faciliter le contrôle du respect de la législation, et la collecte de données sur le marché de la «banque ouverte» comblera une lacune dans les données qui existe actuellement et qui empêche de mesurer efficacement l'adoption effective de la «banque ouverte» dans l'Union. Les prestataires de services de paiement gestionnaires de comptes et les prestataires de services d'information sur les comptes et de services d'initiation de paiement devraient avoir accès aux organismes de règlement des litiges, conformément à l'article 10 de la proposition de règlement sur les données, lorsque ledit règlement sera entré en vigueur.

(69) L'utilisation parallèle des termes «consentement explicite» dans la directive (UE) 2015/2366 et dans le règlement (UE) 2016/679 du Parlement européen et du Conseil[48] a donné lieu à des interprétations erronées. L'objet du consentement explicite au sens de l'article 94, paragraphe 2, de la directive (UE) 2015/2366 est la permission d'obtenir l'accès à ces données à caractère personnel afin de pouvoir traiter et stocker les données à caractère personnel qui sont nécessaires aux fins de la prestation du service de paiement. Il conviendrait par conséquent d'apporter une clarification afin d'accroître la sécurité juridique et d'établir une distinction claire avec les règles relatives à la protection des données. Là où les termes «consentement explicite» ont été employés dans la directive (UE) 2015/2366, c'est le terme «permission» qu'il conviendrait d'employer dans le présent règlement. Lorsqu'il est fait référence à une «permission», cette référence devrait s'entendre sans préjudice des obligations incombant aux prestataires de services de paiement en application de l'article 6 du règlement (UE) 2016/679. La permission ne devrait, dès lors, pas être interprétée exclusivement comme un «consentement» ou un «consentement explicite» au sens du règlement (UE) 2016/679.

(70) Pour accroître la confiance des utilisateurs de services de paiement dans les virements et faire en sorte qu'ils les utilisent, il est essentiel de garantir la sécurité de ces virements. Lorsqu'un payeur souhaite envoyer un virement à un bénéficiaire donné, il peut arriver qu'il fournisse, à la suite d'une fraude ou par erreur, un identifiant unique qui n'est pas celui d'un compte détenu par ce bénéficiaire. Afin de contribuer à la réduction des fraudes et des erreurs, les utilisateurs de services de paiement devraient bénéficier d'un service permettant de vérifier si l'identifiant unique du bénéficiaire et le nom de celui-ci fournis par le payeur concordent, et de notifier à ce payeur toute divergence éventuellement détectée. Ces services, dans les pays où ils existent, ont eu une incidence positive considérable sur le niveau de fraude et d'erreurs. Compte tenu de l'importance de ce service pour la prévention des fraudes et des erreurs, il devrait être mis gratuitement à la disposition des consommateurs. Afin que le traitement de l'opération ne soit pas indûment bloqué ou retardé, le prestataire de services de paiement du payeur devrait émettre cette notification en l'espace de quelques secondes seulement à compter du moment où le payeur a saisi les informations relatives au bénéficiaire. Le prestataire de services de paiement du payeur devrait donner notification au payeur avant que ce dernier n'autorise l'opération envisagée, afin qu'il puisse décider s'il convient ou non de procéder à celle-ci. Certaines solutions d'initiation de virement peuvent être mises à la disposition des payeurs pour leur permettre de passer un ordre de paiement sans qu'ils aient à saisir eux-mêmes l'identifiant unique. En effet, ces éléments de données sont fournis par le fournisseur de cette solution d'initiation. En pareils cas, un service de vérification de la concordance entre l'identifiant unique et le nom du bénéficiaire n'est pas nécessaire, étant donné que le risque de fraude ou d'erreurs est considérablement réduit.

(71) Le règlement (UE) XXX modifiant le règlement (UE) nº 260/2012 prévoit qu'un service de vérification de la concordance entre l'identifiant unique et le nom du bénéficiaire doit être proposé aux utilisateurs de virements instantanés en euros. Afin d'obtenir un cadre cohérent pour l'ensemble des virements tout en évitant tout

[48] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

chevauchement indu, le service de vérification prévu dans le présent règlement ne devrait s'appliquer qu'aux virements qui ne relèvent pas du règlement (UE) XXX modifiant le règlement (UE) nº 260/2012.

(72) Certaines caractéristiques du nom du bénéficiaire sur le compte duquel le payeur souhaite faire un virement peuvent accroître la probabilité que le prestataire de services de paiement détecte une divergence, notamment la présence de signes diacritiques ou l'existence de plusieurs translittérations possibles du nom dans différents alphabets, le fait que le nom d'usage diffère du nom indiqué sur les documents d'identité officiels dans le cas d'une personne physique, ou le fait que le nom commercial diffère de la dénomination sociale dans le cas d'une personne morale. Afin d'éviter que le traitement de virements ne soit indûment bloqué et de faciliter la décision du payeur de procéder ou non à l'opération envisagée, les prestataires de services de paiement devraient préciser le degré de cette divergence, en indiquant dans la notification s'il y a absence de concordance ou «quasi»-concordance.

(73) Le fait d'autoriser une opération de paiement bien que le service de vérification de la concordance ait détecté une divergence et l'ait notifiée à l'utilisateur de services de paiement peut conduire à ce que les fonds soient virés au mauvais bénéficiaire. Les prestataires de services de paiement devraient informer les utilisateurs de services de paiement des conséquences possibles de leur choix de ne pas tenir compte de la divergence notifiée et de procéder à l'exécution de l'opération. Tout au long de leur relation contractuelle avec un prestataire de services de paiement, les utilisateurs de services de paiement devraient avoir la possibilité de renoncer à utiliser un tel service. Après avoir renoncé à ce service, les utilisateurs de services de paiement devraient avoir la possibilité d'y avoir de nouveau recours.

(74) L'utilisateur de services de paiement devrait notifier dès que possible au prestataire de services de paiement toute contestation relative à des opérations de paiement prétendument non autorisées ou mal exécutées ou à des virements autorisés alors que le service de vérification de la concordance dysfonctionnait, à condition que le prestataire de services de paiement ait satisfait à ses obligations d'information. Si l'utilisateur de services de paiement a respecté le délai de notification, il devrait pouvoir faire valoir ces réclamations sous réserve des délais nationaux de prescription. Cela ne devrait pas avoir d'incidence sur les autres litiges entre utilisateurs et prestataires de services de paiement.

(75) Il y a lieu de prévoir la répartition des pertes en cas d'opérations de paiement non autorisées ou de certains virements autorisés. Des dispositions différentes peuvent s'appliquer à des utilisateurs de services de paiement qui ne sont pas des consommateurs, de tels utilisateurs étant généralement plus à même d'apprécier le risque de fraude et de prendre des mesures compensatoires. Afin de garantir un niveau élevé de protection des consommateurs, le payeur devrait toujours être en droit d'adresser sa demande de remboursement à son prestataire de services de paiement gestionnaire du compte, même lorsqu'un prestataire de services d'initiation de paiement intervient dans l'opération de paiement. Cette disposition serait sans préjudice de la répartition des responsabilités entre les prestataires de services de paiement.

(76) Dans le cas des services d'initiation de paiement, la répartition des responsabilités entre le prestataire de services de paiement qui gère le compte et le prestataire de services d'initiation de paiement intervenant dans l'opération devrait contraindre ceux-

ci à assumer la responsabilité des parties de l'opération qui sont sous leur contrôle respectif.

(77) En cas d'opération de paiement non autorisée, le prestataire de services de paiement devrait immédiatement rembourser le montant de cette opération au payeur. Toutefois, s'il existe de forts soupçons qu'une opération non autorisée résulte d'un comportement frauduleux du payeur et que ces soupçons reposent sur des raisons objectives qui sont communiquées à l'autorité nationale concernée par le prestataire de services de paiement, ce dernier devrait être en mesure de mener une enquête avant de rembourser le payeur. Le prestataire de services de paiement devrait, dans un délai de dix jours ouvrables après avoir pris connaissance de l'opération ou après en avoir été informé, soit rembourser au payeur le montant de l'opération de paiement non autorisée, soit fournir au payeur les motifs et les éléments justifiant le refus de remboursement et indiquer les organismes que le payeur peut alors saisir s'il n'accepte pas les motifs invoqués. Afin de protéger le payeur contre tout préjudice, la date de valeur du remboursement ne devrait pas être postérieure à la date à laquelle le montant a été débité. Afin d'inciter l'utilisateur de services de paiement à signaler dans les meilleurs délais au prestataire de services de paiement le vol ou la perte d'un instrument de paiement et de limiter ainsi le risque d'opérations de paiement non autorisées, la responsabilité de l'utilisateur ne devrait être engagée, sauf agissement frauduleux ou négligence grave de sa part, qu'à concurrence d'un montant très limité. Dans ce contexte, un montant de 50 EUR semble adéquat pour garantir un niveau élevé et harmonisé de protection des utilisateurs dans l'Union. La responsabilité du payeur ne devrait pas être engagée lorsque celui-ci n'est pas en mesure de prendre conscience de la perte, du vol ou du détournement de l'instrument de paiement. En outre, une fois qu'il a informé le prestataire de services de paiement du risque d'utilisation frauduleuse de son instrument de paiement, l'utilisateur de services de paiement ne devrait pas être tenu de couvrir toute autre perte pouvant résulter de cette utilisation frauduleuse. Les prestataires de services de paiement devraient être responsables de la sécurité technique de leurs propres produits.

(78) Des dispositions en matière de responsabilité dans le cas de virements autorisés pour lesquelles il y a eu une application incorrecte ou un dysfonctionnement du service de détection des divergences entre le nom et l'identifiant unique d'un bénéficiaire créeraient des incitations appropriées pour que les prestataires de services de paiement fournissent un service pleinement opérationnel, dans le but de réduire le risque d'autorisations de paiement reposant sur une mauvaise information. Si le payeur a décidé de recourir à un tel service, son prestataire de services de paiement devrait être tenu pour responsable du montant total du virement dans les cas où ce prestataire de services de paiement a omis de notifier au payeur une divergence entre l'identifiant unique et le nom du bénéficiaire fourni par le payeur alors qu'il aurait dû notifier cette divergence si le service avait correctement fonctionné, et où cette omission a causé un préjudice financier au payeur. Lorsque la responsabilité du prestataire de services de paiement du payeur est imputable au prestataire de services de paiement du bénéficiaire, ce dernier prestataire devrait indemniser le prestataire de services de paiement du payeur pour le préjudice financier subi.

(79) Les consommateurs devraient être protégés de manière adéquate dans le cadre de certaines opérations de paiement frauduleuses qu'ils ont autorisées sans savoir que ces opérations étaient frauduleuses. Le nombre de cas d'«ingénierie sociale» dans lesquels les consommateurs sont induits en erreur pour autoriser une opération de paiement en faveur d'un fraudeur a considérablement augmenté ces dernières années. Les cas

d'usurpation d'identité («spoofing») dans lesquels les fraudeurs se font passer pour des employés d'un prestataire de services de paiement d'un client et utilisent frauduleusement le nom, l'adresse électronique ou le numéro de téléphone du prestataire de services de paiement pour gagner la confiance des clients et les inciter à réaliser certaines actions sont malheureusement de plus en plus répandus dans l'Union. Ces nouveaux types de fraude par usurpation d'identité rendent plus floue la différence qui existait dans la directive (UE) 2015/2366 entre les opérations autorisées et les opérations non autorisées. Les moyens par lesquels le consentement peut être présumé avoir été accordé deviennent également plus complexes à déterminer, étant donné que les fraudeurs peuvent prendre le contrôle de l'ensemble du processus de consentement et d'authentification, y compris de l'authentification forte du client. Les conditions dans lesquelles le client a autorisé une opération en donnant sa permission devraient être dûment prises en considération, y compris par les tribunaux, pour déterminer si une opération a été autorisée ou non. Une opération peut en effet avoir été autorisée dans des circonstances telles que l'autorisation accordée a reposé sur des prémisses viciées qui compromettent l'intégrité de la permission donnée. Il n'est donc plus possible, comme c'était le cas dans la directive (UE) 2015/2366, de limiter les remboursements aux seules opérations non autorisées. Il serait toutefois disproportionné et financièrement très coûteux pour les prestataires de services de paiement de prévoir un droit systématique au remboursement de toute opération frauduleuse, autorisée ou non. Cela pourrait également entraîner un aléa moral et une diminution de la vigilance du client.

(80) Les prestataires de services de paiement pourraient également être considérés comme des victimes de cas d'usurpation d'identité, puisque leurs coordonnées auront été usurpées. Toutefois, les prestataires de services de paiement disposent de plus de moyens que les consommateurs pour mettre un terme à ces cas de fraude, au moyen d'une prévention adéquate et de garanties techniques solides mises au point avec les prestataires de services de communications électroniques tels que les opérateurs de réseaux mobiles, les plates-formes internet, etc. Les fraudes par usurpation de l'identité d'employés de banque nuisent à la réputation de la banque ainsi que du secteur bancaire dans son ensemble et peuvent causer des préjudices financiers importants aux consommateurs de l'Union et saper leur confiance dans les paiements électroniques et dans le système bancaire. Un consommateur de bonne foi qui a été victime d'une telle fraude par usurpation d'identité dans laquelle les fraudeurs se font passer pour des employés du prestataire de services de paiement d'un client et utilisent frauduleusement le nom, l'adresse électronique ou le numéro de téléphone du prestataire de services de paiement devrait, par conséquent, avoir droit au remboursement par le prestataire de services de paiement de l'intégralité du montant de l'opération de paiement frauduleuse, sauf agissement frauduleux ou «négligence grave» de la part du payeur. Dès que le consommateur apprend qu'il a été victime de ce type de fraude par usurpation d'identité, il devrait signaler l'incident à la police dans les meilleurs délais, de préférence au moyen de procédures de réclamation en ligne, lorsqu'elles sont mises à disposition par la police, et à son prestataire de services de paiement, en fournissant tous les éléments de preuve nécessaires à l'appui. Aucun remboursement ne devrait être accordé lorsque ces conditions de procédure ne sont pas remplies.

(81) Compte tenu de leurs obligations de garantir la sécurité de leurs services conformément à la directive 2002/58/CE du Parlement européen et du Conseil[49], les prestataires de services de communications électroniques ont la capacité de contribuer à la lutte collective contre la fraude par usurpation d'identité. Dès lors, et sans préjudice des obligations prévues par le droit national transposant ladite directive, les prestataires de services de communications électroniques devraient coopérer avec les prestataires de services de paiement en vue de prévenir de nouveaux cas de fraude de ce type, notamment en agissant rapidement pour faire en sorte que des mesures organisationnelles et techniques appropriées soient mises en place pour préserver la sécurité et la confidentialité des communications conformément à la directive 2002/58/CE. Toute réclamation d'un prestataire de services de paiement contre d'autres prestataires, tels que des prestataires de services de communications électroniques, portant sur un préjudice financier causé dans le cadre de ce type de fraude devrait être introduite conformément au droit national.

(82) Afin d'évaluer l'éventualité d'une négligence ou d'une négligence grave de la part de l'utilisateur de services de paiement, il convient de tenir compte de toutes les circonstances. Les preuves et le degré de négligence allégué devraient en général être évalués conformément au droit national. Toutefois, si la négligence implique un manquement au devoir de diligence, la «négligence grave» devrait impliquer plus que de la simple négligence et comporter un défaut de vigilance caractérisé, comme le serait le fait de conserver les données de sécurité utilisées pour autoriser une opération de paiement à côté de l'instrument de paiement, sous une forme aisément accessible et reconnaissable par des tiers. Le fait qu'un consommateur ait déjà reçu un remboursement d'un prestataire de services de paiement après avoir été victime d'une fraude par usurpation de l'identité d'un employé de banque et qu'il introduise une autre demande de remboursement auprès du même prestataire de services de paiement après avoir été à nouveau victime du même type de fraude pourrait être considéré comme une «négligence grave» car cela pourrait indiquer un niveau élevé d'imprudence de la part de l'utilisateur qui aurait dû être plus vigilant après avoir déjà été victime du même mode opératoire frauduleux.

(83) Les clauses et conditions contractuelles concernant la mise à disposition et l'utilisation d'un instrument de paiement qui auraient pour effet d'alourdir la charge de la preuve incombant au consommateur ou d'alléger la charge de la preuve pesant sur l'émetteur devraient être considérées comme nulles et non avenues. En outre, dans des situations spécifiques et en particulier lorsque l'instrument de paiement n'est pas présent au point de vente, par exemple dans le cas de paiements en ligne, il convient d'exiger du prestataire de services de paiement qu'il apporte la preuve de la négligence alléguée, le payeur n'ayant, dans ce cas, que des moyens très limités de le faire.

(84) Les consommateurs sont particulièrement vulnérables dans le cas d'opérations de paiement liées à une carte où le montant exact de l'opération n'est pas connu au moment où le payeur donne la permission d'exécuter l'opération de paiement, par exemple dans les stations-service automatiques ou dans le cas de contrats de location de voiture ou de réservations d'hôtel. Le prestataire de services de paiement du payeur devrait pouvoir bloquer un montant de fonds sur le compte de paiement du payeur en proportion du montant de l'opération de paiement auquel le payeur peut

[49] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (JO L 201 du 31.7.2002, p. 37).

raisonnablement s'attendre, et uniquement si le payeur a donné son accord pour que ce montant précis soit bloqué. Ces fonds devraient être débloqués immédiatement après réception des informations sur le montant final exact de l'opération de paiement et au plus tard immédiatement après la réception de l'ordre de paiement. Afin de garantir un déblocage rapide de la différence entre le montant bloqué et le montant exact de l'opération de paiement, le bénéficiaire devrait informer le prestataire de services de paiement immédiatement après la livraison du service ou des biens au payeur.

(85) D'anciens schémas de prélèvement dans des devises autres que l'euro continuent d'exister dans les États membres dont la monnaie n'est pas l'euro. Ces schémas sont efficaces et assurent le même niveau élevé de protection du payeur par d'autres garde-fous qui ne sont pas toujours fondés sur un droit inconditionnel au remboursement. Dans ce cas, le payeur devrait être protégé par la règle générale du remboursement lorsque l'opération de paiement exécutée dépasse le montant auquel on aurait pu raisonnablement s'attendre. Par ailleurs, les États membres devraient avoir la possibilité d'édicter, en matière de droit au remboursement, des règles plus favorables pour le payeur que celles prévues dans le présent règlement. Il serait approprié de permettre que le payeur et son prestataire de services de paiement conviennent dans un contrat-cadre que le payeur n'a pas droit à un remboursement dans les cas où il est protégé, soit parce que le payeur a donné la permission d'exécuter une opération directement à son prestataire de services de paiement, y compris lorsque le prestataire de services de paiement agit pour le compte du bénéficiaire, soit parce que les informations relatives à la future opération de paiement ont été fournies au payeur ou mises à sa disposition de la manière convenue, quatre semaines au moins avant l'échéance, par le prestataire de services de paiement ou par le bénéficiaire. En tout état de cause, le payeur devrait être protégé par la règle générale de remboursement en cas d'opérations de paiement non autorisées ou mal exécutées ou de virements autorisés ayant fait l'objet d'une application incorrecte du service de vérification de la concordance ou en cas de fraude par usurpation de l'identité du prestataire de services de paiement.

(86) Afin de pouvoir établir leur programmation financière et remplir leurs obligations de paiement en temps utile, les consommateurs et les entreprises ont besoin de connaître avec certitude la durée d'exécution d'un ordre de paiement. Il est donc nécessaire de préciser le moment où les droits et obligations prennent effet, c'est-à-dire lorsque le prestataire de services de paiement reçoit l'ordre de paiement, y compris lorsqu'il a eu la possibilité de le recevoir via les moyens de communication convenus dans le contrat de services de paiement, nonobstant toute participation antérieure au processus ayant conduit à la formulation et à la transmission de l'ordre de paiement, notamment les vérifications de la sécurité et de la disponibilité des fonds, les informations sur l'utilisation du numéro d'identification personnel (PIN) ou la délivrance d'une promesse de paiement. En outre, la réception d'un ordre de paiement devrait intervenir lorsque le prestataire de services de paiement du payeur reçoit l'ordre de paiement devant être débité du compte du payeur. Le moment où un bénéficiaire transmet des ordres de paiement au prestataire de services de paiement en vue de la collecte, par exemple, de paiements par carte ou de prélèvements ou le moment où le bénéficiaire se voit accorder par le prestataire de services de paiement une avance sur les montants concernés (une somme étant créditée de manière conditionnelle sur le compte) ne devrait aucunement entrer en ligne de compte à cet égard. Les utilisateurs devraient pouvoir être assurés de la bonne exécution d'un ordre de paiement dûment complété et valide si le prestataire de services de paiement ne peut faire état d'un motif de refus contractuel ou légal. Si le prestataire de services de paiement refuse un ordre de

paiement, il devrait en informer le plus rapidement possible l'utilisateur de services de paiement en lui précisant les raisons de ce refus, dans le respect des exigences du droit de l'Union et du droit national. Lorsque le contrat-cadre prévoit que le prestataire de services de paiement peut imputer des frais pour le refus, ceux-ci devraient être objectivement justifiés et aussi peu élevés que possible.

(87) Vu la rapidité avec laquelle les systèmes de paiement entièrement automatisés permettent de traiter les opérations de paiement, qui implique que, passé un certain délai, les ordres de paiement ne peuvent être révoqués sans coûts d'intervention manuelle élevés, il est nécessaire de fixer clairement un délai de révocation du paiement. Cependant, selon le type de service de paiement et d'ordre de paiement, le délai de révocation du paiement devrait pouvoir varier si les parties concernées en conviennent. La révocation dans un tel contexte devrait s'appliquer uniquement entre l'utilisateur de services de paiement et le prestataire de services de paiement, et elle ne devrait pas remettre en cause le caractère irrévocable et définitif des opérations de paiement effectuées dans les systèmes de paiement.

(88) L'irrévocabilité d'un ordre de paiement ne devrait pas porter atteinte aux droits ou aux obligations d'un prestataire de services de paiement prévus par les législations des États membres, en application du contrat-cadre du payeur ou des lois, réglementations, lignes directrices ou dispositions administratives nationales, de rembourser au payeur le montant de l'opération de paiement exécutée, en cas de litige entre le payeur et le bénéficiaire. Un tel remboursement devrait être considéré comme un nouvel ordre de paiement. À l'exception de ces cas, les litiges découlant de la relation sous-jacente à l'ordre de paiement devraient être réglés uniquement entre le payeur et le bénéficiaire.

(89) Aux fins du traitement pleinement intégré et automatisé des paiements, comme aux fins de la sécurité juridique quant à l'exécution de toute obligation sous-jacente entre utilisateurs de services de paiement, il est essentiel que l'intégralité de la somme transférée par le payeur soit créditée sur le compte du bénéficiaire. En conséquence, aucun des intermédiaires intervenant dans l'exécution des opérations de paiement ne devrait avoir la faculté d'opérer des déductions sur les montants transférés. Le bénéficiaire devrait cependant avoir la faculté de conclure, avec son prestataire de services de paiement, un accord autorisant ce dernier à prélever ses propres frais. Néanmoins, afin de permettre au bénéficiaire de vérifier que la somme due est correctement payée, les informations ultérieures relatives à l'opération de paiement devraient mentionner, outre le montant intégral des fonds transférés, le montant des frais éventuels qui ont été déduits.

(90) Afin d'améliorer l'efficience des paiements dans toute l'Union, il conviendrait de fixer un délai d'exécution d'un jour maximum pour tous les ordres de paiement initiés par le payeur et libellés en euros ou dans la devise d'un État membre dont la monnaie n'est pas l'euro, y compris les virements et transmissions de fonds non instantanés. Pour tous les autres paiements, tels que les paiements initiés par un bénéficiaire ou par son intermédiaire, y compris les prélèvements et les paiements par carte, en l'absence d'accord entre le prestataire de services de paiement et le payeur prévoyant expressément un délai d'exécution plus long, le même délai d'un jour devrait s'appliquer. Il devrait être possible de prolonger ces délais d'un jour ouvrable lorsqu'un ordre de paiement est donné sur support papier, afin que des services de paiement puissent continuer d'être fournis aux consommateurs habitués à n'utiliser que des documents sur support papier. Lorsqu'un système de prélèvement est utilisé, le prestataire de services de paiement du bénéficiaire devrait transmettre l'ordre de débit dans les délais dont le bénéficiaire et le prestataire de services de paiement sont

convenus, afin de rendre possible un règlement à l'échéance convenue. Il devrait être possible de maintenir ou d'établir des règles prévoyant un délai d'exécution inférieur à un jour ouvrable.

(91) Les règles relatives à l'exécution du montant intégral et au délai d'exécution devraient constituer des bonnes pratiques lorsque l'un des prestataires de services de paiement n'est pas situé dans l'Union. Lorsqu'il effectue un virement ou une transmission de fonds en faveur d'un bénéficiaire situé en dehors de l'Union, le prestataire de services de paiement du payeur devrait fournir au payeur une estimation du délai nécessaire pour que les fonds virés ou transmis soient crédités au prestataire de services de paiement du bénéficiaire situé en dehors de l'Union. On ne saurait attendre d'un prestataire de services de paiement établi dans l'Union qu'il évalue le délai nécessaire à un prestataire de services de paiement établi en dehors de l'Union pour créditer ces fonds sur le compte du bénéficiaire après réception de ceux-ci.

(92) Pour renforcer leur confiance à l'égard des marchés des paiements, il est essentiel que les utilisateurs de services de paiement aient connaissance des frais réels des services de paiement qui leur seront appliqués. En conséquence, l'emploi de méthodes de tarification non transparentes devrait être interdit car il est communément admis que, avec de telles méthodes, l'utilisateur a le plus grand mal à déterminer le prix réel du service de paiement. En particulier, l'utilisation de dates de valeur défavorables à l'utilisateur ne devrait pas être autorisée.

(93) Le prestataire de services de paiement devrait avoir la possibilité de préciser clairement les informations exigées aux fins de l'exécution correcte d'un ordre de paiement. Le prestataire de services de paiement du payeur devrait agir avec toute la diligence requise et, lorsque cela est techniquement possible et ne nécessite pas d'intervention manuelle, vérifier la cohérence de l'identifiant unique, et, s'il apparaît que cet identifiant unique n'est pas cohérent, refuser l'ordre de paiement et en informer le payeur.

(94) Le fonctionnement harmonieux et efficient des systèmes de paiement dépend de la confiance que peut avoir l'utilisateur dans le fait que le prestataire de services de paiement va exécuter l'opération de paiement correctement et dans le délai convenu. En général, le prestataire de services de paiement est en mesure d'apprécier les risques associés à une opération de paiement. C'est lui qui fournit le système de paiement, qui prend les dispositions nécessaires pour rappeler des fonds erronément alloués et qui choisit, dans la plupart des cas, les intermédiaires intervenant dans l'exécution d'une opération de paiement. Eu égard à l'ensemble de ces considérations, il convient que, sauf en cas de situations anormales et imprévisibles, le prestataire de services de paiement soit tenu pour responsable de l'exécution de toute opération de paiement qu'il a acceptée d'un utilisateur, sauf en cas d'actes et d'omissions du prestataire de services de paiement du bénéficiaire, dont le choix dépend du seul bénéficiaire. Toutefois, afin de ne pas laisser le payeur sans protection dans la situation, peu probable, où il ne serait pas évident que le montant du paiement a bien été reçu par le prestataire de services de paiement du bénéficiaire, la charge de la preuve correspondante devrait incomber au prestataire de services de paiement du payeur. D'une manière générale, il peut être supposé que l'établissement intermédiaire, habituellement un organisme impartial tel qu'une banque centrale ou un organisme de compensation, chargé du transfert du montant du paiement entre le prestataire de services de paiement émetteur et le prestataire de services de paiement destinataire, conservera les données relatives au compte et sera en mesure de les fournir, si nécessaire. Lorsque le montant du paiement est crédité sur le compte du prestataire de

services de paiement destinataire, le bénéficiaire devrait avoir immédiatement le droit d'exiger du prestataire de services de paiement que la somme soit créditée sur son compte.

(95) Le prestataire de services de paiement du payeur, à savoir le prestataire de services de paiement gestionnaire du compte ou, le cas échéant, le prestataire de services d'initiation de paiement, devrait être tenu pour responsable de l'exécution correcte de l'opération de paiement, notamment de son exécution pour son montant intégral et du respect du délai d'exécution, et sa pleine responsabilité devrait être engagée pour toute défaillance d'une autre partie intervenant dans la chaîne de paiement jusqu'au compte du bénéficiaire inclus. Il résulte de cette responsabilité que, lorsque le montant intégral n'est pas porté au crédit du prestataire de services de paiement du bénéficiaire ou qu'il l'est avec retard, le prestataire de services de paiement du payeur devrait corriger l'opération de paiement ou rembourser au payeur dans les meilleurs délais le montant correspondant de l'opération, sans préjudice de tout autre recours susceptible d'être formé conformément au droit national. Du fait de la responsabilité du prestataire de services de paiement, le payeur ou le bénéficiaire ne devraient supporter aucun coût lié à l'exécution incorrecte d'un paiement. En cas de non-exécution, de mauvaise exécution ou d'exécution tardive d'opérations de paiement, la date de valeur des paiements correctifs effectués par les prestataires de services de paiement devrait toujours être identique à ce qu'aurait été la date de valeur en cas d'exécution correcte.

(96) Le bon fonctionnement des virements et des autres services de paiement requiert que les prestataires de services de paiement et leurs intermédiaires, notamment les responsables du traitement, soient liés par des contrats définissant leurs droits et obligations réciproques. Les questions de responsabilité constituent une partie essentielle de ces contrats. Pour assurer la confiance mutuelle entre les prestataires de services de paiement et les intermédiaires participant à une opération de paiement, la sécurité juridique doit être garantie afin qu'un prestataire de services de paiement qui n'est pas responsable obtienne, au titre des règles en matière de responsabilité, une indemnisation pour les pertes subies ou les sommes payées. Les autres droits et la teneur détaillée du recours (action récursoire) ainsi que les modalités de traitement des réclamations à l'égard du prestataire de services de paiement ou de l'intermédiaire concernant une opération de paiement mal exécutée devraient faire l'objet d'une convention.

(97) La prestation de services de paiement par les prestataires de services de paiement peut comporter le traitement de données à caractère personnel. La prestation de services d'information sur les comptes peut comporter le traitement de données à caractère personnel relatives à une personne concernée qui n'est pas l'utilisateur d'un prestataire de services de paiement donné, mais dont le traitement des données à caractère personnel par ledit prestataire est nécessaire aux fins de l'exécution d'un contrat entre ce prestataire et l'utilisateur de services de paiement. Lorsque des données à caractère personnel font l'objet d'un traitement, ce traitement devrait être conforme au règlement (UE) 2016/679 et au règlement (UE) 2018/1725 du Parlement européen et du Conseil[50], notamment aux principes de limitation de la finalité, de minimisation des données et de limitation de la conservation des données. La protection des données dès

[50] 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).

la conception et la protection des données par défaut devraient être intégrées dans tous les systèmes de traitement des données mis au point et utilisés dans le cadre du présent règlement. En conséquence , les autorités de contrôle prévues par le règlement (UE) 2016/679 et le règlement (UE) 2018/1725 devraient être responsables du contrôle du traitement des données à caractère personnel effectué dans le cadre du présent règlement.

(98) Comme la Commission le reconnaît dans sa communication sur une stratégie en matière de paiements de détail pour l'UE, le bon fonctionnement des marchés des paiements de l'UE revêt un intérêt public important. En conséquence, lorsque cela est nécessaire dans le cadre du présent règlement aux fins de la prestation de services de paiement et du respect du présent règlement, les prestataires de services de paiement et les opérateurs de systèmes de paiement devraient pouvoir traiter des catégories particulières de données à caractère personnel au sens de l'article 9, paragraphe 1, du règlement (UE) 2016/679 et de l'article 10, paragraphe 1, du règlement (UE) 2018/1725. Lorsque des catégories particulières de données à caractère personnel font l'objet d'un traitement, les prestataires de services de paiement et les opérateurs de systèmes de paiement devraient mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les libertés et droits fondamentaux des personnes physiques. Ces mesures devraient inclure des limitations techniques à la réutilisation des données et le recours aux mesures techniques les plus avancées de sécurité et de protection de la vie privée, notamment la pseudonymisation ou le chiffrement, afin de garantir le respect des principes de limitation de la finalité, de minimisation des données et de limitation de la conservation des données, énoncés dans le règlement (UE) 2016/679. Les prestataires de services de paiement et les opérateurs de systèmes de paiement devraient également mettre en œuvre des mesures d'organisation spéciales, notamment une formation au traitement de ces données, la limitation de l'accès aux catégories particulières de données et l'enregistrement de cet accès.

(99) La communication aux personnes d'informations sur le traitement des données à caractère personnel devrait être effectuée conformément au règlement (UE) 2016/679 et au règlement (UE) 2018/1725.

(100) Les fraudeurs prennent souvent pour cibles les personnes les plus vulnérables de notre société. La détection en temps utile des opérations de paiement frauduleuses est essentielle et le contrôle des opérations joue un rôle important dans cette détection. Il convient donc d'exiger des prestataires de services de paiement qu'ils disposent de mécanismes de contrôle des opérations à la hauteur de la contribution essentielle que ces mécanismes apportent à la prévention de la fraude, en allant au-delà de la protection offerte par l'authentification forte du client en ce qui concerne les opérations de paiement, y compris celles qui font appel à des services d'initiation de paiement.

(101) L'ABE devrait élaborer des projets de normes techniques de réglementation relatives aux exigences techniques particulières liées aux mécanismes de contrôle des opérations. Ces exigences devraient s'appuyer sur la valeur ajoutée découlant des caractéristiques environnementales et comportementales liées aux habitudes de paiement de l'utilisateur de services de paiement.

(102) Afin que les mécanismes de contrôle des opérations fonctionnent efficacement de manière à permettre aux prestataires de services de paiement de détecter et de prévenir les fraudes, notamment en détectant une utilisation atypique de services de paiement

qui pourrait indiquer une opération potentiellement frauduleuse, les prestataires de services de paiement devraient être en mesure de traiter les informations relatives aux opérations de leurs clients et à leurs comptes de paiement. Les prestataires de services de paiement devraient toutefois fixer des durées de conservation appropriées pour les différents types de données utilisés à des fins de prévention de la fraude. Ces durées de conservation devraient être strictement limitées à la durée nécessaire pour détecter les comportements atypiques et potentiellement frauduleux, et les prestataires de services de paiement devraient régulièrement supprimer les données qui ne sont plus nécessaires à la détection et à la prévention de la fraude. Les données traitées à des fins de contrôle des opérations ne devraient pas être utilisées après que l'utilisateur de services de paiement a cessé d'être un client du prestataire de services de paiement.

(103) La fraude en matière de virements possède une capacité intrinsèque d'adaptation et comprend une diversité illimitée de pratiques et de techniques, telles que le vol de données de sécurité d'authentification, la falsification de factures et la manipulation sociale. Dès lors, pour pouvoir prévenir des types de fraude toujours nouveaux, il conviendrait d'améliorer constamment le contrôle des opérations en tirant pleinement partie de technologies telles que l'intelligence artificielle. Un prestataire de services de paiement ne dispose souvent pas d'une vue d'ensemble complète de tous les éléments susceptibles de conduire à une détection rapide de la fraude. Toutefois, il peut gagner en efficacité grâce à une plus grande quantité d'informations sur les activités potentiellement frauduleuses émanant d'autres prestataires de services de paiement. Il devrait donc être possible, pour les prestataires de services de paiements, de se communiquer toutes les informations utiles. Pour mieux détecter les opérations de paiement frauduleuses et protéger leurs clients, les prestataires de services de paiement devraient, aux fins du contrôle des opérations, exploiter les données relatives à la fraude aux paiements partagées par d'autres prestataires de services de paiement de manière multilatérale, par exemple sur les plates-formes informatiques spécialisées fondées sur des dispositifs de partage d'informations. Afin d'améliorer la protection des payeurs contre la fraude aux virements, les prestataires de services de paiement devraient pouvoir s'appuyer sur des informations aussi exhaustives et à jour que possible, notamment en faisant un usage collectif des informations concernant les identifiants uniques, les techniques de manipulation et d'autres circonstances associées aux virements frauduleux recensées individuellement par chaque prestataire de services de paiement. Avant d'adopter un dispositif de partage d'informations, les prestataires de services de paiement devraient procéder à une analyse d'impact relative à la protection des données, conformément à l'article 35 du règlement (UE) 2016/679. Lorsqu'il ressort de l'analyse d'impact relative à la protection des données que, en l'absence de garanties, de mesures de sécurité et de mécanismes pour atténuer le risque, le traitement présenterait un risque élevé pour les droits et libertés des personnes physiques, les prestataires de services de paiement devraient consulter l'autorité chargée de la protection des données concernée conformément à l'article 36 dudit règlement. Une nouvelle analyse d'impact ne devrait pas être requise lorsqu'un prestataire de services de paiement adhère à un dispositif de partage d'informations existant pour lequel une analyse d'impact relative à la protection des données a déjà été réalisée. Le dispositif de partage d'informations devrait prévoir des mesures techniques et organisationnelles destinées à protéger les données à caractère personnel. Il devrait définir les rôles et les responsabilités de tous les prestataires de services de paiement au titre de la législation sur la protection des données, y compris dans le cas de responsables conjoints du traitement.

(104) Aux fins de l'échange de données à caractère personnel avec d'autres prestataires de services de paiement qui sont soumis à des dispositifs de partage d'informations, il conviendrait d'entendre par «identifiant unique» le «numéro IBAN» tel qu'il est défini à l'article 2, point 15), du règlement (UE) nº 260/2012.

(105) Afin d'empêcher que des échanges légitimes d'informations sur des activités potentiellement frauduleuses conduisent à une «réduction des risques» injustifiée ou à un retrait injustifié des services de comptes de paiement de certains utilisateurs de services de paiement sans explication ni recours, il convient d'instituer des garanties. Les données relatives à la fraude aux paiements communiquées au sein d'un dispositif multilatéral de partage d'informations qui peut entraîner la divulgation de données à caractère personnel, y compris d'identifiants uniques de bénéficiaires potentiellement impliqués dans une fraude aux virements, ne devraient être utilisées par les prestataires de services de paiement qu'aux fins de l'amélioration du contrôle des opérations. Les prestataires de services de paiement devraient instituer des garanties supplémentaires, telles que la prise de contact avec le client s'il est le payeur d'un virement dont on peut supposer qu'il est frauduleux et le contrôle plus approfondi d'un compte lorsque l'identifiant unique signalé comme potentiellement frauduleux désigne un client de ce prestataire de services de paiement. Les données relatives à la fraude aux paiements que les prestataires de services de paiement se communiquent dans le cadre de tels dispositifs ne devraient pas constituer un motif de retrait des services bancaires sans enquête approfondie.

(106) La fraude aux paiements devient de plus en plus sophistiquée, les fraudeurs utilisant des techniques de manipulation et d'usurpation d'identité qui sont difficiles à détecter pour les utilisateurs de services de paiement qui ne sont pas suffisamment sensibilisés à la fraude ni suffisamment informés sur cette problématique. Les prestataires de services de paiement peuvent jouer un rôle important dans le renforcement de la prévention de la fraude en prenant régulièrement toutes les initiatives nécessaires pour que leurs utilisateurs de services de paiement comprennent mieux les risques et tendances de fraude en matière de paiement et y soient davantage sensibilisés. En particulier, les prestataires de services de paiement devraient mener des programmes et des campagnes de sensibilisation appropriés sur les tendances et risques de fraude à l'intention de leurs clients et des employés des prestataires de services de paiement, dans le but d'aider les clients à se rendre compte qu'ils sont victimes d'une tentative de fraude. Les prestataires de services de paiement devraient communiquer à leurs consommateurs, par divers supports, des informations adaptées sur la fraude, en leur envoyant des messages et des avertissements clairs et en les aidant à réagir correctement lorsqu'ils sont exposés à des situations potentiellement frauduleuses. L'ABE devrait élaborer des orientations concernant les différents types de programmes que les prestataires de services de paiement doivent mettre au point sur les risques de fraude aux paiements, en tenant compte de l'évolution constante de la nature des risques liés à la fraude.

(107) La sécurité des paiements électroniques est fondamentale pour garantir la protection des utilisateurs et le développement d'un environnement sain pour le commerce électronique. Tous les services de paiement proposés par voie électronique devraient être sécurisés, grâce à des technologies permettant de garantir une authentification sûre de l'utilisateur et de réduire, dans toute la mesure du possible, les risques de fraude. Dans le domaine de la fraude, la principale innovation de la directive (UE) 2015/2366 a été l'introduction de l'authentification forte du client. Dans son évaluation de la mise

en œuvre de la directive (UE) 2015/2366, la Commission a conclu que l'authentification forte du client avait déjà été très efficace pour réduire la fraude.

(108) L'authentification forte du client ne devrait pas être contournée, notamment par un recours injustifié aux dérogations à l'authentification forte du client. Il convient d'introduire des définitions claires des opérations initiées par les commerçants et des ordres de paiement passés par courrier ou par téléphone, étant donné que ces notions, qui peuvent être invoquées pour justifier la non-application de l'authentification forte du client, sont diversement comprises et appliquées et sont parfois invoquées d'une manière abusive. En ce qui concerne les opérations initiées par les commerçants, l'authentification forte du client devrait être appliquée lors de l'établissement du mandat initial, sans qu'il soit nécessaire d'appliquer l'authentification forte du client pour les opérations de paiement ultérieures initiées par les commerçants. En ce qui concerne les ordres de paiement passés par courrier ou par téléphone, seule l'initiation d'opérations de paiement, et non leur exécution, devrait être non numérique pour qu'une opération soit considérée comme un ordre de paiement passé par courrier ou par téléphone et, partant, ne relève pas de l'obligation d'appliquer l'authentification forte du client. Toutefois, les opérations de paiement fondées sur des ordres de paiement passés par le payeur sur support papier, par courrier ou par téléphone devraient toujours comporter des exigences de sécurité et des vérifications par le prestataire de services de paiement du payeur permettant l'authentification de l'opération de paiement. L'authentification forte du client ne devrait pas non plus être contournée par des pratiques telles que le recours à un acquéreur établi en dehors de l'Union en vue d'échapper aux exigences en matière d'authentification forte du client.

(109) Étant donné que le prestataire de services de paiement qui devrait appliquer l'authentification forte du client est celui qui délivre les données de sécurité personnalisées, les opérations de paiement qui ne sont pas initiées par le payeur mais uniquement par le bénéficiaire ne devraient pas être soumises à une authentification forte du client dans la mesure où ces opérations sont initiées sans aucune interaction avec le payeur ni intervention de celui-ci. L'approche réglementaire des opérations initiées par les commerçants et des prélèvements, qui sont deux formes d'opérations initiées par le bénéficiaire, devrait être harmonisée et bénéficier des mêmes mesures de protection des consommateurs, dont les remboursements.

(110) Afin d'améliorer l'inclusion financière, et conformément à la directive (UE) 2019/882 du Parlement européen et du Conseil[51] relative aux exigences en matière d'accessibilité applicables aux produits et services, tous les utilisateurs de services de paiement, y compris les personnes handicapées, les personnes âgées, les personnes ayant de faibles compétences numériques et celles qui n'ont pas accès à des appareils numériques tels que les téléphones intelligents, devraient bénéficier de la protection contre la fraude procurée par l'authentification forte du client, en particulier en ce qui concerne l'utilisation des opérations de paiement numériques à distance et l'accès en ligne aux comptes de paiement en tant que services financiers fondamentaux. Avec l'introduction de l'authentification forte du client, il est devenu impossible, pour certains consommateurs de l'Union, d'effectuer des opérations en ligne en raison de leur incapacité matérielle de réaliser l'authentification forte du client. C'est pourquoi les prestataires de services de paiement devraient veiller à ce que leurs clients puissent bénéficier de diverses méthodes d'exécution de l'authentification forte du client qui

[51] Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services (JO L 151 du 7.6.2019, p. 70).

soient adaptées à leurs besoins et à leur situation. Ces méthodes ne devraient pas imposer l'utilisation d'une seule technologie, d'un seul dispositif ou mécanisme, ni la possession d'un téléphone intelligent.

(111) Les portefeuilles européens d'identité numérique mis en œuvre en vertu du règlement (UE) nº 910/2014[52] du Parlement européen et du Conseil, tel que modifié par le règlement (UE) [XXX], sont des moyens d'identification électronique qui offrent des outils d'identification et d'authentification permettant l'accès transfrontière à des services financiers, y compris aux services de paiement. L'introduction du portefeuille européen d'identité numérique rendrait encore plus aisées l'identification et l'authentification numériques transfrontières pour les paiements numériques sécurisés et faciliterait le développement d'un paysage paneuropéen des paiements numériques.

(112) La croissance du commerce électronique et des paiements par téléphone mobile devrait aller de pair avec un renforcement généralisé des mesures de sécurité. En cas d'initiation à distance d'une opération de paiement, c'est-à-dire lorsqu'un ordre de paiement est passé sur l'internet, l'authentification des opérations devrait s'appuyer sur des codes dynamiques afin que l'utilisateur soit à tout moment conscient du montant et du bénéficiaire de l'opération qu'il autorise.

(113) L'obligation d'appliquer l'authentification forte du client aux opérations de paiement à distance au moyen de codes qui établissent un lien dynamique entre l'opération, d'une part, et un montant et un bénéficiaire donnés, d'autre part, devrait être le reflet de la croissance des paiements par téléphone mobile et de l'apparition d'une variété de modèles au moyen desquels ces paiements sont exécutés.

(114) Étant donné que l'établissement d'un lien dynamique permet de parer aux risques de falsification du nom du bénéficiaire et du montant donné de l'opération entre le moment où un ordre de paiement est passé et où les paiements sont authentifiés, mais aussi, plus généralement, de parer au risque de fraude pour les paiements par téléphone mobile pour lesquels l'exécution d'une authentification forte du client nécessite l'utilisation de l'internet sur le dispositif du payeur, les prestataires de services de paiement devraient également appliquer des éléments qui établissent un lien dynamique entre l'opération, d'une part, et un montant et un bénéficiaire donnés, d'autre part, ou des mesures de sécurité harmonisées d'effet identique, qui garantissent la confidentialité, l'authenticité et l'intégrité de l'opération au cours de toutes les phases de l'initiation du paiement.

(115) En vertu de la dérogation à l'authentification forte du client prévue à l'article 18 du règlement délégué (UE) 2018/389, les prestataires de services de paiement étaient autorisés à ne pas appliquer l'authentification forte du client lorsque le payeur initiait une opération de paiement électronique à distance que le prestataire de services de paiement considérait comme présentant un faible niveau de risque en s'appuyant sur les mécanismes de contrôle des opérations. Les réactions du marché ont toutefois montré que, pour qu'un plus grand nombre de prestataires de services de paiement mettent en œuvre l'analyse des risques liés à l'opération, il était nécessaire d'adopter des règles appropriées sur la portée d'une telle analyse, qui introduisent des exigences claires en matière d'audit, fournissent davantage de détails et de meilleures définitions concernant les exigences en matière de suivi des risques et les données à partager, et

[52] Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73).

d'évaluer les avantages potentiels qu'il y aurait à autoriser les prestataires de services de paiement à signaler les opérations frauduleuses dont ils sont seuls responsables. L'ABE devrait élaborer des projets de normes techniques de réglementation établissant des règles relatives à l'analyse des risques liés aux opérations.

(116) Les mesures de sécurité devraient être compatibles avec le niveau de risque associé aux services de paiement. Afin de permettre le développement de moyens de paiement accessibles et faciles à utiliser pour les paiements présentant peu de risques, tels que les paiements de faible valeur sans contact au point de vente, que ces paiements soient ou non fondés sur la téléphonie mobile, les dérogations à l'application des exigences de sécurité devraient être précisées dans les normes techniques de réglementation. La sécurité de l'utilisation des données de sécurité personnalisées doit être assurée afin de limiter les risques d'usurpation d'identité («spoofing»), d'hameçonnage («phishing») et d'autres activités frauduleuses. L'utilisateur devrait pouvoir s'en remettre à l'adoption de mesures qui protègent la confidentialité et l'intégrité des données de sécurité personnalisées.

(117) Les prestataires de services de paiement devraient appliquer l'authentification forte du client lorsque, entre autres, l'utilisateur de services de paiement exécute, grâce à un moyen de communication à distance, une action susceptible de comporter un risque de fraude en matière de paiements ou de toute autre utilisation frauduleuse. Les prestataires de services de paiement devraient mettre en place des mesures de sécurité adéquates pour protéger la confidentialité et l'intégrité des données de sécurité personnalisées des utilisateurs de services de paiement.

(118) Les acteurs du marché des différents États membres ne comprennent pas de la même manière les exigences en matière d'authentification forte du client applicables à l'enregistrement d'instruments de paiement, en particulier de cartes de paiement, dans des portefeuilles numériques. La création d'un jeton ou son remplacement peut donner lieu à un risque de fraude aux paiements ou à d'autres abus. La création ou le remplacement d'un jeton d'instrument de paiement, qui se fait grâce à un moyen de communication à distance avec la participation de l'utilisateur de services de paiement, devrait donc nécessiter l'application de l'authentification forte du client par le prestataire de services de paiement de l'utilisateur de services de paiement lors de l'émission ou du remplacement du jeton. En appliquant l'authentification forte du client au stade de la création ou du remplacement du jeton, le prestataire de services de paiement devrait vérifier à distance que l'utilisateur de services de paiement est l'utilisateur légitime de l'instrument de paiement et associer l'utilisateur et la version numérisée de l'instrument de paiement au dispositif correspondant.

(119) Les opérateurs de portefeuilles numériques de type «pass-through» (à transfert direct) qui vérifient les éléments de l'authentification forte du client lorsque des instruments tokenisés stockés dans les portefeuilles numériques sont utilisés à des fins de paiement devraient être tenus de conclure des accords d'externalisation avec les prestataires de services de paiement des payeurs afin d'autoriser ces prestataires à continuer d'effectuer ces vérifications, tout en leur imposant de se conformer aux exigences essentielles en matière de sécurité. Les prestataires de services de paiement du payeur devraient, en application de ces accords, assumer l'entière responsabilité de tout défaut d'application, par les opérateurs de portefeuilles de type «pass-through» (à transfert direct), de l'authentification forte du client et avoir le droit de réaliser un audit des dispositions de sécurité de l'opérateur du portefeuille et de contrôler celles-ci.

(120) Lorsque les prestataires de services techniques ou les opérateurs de schémas de paiement fournissent des services aux bénéficiaires ou aux prestataires de services de paiement des bénéficiaires ou des payeurs, ils devraient rendre possible l'application d'une authentification forte du client dans le cadre de leur rôle dans l'initiation ou l'exécution des opérations de paiement. Étant donné le rôle qu'ils jouent pour ce qui est d'assurer la bonne mise en œuvre des exigences essentielles en matière de sécurité concernant les paiements de détail, notamment en fournissant des solutions informatiques appropriées, les prestataires de services techniques et les opérateurs de schémas de paiement devraient être tenus pour responsables des préjudices financiers causés aux bénéficiaires ou aux prestataires de services de paiement des bénéficiaires ou des payeurs au cas où ils ne rendraient pas possible l'application d'une authentification forte du client.

(121) Les États membres devraient désigner les autorités compétentes pour l'octroi d'agrément aux établissements de paiement et pour l'accréditation et le suivi des procédures de règlement extrajudiciaire des litiges.

(122) Sans préjudice du droit de recours juridictionnel des consommateurs, les États membres devraient veiller à ce qu'il existe des procédures aisément accessibles, adéquates, indépendantes, impartiales, transparentes et efficaces de règlement extrajudiciaire des litiges opposant prestataires de services de paiement et utilisateurs de services de paiement. Le règlement (CE) nº 593/2008 du Parlement européen et du Conseil[53] prévoit que la protection offerte au consommateur par les dispositions impératives de la loi du pays dans lequel il a sa résidence habituelle ne doit pas être remise en cause du fait d'une clause contractuelle relative à la loi applicable au contrat. En vue d'instaurer une procédure de règlement des litiges efficiente et efficace, les États membres devraient veiller à ce que les prestataires de services de paiement adhèrent à une procédure de règlement extrajudiciaire des litiges conformément aux exigences de qualité énoncées dans la directive 2013/11/UE du Parlement européen et du Conseil[54], pour régler les litiges avant la saisie d'une juridiction. Les autorités compétentes désignées devraient notifier à la Commission le nom d'une ou plusieurs entités de règlement extrajudiciaire des litiges de qualité compétentes sur leur territoire pour régler les litiges nationaux et transfrontières et coopérer en ce qui concerne les litiges relatifs aux droits et obligations prévus par le présent règlement.

(123) Les consommateurs devraient être autorisés à faire respecter leurs droits en lien avec les obligations imposées aux prestataires de services de paiement et de services de monnaie électronique dans le cadre du présent règlement, au moyen d'actions représentatives conformément à la directive (UE) 2020/1828 du Parlement européen et du Conseil[55].

(124) Il convient d'instaurer des procédures appropriées pour donner suite aux réclamations introduites ontre les prestataires de services de paiement qui ne se conforment pas à leurs obligations et de veiller, s'il y a lieu, à ce que des sanctions effectives, proportionnées et dissuasives soient infligées. Afin de garantir le respect effectif du

---

53 JO L 177 du 4.7.2008, p. 6.

54 Directive 2013/11/UE du Parlement européen et du Conseil du 21 mai 2013 relative au règlement extrajudiciaire des litiges de consommation et modifiant le règlement (CE) nº 2006/2004 et la directive 2009/22/CE (JO L 165 du 18.6.2013, p. 63).

55 Directive (UE) 2020/1828 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE (JO L 409 du 4.12.2020, p. 1).

présent règlement, les États membres devraient désigner des autorités compétentes qui remplissent les conditions fixées par le règlement (UE) nº 1093/2010 du Parlement européen et du Conseil[56] et qui agissent indépendamment des prestataires de services de paiement. Les États membres devraient notifier à la Commission les autorités qui ont été désignées et lui communiquer une description précise des missions de ces autorités.

(125) Sans préjudice du droit de recours juridictionnel en vue de garantir le respect du présent règlement, les autorités compétentes devraient exercer les pouvoirs nécessaires accordés par le présent règlement, notamment le pouvoir d'enquêter sur les manquements allégués, d'infliger des sanctions administratives et d'imposer des mesures administratives, lorsque le prestataire de services de paiement ne se conforme pas aux droits et obligations définis par le présent règlement, en particulier s'il existe un risque de récidive ou une autre menace pour les intérêts collectifs des consommateurs. Les autorités compétentes devraient mettre en place des mécanismes efficaces pour encourager le signalement des infractions potentielles ou réelles. Ces mécanismes devraient être sans préjudice des droits de défense garantis à tout accusé.

(126) Les États membres devraient être tenus de prévoir des sanctions et mesures administratives effectives, proportionnées et dissuasives en cas d'infraction aux dispositions du présent règlement. Ces sanctions administratives, astreintes et mesures administratives devraient satisfaire à certaines exigences minimales, concernant notamment les pouvoirs minimaux que les autorités compétentes devraient se voir conférer pour être en mesure de les imposer et les critères que les autorités compétentes devraient prendre en considération dans leur application, pour leur publication et lorsqu'elles en rendent compte. Les États membres devraient établir des règles spéciales et des mécanismes efficaces concernant l'application des astreintes.

(127) Les autorités compétentes devraient être habilitées à infliger des sanctions pécuniaires administratives suffisamment élevées pour contrebalancer les avantages attendus de l'infraction et avoir un effet dissuasif même pour les établissements de plus grande taille.

(128) Lorsqu'elles imposent des sanctions administratives et des mesures administratives, les autorités compétentes devraient tenir compte de toute sanction pénale antérieure qui aurait été infligée à la même personne physique ou morale responsable de la même infraction, lorsqu'elles déterminent le type de sanctions administratives ou d'autres mesures administratives et le niveau des sanctions pécuniaires administratives. Il s'agit de faire en sorte que la sévérité de toutes les sanctions et autres mesures administratives imposées à des fins punitives, en cas de cumul de poursuites de nature administrative et de poursuites de nature pénale, soit limitée à ce que requiert la gravité de l'infraction.

(129) Un système de surveillance efficace exige que les autorités de surveillance soient conscientes des lacunes que présentent les prestataires de services de paiement en matière de respect des règles du présent règlement. Il importe donc que les autorités de surveillance puissent s'informer mutuellement des sanctions et mesures

[56] 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).

administratives imposées aux prestataires de services de paiement lorsque ces informations sont également utiles à d'autres autorités de surveillance.

(130) L'efficacité du cadre de l'Union relatif aux services de paiement dépend de la coopération entre de multiples autorités compétentes, notamment des autorités nationales chargées de la fiscalité, de la protection des données, de la concurrence, de la protection des consommateurs, de l'audit, de la police et d'autres autorités chargées de faire respecter la législation. Les États membres devraient veiller à ce que leur cadre juridique permette et facilite cette coopération en tant que de besoin pour atteindre les objectifs du cadre de l'Union relatif aux services de paiement, y compris par la bonne application de ses règles. Cette coopération devrait comprendre l'échange d'informations ainsi que l'assistance mutuelle en vue de l'application effective des sanctions administratives, en particulier dans le cadre du recouvrement transfrontière des sanctions pécuniaires.

(131) Quelle que soit leur dénomination en droit national, des formes de procédure d'exécution accélérée ou d'accord transactionnel existent dans de nombreux États membres et sont utilisées comme alternative à une procédure formelle pour parvenir à une adoption plus rapide d'une décision visant à imposer une sanction administrative ou une mesure administrative ou pour mettre fin à l'infraction alléguée et à ses conséquences avant l'ouverture d'une procédure formelle de sanction. S'il ne semble pas approprié de chercher à harmoniser au niveau de l'Union les méthodes visant à faire respecter la réglementation qu'ont établies de nombreux États membres, en raison des approches juridiques très variées adoptées au niveau national, il convient de reconnaître que ces méthodes permettent aux autorités compétentes qui peuvent les mettre en œuvre de traiter les dossiers d'infraction d'une manière plus rapide, moins coûteuse et globalement efficace dans certaines circonstances, et qu'elles devraient, dès lors, être encouragées. Toutefois, les États membres ne devraient pas être tenus d'introduire de telles méthodes dans leur cadre juridique ni de contraindre les autorités compétentes à y recourir si elles ne le jugent pas approprié.

(132) Actuellement, les sanctions et mesures administratives instituées par les États membres en cas d'infraction aux principales dispositions régissant la prestation de services de paiement sont diversifiées et les approches concernant les enquêtes sur les violations de ces dispositions et les sanctions en la matière manquent de cohérence. Le fait de ne pas définir plus clairement quelles dispositions essentielles doivent déclencher des mesures d'exécution suffisamment dissuasives partout dans l'Union irait à l'encontre de la réalisation du marché unique des services de paiement et risquerait d'encourager le «forum shopping» dans la mesure où les autorités compétentes sont inégalement équipées pour réprimer rapidement et avec le même effet dissuasif ces infractions dans les États membres.

(133) Étant donné que l'objet des astreintes est de contraindre les personnes physiques ou morales qui sont identifiées comme responsables d'une infraction en cours ou qui se voient imposer de se conformer à une injonction de l'autorité compétente chargée de l'enquête, à se conformer à cette injonction ou à mettre fin à l'infraction en cours, l'application d'astreintes ne devrait pas faire obstacle à ce que les autorités compétentes infligent ultérieurement des sanctions administratives à raison de la même infraction.

(134) Sauf disposition contraire prévue par les États membres, les astreintes devraient être calculées sur une base journalière.

(135) Les autorités compétentes devraient être habilitées par les États membres à imposer ces sanctions et mesures administratives aux prestataires de services de paiement ou à d'autres personnes physiques ou morales, s'il y a lieu, afin de remédier à la situation en cas d'infraction. Cet ensemble de sanctions et de mesures devrait être suffisamment vaste pour permettre aux États membres et aux autorités compétentes de tenir compte des différences existant entre les prestataires de services de paiement, en particulier entre les établissements de crédit et les autres établissements de paiement, au regard de leur taille, de leurs caractéristiques et de leur domaine d'activité.

(136) La publication d'une sanction administrative ou d'une mesure administrative pour infraction aux dispositions du présent règlement peut avoir un effet dissuasif important sur la récidive d'une telle infraction. La publication permet en outre non seulement d'informer les autres entités des risques associés au prestataire de services de paiement sanctionné avant qu'elles ne s'engagent dans une relation d'affaires, mais aussi d'aider les autorités compétentes des autres États membres en ce qui concerne les risques associés à un prestataire de services de paiement lorsque celui-ci opère dans ces autres États membres dans un contexte transfrontière. Pour ces raisons, la publication des décisions relatives aux sanctions et mesures administratives devrait être autorisée pour autant qu'elle concerne des personnes morales. Lorsqu'elles décident de publier une sanction administrative ou une mesure administrative, les autorités compétentes devraient tenir compte de la gravité de l'infraction et de l'effet dissuasif que cette publication est susceptible de produire. Toutefois, toute publication de ce type faisant référence à des personnes physiques peut empiéter de manière disproportionnée sur les droits qui résultent de la charte des droits fondamentaux et de la législation de l'Union applicable en matière de protection des données. En conséquence, la publication devrait avoir lieu de manière anonymisée, à moins que l'autorité compétente ne juge nécessaire de publier des décisions contenant des données à caractère personnel aux fins de l'application effective du présent règlement, y compris dans les cas de déclarations publiques ou d'interdictions temporaires. En pareils cas, l'autorité compétente devrait justifier sa décision.

(137) Afin de recueillir des informations plus précises sur le niveau de conformité avec le droit de l'Union sur le terrain, tout en donnant plus de visibilité au contrôle du respect de la législation assuré par les autorités compétentes, il est nécessaire d'élargir le champ d'application et d'améliorer la qualité des données que les autorités compétentes communiquent à l'ABE. Il conviendrait d'anonymiser les informations à communiquer afin de respecter les règles en vigueur en matière de protection des données, et de les fournir sous une forme agrégée afin de respecter les règles en matière de secret professionnel et de confidentialité en ce qui concerne les procédures. L'ABE devrait rendre compte régulièrement à la Commission de l'état d'avancement des mesures visant à faire respecter la réglementation dans les États membres.

(138) Il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne pour mettre à jour, afin de tenir compte de l'inflation, les montants à concurrence desquels un payeur peut être tenu de supporter les pertes liées à toute opération de paiement non autorisée résultant de l'utilisation d'un instrument de paiement perdu ou volé ou du détournement d'un instrument de paiement. Il convient que, lorsqu'elle prépare des actes délégués, la Commission veille à ce que les documents pertinents soient transmis simultanément, en temps utile et de façon appropriée, au Parlement européen et au Conseil.

(139) Afin de garantir une application cohérente du présent règlement, la Commission devrait pouvoir s'appuyer sur l'expertise et le soutien de l'ABE, laquelle devrait être chargée d'élaborer des orientations et des projets de normes techniques de réglementation et d'exécution. La Commission devrait être habilitée à adopter ces projets de normes techniques de réglementation. Lorsqu'elle élabore des orientations, des projets de normes techniques de réglementation et des projets de normes techniques d'exécution en application du présent règlement et conformément au règlement (UE) nº 1093/2010, l'ABE devrait consulter toutes les parties concernées, notamment sur le marché des services de paiement, qui représentent tous les intérêts en présence.

(140) L'ABE devrait, conformément à l'article 9, paragraphe 5, du règlement (UE) nº 1093/2010, se voir accorder des pouvoirs d'intervention sur les produits afin de pouvoir temporairement interdire ou restreindre dans l'Union un type ou une fonctionnalité spécifique de service de paiement ou de service de monnaie électronique dont il est établi qu'il est susceptible de léser les consommateurs et qu'il menace le bon fonctionnement et l'intégrité des marchés financiers. Il y a donc lieu de modifier le règlement (UE) nº 1093/2010 en conséquence.

(141) Il convient de modifier l'annexe du règlement (UE) 2017/2394 du Parlement européen et du Conseil[57] pour y insérer une référence au présent règlement, de manière à faciliter la coopération transfrontière pour ce qui concerne l'exécution du présent règlement.

(142) Étant donné que l'objectif du présent règlement, à savoir une intégration plus poussée d'un marché intérieur des services de paiement, ne peut pas être atteint de manière suffisante par les États membres, puisqu'il suppose d'harmoniser plusieurs règles différentes du droit de l'Union et du droit national, mais qu'il peut, en raison de ses dimensions et de ses effets, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(143) Étant donné que le présent règlement et la directive (UE) XXX (DSP3) établissent le cadre juridique régissant la prestation de services de paiement de détail et de services de monnaie électronique dans l'Union, afin de garantir la sécurité juridique et la cohérence du cadre juridique de l'Union, le présent règlement devrait s'appliquer à partir de la même date que la date d'application des dispositions législatives, réglementaires et administratives que les États membres sont tenus d'adopter pour se conformer à la directive (UE) XXX (DSP3). Toutefois, les dispositions imposant aux prestataires de services de paiement de vérifier les divergences entre le nom et l'identifiant unique d'un bénéficiaire en cas de virement et le régime de responsabilité correspondant devraient s'appliquer à partir de 24 mois après la date d'entrée en vigueur du présent règlement, ce qui laisserait aux prestataires de services de paiement suffisamment de temps pour prendre les mesures nécessaires pour adapter leurs systèmes internes afin de se conformer à ces exigences.

---

[57] Règlement (UE) 2017/2394 du Parlement européen et du Conseil du 12 décembre 2017 sur la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs et abrogeant le règlement (CE) nº 2006/2004 (JO L 345 du 27.12.2017, p. 1).

(144) Conformément aux principes d'amélioration de la réglementation, le présent règlement devrait être réexaminé afin de déterminer s'il a atteint ses objectifs de manière efficace et efficiente. Le réexamen devrait avoir lieu suffisamment longtemps après la date d'application du présent règlement afin qu'il existe des éléments probants appropriés sur lesquels fonder ce réexamen. Une période de cinq ans est considérée comme une période appropriée. S'il convient que le réexamen porte sur le présent règlement dans son ensemble, une attention particulière devrait être accordée à certains sujets, à savoir le fonctionnement de la banque ouverte, la tarification des services de paiement et la proposition de solutions supplémentaires pour lutter contre la fraude. En ce qui concerne le champ d'application du présent règlement, il convient toutefois qu'un réexamen ait lieu plus tôt, à savoir trois ans après son entrée en application, compte tenu de l'importance attachée à cette question à l'article 58, paragraphe 2, du règlement (UE) 2022/2554 du Parlement européen et du Conseil[58]. Ce réexamen du champ d'application devrait porter à la fois sur l'éventuelle extension de la liste des services de paiement couverts à des services tels que ceux fournis par les systèmes de paiement et les schémas de paiement, et sur l'éventuelle inclusion dans le champ d'application de certains services techniques actuellement exclus.

(145) Le présent règlement respecte les droits fondamentaux et observe les principes reconnus par la charte des droits fondamentaux de l'Union européenne, notamment le droit au respect de la vie privée et familiale, le droit à la protection des données à caractère personnel, la liberté d'entreprise, le droit à un recours effectif et le droit à ne pas être jugé ou puni pénalement deux fois pour une même infraction. Le présent règlement doit être appliqué dans le respect de ces droits et de ces principes.

(146) Les références à des montants en euros s'entendent comme la contre-valeur en monnaie nationale définie par chaque État membre dont la monnaie n'est pas l'euro.

(147) 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[59] et a rendu un avis le [XX XX 2023][60],

---

58 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 (JO L 333 du 27.12.2022, p. 1).

59 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 (Texte présentant de l'intérêt pour l'EEE) (JO L 295 du 21.11.2018, p. 39).

60 JO C […], […], p. […].

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

TITRE I

OBJET, CHAMP D'APPLICATION ET DÉFINITIONS

Article premier

Objet

1. Le présent règlement établit des exigences uniformes applicables à la prestation de services de paiement et de services de monnaie électronique concernant:

   a) la transparence des conditions et des exigences en matière d'information en ce qui concerne les services de paiement et les services de monnaie électronique;

   b) les droits et obligations respectifs des utilisateurs de services de paiement et de monnaie électronique et des prestataires de services de paiement et de monnaie électronique dans le cadre de la prestation de services de paiement et de services de monnaie électronique.

2. Sauf indication contraire, toute référence aux services de paiement s'entend dans le présent règlement comme désignant les services de paiement et de monnaie électronique.

3. Sauf indication contraire, toute référence aux prestataires de services de paiement s'entend dans le présent règlement comme désignant les prestataires de services de paiement et les prestataires de services de monnaie électronique.

Article 2

Champ d'application

1. Le présent règlement s'applique aux services de paiement fournis dans l'Union par les catégories de prestataires de services de paiement suivantes:

   a) les établissements de crédit au sens de l'article 4, paragraphe 1, point 1), du règlement (UE) nº 575/2013 du Parlement européen et du Conseil[61], y compris leurs succursales lorsque ces succursales sont situées dans l'Union, que leur administration centrale soit située dans l'Union ou en dehors de celle-ci;

   b) les offices de chèques postaux qui sont habilités en droit national à fournir des services de paiement;

   c) les établissements de paiement;

[61] Règlement (UE) nº 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) nº 648/2012 (JO L 176 du 27.6.2013, p. 1).

d) la BCE et les banques centrales nationales lorsqu'elles n'agissent pas en qualité d'autorités monétaires ou d'autres autorités publiques;

e) les États membres ou leurs autorités régionales ou locales lorsqu'ils n'agissent pas en qualité d'autorités publiques.

2. Le présent règlement ne s'applique pas aux services suivants:

a) aux opérations de paiement effectuées exclusivement en espèces et allant directement du payeur au bénéficiaire, sans l'intervention du moindre intermédiaire;

b) aux opérations de paiement allant du payeur au bénéficiaire, par l'intermédiaire d'un agent commercial au sens de l'article 1er, paragraphe 2, de la directive 86/653/CEE, sous réserve que toutes les conditions suivantes soient remplies: i) l'agent commercial est autorisé, en vertu d'un accord, à négocier ou à conclure la vente ou l'achat de biens ou de services pour le compte du seul payeur ou du seul bénéficiaire, mais pas des deux, que l'agent commercial soit ou non en possession des fonds du client; et ii) cet accord confère au payeur ou au bénéficiaire une marge réelle pour négocier avec l'agent commercial ou pour conclure la vente ou l'achat de biens ou de services;

c) aux opérations de paiement consistant en la collecte et la remise d'espèces à titre non professionnel, dans le cadre d'une activité à but non lucratif ou caritative;

d) aux services pour lesquels des espèces sont fournies par le bénéficiaire au bénéfice du payeur dans le cadre d'une opération de paiement pour l'achat de biens et de services, à la demande expresse de l'utilisateur de services de paiement formulée juste avant l'exécution de l'opération de paiement;

e) aux services pour lesquels des espèces sont fournies dans des magasins de détail à la demande expresse de l'utilisateur de services de paiement, mais indépendamment de l'exécution de toute opération de paiement et sans obligation d'achat de biens et de services. L'utilisateur de services de paiement reçoit des informations sur les frais éventuels pour ce service avant que les espèces demandées ne lui soient fournies;

f) aux opérations de paiement fondées sur l'un des documents suivants, tiré sur le prestataire de services de paiement afin de mettre des fonds à la disposition du bénéficiaire:

i) un chèque papier régi par les dispositions de la convention de Genève du 19 mars 1931 portant loi uniforme sur les chèques;

ii) un chèque papier semblable à celui visé au point i) et régi par le droit d'un État membre non partie à la convention de Genève du 19 mars 1931 portant loi uniforme sur les chèques;

iii) une traite sur support papier relevant de la convention de Genève du 7 juin 1930 portant loi uniforme sur les lettres de change et billets à ordre;

iv) une traite sur support papier semblable à celle visée au point iii) et régie par le droit d'un État membre non partie à la convention de Genève du 7 juin 1930 portant loi uniforme sur les lettres de change et billets à ordre;

v) un titre-service sur support papier;

vi) un chèque de voyage sur support papier;

vii) un mandat postal sur support papier tel que défini par l'Union postale universelle;

g) aux opérations de paiement effectuées au sein d'un système de paiement ou de règlement des opérations sur titres entre des agents de règlement, des contreparties centrales, des chambres de compensation ou des banques centrales et d'autres participants au système, et des prestataires de services de paiement, sans préjudice de l'article 31;

h) aux opérations de paiement liées au service d'actifs et de titres, y compris la distribution de dividendes, de revenus ou autres, les remboursements ou les ventes, effectuées par les personnes visées au point g) ou par des entreprises d'investissement, des établissements de crédit, des organismes de placement collectif ou des sociétés de gestion de portefeuille fournissant des services d'investissement et toute autre entité autorisée à garder en dépôt des instruments financiers;

i) sans préjudice de l'article 23, paragraphe 2, et des articles 58 et 87, aux services fournis par les prestataires de services techniques;

j) aux services reposant sur des instruments de paiement spécifiques qui satisfont à l'une des conditions suivantes:

i) instruments ne permettant à leur détenteur d'acquérir des biens ou des services que dans les locaux de l'émetteur ou au sein d'un seul réseau limité de prestataires de services directement liés par un contrat commercial à un émetteur professionnel;

ii) instruments ne pouvant être utilisés que pour acquérir un éventail très limité de biens ou de services;

iii) instruments valables dans un seul État membre, qui sont fournis à la demande d'une entreprise ou d'un organisme public, qui sont réglementés par une autorité publique nationale ou régionale, à des fins sociales ou fiscales spécifiques, et qui permettent d'acquérir des biens ou des services spécifiques auprès de fournisseurs ayant conclu un accord commercial avec l'émetteur;

k) aux opérations de paiement proposées par un fournisseur de réseaux de communications électroniques au sens de l'article 2, point 1), de la directive (UE) 2018/1972 du Parlement européen et du Conseil[62], ou de services en plus des services de communications électroniques définis à l'article 2, point 4), de ladite directive à un abonné au réseau ou au service:

i) effectuées pour l'achat de contenu numérique et de services vocaux, quel que soit le dispositif utilisé pour l'achat ou la consommation du contenu numérique et imputées sur la facture correspondante; ou

[62] Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (JO L 321 du 17.12.2018, p. 36).

ii) exécutées depuis ou au moyen d'un dispositif électronique et imputées sur la facture correspondante dans le cadre d'activités caritatives ou pour l'achat de billets;

à condition que la valeur de chaque opération de paiement isolée ne dépasse pas 50 EUR et que:

– la valeur cumulée des opérations de paiement pour un même abonné ne dépasse pas 300 EUR par mois; ou

– lorsqu'un abonné préfinance son compte auprès du fournisseur de réseau ou de services de communications électroniques, la valeur cumulée des opérations de paiement ne dépasse pas 300 EUR par mois;

l) aux opérations de paiement effectuées entre prestataires de services de paiement, leurs agents ou succursales pour leur propre compte;

m) aux opérations de paiement et services connexes entre une entreprise mère et sa filiale, ou entre filiales d'une même entreprise mère, sans qu'un prestataire de services de paiement autre qu'une entreprise du même groupe ne fasse office d'intermédiaire, et à la centralisation des ordres de paiement pour le compte d'un groupe par une entreprise mère ou sa filiale pour transmission ultérieure à un prestataire de services de paiement.

3. Les titres II et III s'appliquent aux opérations de paiement dans la devise d'un État membre lorsque le prestataire de services de paiement du payeur et celui du bénéficiaire sont tous deux situés dans l'Union ou lorsque l'unique prestataire de services de paiement intervenant dans l'opération de paiement est situé dans l'Union.

4. Le titre II, à l'exception de l'article 13, paragraphe 1, point b), de l'article 20, point 2) e), et de l'article 24, point a), et le titre III, à l'exception des articles 67 à 72, s'appliquent aux opérations de paiement dans une devise qui n'est pas la devise d'un État membre lorsque le prestataire de services de paiement du payeur et celui du bénéficiaire sont tous deux situés dans l'Union ou lorsque l'unique prestataire de services de paiement intervenant dans l'opération de paiement est situé dans l'Union, pour ce qui concerne les parties de l'opération de paiement qui sont effectuées dans l'Union.

5. Le titre II, à l'exception de l'article 13, paragraphe 1, point b), de l'article 20, points 2) e) et 5) h), et de l'article 24, point a), et le titre III, à l'exception de l'article 28, paragraphes 2 et 3, des articles 62, 63 et 67, de l'article 69, paragraphe 1, et des articles 75 et 78, s'appliquent aux opérations de paiement dans toutes les devises lorsqu'un seul des prestataires de services de paiement est situé dans l'Union, pour ce qui concerne les parties de l'opération de paiement qui sont effectuées dans l'Union.

6. Les États membres peuvent exempter les établissements énumérés à l'article 2, paragraphe 5, points 4) à 23), de la directive 2013/36/UE de l'application de tout ou partie des dispositions du présent règlement.

7. Au plus tard le [OP: veuillez insérer la date correspondant à un an après la date d'entrée en vigueur du présent règlement], l'ABE émet, conformément à l'article 16 du règlement (UE) nº 1093/2010, des orientations à l'intention des autorités compétentes désignées en application du présent règlement sur l'exclusion des opérations de paiement allant du payeur au bénéficiaire par l'intermédiaire d'un agent commercial visées au paragraphe 2, point b), du présent article.

8. L'ABE élabore des projets de normes techniques de réglementation pour préciser les conditions des exclusions prévues au paragraphe 2, point j). L'ABE tient compte de l'expérience acquise dans l'application des orientations de l'ABE du 24 février 2022 sur l'exclusion relative aux réseaux limités en vertu de la directive (UE) 2015/2366.

L'ABE soumet les normes techniques de réglementation visées au premier alinéa à la Commission au plus tard le [OP: veuillez insérer la date correspondant à un an après la date d'entrée en vigueur du présent règlement]. La Commission est habilitée à adopter les normes techniques de réglementation visées au premier alinéa, conformément aux articles 10 à 14 du règlement (UE) nº 1093/2010.

9. Les États membres notifient à la Commission les dispositions légales qu'ils adoptent en vertu du paragraphe 6 au plus tard à la date d'application du présent règlement, et, sans tarder, toute modification ultérieure les concernant.

Article 3

Définitions

Aux fins du présent règlement, on entend par:

1) «État membre d'origine», l'un des États membres suivants:

   a) l'État membre dans lequel le prestataire de services de paiement a son siège statutaire; ou

   b) si, conformément à son droit national, le prestataire de services de paiement n'a pas de siège statutaire, l'État membre dans lequel il a son administration centrale;

2) «État membre d'accueil», l'État membre, autre que l'État membre d'origine, dans lequel un prestataire de services de paiement a un agent ou un distributeur ou détient une succursale ou fournit des services de paiement;

3) «service de paiement», une ou plusieurs des activités énumérées à l'annexe I exercées à titre professionnel;

4) «établissement de paiement», une personne morale qui, conformément à l'article 13 de la directive (UE) [DSP3], a obtenu un agrément l'autorisant à fournir des services de paiement ou des services de monnaie électronique dans toute l'Union;

5) «opération de paiement», une action consistant à verser, à transférer ou à retirer des fonds, sur le fondement d'un ordre de paiement passé par le payeur ou pour son compte, ou par le bénéficiaire ou pour son compte, indépendamment de toute obligation sous-jacente entre le payeur et le bénéficiaire;

6) «initiation d'une opération de paiement», les étapes nécessaires pour préparer l'exécution d'une opération de paiement, notamment la passation d'un ordre de paiement et l'achèvement du processus d'authentification;

7) «initiation à distance d'une opération de paiement», une opération de paiement pour laquelle un ordre de paiement est passé par l'internet;

8) «exécution d'une opération de paiement», le processus commençant une fois que l'initiation d'une opération de paiement est achevée et prenant fin une fois que les fonds versés, retirés ou transférés sont à la disposition du bénéficiaire;

9) «système de paiement», un système permettant de transférer des fonds régi par des procédures formelles standardisées et des règles communes pour le traitement, la compensation ou le règlement d'opérations de paiement;

10) «opérateur de système de paiement», l'entité juridique légalement responsable de l'exploitation d'un système de paiement;

11) «payeur», une personne physique ou morale qui est titulaire d'un compte de paiement et passe un ordre de paiement à partir de ce compte de paiement, ou, en l'absence de compte de paiement, une personne physique ou morale qui passe un ordre de paiement;

12) «bénéficiaire», une personne physique ou morale qui est le destinataire prévu de fonds faisant l'objet d'une opération de paiement;

13) «utilisateur de services de paiement», une personne physique ou morale qui utilise un service de paiement ou un service de monnaie électronique en qualité de payeur, de bénéficiaire ou des deux;

14) «prestataire de services de paiement», une entité visée à l'article 2, paragraphe 1, ou une personne physique ou morale bénéficiant d'une dérogation en vertu des articles 34, 36 ou 38 de la directive (UE) [DSP3];

15) «compte de paiement», un compte détenu par un prestataire de services de paiement au nom d'un ou de plusieurs utilisateurs de services de paiement, qui est utilisé aux fins de l'exécution d'une ou de plusieurs opérations de paiement et qui permet d'envoyer et de recevoir des fonds à destination et en provenance de tiers;

16) «ordre de paiement», une instruction d'un payeur ou d'un bénéficiaire à son prestataire de services de paiement demandant l'exécution d'une opération de paiement;

17) «mandat», l'expression de l'autorisation donnée par le payeur au bénéficiaire et (directement ou indirectement par l'intermédiaire du bénéficiaire) au prestataire de services de paiement du payeur permettant au bénéficiaire d'initier une opération de paiement en vue de débiter le compte de paiement spécifié du payeur et permettant au prestataire de services de paiement du payeur de se conformer à ces instructions;

18) «instrument de paiement», un ou plusieurs dispositifs individualisés et/ou un ensemble de procédures convenu entre l'utilisateur de services de paiement et le prestataire de services de paiement permettant l'initiation d'une opération de paiement;

19) «prestataire de services de paiement gestionnaire du compte», un prestataire de services de paiement qui fournit et gère un compte de paiement pour un payeur;

20) «service d'initiation de paiement», un service consistant à passer un ordre de paiement à la demande du payeur ou du bénéficiaire concernant un compte de paiement détenu auprès d'un autre prestataire de services de paiement;

21) «service d'information sur les comptes», un service en ligne consistant à collecter, directement ou par l'intermédiaire d'un prestataire de services techniques, et à consolider des informations concernant un ou plusieurs comptes de paiement détenus par un utilisateur de services de paiement auprès d'un ou de plusieurs prestataires de services de paiement gestionnaires de comptes;

22) «prestataire de services d'initiation de paiement», un prestataire de services de paiement fournissant des services d'initiation de paiement;

23) «prestataire de services d'information sur les comptes», un prestataire de services de paiement fournissant des services d'information sur les comptes;

24) «consommateur», une personne physique qui, dans le cadre des contrats de services de paiement régis par le présent règlement, agit dans un but autre que son activité commerciale ou professionnelle;

25) «contrat-cadre», un contrat de services de paiement qui régit l'exécution future d'opérations de paiement particulières et successives et peut énoncer les obligations et les conditions liées à l'ouverture d'un compte de paiement;

26) «transmission de fonds» (money remittance), un service de paiement pour lequel les fonds sont reçus de la part d'un payeur, sans création de comptes de paiement au nom du payeur ou du bénéficiaire, à la seule fin de transférer un montant correspondant vers un bénéficiaire ou un autre prestataire de services de paiement agissant pour le compte du bénéficiaire, ou pour lequel de tels fonds sont reçus pour le compte du bénéficiaire et mis à la disposition de celui-ci;

27) «prélèvement», un service de paiement visant à débiter le compte de paiement d'un payeur, lorsqu'une opération de paiement est initiée par le bénéficiaire sur le fondement d'un mandat donné par le payeur au bénéficiaire, au prestataire de services de paiement du bénéficiaire ou au propre prestataire de services de paiement du payeur;

28) «virement», un service de paiement, y compris les virements instantanés, fourni par le prestataire de services de paiement qui détient le compte de paiement du payeur et consistant à créditer, sur le fondement d'une instruction du payeur, le compte de paiement d'un bénéficiaire par une opération ou une série d'opérations de paiement réalisées à partir du compte de paiement du payeur;

29) «virement instantané», un virement qui est exécuté immédiatement, quels que soient le jour ou l'heure;

30) «fonds», la monnaie de banque centrale émise pour une utilisation de détail, la monnaie scripturale et la monnaie électronique;

31) «date de valeur», la date de référence utilisée par un prestataire de services de paiement pour calculer les intérêts applicables aux fonds débités d'un compte de paiement ou crédités sur un compte de paiement;

32) «taux de change de référence», le taux de change qui sert de base pour calculer les coûts de conversion monétaire et qui est communiqué par le prestataire de services de paiement ou provient d'une source accessible au public;

33) «taux d'intérêt de référence», le taux d'intérêt qui sert de base pour calculer les intérêts à appliquer et qui provient d'une source accessible au public pouvant être vérifiée par les deux parties à un contrat de services de paiement;

34) «authentification», une procédure permettant au prestataire de services de paiement de vérifier l'identité d'un utilisateur de services de paiement ou la validité de l'utilisation d'un instrument de paiement particulier, y compris l'utilisation des données de sécurité personnalisées de l'utilisateur;

35) «authentification forte du client», une authentification qui repose sur l'utilisation de deux éléments ou plus appartenant aux catégories «connaissance» (quelque chose que seul l'utilisateur connaît), «possession» (quelque chose que seul l'utilisateur possède) et «inhérence» (quelque chose que l'utilisateur est) et indépendants en ce sens que la

compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification;

36) «prestataire de services techniques», un prestataire qui fournit des services à l'appui de la prestation de services de paiement, sans entrer à aucun moment en possession des fonds à transférer;

37) «données de sécurité personnalisées», des données personnalisées fournies à un utilisateur de services de paiement par le prestataire de services de paiement à des fins d'authentification;

38) «données de paiement sensibles», des données qui sont susceptibles d'être utilisées pour commettre une fraude, y compris les données de sécurité personnalisées;

39) «identifiant unique», la combinaison de lettres, de chiffres ou de symboles indiquée par le prestataire de services de paiement à l'utilisateur de services de paiement, que ce dernier doit fournir pour permettre l'identification certaine d'un autre utilisateur de services de paiement ou du compte de paiement de cet autre utilisateur de services de paiement pour une opération de paiement;

40) «moyen de communication à distance», toute méthode qui peut être utilisée pour la conclusion d'un contrat de services de paiement sans la présence physique simultanée du prestataire de services de paiement et de l'utilisateur de services de paiement;

41) «support durable», tout instrument permettant à l'utilisateur de services de paiement de stocker les informations qui lui sont personnellement adressées d'une manière telle que ces informations puissent être consultées ultérieurement pendant une période adaptée à leur finalité et reproduites à l'identique;

42) «microentreprise», une entreprise qui, au moment de la conclusion du contrat de service de paiement, est une entreprise au sens de l'article 1er et de l'article 2, paragraphes 1 et 3, de l'annexe de la recommandation 2003/361/CE;

43) «jour ouvrable», un jour au cours duquel le prestataire de services de paiement du payeur ou du bénéficiaire intervenant dans l'exécution d'une opération de paiement exerce une activité permettant d'exécuter des opérations de paiement;

44) «agent», une personne physique ou morale qui agit pour le compte d'un établissement de paiement pour la fourniture des services de paiement, à l'exclusion des services de monnaie électronique;

45) «succursale», un siège d'exploitation autre que l'administration centrale qui constitue une partie d'un établissement de paiement, qui n'a pas de personnalité juridique et qui effectue directement, en tout ou en partie, les opérations inhérentes à l'activité d'un établissement de paiement; l'ensemble des sièges d'exploitation créés dans le même État membre par un établissement de paiement ayant son administration centrale dans un autre État membre sont considérés comme une seule succursale;

46) «groupe», un groupe d'entreprises qui sont liées entre elles par une relation au sens de l'article 22, paragraphe 1, point 2) ou 7), de la directive 2013/34/UE du Parlement européen et du Conseil[63] ou d'établissements visés aux articles 4, 5, 6 et 7 du

[63] Directive 2013/34/UE du Parlement européen et du Conseil du 26 juin 2013 relative aux états financiers annuels, aux états financiers consolidés et aux rapports y afférents de certaines formes d'entreprises,

règlement délégué (UE) nº 241/2014 de la Commission[64] qui sont liés entre eux par une relation au sens de l'article 10, paragraphe 1, de l'article 113, paragraphe 6, premier alinéa, ou de l'article 113, paragraphe 7, premier alinéa, du règlement (UE) nº 575/2013;

47) «contenu numérique», des biens ou des services qui sont produits et fournis sous forme numérique, dont l'utilisation ou la consommation est limitée à un dispositif technique et qui ne prévoient en aucune façon l'utilisation ou la consommation de biens et de services physiques;

48) «acquisition d'opérations de paiement», un service de paiement fourni par un prestataire de services de paiement convenant par contrat avec un bénéficiaire d'accepter et de traiter des opérations de paiement, de telle sorte que les fonds soient transférés au bénéficiaire;

49) «émission d'instruments de paiement», un service de paiement fourni par un prestataire de services de paiement convenant par contrat de fournir au payeur un instrument de paiement en vue d'initier et de traiter les opérations de paiement du payeur;

50) «monnaie électronique», une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement et qui est acceptée par des personnes physiques ou morales autres que l'émetteur;

51) «distributeur», une personne physique ou morale qui distribue ou rembourse de la monnaie électronique pour le compte d'un établissement de paiement;

52) «services de monnaie électronique», l'émission de monnaie électronique, la tenue de comptes de paiement stockant des unités de monnaie électronique et le transfert d'unités de monnaie électronique;

53) «dénomination commerciale», le nom communément utilisé par le bénéficiaire pour s'identifier auprès du payeur;

54) «fournisseurs de distributeurs automatiques de billets (DAB)», les opérateurs de distributeurs automatiques de billets qui ne gèrent pas de comptes de paiement.

55) «établissement de paiement fournissant des services de monnaie électronique», un établissement de paiement qui fournit des services d'émission de monnaie électronique, de tenue de comptes de paiement stockant des unités de monnaie électronique, et de transfert d'unités de monnaie électronique, qu'il fournisse ou non l'un des services énumérés à l'annexe I.

---

modifiant la directive 2006/43/CE du Parlement européen et du Conseil et abrogeant les directives 78/660/CEE et 83/349/CEE du Conseil (JO L 182 du 29.6.2013, p. 19).

64 Règlement délégué (UE) nº 241/2014 de la Commission du 7 janvier 2014 complétant le règlement (UE) nº 575/2013 du Parlement européen et du Conseil par des normes techniques de réglementation concernant les exigences de fonds propres applicables aux établissements (JO L 74 du 14.3.2014, p. 8).

TITRE II

TRANSPARENCE DES CONDITIONS ET EXIGENCES EN MATIÈRE D'INFORMATIONS RÉGISSANT LES SERVICES DE PAIEMENT

CHAPITRE I

Règles générales

Article 4

Champ d'application

1. Le présent titre s'applique aux opérations de paiement isolées, aux contrats-cadres et aux opérations de paiement qui relèvent de ces contrats. Les parties à ces opérations de paiement isolées, contrats-cadres et opérations de paiement qui en relèvent peuvent décider que le présent titre ne s'applique pas, en tout ou en partie, lorsque l'utilisateur de services de paiement n'est pas un consommateur.
2. Les États membres peuvent appliquer le présent titre aux microentreprises de la même manière qu'aux consommateurs.
3. Les États membres notifient à la Commission les dispositions légales qu'ils adoptent en vertu du paragraphe 2 au plus tard à la date d'application du présent règlement et, sans tarder, toute modification ultérieure les concernant.

Article 5

Devise et conversion monétaire

1. Les paiements sont effectués dans la devise convenue par les parties.
2. Lorsqu'un service de conversion monétaire est proposé avant l'initiation de l'opération de paiement et lorsque ce service de conversion monétaire est proposé au distributeur automatique de billets, au point de vente ou par le bénéficiaire, la partie qui le propose au payeur est tenue d'informer celui-ci de tous les frais appliqués et du taux de change qui sera utilisé aux fins de la conversion de l'opération de paiement.
3. Le payeur a la possibilité d'accepter le service de conversion monétaire sur cette base.

Article 6

Informations relatives aux frais supplémentaires ou aux réductions

1. Lorsque, aux fins de l'utilisation d'un instrument de paiement donné, le bénéficiaire applique des frais ou offre une réduction, il en informe le payeur avant l'initiation de l'opération de paiement.
2. Lorsque, aux fins de l'utilisation d'un instrument de paiement donné, le prestataire de services de paiement ou une autre partie intervenant dans l'opération applique des

frais, il en informe l'utilisateur de services de paiement avant l'initiation de l'opération de paiement.

3. Le payeur n'est tenu d'acquitter les frais visés aux paragraphes 1 et 2 que s'il a eu connaissance de leur montant total avant l'initiation de l'opération de paiement.

Article 7

Exigences en matière d'information applicables aux services de retrait d'espèces

Les personnes physiques ou morales fournissant les services de retrait d'espèces visés à l'article 38 de la directive (UE) [DSP3] fournissent à leurs clients ou mettent à leur disposition les informations sur les frais éventuels avant que les clients ne procèdent au retrait, ainsi qu'à la réception des espèces lorsque l'opération est achevée.

Article 8

Frais d'information

1. Les prestataires de services de paiement n'imputent pas de frais aux utilisateurs de services de paiement pour leur fournir des informations en vertu du présent titre.

2. Les prestataires de services de paiement et les utilisateurs de services de paiement peuvent d'un commun accord fixer les frais pour des informations supplémentaires, ou communiquées de manière plus fréquente, ou transmises par d'autres moyens de communication que ceux prévus par le contrat-cadre, et fournies à la demande de l'utilisateur de services de paiement.

3. Les frais d'information visés au paragraphe 2 sont raisonnables et correspondent aux coûts réels supportés par le prestataire de services de paiement.

Article 9

Charge de la preuve s'agissant des exigences en matière d'information

Il incombe aux prestataires de services de paiement de prouver qu'ils ont satisfait aux exigences en matière d'information prévues dans le présent titre.

Article 10

Dérogation aux exigences en matière d'information pour les instruments de paiement relatifs à des montants de faible valeur et la monnaie électronique

Dans le cas d'instruments de paiement qui, conformément au contrat-cadre applicable, concernent exclusivement des opérations de paiement dont le montant unitaire n'excède pas 50 EUR ou qui soit ont une limite de dépenses de 200 EUR, soit stockent des fonds dont le montant n'excède à aucun moment 200 EUR:

a) par dérogation aux articles 19, 20 et 24, le prestataire de services de paiement fournit au payeur uniquement des informations sur les principales caractéristiques du service de paiement, y compris la manière dont l'instrument de paiement peut être utilisé, la responsabilité, les frais perçus et d'autres informations concrètes nécessaires au payeur pour prendre une décision en

connaissance de cause, ainsi qu'une indication de l'endroit où les autres informations et conditions prévues à l'article 20 sont disponibles de manière aisée;

b) il peut être convenu entre les parties au contrat-cadre que, par dérogation à l'article 22, le prestataire de services de paiement n'est pas tenu de proposer une modification des clauses du contrat-cadre de la manière prévue à l'article 19, paragraphe 1;

c) il peut être convenu par les parties au contrat-cadre que, par dérogation aux articles 25 et 26, après exécution d'une opération de paiement:

i) le prestataire de services de paiement fournit ou met à disposition uniquement une référence permettant à l'utilisateur de services de paiement d'identifier l'opération de paiement, son montant et les frais ou, en cas de multiples opérations de paiement de même type au profit du même bénéficiaire, uniquement des informations concernant le montant total et les frais appliqués à ces opérations de paiement;

ii) le prestataire de services de paiement n'est pas tenu de fournir ou de mettre à disposition les informations visées au point i) si l'instrument de paiement est utilisé de manière anonyme ou si le prestataire de services de paiement n'est pas par ailleurs techniquement en mesure de les fournir. Le prestataire de services de paiement fournit au payeur la possibilité de vérifier le montant des fonds stockés.

CHAPITRE 2

Opérations de paiement isolées

Article 11

Champ d'application

1. Le présent chapitre s'applique aux opérations de paiement isolées, non couvertes par un contrat-cadre.

2. Lorsqu'un ordre de paiement relatif à une opération de paiement isolée est transmis par l'intermédiaire d'un instrument de paiement relevant d'un contrat-cadre, le prestataire de services de paiement n'est pas obligé de fournir ou de mettre à disposition des informations qui ont déjà été données à l'utilisateur de services de paiement sur la base d'un contrat-cadre avec un autre prestataire de services de paiement ou qui seront données à l'utilisateur de services de paiement conformément audit contrat-cadre.

Article 12

Informations générales préalables

1. Avant que l'utilisateur de services de paiement ne soit lié par un contrat ou une offre de service de paiement isolé, le prestataire de services de paiement met à sa disposition, sous une forme aisément accessible, les informations et les conditions

mentionnées à l'article 13 en ce qui concerne ses propres services. Sur demande de l'utilisateur de services de paiement, le prestataire de services de paiement fournit ces informations et conditions sur support papier ou sur un autre support durable. Ces informations et conditions sont fournies dans des termes aisément compréhensibles et sous une forme claire et compréhensible, dans une langue officielle de l'État membre dans lequel le service de paiement est proposé ou dans toute autre langue convenue par les parties.

2. Si, à la demande de l'utilisateur de services de paiement, le contrat de service de paiement isolé est conclu par un moyen de communication à distance ne permettant pas au prestataire de services de paiement de se conformer au paragraphe 1, ce dernier satisfait aux obligations découlant dudit paragraphe immédiatement après l'exécution de l'opération de paiement.

3. Les prestataires de services de paiement peuvent également s'acquitter des obligations découlant du paragraphe 1 en fournissant aux utilisateurs de services de paiement une copie du projet de contrat de service de paiement isolé ou du projet d'ordre de paiement comportant les informations et conditions mentionnées à l'article 13.

Article 13

Informations et conditions

1. Les prestataires de services de paiement fournissent aux utilisateurs de services de paiement ou mettent à leur disposition les informations et conditions suivantes:

   a) les informations précises ou l'identifiant unique que l'utilisateur de services de paiement doit fournir aux fins de la passation ou de l'exécution correcte de son ordre de paiement;

   b) le délai d'exécution maximal dans lequel le service de paiement doit être fourni;

   c) le délai estimé pour que les fonds des virements et des opérations de transmission de fonds soient reçus par le prestataire de services de paiement du bénéficiaire situé en dehors de l'Union;

   d) tous les frais payables par l'utilisateur de services de paiement à son prestataire de services de paiement et, le cas échéant, la ventilation de ces frais;

   e) le cas échéant, le taux de change réel ou de référence qui doit être appliqué à l'opération de paiement;

   f) le cas échéant, les frais estimés de conversion monétaire liés aux virements et aux opérations de transmission de fonds, exprimés en marge de pourcentage sur le dernier taux de change de référence applicable disponible émis par la banque centrale concernée;

   g) les procédures de règlement extrajudiciaire des litiges à la disposition de l'utilisateur de services de paiement conformément aux articles 90, 94 et 95.

2. En outre, les prestataires de services d'initiation de paiement, avant d'initier un paiement, fournissent au payeur, ou mettent à sa disposition, des informations claires et complètes sur l'ensemble des points suivants:

a) le nom du prestataire de services d'initiation de paiement, l'adresse géographique de son administration centrale, le cas échéant, l'adresse géographique de son agent ou de sa succursale dans l'État membre dans lequel le service de paiement est proposé, et toutes les autres coordonnées, y compris l'adresse électronique, à prendre en compte pour la communication avec le prestataire de services d'initiation de paiement; et

b) les coordonnées de l'autorité compétente désignée en vertu du présent règlement.

3. Le cas échéant, les autres informations et conditions utiles mentionnées à l'article 20 sont mises à la disposition de l'utilisateur de services de paiement, sous une forme aisément accessible.

Article 14

Informations destinées au payeur et au bénéficiaire après la passation d'un ordre de paiement

Lorsqu'un ordre de paiement est passé par l'intermédiaire d'un prestataire de services d'initiation de paiement, ce dernier fournit au payeur et, le cas échéant, au bénéficiaire, ou met à leur disposition immédiatement après avoir initié l'ordre de paiement l'ensemble des données suivantes :

a) une confirmation de la réussite de la passation de l'ordre de paiement auprès du prestataire de services de paiement gestionnaire du compte du payeur;

b) une référence permettant au payeur et au bénéficiaire d'identifier l'opération de paiement et, le cas échéant, permettant au bénéficiaire d'identifier le payeur, ainsi que toute information communiquée lors de l'opération de paiement;

c) le montant de l'opération de paiement;

d) s'il y a lieu, le montant des frais payables au prestataire de services d'initiation de paiement pour l'opération de paiement et, le cas échéant, la ventilation des montants de ces frais.

Article 15

Informations destinées au prestataire de services de paiement gestionnaire du compte du payeur lorsqu'un ordre de paiement est passé par l'intermédiaire d'un service d'initiation de paiement

Lorsqu'un ordre de paiement est passé par l'intermédiaire d'un prestataire de services d'initiation de paiement, ce dernier met à la disposition du prestataire de services de paiement gestionnaire du compte du payeur la référence de l'opération de paiement.

Article 16

Informations destinées au payeur après la réception de l'ordre de paiement

Immédiatement après avoir reçu l'ordre de paiement, le prestataire de services de paiement du payeur fournit à celui-ci, ou met à sa disposition, selon les modalités prévues à l'article 12, paragraphe 1, l'ensemble des données suivantes en ce qui concerne ses propres services:

a) une référence permettant au payeur d'identifier l'opération de paiement ainsi que les informations nécessaires pour permettre l'identification certaine du bénéficiaire, y compris une référence à sa dénomination commerciale;

b) le montant de l'opération de paiement exprimé dans la devise utilisée dans l'ordre de paiement;

c) le montant des frais imputables au payeur pour l'opération de paiement et, le cas échéant, la ventilation des montants de ces frais;

d) le cas échéant, le taux de change appliqué à l'opération de paiement par le prestataire de services de paiement du payeur ou une référence à ce taux, lorsqu'il est différent de celui prévu conformément à l'article 13, paragraphe 1, point e), et le montant de l'opération de paiement après cette conversion monétaire;

e) la date de réception de l'ordre de paiement.

Article 17

Informations destinées au bénéficiaire après l'exécution

Immédiatement après l'exécution de l'opération de paiement, le prestataire de services de paiement du bénéficiaire fournit à celui-ci ou met à sa disposition, selon les modalités prévues à l'article 12, paragraphe 1, l'ensemble des données suivantes en ce qui concerne ses propres services:

a) une référence permettant au bénéficiaire d'identifier l'opération de paiement et, le cas échéant, le payeur, ainsi que toute information communiquée lors de l'opération de paiement;

b) le montant de l'opération de paiement dans la devise dans laquelle les fonds sont à la disposition du bénéficiaire;

c) le montant des frais imputables au bénéficiaire pour l'opération de paiement et, le cas échéant, la ventilation des montants de ces frais;

d) le cas échéant, le taux de change appliqué à l'opération de paiement par le prestataire de services de paiement du bénéficiaire et le montant de l'opération de paiement avant cette conversion monétaire;

e) la date de valeur du crédit.

CHAPITRE 3

Contrats-cadres

Article 18

Champ d'application

Le présent chapitre s'applique aux opérations de paiement couvertes par un contrat-cadre.

Article 19

Informations générales préalables

1. Bien avant que l'utilisateur de services de paiement ne soit lié par un contrat-cadre ou une offre, le prestataire de services de paiement lui fournit, sur support papier ou sur un autre support durable, les informations et les conditions mentionnées à l'article 20. Ces informations et conditions sont fournies dans des termes aisément compréhensibles et sous une forme claire et compréhensible, dans une langue officielle de l'État membre dans lequel le service de paiement est proposé ou dans toute autre langue convenue par les parties.
2. Lorsque, à la demande de l'utilisateur de services de paiement, le contrat-cadre est conclu par un moyen de communication à distance ne permettant pas au prestataire de services de paiement de se conformer au paragraphe 1, ce dernier satisfait aux obligations découlant dudit paragraphe immédiatement après la conclusion du contrat-cadre.
3. Les prestataires de services de paiement peuvent également s'acquitter des obligations découlant du paragraphe 1 en fournissant aux utilisateurs de services de paiement une copie du projet de contrat-cadre comportant les informations et conditions mentionnées à l'article 20.

Article 20

Informations et conditions

Le prestataire de services de paiement fournit les informations et les conditions suivantes à l'utilisateur de services de paiement:

a) sur le prestataire de services de paiement:

i) le nom du prestataire de services de paiement, l'adresse géographique de son administration centrale et, le cas échéant, l'adresse géographique de son agent, de son distributeur ou de sa succursale dans l'État membre dans lequel le service de paiement est proposé, et toutes les autres adresses, y compris l'adresse de courrier électronique, à prendre en compte pour la communication avec le prestataire de services de paiement;

ii) les coordonnées des autorités de contrôle compétentes désignées en vertu de la directive (UE) [DSP3] et les coordonnées du registre prévu aux articles 17 et 18 de ladite directive ou de tout autre registre public

d’agrément pertinent du prestataire de services de paiement ainsi que son numéro d'enregistrement, ou un moyen équivalent d'identification dans ce registre;

b) sur l’utilisation du service de paiement:

i) une description des principales caractéristiques du service de paiement à fournir;

ii) les informations précises ou l’identifiant unique que l’utilisateur de services de paiement doit fournir aux fins de la passation ou de l’exécution correcte de son ordre de paiement;

iii) la forme et la procédure pour passer un ordre de paiement ou donner la permission d’exécuter une opération de paiement et pour retirer cette permission, conformément aux articles 49 et 66;

iv) une référence au moment de réception de l’ordre de paiement conformément à l’article 64 et l’éventuel délai limite établi par le prestataire de services de paiement;

v) le délai d’exécution maximal dans lequel le service de paiement doit être fourni;

vi) le délai estimé pour que les fonds des virements soient reçus par le prestataire de services de paiement du bénéficiaire situé en dehors de l’Union;

vii) la possibilité de convenir de limites de dépenses pour l’utilisation de l’instrument de paiement, conformément à l’article 51, paragraphe 1;

viii) dans le cas d’instruments de paiement liés à une carte cobadgés, les droits de l’utilisateur de services de paiement au titre de l’article 8 du règlement (UE) 2015/751;

c) sur les frais, les taux d’intérêt et les taux de change:

i) tous les frais payables par l’utilisateur de services de paiement au prestataire de services de paiement, y compris ceux liés aux modalités et à la fréquence selon lesquelles les informations prévues par le présent règlement sont fournies ou mises à disposition, et, le cas échéant, la ventilation des montants de ces frais;

ii) tous les frais éventuels que les utilisateurs de services de paiement doivent payer à leur prestataire de services de paiement pour les retraits à un distributeur automatique de billets (DAB):

1) de leur prestataire de services de paiement;

2) d’un prestataire de services de paiement appartenant au même réseau de DAB que le prestataire de services de paiement de l’utilisateur;

3) d’un prestataire de services de paiement appartenant à un réseau de DAB avec lequel le prestataire de services de paiement de l’utilisateur a une relation contractuelle;

4) d’un fournisseur de DAB qui ne gère pas de comptes de paiement lorsqu’il propose des services de retrait d’espèces;

iii) le cas échéant, les taux d'intérêt et de change à appliquer ou, si des taux d'intérêt et de change de référence doivent être utilisés, la méthode de calcul de l'intérêt réel ainsi que la date retenue et l'indice ou la base pour déterminer un tel taux d'intérêt ou de change de référence;

iv) lorsqu'il en est convenu ainsi, l'application immédiate des modifications apportées aux taux d'intérêt ou de change de référence et les exigences en matière d'informations afférentes à ces modifications, conformément à l'article 22, paragraphe 3;

v) le cas échéant, les frais estimés des services de conversion monétaire liés à un virement exprimé en marge de pourcentage sur le dernier taux de change de référence applicable disponible émis par la banque centrale concernée;

d) sur la communication:

i) le cas échéant, les moyens de communication, y compris les exigences techniques applicables à l'équipement et aux logiciels de l'utilisateur de services de paiement, convenus entre les parties aux fins de la transmission d'informations ou de notifications au titre du présent règlement;

ii) les modalités et la fréquence selon lesquelles les informations prévues par le présent règlement doivent être fournies ou mises à disposition;

iii) la ou les langues dans lesquelles le contrat-cadre sera conclu et la communication effectuée au cours de cette relation contractuelle;

iv) la mention du droit de l'utilisateur de services de paiement de recevoir les termes contractuels du contrat-cadre ainsi que les informations et conditions prévues à l'article 21;

e) sur les mesures de protection et les mesures correctives:

i) le cas échéant, une description des mesures que l'utilisateur de services de paiement doit prendre pour préserver la sécurité d'un instrument de paiement et les modalités de notification au prestataire de services de paiement aux fins de l'article 52, point b);

ii) la procédure sécurisée applicable par le prestataire de services de paiement pour la notification à l'utilisateur de services de paiement en cas de soupçon de fraude ou de fraude avérée ou de menaces pour la sécurité;

iii) lorsqu'il en est convenu ainsi, les conditions dans lesquelles le prestataire de services de paiement se réserve le droit de bloquer un instrument de paiement, conformément à l'article 51;

iv) la responsabilité du payeur conformément à l'article 57, paragraphe 5, à l'article 59, paragraphe 3, et à l'article 60, y compris des informations sur le montant concerné;

v) la manière dont l'utilisateur de services de paiement doit notifier au prestataire de services de paiement et à la police, en cas de fraude par usurpation d'identité visée à l'article 59, toute opération de paiement non autorisée ou mal initiée ou mal exécutée ou tout virement autorisé effectué à la suite d'une application incorrecte du service de vérification

de la concordance entre le nom et l'identifiant unique ou à la suite d'une fraude par usurpation d'identité, conformément à l'article 54, et le délai dont il dispose pour le faire;

vi) la responsabilité du prestataire de services de paiement en cas d'opérations de paiement non autorisées conformément à l'article 56, d'application incorrecte du service de vérification de la concordance entre le nom et l'identifiant unique conformément à l'article 57, et de fraude par usurpation d'identité conformément à l'article 59;

vii) la responsabilité du prestataire de services de paiement liée à l'initiation ou à l'exécution d'opérations de paiement, conformément aux articles 75 et 76;

viii) les conditions de remboursement conformément aux articles 62 et 63;

f) sur la modification et la résiliation d'un contrat-cadre:

i) lorsqu'il en est convenu ainsi, le fait que l'utilisateur de services de paiement est réputé avoir accepté la modification des conditions conformément à l'article 22, à moins que l'utilisateur de services de paiement n'ait notifié au prestataire de services de paiement son refus de cette modification avant la date proposée pour l'entrée en vigueur de celle-ci;

ii) la durée du contrat-cadre;

iii) le droit de l'utilisateur de services de paiement de résilier le contrat-cadre et tout accord lié à cette résiliation, conformément à l'article 22, paragraphe 1, et à l'article 23;

g) sur les recours:

i) toute clause contractuelle relative au droit applicable au contrat-cadre ou à la juridiction compétente;

ii) les procédures de règlement extrajudiciaire des litiges à la disposition de l'utilisateur de services de paiement conformément aux articles 90, 94 et 95.

Article 21

Accès aux informations et aux conditions associées au contrat-cadre

À tout moment de la relation contractuelle, l'utilisateur de services de paiement a le droit de recevoir, sur demande, les termes contractuels du contrat-cadre ainsi que les informations et conditions mentionnées à l'article 20, sur support papier ou un autre support durable.

Article 22

Modification des conditions du contrat-cadre

1. Le prestataire de services de paiement propose toute modification du contrat-cadre ou des informations et conditions mentionnées à l'article 20 selon les modalités prévues à l'article 19, paragraphe 1, et au plus tard deux mois avant la date proposée

pour son application. L'utilisateur de services de paiement peut accepter ou rejeter la modification avant la date proposée pour son entrée en vigueur.

2. Le cas échéant, conformément à l'article 20, point f) i), le prestataire de services de paiement informe l'utilisateur de services de paiement que ce dernier est réputé avoir accepté la modification s'il n'a pas notifié au prestataire de services de paiement, avant la date d'entrée en vigueur proposée de cette modification, qu'il ne l'acceptait pas. Le prestataire de services de paiement informe également l'utilisateur de services de paiement que, si ledit utilisateur rejette la modification, l'utilisateur de services de paiement a le droit de résilier le contrat-cadre sans frais et avec effet à tout moment jusqu'à la date à laquelle la modification aurait été appliquée.

3. Les modifications des taux d'intérêt ou de change peuvent être appliquées par le prestataire de services de paiement immédiatement et sans préavis, à condition que le contrat-cadre prévoie ce droit et que les modifications des taux d'intérêt ou de change se fondent sur les taux d'intérêt ou de change de référence convenus conformément à l'article 20, point c) iii) et iv). Le prestataire de services de paiement informe l'utilisateur de services de paiement le plus rapidement possible de toute modification du taux d'intérêt, selon les modalités prévues à l'article 19, paragraphe 1, à moins que les parties ne soient convenues d'une fréquence ou de modalités particulières en matière de fourniture ou de mise à disposition des informations. Néanmoins, les modifications des taux d'intérêt ou de change peuvent être appliquées sans préavis par le prestataire de services de paiement si elles sont plus favorables aux utilisateurs de services de paiement.

4. Le prestataire de services de paiement met en œuvre et calcule les modifications des taux d'intérêt ou de change appliqués aux opérations de paiement d'une manière neutre qui n'établit pas de discrimination à l'encontre des utilisateurs de services de paiement.

Article 23

Résiliation

1. L'utilisateur de services de paiement peut résilier le contrat-cadre à tout moment à moins que les parties ne soient convenues d'un délai de préavis. Ce délai n'est pas supérieur à un mois.

2. La résiliation du contrat-cadre n'entraîne aucun frais pour l'utilisateur de services de paiement, sauf si le contrat est en vigueur depuis moins de six mois. Tous frais de résiliation du contrat-cadre doivent être appropriés et correspondre aux coûts. Lorsque, en vertu du contrat-cadre, des services de paiement sont proposés conjointement avec des services techniques qui soutiennent la prestation de services de paiement et sont fournis par le prestataire de services de paiement ou par un tiers avec lequel il collabore, ces services techniques sont soumis aux mêmes exigences relatives aux frais de résiliation que le contrat-cadre.

3. Si le contrat-cadre le prévoit, le prestataire de services de paiement peut résilier un contrat-cadre conclu pour une durée indéterminée, moyennant un préavis d'au moins deux mois selon les modalités prévues à l'article 19, paragraphe 1.

4. Les frais régulièrement imputés pour la prestation de services de paiement ne sont dus par l'utilisateur de services de paiement qu'au prorata de la période échue à la

date de résiliation du contrat. S'ils ont été payés à l'avance, ces frais sont remboursés au prorata par le prestataire de services de paiement.

5. Les dispositions du présent article sont sans préjudice des dispositions législatives et réglementaires des États membres qui régissent le droit pour les parties de déclarer le contrat-cadre inexécutoire ou nul.

6. Les États membres peuvent prévoir des dispositions relatives à la résiliation plus favorables pour les utilisateurs de services de paiement.

7. Les États membres notifient à la Commission, au plus tard le [OP: veuillez insérer la date d'application du présent règlement], les dispositions légales qu'ils adoptent en application du paragraphe 6. Ils notifient, sans retard, toute modification ultérieure desdites dispositions.

Article 24

Informations à fournir avant l'exécution d'opérations de paiement individuelles

Pour toute opération de paiement individuelle initiée par le payeur et relevant d'un contrat-cadre, le prestataire de services de paiement fournit, à la demande du payeur, pour cette opération de paiement spécifique, des informations explicites sur l'ensemble des points suivants:

a) le délai d'exécution maximal;

b) les frais qui doivent être payés par le payeur;

c) le cas échéant, la ventilation des montants de ces frais.

Article 25

Informations destinées au payeur concernant les opérations de paiement individuelles

1. Après que le montant d'une opération de paiement individuelle a été débité du compte du payeur ou, lorsque le payeur n'utilise pas de compte de paiement, après réception de l'ordre de paiement, le prestataire de services de paiement du payeur fournit à celui-ci, dans les meilleurs délais et selon les modalités prévues à l'article 19, paragraphe 1, l'ensemble des informations suivantes:

a) une référence permettant au payeur d'identifier chaque opération de paiement et les informations nécessaires pour permettre l'identification certaine du bénéficiaire, y compris la dénomination commerciale du bénéficiaire;

b) le montant de l'opération de paiement exprimé dans la devise dans laquelle le compte de paiement du payeur est débité ou dans la devise utilisée dans l'ordre de paiement;

c) le montant de tous les frais appliqués à l'opération de paiement et, le cas échéant, la ventilation des montants de ces frais, ou l'intérêt dû par le payeur;

d) le cas échéant, le taux de change appliqué à l'opération de paiement par le prestataire de services de paiement du payeur et le montant de l'opération de paiement après cette conversion monétaire;

e) la date de valeur du débit ou la date de réception de l'ordre de paiement.

2. Un contrat-cadre prévoit une condition selon laquelle le payeur peut demander que les informations visées au paragraphe 1 soient fournies ou mises à disposition périodiquement, au moins une fois par mois, gratuitement et selon des modalités convenues qui permettent au bénéficiaire de les stocker et de les reproduire à l'identique.

3. Les États membres peuvent exiger que les prestataires de services de paiement fournissent ces informations sur support papier ou sur un autre support durable au moins une fois par mois gratuitement.

4. Les États membres notifient à la Commission, au plus tard le [OP: veuillez insérer la date d'application du présent règlement], les dispositions légales qu'ils adoptent en application du paragraphe 3. Ils notifient, sans retard, toute modification ultérieure desdites dispositions.

Article 26

Informations destinées au bénéficiaire concernant les opérations de paiement individuelles

1. Après avoir exécuté une opération de paiement individuelle, le prestataire de services de paiement du bénéficiaire fournit à celui-ci, dans les meilleurs délais et selon les modalités prévues à l'article 19, paragraphe 1, l'ensemble des informations suivantes:

   a) une référence permettant au bénéficiaire d'identifier l'opération de paiement et le payeur, ainsi que toute information communiquée lors de l'opération de paiement;

   b) le montant de l'opération de paiement exprimé dans la devise dans laquelle le compte de paiement du bénéficiaire est crédité;

   c) le montant de tous les frais appliqués à l'opération de paiement et, le cas échéant, la ventilation des montants de ces frais, ou l'intérêt dû par le bénéficiaire;

   d) le cas échéant, le taux de change appliqué à l'opération de paiement par le prestataire de services de paiement du bénéficiaire et le montant de l'opération de paiement avant cette conversion monétaire;

   e) la date de valeur du crédit.

2. Un contrat-cadre peut prévoir une condition selon laquelle les informations visées au paragraphe 1 doivent être fournies ou mises à disposition périodiquement, au moins une fois par mois, et selon des modalités convenues qui permettent au bénéficiaire de les stocker et de les reproduire à l'identique.

3. Les États membres peuvent exiger que les prestataires de services de paiement fournissent ces informations sur support papier ou sur un autre support durable au moins une fois par mois gratuitement.

4. Les États membres notifient à la Commission, au plus tard le [OP: veuillez insérer la date d'application du présent règlement], les dispositions légales qu'ils adoptent en application du paragraphe 3. Ils notifient, sans retard, toute modification ultérieure desdites dispositions.

TITRE III

DROITS ET OBLIGATIONS LIÉS À LA PRESTATION ET À L'UTILISATION DE SERVICES DE PAIEMENT

CHAPITRE I

Dispositions communes

Article 27

Champ d'application

1. Lorsque l'utilisateur de services de paiement n'est pas un consommateur, cet utilisateur et le prestataire de services de paiement peuvent décider que l'article 28, paragraphe 1, l'article 49, paragraphe 7, ainsi que les articles 55, 60, 62, 63, 66, 75 et 76 ne s'appliquent pas, en tout ou en partie. L'utilisateur de services de paiement et le prestataire de services de paiement peuvent également convenir de délais différents de ceux prévus à l'article 54.
2. Les États membres peuvent prévoir que l'article 95 ne s'applique pas lorsque l'utilisateur de services de paiement n'est pas un consommateur.
3. Les États membres peuvent prévoir que les dispositions du présent titre s'appliquent aux microentreprises de la même manière qu'aux consommateurs.
4. Les États membres notifient à la Commission, au plus tard le [OP: veuillez insérer la date d'application du présent règlement], les dispositions légales qu'ils adoptent en vertu des paragraphes 2 et 3. Ils notifient, sans retard, toute modification ultérieure desdites dispositions.

Article 28

Frais applicables

1. Le prestataire de services de paiement n'impute pas de frais à l'utilisateur de services de paiement pour l'accomplissement de ses obligations d'information ni pour l'exécution des mesures correctives et préventives en vertu du présent titre, sauf disposition contraire de l'article 65, paragraphe 1, de l'article 66, paragraphe 5, et de l'article 74, paragraphe 4. Ces frais sont convenus entre l'utilisateur de services de paiement et le prestataire de services de paiement, ils sont raisonnables et correspondent aux coûts réels supportés par le prestataire de services de paiement.
2. Pour les opérations de paiement effectuées à l'intérieur de l'Union, lorsque le prestataire de services de paiement du payeur et celui du bénéficiaire sont tous deux situés dans l'Union ou lorsque l'unique prestataire de services de paiement intervenant dans l'opération de paiement est situé dans l'Union, le bénéficiaire paie les frais prélevés par son prestataire de services de paiement et le payeur paie les frais prélevés par le sien.
3. Le bénéficiaire ne peut appliquer des frais pour l'utilisation d'instruments de paiement pour lesquels les commissions d'interchange sont réglementées par le

chapitre II du règlement (UE) 2015/751, ni pour les virements, y compris les virements instantanés, et les opérations de prélèvement à l'intérieur de l'Union.

4. Les États membres peuvent étendre l'interdiction ou limiter le droit du bénéficiaire d'appliquer des frais pour l'utilisation d'instruments de paiement autres que ceux visés au paragraphe 3 compte tenu de la nécessité d'encourager la concurrence et de favoriser l'utilisation de moyens de paiement efficaces.

5. Sans préjudice des paragraphes 3 et 4 et en ce qui concerne les instruments non couverts par lesdits paragraphes, le prestataire de services de paiement n'empêche pas le bénéficiaire d'appliquer des frais, ou de proposer une réduction au payeur, ou d'orienter ce dernier d'une autre manière vers l'utilisation d'un instrument de paiement donné. Les frais appliqués ne peuvent dépasser les coûts directs supportés par le bénéficiaire pour l'utilisation de cet instrument de paiement.

6. Les États membres notifient à la Commission, au plus tard le [OP: veuillez insérer la date d'application du présent règlement], les dispositions légales qu'ils adoptent en vertu du paragraphe 4. Ils notifient, sans retard, toute modification ultérieure desdites dispositions.

Article 29

Dérogation pour les instruments de paiement relatifs à des montants de faible valeur et pour la monnaie électronique

1. Dans le cas d'instruments de paiement qui, conformément au contrat-cadre, concernent uniquement des opérations de paiement individuelles dont le montant n'excède pas 50 EUR ou qui soit ont une limite de dépenses de 200 EUR, soit stockent des fonds dont le montant n'excède à aucun moment 200 EUR, les prestataires de services de paiement peuvent convenir avec leurs utilisateurs de services de paiement que:

   a) l'article 52, point b), l'article 53, paragraphe 1, points c) et d), et l'article 60, paragraphe 4, ne s'appliquent pas si l'instrument de paiement ne peut pas être bloqué ou si la poursuite de l'utilisation de celui-ci ne peut être empêchée;

   b) les articles 55 et 56 et l'article 60, paragraphes 1 et 4, ne s'appliquent pas si l'instrument de paiement est utilisé de manière anonyme ou si le prestataire de services de paiement n'est pas en mesure, pour des raisons autres qui sont inhérentes à l'instrument de paiement, d'apporter la preuve qu'une opération de paiement a été autorisée;

   c) par dérogation à l'article 65, paragraphe 1, le prestataire de services de paiement n'est pas obligé de notifier à l'utilisateur de services de paiement le refus de l'ordre de paiement si la non-exécution ressort du contexte;

   d) par dérogation à l'article 66, le payeur ne révoque pas l'ordre de paiement après avoir transmis cet ordre ou autorisé l'opération de paiement au profit du bénéficiaire;

   e) par dérogation aux articles 69 et 70, d'autres délais d'exécution s'appliquent.

2. Les articles 56 et 60 s'appliquent également à la monnaie électronique, à moins que le prestataire de services de paiement du payeur n'ait pas la capacité de bloquer le compte de paiement sur lequel la monnaie électronique est stockée ou de bloquer

l'instrument de paiement. Les États membres peuvent limiter cette dérogation aux comptes de paiement sur lesquels la monnaie électronique est stockée ou aux instruments de paiement d'une certaine valeur.

3. Les États membres notifient à la Commission, au plus tard à la date d'application du présent règlement, les dispositions légales qu'ils adoptent en vertu du paragraphe 2. Ils notifient, sans retard, toute modification ultérieure desdites dispositions.

Article 30

Émission et remboursement de la monnaie électronique

1. Les émetteurs de monnaie électronique émettent de la monnaie électronique à la valeur nominale contre la remise de fonds.

2. À la demande du détenteur de monnaie électronique, l'émetteur de monnaie électronique rembourse à tout moment et à la valeur nominale, la valeur monétaire de la monnaie électronique détenue.

3. Le contrat conclu entre l'émetteur de monnaie électronique et le détenteur de monnaie électronique établit clairement et de façon bien visible les conditions de remboursement, y compris les éventuels frais applicables, et le détenteur de monnaie électronique est informé de ces conditions avant qu'il ne soit lié par un contrat ou une offre.

4. Le remboursement de la monnaie électronique ne peut donner lieu au prélèvement de frais que si le contrat le prévoit conformément au paragraphe 3 et uniquement dans l'un des cas suivants:

   a) le détenteur de monnaie électronique demande le remboursement avant l'expiration du contrat;

   b) le contrat stipule une date d'expiration et le détenteur de monnaie électronique a mis fin au contrat avant cette date;

   c) le remboursement est demandé plus d'un an après la date d'expiration du contrat.

   Le montant des frais doit être proportionné aux coûts réels supportés par l'émetteur de monnaie électronique et en rapport avec ces coûts réels.

5. Lorsque le détenteur de monnaie électronique demande le remboursement avant l'expiration du contrat, il peut demander le remboursement de la monnaie électronique en tout ou en partie.

6. Lorsque le remboursement est demandé par le détenteur de monnaie électronique à la date d'expiration du contrat ou jusqu'à un an après cette expiration, l'émetteur de monnaie électronique:

   a) rembourse la valeur monétaire totale de la monnaie électronique; soit

   b) rembourse tous les fonds dont le remboursement est demandé par le détenteur de monnaie électronique lorsque l'établissement de paiement exerce une ou plusieurs des activités mentionnées à l'article 10, paragraphe 1, point c), de la directive XXX [DSP3] et que la proportion des fonds qui seront utilisés sous forme de monnaie électronique par les détenteurs de monnaie électronique n'est pas connue à l'avance.

7. Nonobstant les paragraphes 4, 5 et 6, les droits au remboursement des personnes, autres que les consommateurs, qui acceptent de la monnaie électronique sont soumis à l'accord contractuel entre les émetteurs de monnaie électronique et ces personnes.

8. Un établissement de paiement fournissant des services de monnaie électronique n'octroie pas, au détenteur de monnaie électronique, d'intérêts ni aucun autre avantage liés à la durée pendant laquelle le détenteur de monnaie électronique détient de la monnaie électronique.

CHAPITRE 2

Accès aux systèmes de paiement et aux comptes tenus auprès des établissements de crédit

Article 31

Accès aux systèmes de paiement

1. Les opérateurs de systèmes de paiement mettent en place des règles objectives, non discriminatoires, transparentes et proportionnées concernant l'accès à un système de paiement par des prestataires de services de paiement agréés ou enregistrés qui sont des personnes morales. Les opérateurs de systèmes de paiement n'entravent pas l'accès à un système de paiement au-delà de ce qui est nécessaire pour prévenir des risques spécifiques, y compris, le cas échéant, le risque de règlement, le risque opérationnel, le risque de crédit, le risque de liquidité et le risque d'entreprise, ou au-delà de ce qui est nécessaire pour protéger la stabilité financière et opérationnelle du système de paiement.

2. L'opérateur de système de paiement met à la disposition du public ses règles et procédures d'admission à la participation à ce système de paiement ainsi que les critères et méthodes qu'il applique pour évaluer les risques liés aux demandeurs d'une telle participation.

3. Lorsqu'il reçoit une demande de participation d'un prestataire de services de paiement, l'opérateur de système de paiement évalue les risques pertinents liés à l'octroi de l'accès au système au prestataire de services de paiement demandeur. Un opérateur de système de paiement ne refuse la participation à un prestataire de services de paiement demandeur que lorsque celui-ci présente les risques pour le système mentionnés au paragraphe 1. L'opérateur de système de paiement notifie par écrit au prestataire de services de paiement demandeur si la demande de participation est acceptée ou refusée et communique les raisons de tout refus.

4. Les paragraphes 1, 2 et 3 ne s'appliquent pas aux systèmes de paiement composés exclusivement de prestataires de services de paiement appartenant au même groupe.

5. Les opérateurs de systèmes de paiement ne mettent en place aucune des exigences suivantes:

a) des règles restrictives en ce qui concerne l'adhésion effective à d'autres systèmes de paiement;

b) des règles établissant des discriminations entre les prestataires de services de paiement agréés ou entre les prestataires de services de paiement enregistrés en ce qui concerne les droits, obligations et avantages des membres;

c) des restrictions fondées sur la forme sociale.

6. Un participant à un système de paiement qui permet à un prestataire de services de paiement agréé ou enregistré qui n'est pas un participant au système de paiement de transmettre des ordres de transfert via ledit système de paiement offre, sur demande, la même possibilité aux autres prestataires de services de paiement agréés ou enregistrés, de manière objective, proportionnée, transparente et non discriminatoire. En cas de refus d'une telle demande, le participant à un système de paiement en communique les raisons à tout prestataire de services de paiement demandeur.

7. Pour les systèmes de paiement qui ne sont pas couverts par la surveillance de l'Eurosystème en vertu du règlement (UE) nº 795/2014, les États membres désignent une autorité compétente chargée de la surveillance des systèmes de paiement afin d'assurer l'application des paragraphes 1 2, 3, 5 et 6 par les systèmes de paiement régis par leur droit national.

Article 32

Fourniture par les établissements de crédit de comptes de paiement à des établissements de paiement

1. Un établissement de crédit ne refuse d'ouvrir un compte de paiement à un établissement de paiement, à ses agents ou distributeurs ou à un demandeur d'agrément en tant qu'établissement de paiement, ou ne clôture un tel compte, que dans les cas suivants:

   a) l'établissement de crédit a de sérieuses raisons de soupçonner que les contrôles effectués par le demandeur en matière de blanchiment de capitaux ou de financement du terrorisme sont défectueux ou que des activités illégales sont commises soit par le demandeur, soit par ses clients;

   b) une violation du contrat est ou a été commise par le demandeur de compte;

   c) des informations et des documents insuffisants ont été reçus du demandeur de compte;

   d) le demandeur de compte ou son modèle économique présente un profil de risque excessif;

   e) le demandeur de compte entraînerait des coûts de mise en conformité disproportionnés pour l'établissement de crédit.

2. Les droits accordés en vertu du paragraphe 1 à des agents ou distributeurs sont accordés exclusivement pour la prestation de services de paiement pour le compte de l'établissement de paiement.

3. Un établissement de crédit notifie à l'établissement de paiement ou à ses agents ou distributeurs, ou au demandeur de l'agrément en tant qu'établissement de paiement, toute décision de refuser d'ouvrir un compte de paiement à un établissement de paiement, à ses agents ou distributeurs, ou à un demandeur d'agrément en tant qu'établissement de paiement ou toute décision de clôturer un tel compte de paiement; il motive dûment une telle décision. Cette motivation doit être spécifique aux risques représentés par l'activité ou l'activité prévue de cet établissement de

paiement ou de ses agents ou distributeurs, tels qu'évalués par l'établissement de crédit, et ne doit pas revêtir un caractère générique.

4. Un établissement de paiement ou ses agents ou distributeurs, ou un demandeur de l'agrément en tant qu'établissement de paiement qui fait l'objet d'une décision négative d'un établissement de crédit concernant l'accès aux services de comptes de paiement ou d'une décision de clôture de ces services, peuvent former un recours auprès d'une autorité compétente.

5. L'ABE élabore des projets de normes techniques de réglementation précisant le format harmonisé de la notification et de la motivation mentionnées au paragraphe 3 du présent article ainsi que les informations harmonisées qu'elles doivent contenir.

L'ABE soumet les projets de normes techniques de réglementation mentionnés au premier alinéa à la Commission au plus tard le [OP: veuillez insérer la date correspondant à un an après la date d'entrée en vigueur du présent règlement]. La Commission est habilitée à adopter les normes techniques de réglementation visées au premier alinéa, conformément aux articles 10 à 14 du règlement (UE) nº 1093/2010.

Chapitre 3

Services d'information sur les comptes et services d'initiation de paiement

SECTION 1

PRINCIPES GENERAUX

Article 33

Droits des utilisateurs de services de paiement

1. Les prestataires de services de paiement n'empêchent pas les utilisateurs de services de paiement d'avoir recours à un prestataire de services d'initiation de paiement pour obtenir les services d'initiation de paiement mentionnés à l'annexe I, point 6) . Cette prescription s'applique à tous les comptes de paiement détenus par l'utilisateur de services de paiement qui sont accessibles en ligne.

2. Les prestataires de services de paiement n'empêchent pas les utilisateurs de services de paiement d'avoir recours aux services d'information sur les comptes mentionnés à l'annexe I, point 7). Cette prescription s'applique à tous les comptes de paiement détenus par l'utilisateur de services de paiement qui sont accessibles en ligne.

Article 34

Relations contractuelles

1. La fourniture de services d'information sur les comptes et de services d'initiation de paiement n'est conditionnée par aucune partie à l'existence de relations contractuelles à cette fin entre les prestataires de tels services et un prestataire de services de paiement gestionnaire du compte.

2. Lorsqu'un accord contractuel multilatéral est en place et que les mêmes données relatives aux comptes de paiement que celles réglementées par le présent règlement sont également disponibles dans le cadre de cet accord contractuel multilatéral, l'accès des prestataires de services d'information sur les comptes et de services d'initiation de paiement aux données relatives aux comptes de paiement réglementées par le présent règlement est toujours possible sans que lesdits prestataires soient tenus d'être parties à cet accord contractuel multilatéral.

SECTION 2

INTERFACES D'ACCES AUX DONNEES POUR LES SERVICES D'INFORMATION SUR LES COMPTES ET LES SERVICES D'INITIATION DE PAIEMENT

Article 35

Fourniture d'interfaces d'accès spécifiques

1. Les prestataires de services de paiement gestionnaires de comptes qui proposent à un payeur un compte de paiement accessible en ligne mettent en place au moins une interface spécifique aux fins de l'échange de données avec les prestataires de services d'information sur les comptes et de services d'initiation de paiement.

2. Sans préjudice des articles 38 et 39, les prestataires de services de paiement gestionnaires de comptes qui proposent à un payeur un compte de paiement accessible en ligne et qui ont mis en place une interface spécifique telle que visée au paragraphe 1 du présent article ne sont pas tenus de conserver également en permanence une autre interface comme solution de secours aux fins de l'échange de données avec les prestataires de services d'information sur les comptes et de services d'initiation de paiement.

3. Les prestataires de services de paiement gestionnaires de comptes veillent à ce que leurs interfaces spécifiques mentionnées au paragraphe 1 utilisent des normes de communication émises par des organisations européennes ou internationales de normalisation telles que le Comité européen de normalisation (CEN) ou l'Organisation internationale de normalisation (ISO). Les prestataires de services de paiement gestionnaires de comptes veillent également à ce que les spécifications techniques de toutes les interfaces mentionnées au paragraphe 1 fassent l'objet d'une documentation précisant une série de routines, de protocoles et d'outils dont les prestataires de services d'initiation de paiement et les prestataires de services d'information sur les comptes ont besoin pour permettre l'interopérabilité de leurs logiciels et applications avec les systèmes d'un prestataire de services de paiement gestionnaire du compte. Les prestataires de services de paiement gestionnaires de comptes mettent à disposition, sans frais et sans retard, la documentation relative aux spécifications techniques de leurs interfaces spécifiques mentionnées au paragraphe 1, à la demande des prestataires agréés de services d'initiation de paiement et de services d'information sur les comptes ou des prestataires de services de paiement qui ont demandé l'agrément nécessaire à leurs autorités compétentes, et publient sur leur site internet un résumé de cette documentation.

4. Les prestataires de services de paiement gestionnaires de comptes veillent à ce que, sauf en cas d'urgence les empêchant de satisfaire à cette exigence, toute modification

des spécifications techniques de leur interface spécifique mentionnée au paragraphe 1 soit mise à la disposition des prestataires agréés de services d'initiation de paiement et de services d'information sur les comptes ou des prestataires de services de paiement qui ont demandé l'agrément nécessaire à leurs autorités compétentes, dans les plus brefs délais et au moins trois mois avant la mise en œuvre de la modification. Les prestataires de services de paiement gestionnaires de comptes décrivent par écrit les situations d'urgence dans lesquelles les modifications ont été mises en œuvre sans une telle information préalable et mettent cette documentation à la disposition des autorités compétentes sur demande.

5. Les prestataires de services de paiement gestionnaires de comptes publient sur leur site internet des statistiques trimestrielles relatives à la disponibilité et aux performances de leurs interfaces spécifiques. Les performances des interfaces spécifiques sont mesurées d'après le nombre de demandes d'informations sur les comptes satisfaites par rapport au nombre total de demandes d'informations sur les comptes, ainsi que d'après le nombre et le volume d'opérations des demandes d'initiation de paiement satisfaites par rapport au nombre total et au volume d'opérations total de demandes d'initiation de paiement.

6. Les prestataires de services de paiement gestionnaires de comptes mettent à disposition un dispositif d'essai, comprenant une assistance et permettant des tests de connexion aux interfaces spécifiques et des tests de fonctionnement, afin que les prestataires agréés de services d'initiation de paiement et de services d'information sur les comptes ou les prestataires de services de paiement qui ont demandé l'agrément nécessaire puissent tester les logiciels et applications qu'ils utilisent pour proposer un service de paiement aux utilisateurs. Les données de paiement sensibles ou autres données à caractère personnel ne sont pas partagées par l'intermédiaire du dispositif d'essai.

7. En cas d'erreur ou d'événement imprévu au cours de la procédure d'identification ou d'authentification ou lors de l'échange d'éléments d'information au moyen de l'interface spécifique, le prestataire de services de paiement gestionnaire du compte envoie au prestataire de services d'initiation de paiement ou au prestataire de services d'information sur les comptes un message de notification indiquant les raisons de l'erreur ou de l'événement imprévu.

Article 36

Exigences relatives aux interfaces spécifiques d'accès aux données

1. Les prestataires de services de paiement gestionnaires de comptes veillent à ce que l'interface spécifique mentionnée à l'article 35, paragraphe 1, satisfasse aux exigences de sécurité et de performance suivantes:

   a) l'interface spécifique établit et maintient des sessions de communication entre le prestataire de services de paiement gestionnaire du compte, le prestataire de services d'information sur les comptes, le prestataire de services d'initiation de paiement et tout utilisateur de services de paiement concerné tout au long de l'authentification de l'utilisateur de services de paiement;

   b) l'interface spécifique garantit l'intégrité et la confidentialité des données de sécurité personnalisées et des codes d'authentification transmis par ou via le

prestataire de services d'initiation de paiement ou le prestataire de services d'information sur les comptes;

c) le temps de réponse de l'interface spécifique aux demandes d'accès des prestataires de services d'information sur les comptes et des prestataires de services d'initiation de paiement ne dépasse pas le temps de réponse de l'interface que le prestataire de services de paiement gestionnaire du compte met à la disposition de ses utilisateurs de services de paiement pour accéder directement à leur compte de paiement en ligne.

2. Les prestataires de services de paiement gestionnaires de comptes veillent à ce que l'interface spécifique mentionnée à l'article 35, paragraphe 1, permette à la fois aux prestataires de services d'information sur les comptes et aux prestataires de services d'initiation de paiement:

a) de s'identifier auprès du prestataire de services de paiement gestionnaire du compte;

b) de donner instruction au prestataire de services de paiement gestionnaire du compte de commencer l'authentification sur la base de la permission donnée par l'utilisateur de services de paiement au prestataire de services d'information sur les comptes ou aux prestataires de services d'initiation de paiement conformément à l'article 49, paragraphe 2;

c) de faire usage, de manière non discriminatoire, de toute dérogation en matière d'authentification appliquée par le prestataire de services de paiement gestionnaire du compte;

d) de consulter, avant l'initiation du paiement dans le cas des prestataires de services d'initiation de paiement, l'identifiant unique du compte, les noms associés du titulaire du compte et les devises dont dispose l'utilisateur de services de paiement.

3. Les prestataires de services de paiement gestionnaires de comptes permettent aux prestataires de services d'information sur les comptes de communiquer de manière sécurisée, au moyen de l'interface spécifique, afin de demander et de recevoir des informations concernant un ou plusieurs comptes de paiement désignés et les opérations de paiement associées.

4. Les prestataires de services de paiement gestionnaires de comptes veillent à ce que l'interface spécifique permette aux prestataires de services d'initiation de paiement, au minimum:

a) de passer et de révoquer un ordre de paiement permanent ou un prélèvement;

b) d'initier un paiement isolé;

c) d'initier et de révoquer un paiement à date ultérieure;

d) d'initier des paiements en faveur de plusieurs bénéficiaires;

e) d'initier des paiements, que le bénéficiaire figure ou non sur la liste des bénéficiaires du payeur;

f) de communiquer de manière sécurisée pour passer un ordre de paiement à partir du compte de paiement du payeur et de recevoir toutes les informations sur l'initiation de l'opération de paiement et toutes les informations auxquelles

le prestataire de services de paiement gestionnaire du compte a accès concernant l'exécution de l'opération de paiement;

g) de vérifier le nom du titulaire du compte avant que le paiement ne soit initié, que le nom du titulaire du compte soit ou non disponible par l'intermédiaire de l'interface directe;

h) d'initier un paiement avec une seule authentification forte du client, à condition que le prestataire de services d'initiation de paiement ait fourni au prestataire de services de paiement gestionnaire du compte l'ensemble des informations suivantes:

i) l'identifiant unique du payeur;

ii) la raison sociale, la dénomination commerciale et l'«identifiant unique» du bénéficiaire;

iii) une référence d'opération;

iv) le montant du paiement et la devise du paiement sur la base desquels une seule authentification forte du client est déclenchée.

5. Les prestataires de services de paiement gestionnaires de comptes veillent à ce que l'interface spécifique fournisse aux prestataires de services d'initiation de paiement:

a) la confirmation immédiate, sur demande et sous la forme d'un simple «oui» ou «non», que le montant nécessaire à l'exécution d'une opération de paiement est disponible ou non sur le compte de paiement du payeur;

b) la confirmation par le prestataire de services de paiement gestionnaire du compte que le paiement sera exécuté sur la base des informations dont celui-ci dispose, en tenant compte de tout ordre de paiement préexistant susceptible d'empêcher l'exécution intégrale de l'ordre de paiement passé.

Les informations mentionnées au point b) ne sont pas partagées avec le prestataire de services d'initiation de paiement mais peuvent être utilisées par le prestataire de services de paiement gestionnaire du compte pour confirmer l'exécution de l'opération.

Article 37

Accès paritaire aux données depuis l'interface d'accès spécifique et l'interface client

1. Sans préjudice de l'article 36, les prestataires de services de paiement gestionnaires de comptes veillent à ce que leur interface spécifique mentionnée à l'article 35, paragraphe 1, offre à tout moment au moins le même niveau de disponibilité et de performances, y compris en ce qui concerne l'assistance technique et informatique, que les interfaces qu'ils mettent à la disposition de l'utilisateur de services de paiement pour qu'il accède directement à son compte de paiement en ligne.

2. Les prestataires de services de paiement gestionnaires de comptes fournissent aux prestataires de services d'information sur les comptes au moins les mêmes informations provenant des comptes de paiement désignés et des opérations de paiement associées que celles qui sont mises à la disposition de l'utilisateur de services de paiement en cas de demande directe d'accès aux informations sur le compte, pour autant que ces informations ne comportent pas de données de paiement sensibles.

3. Les prestataires de services de paiement gestionnaires de comptes fournissent aux prestataires de services d'initiation de paiement au moins les mêmes informations sur l'initiation et l'exécution de l'opération de paiement que celles qui sont fournies à l'utilisateur de services de paiement ou mises à sa disposition lorsque ce dernier initie directement l'opération. Ces informations sont fournies immédiatement après la réception de l'ordre de paiement et en continu jusqu'à ce que le paiement soit définitif.

Article 38

Mesures d'urgence en cas d'indisponibilité d'une interface spécifique

1. Les prestataires de services de paiement gestionnaires de comptes prennent toutes les mesures en leur pouvoir pour éviter l'indisponibilité de l'interface spécifique. Une indisponibilité peut être présumée lorsque cinq demandes consécutives d'accès aux informations pour la prestation de services d'initiation de paiement ou de services d'information sur les comptes n'obtiennent pas de réponse de l'interface spécifique du prestataire de services de paiement gestionnaire du compte dans les 30 secondes.

2. En cas d'indisponibilité de l'interface spécifique, les prestataires de services de paiement gestionnaires de comptes informent les prestataires de services de paiement utilisant cette interface des mesures prises pour rétablir l'interface et du délai estimé nécessaire pour résoudre le problème. Pendant la période d'indisponibilité, les prestataires de services de paiement gestionnaires de comptes proposent sans tarder aux prestataires de services d'information sur les comptes et de services d'initiation de paiement une autre solution efficace, telle que l'utilisation de l'interface que le prestataire de services de paiement gestionnaire du compte utilise pour l'authentification et la communication avec ses utilisateurs pour l'accès aux données des comptes de paiement.

3. Lorsque l'interface spécifique n'est pas disponible et que le prestataire de services de paiement gestionnaire du compte n'a pas proposé une autre solution rapide et efficace conformément au paragraphe 2, les prestataires de services d'initiation de paiement ou les prestataires de services d'information sur les comptes peuvent demander à leur autorité compétente, en lui fournissant toutes les informations et preuves nécessaires, de les autoriser à utiliser l'interface que le prestataire de services de paiement gestionnaire du compte utilise pour l'authentification et la communication avec ses utilisateurs pour l'accès aux données des comptes de paiement.

4. Sur la base de la demande mentionnée au paragraphe 3, l'autorité compétente peut, pour une durée limitée jusqu'au rétablissement de la disponibilité de l'interface spécifique, autoriser tous les prestataires de services d'initiation de paiement et prestataires de services d'information sur les comptes à accéder aux données des comptes de paiement par l'intermédiaire d'une interface que le prestataire de services de paiement gestionnaire du compte utilise pour l'authentification et la communication avec ses utilisateurs. L'autorité compétente communique sa décision au prestataire de services d'information sur les comptes ou au prestataire de services d'initiation de paiement demandeur et la publie sur son site internet. L'autorité compétente donne instruction au prestataire de services de paiement gestionnaire du compte de rétablir le bon fonctionnement de l'interface spécifique avant l'expiration de l'autorisation temporaire.

5. L’autorité compétente statue dans les meilleurs délais sur toute demande introduite au titre du paragraphe 3. Tant que l’autorité compétente n’a pas statué sur la demande, le prestataire de services d’initiation de paiement ou le prestataire de services d’information sur les comptes demandeur peut exceptionnellement accéder aux données relatives aux comptes de paiement par l’intermédiaire d’une interface que le prestataire de services de paiement gestionnaire du compte utilise pour l’authentification et la communication avec ses utilisateurs. Le prestataire de services d’initiation de paiement ou le prestataire de services d’information sur les comptes demandeur cesse d’user de cette possibilité lorsque la disponibilité de l’interface spécifique est rétablie ou lorsque l’autorité compétente adopte une décision refusant une telle utilisation, l'événement déterminant étant celui qui se produit le premier.

6. Dans les cas où les prestataires de services de paiement gestionnaires de comptes sont tenus d’autoriser les prestataires de services d’information sur les comptes ou les prestataires de services d’initiation de paiement à accéder à l’interface qu'ils utilisent pour l’authentification et la communication avec leurs utilisateurs, les prestataires de services de paiement gestionnaires de comptes mettent immédiatement à disposition toutes les spécifications techniques nécessaires aux prestataires de services d’information sur les comptes ou aux prestataires de services d’initiation de paiement pour se connecter de manière adéquate à l’interface qu'ils utilisent pour l’authentification et la communication avec leurs utilisateurs.

7. Lorsqu’ils accèdent à l’interface que le prestataire de services de paiement gestionnaire du compte utilise pour l’authentification et la communication avec ses utilisateurs, les prestataires de services d’information sur les comptes ou les prestataires de services d’initiation de paiement satisfont à toutes les exigences énoncées à l’article 45, paragraphe 2. En particulier, les prestataires de services d’information sur les comptes ou les prestataires de services d’initiation de paiement s’identifient toujours dûment auprès du prestataire de services de paiement gestionnaire du compte.

Article 39

Dérogation à l’obligation de disposer d’une interface spécifique pour l’accès aux données

1. Par dérogation à l’article 35, paragraphe 1, à la demande d’un prestataire de services de paiement gestionnaire du compte, l’autorité compétente peut exempter ce dernier de l’obligation de disposer d’une interface spécifique et l’autoriser soit à proposer, comme interface pour l’échange sécurisé de données, l’une des interfaces que le prestataire de services de paiement gestionnaire du compte utilise pour l’authentification et la communication avec ses utilisateurs de services de paiement, soit, lorsque cela se justifie, à ne proposer aucune interface pour un échange sécurisé de données.

2. L’ABE élabore des projets de normes techniques de réglementation qui précisent les critères sur la base desquels, conformément au paragraphe 1, un prestataire de services de paiement gestionnaire du compte peut être exempté de l’obligation de disposer d’une interface spécifique et être autorisé soit à fournir, comme interface pour l’échange sécurisé de données avec les prestataires de services d’information sur les comptes et les prestataires de services d’initiation de paiement, l’interface qu’il met à la disposition de son utilisateur de services de paiement pour lui

permettre d'accéder à ses comptes de paiement en ligne, soit, le cas échéant, à ne disposer d'aucune interface pour un échange sécurisé de données.

L'ABE soumet les projets de normes techniques de réglementation mentionnés au premier alinéa à la Commission au plus tard le [OP: veuillez insérer la date correspondant à un an après la date d'entrée en vigueur du présent règlement]. La Commission est habilitée à adopter les normes techniques de réglementation mentionnées au premier alinéa, conformément aux articles 10 à 14 du règlement (UE) nº 1093/2010.

SECTION 3

DROITS ET OBLIGATIONS DES PRESTATAIRES DE SERVICES DE PAIEMENT GESTIONNAIRES DE COMPTES

Article 40

Obligations incombant aux prestataires de services de paiement gestionnaires de comptes en ce qui concerne les services d'initiation de paiement

Le prestataire de services de paiement gestionnaire du compte prend les mesures suivantes pour garantir le droit du payeur d'utiliser le service d'initiation de paiement:

a) il communique de manière sécurisée avec les prestataires de services d'initiation de paiement;

b) immédiatement après avoir reçu l'ordre de paiement d'un prestataire de services d'initiation de paiement, il fournit au prestataire de services d'initiation de paiement, ou met à sa disposition, toutes les informations sur l'initiation de l'opération de paiement et toutes les informations auxquelles il a lui-même accès concernant l'exécution de l'opération de paiement;

c) il traite les ordres de paiement transmis grâce aux services d'un prestataire de services d'initiation de paiement comme si ces ordres de paiement avaient été transmis directement par le payeur ou le bénéficiaire, en particulier en ce qui concerne le délai, la priorité ou les frais.

Aux fins du point b), lorsque tout ou partie des informations figurant audit point ne sont pas disponibles immédiatement après la réception de l'ordre de paiement, le prestataire de services de paiement gestionnaire du compte veille à ce que toute information relative à l'exécution de l'ordre de paiement soit mise à la disposition du prestataire de services d'initiation de paiement dès qu'il dispose de ces informations.

Article 41

Obligations des prestataires de services de paiement gestionnaires de comptes en ce qui concerne les services d'information sur les comptes

1. Le prestataire de services de paiement gestionnaire du compte prend les mesures suivantes pour garantir le droit de l'utilisateur de services de paiement d'utiliser le service d'information sur les comptes:

a) il communique de manière sécurisée avec le prestataire de services d'information sur les comptes;

b) il traite les demandes de données transmises par l'intermédiaire des services d'un prestataire de services d'information sur les comptes comme si les données étaient demandées par l'utilisateur de services de paiement au moyen de l'interface que le prestataire de services de paiement gestionnaire du compte met à la disposition de ses utilisateurs de services de paiement pour leur permettre d'accéder directement à leur compte de paiement.

2. Les prestataires de services de paiement gestionnaires de comptes permettent aux prestataires de services d'information sur les comptes d'accéder aux informations provenant des comptes de paiement désignés et des opérations de paiement associées qui sont détenues par les prestataires de services de paiement gestionnaires de comptes aux fins de la prestation des services d'information sur les comptes, que l'utilisateur de services de paiement demande ou non spontanément ces informations.

Article 42

Restriction de l'accès des prestataires de services d'information sur les comptes et des prestataires de services d'initiation de paiement aux comptes de paiement

1. Un prestataire de services de paiement gestionnaire du compte peut refuser à un prestataire de services d'information sur les comptes ou à un prestataire de services d'initiation de paiement l'accès à un compte de paiement pour des raisons objectivement motivées et documentées. Ces raisons sont liées à un accès non autorisé au compte de paiement, au sens de l'article 49, paragraphe 3, ou à un accès frauduleux au compte de paiement par ce prestataire de services d'information sur les comptes ou ce prestataire de services d'initiation de paiement, y compris à l'initiation non autorisée ou frauduleuse d'une opération de paiement. Dans ces cas, le prestataire de services de paiement gestionnaire du compte informe l'utilisateur de services de paiement du refus d'accès au compte de paiement et lui fournit les raisons de ce refus. Cette information est, si possible, donnée à l'utilisateur de services de paiement avant que l'accès ne soit refusé et au plus tard immédiatement après ce refus, à moins que le fait de fournir cette information ne soit pas acceptable pour des raisons de sécurité objectivement justifiées ou soit interdit par une autre disposition du droit de l'Union ou de droit national pertinente.

2. Dans les cas mentionnés au paragraphe 1, le prestataire de services de paiement gestionnaire du compte notifie immédiatement à l'autorité compétente l'incident concernant le prestataire de services d'information sur les comptes ou le prestataire de services d'initiation de paiement. La notification contient les informations pertinentes relatives à la situation et les raisons justifiant les mesures prises. L'autorité compétente évalue la situation et prend au besoin des mesures appropriées.

Article 43

Gestion de l'accès aux données par les utilisateurs de services de paiement

1. Le prestataire de services de paiement gestionnaire du compte fournit à l'utilisateur de services de paiement un tableau de bord, intégré dans son interface utilisateur, pour contrôler et gérer les permissions que celui-ci a accordées aux fins des services

d'information sur les comptes ou des services d'initiation de paiement portant sur des paiements multiples ou récurrents.

2. Le tableau de bord:

a) fournit à l'utilisateur de services de paiement une vue d'ensemble de chaque permission en cours accordée aux fins de services d'information sur les comptes ou de services d'initiation de paiement, comprenant:

i) le nom du prestataire de services d'information sur les comptes ou du prestataire de services d'initiation de paiement auquel l'accès a été accordé;

ii) le compte client auquel l'accès a été accordé;

iii) l'objet de la permission;

iv) la durée de validité de la permission;

v) les catégories de données partagées;

b) permet à l'utilisateur de services de paiement de retirer à un prestataire de services d'information sur les comptes ou prestataire de services d'initiation de paiement donné l'accès aux données;

c) permet à l'utilisateur de services de paiement de rétablir tout accès aux données retiré;

d) comporte un registre des permissions d'accès aux données qui ont été retirées ou qui ont expiré sur une durée de deux ans.

3. Le prestataire de services de paiement gestionnaire du compte veille à ce que le tableau de bord soit facile à trouver dans son interface utilisateur et à ce que les informations qui s'affichent sur le tableau de bord soient claires, précises et facilement compréhensibles pour l'utilisateur de services de paiement.

4. Le prestataire de services de paiement gestionnaire du compte et le prestataire de services d'information sur les comptes ou de services d'initiation de paiement auquel la permission a été accordée coopèrent pour mettre les informations à la disposition de l'utilisateur de services de paiement sur le tableau de bord en temps réel. Aux fins du paragraphe 2, points a), b), c) et e):

a) le prestataire de services de paiement gestionnaire du compte informe en temps réel le prestataire de services d'information sur les comptes ou de services d'initiation de paiement des modifications apportées, au moyen du tableau de bord, par un utilisateur de services de paiement à une permission concernant ce prestataire;

b) un prestataire de services d'information sur les comptes ou de services d'initiation de paiement informe en temps réel le prestataire de services de paiement gestionnaire du compte de toute nouvelle permission accordée par un utilisateur de services de paiement concernant un compte de paiement fourni par ce prestataire de services de paiement gestionnaire du compte, en précisant:

i) la finalité de la permission accordée par l'utilisateur de services de paiement;

ii) la durée de validité de la permission;

iii) les catégories de données concernées.

Article 44

Entraves interdites à l'accès aux données

1. Les prestataires de services de paiement gestionnaires de comptes veillent à ce que leur interface spécifique n'entrave pas la prestation de services d'initiation de paiement et de services d'information sur les comptes.

   Constituent des entraves interdites:

   a) le fait d'empêcher l'utilisation par les prestataires de services d'initiation de paiement ou les prestataires de services d'information sur les comptes des données de sécurité émises par les prestataires de services de paiement gestionnaires de comptes à l'intention de leurs utilisateurs de services de paiement;

   b) le fait d'exiger des utilisateurs de services de paiement qu'ils saisissent manuellement leur identifiant unique dans le domaine du prestataire de services de paiement gestionnaire du compte pour pouvoir utiliser les services d'information sur les comptes ou d'initiation de paiement;

   c) le fait de demander des vérifications supplémentaires de la permission donnée par les utilisateurs de services de paiement à un prestataire de services d'initiation de paiement ou à un prestataire de services d'information sur les comptes;

   d) le fait d'exiger des prestataires de services d'initiation de paiement et de services d'information sur les comptes des enregistrements supplémentaires pour qu'ils puissent accéder au compte de paiement de l'utilisateur de services de paiement ou à l'interface spécifique;

   e) le fait d'exiger, sauf si cela est indispensable pour faciliter l'échange d'informations entre les prestataires de services de paiement gestionnaires de comptes et les prestataires de services d'initiation de paiement et de services d'information sur les comptes en liaison, en particulier, avec la mise à jour du tableau de bord visé à l'article 43, que les prestataires de services d'initiation de paiement et de services d'information sur les comptes enregistrent préalablement leurs coordonnées auprès du prestataire de services de paiement gestionnaire du compte;

   f) le fait de limiter la possibilité pour un utilisateur de services de paiement d'initier des paiements par l'intermédiaire d'un prestataire de services d'initiation de paiement aux seuls bénéficiaires figurant sur la liste des bénéficiaires du payeur;

   g) le fait de limiter les initiations de paiement aux opérations vers les identifiants uniques nationaux ou à partir de ces derniers;

   h) le fait d'exiger que l'authentification forte du client soit appliquée plus fréquemment que l'authentification forte du client requise par le prestataire de services de paiement gestionnaire du compte lorsque l'utilisateur de services de paiement accède directement à son compte de paiement ou initie un paiement à l'aide du prestataire de services de paiement gestionnaire du compte;

   i) le fait de fournir une interface spécifique qui ne prend pas en charge toutes les procédures d'authentification mises à la disposition de son utilisateur de

services de paiement par le prestataire de services de paiement gestionnaire du compte;

j) le fait d'imposer un parcours d'information sur le compte ou d'initiation de paiement selon une approche de «redirection» ou «découplée», consistant à ce que l'authentification de l'utilisateur de services de paiement auprès du prestataire de services de paiement gestionnaire du compte ajoute des étapes ou des actions obligatoires dans le parcours de l'utilisateur par rapport à la procédure d'authentification équivalente proposée aux utilisateurs de services de paiement lorsqu'ils accèdent directement à leurs comptes de paiement ou initient un paiement à l'aide du prestataire de services de paiement gestionnaire du compte;

k) le fait d'imposer que l'utilisateur soit automatiquement redirigé, au stade de l'authentification, vers l'adresse de la page internet du prestataire de services de paiement gestionnaire du compte lorsque c'est la seule méthode d'authentification de l'utilisateur de services de paiement qui est prise en charge par un prestataire de services de paiement gestionnaire du compte;

l) le fait d'exiger deux authentifications fortes du client dans le cadre d'un parcours du seul service d'initiation de paiement lorsque le prestataire de services d'initiation de paiement transmet au prestataire de services de paiement gestionnaire du compte toutes les informations nécessaires pour initier le paiement, à savoir une authentification forte du client pour la confirmation par «oui/non» et une deuxième authentification forte du client pour l'initiation du paiement.

2. Concernant les activités des prestataires de services d'initiation de paiement et des prestataires de services d'information sur les comptes, le nom et le numéro de compte du titulaire du compte ne constituent pas des données de paiement sensibles.

SECTION 4

DROITS ET OBLIGATIONS DES PRESTATAIRES DE SERVICES D'INFORMATION SUR LES COMPTES ET DES PRESTATAIRES DE SERVICES D'INITIATION DE PAIEMENT

Article 45

Utilisation de l'interface client par les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement

1. Les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement accèdent aux données des comptes de paiement exclusivement au moyen de l'interface spécifique mentionnée à l'article 35, sauf dans les circonstances énoncées à l'article 38, paragraphes 4 et 5, et à l'article 39.

2. Lorsqu'un prestataire de services d'information sur les comptes ou un prestataire de services d'initiation de paiement accède aux données d'un compte de paiement par l'intermédiaire d'une interface que le prestataire de services de paiement gestionnaire du compte met à la disposition de ses utilisateurs de services de paiement pour leur permettre d'accéder directement à leur compte de paiement, conformément à l'article 38, paragraphes 4 et 5, ou lorsqu'il s'agit de la seule interface accessible

conformément à l'article 39, le prestataire de services d'information sur les comptes ou le prestataire de services d'initiation de paiement, à tout moment:

a) s'identifie auprès du prestataire de services de paiement gestionnaire du compte;

b) se fonde sur les procédures d'authentification prévues par le prestataire de services de paiement gestionnaire du compte à l'intention de l'utilisateur de services de paiement;

c) prend les mesures nécessaires pour garantir qu'il ne traite pas de données (ni n'accède à des données ou ne conserve des données) à des fins autres que la prestation du service demandé par l'utilisateur de services de paiement;

d) enregistre les données auxquelles il a accès par l'intermédiaire de l'interface exploitée par le prestataire de services de paiement gestionnaire du compte pour ses utilisateurs de services de paiement et fournit ce registre, sur demande et dans les meilleurs délais, à l'autorité compétente. Les registres sont effacés trois ans après leur création. Les registres peuvent être conservés plus longtemps s'ils sont nécessaires à des procédures de contrôle déjà en cours.

Aux fins du point d), les registres sont effacés trois ans après leur création. Les registres peuvent être conservés plus longtemps s'ils sont nécessaires à des procédures de contrôle déjà en cours.

Article 46

Obligations spécifiques des prestataires de services d'initiation de paiement

1. Les prestataires de services d'initiation de paiement:

a) fournissent aux prestataires de services de paiement gestionnaires de comptes les mêmes informations que celles qui sont demandées à l'utilisateur de services de paiement lors de l'initiation directe de l'opération de paiement;

b) fournissent des services uniquement sur la base de la permission de l'utilisateur de services de paiement, conformément à l'article 49;

c) ne détiennent à aucun moment les fonds du payeur en liaison avec la prestation du service d'initiation de paiement;

d) veillent à ce que les données de sécurité personnalisées de l'utilisateur de services de paiement ne soient pas accessibles à d'autres parties que le payeur et l'émetteur desdites données et veillent à transmettre celles-ci au moyen de canaux sûrs et efficaces;

e) veillent à ce que toute autre information relative à l'utilisateur de services de paiement obtenue lors de la prestation de services d'initiation de paiement ne soit communiquée qu'au bénéficiaire et uniquement avec la permission de l'utilisateur de services de paiement;

f) chaque fois qu'un paiement est initié, s'identifient auprès du prestataire de services de paiement gestionnaire du compte et communiquent avec ce dernier, avec le payeur et avec le bénéficiaire de manière sécurisée.

2. Les prestataires de services d'initiation de paiement:

a) ne stockent pas de données de paiement sensibles concernant l'utilisateur de services de paiement;

b) ne demandent pas à l'utilisateur de services de paiement des données autres que celles nécessaires pour fournir le service d'initiation de paiement;

c) ne traitent pas des données à caractère personnel ou non personnel (c'est-à-dire ni n'utilisent, ni ne consultent, ni ne conservent des données) à des fins autres que la prestation du service d'initiation de paiement autorisée par l'utilisateur de services de paiement;

d) ne modifient pas le montant, le bénéficiaire ou tout autre caractéristique de l'opération.

Article 47

Obligations spécifiques et autres dispositions concernant les prestataires de services d'information sur les comptes

1. Le prestataire de services d'information sur les comptes:

a) fournit des services uniquement sur la base de la permission de l'utilisateur de services de paiement, conformément à l'article 49;

b) veille à ce que les données de sécurité personnalisées de l'utilisateur de services de paiement ne soient pas accessibles à d'autres parties que l'utilisateur et l'émetteur desdites données et veille, lorsqu'il transmet celles-ci, à utiliser à cet effet des canaux sûrs et efficaces;

c) pour chaque session de communication, s'identifie auprès du prestataire de services de paiement gestionnaire du compte de l'utilisateur de services de paiement et communique avec le prestataire de services de paiement gestionnaire du compte et l'utilisateur de services de paiement de manière sécurisée;

d) accède uniquement aux informations provenant des comptes de paiement désignés et des opérations de paiement associées;

e) met en place des mécanismes appropriés et efficaces qui empêchent l'accès à d'autres informations que celles provenant des comptes de paiement désignés et des opérations de paiement associées, conformément à la permission de l'utilisateur de services de paiement.

2. Le prestataire de services d'information sur les comptes:

a) ne demande pas des données de paiement sensibles liées à des comptes de paiement;

b) n'utilise pas, ni ne consulte, ni ne stocke des données à des fins autres que la prestation du service d'information sur les comptes autorisée par l'utilisateur de services de paiement, conformément au règlement (UE) 2016/679.

3. Les articles suivants ne s'appliquent pas aux prestataires de services d'information sur les comptes: articles 4 à 8, articles 10, 11 et 12, articles 14 à 19, articles 21 à 29, articles 50 et 51, articles 53 à 79 et articles 83 et 84.

SECTION 5

MISE EN ŒUVRE

Article 48

Rôle des autorités compétentes

1. Les autorités compétentes veillent à ce que les prestataires de services de paiement gestionnaires de comptes respectent à tout moment leurs obligations en ce qui concerne l'interface spécifique mentionnée à l'article 35, paragraphe 1, et à ce que toute entrave interdite visée à l'article 44 soit immédiatement levée par le prestataire de services de paiement gestionnaire du compte concerné. Lorsqu'elles constatent que les interfaces spécifiques ne sont pas conformes au présent règlement ou qu'il existe des entraves, notamment sur la base des informations transmises par les prestataires de services d'initiation de paiement et de services d'information sur les comptes, les autorités compétentes prennent sans tarder les mesures d'application nécessaires et imposent toute sanction appropriée ou, le cas échéant, accordent les droits d'accès prévus à l'article 38, paragraphe 4.
2. Les autorités compétentes prennent sans délai toutes les mesures visant à faire respecter la réglementation requises lorsque cela est nécessaire pour préserver les droits d'accès des prestataires de services d'initiation de paiement et de services d'information sur les comptes. Les mesures visant à faire respecter la réglementation peuvent comprendre des sanctions appropriées.
3. Les autorités compétentes veillent à ce que les prestataires de services d'initiation de paiement et de services d'information sur les comptes respectent à tout moment leurs obligations relatives à l'utilisation des interfaces d'accès aux données.
4. Les autorités compétentes disposent des ressources nécessaires, notamment en ce qui concerne le personnel spécialisé, pour s'acquitter à tout moment de leurs missions.
5. Les autorités compétentes coopèrent avec les autorités de contrôle au titre du règlement (UE) 2016/679 en ce qui concerne le traitement de données à caractère personnel.
6. Les autorités compétentes tiennent régulièrement, à leur initiative, des réunions conjointes avec les prestataires de services de paiement gestionnaires de comptes et les prestataires de services d'initiation de paiement et de services d'information sur les comptes et mettent tout en œuvre pour faire en sorte que les problèmes éventuels découlant de l'utilisation des interfaces d'échange de données et de l'accès à ces interfaces entre les prestataires de services de paiement gestionnaires de comptes et les prestataires de services d'initiation de paiement et de services d'information sur les comptes soient résolus rapidement et durablement.
7. Les prestataires de services de paiement gestionnaires de comptes fournissent aux autorités compétentes des données sur l'accès des prestataires de services d'information sur les comptes et de services d'initiation de paiement aux comptes de paiement qu'ils gèrent. Les autorités compétentes peuvent également, le cas échéant, exiger des prestataires de services d'information sur les comptes et des prestataires

de services d'initiation de paiement qu'ils fournissent toutes les données pertinentes sur leurs opérations. Conformément aux pouvoirs qui lui sont conférés en vertu de l'article 29, point b), de l'article 31 et de l'article 35, paragraphe 2, du règlement (UE) nº 1093/2010, l'ABE coordonne cette activité de surveillance menée par les autorités compétentes, en évitant les communications de données faisant double emploi. L'ABE présente tous les deux ans à la Commission un rapport sur la taille et le fonctionnement des marchés des services d'information sur les comptes et des services d'initiation de paiement dans l'Union. Ces rapports périodiques peuvent, le cas échéant, contenir des recommandations.

8. L'ABE élabore des projets de normes techniques de réglementation précisant les données à fournir aux autorités compétentes en vertu du paragraphe 7 ainsi que la méthode et la périodicité à appliquer pour la fourniture de ces données.

L'ABE soumet ces projets de normes techniques de réglementation à la Commission au plus tard le [OP: veuillez insérer la date correspondant à 18 mois après la date d'entrée en vigueur du présent règlement].

La Commission est habilitée à adopter les normes techniques de réglementation mentionnées au premier alinéa, conformément aux articles 10 à 14 du règlement (UE) nº 1093/2010.

CHAPITRE 4

Autorisation des opérations de paiement

Article 49

Autorisation

1. Une opération de paiement ou une série d'opérations de paiement n'est autorisée que si le payeur a donné sa permission à l'exécution de l'opération de paiement. Une opération de paiement peut être autorisée par le payeur avant ou, si le payeur et le prestataire de services de paiement gestionnaire du compte en ont convenu ainsi, après son exécution.

2. L'accès de prestataires de services de paiement à un compte de paiement aux fins de services d'information sur les comptes ou de services d'initiation de paiement n'est autorisé que si l'utilisateur de services de paiement a donné, selon le cas, au prestataire de services d'information sur les comptes ou au prestataire de services d'initiation de paiement la permission d'accéder au compte de paiement et aux données pertinentes de ce compte.

3. En l'absence de permission, une opération de paiement ou l'accès d'un prestataire de services d'information sur les comptes ou d'un prestataire de services d'initiation de paiement à un compte de paiement sont réputés non autorisés.

4. Les prestataires de services de paiement gestionnaires de comptes ne vérifient pas la permission donnée par l'utilisateur de services de paiement au prestataire de services d'information sur les comptes ou au prestataire de services d'initiation de paiement.

5. La permission visée aux paragraphes 1 et 2 est exprimée sous la forme convenue entre le payeur et le prestataire de services de paiement concerné. La permission de

l'exécution d'une opération de paiement peut aussi être donnée par l'intermédiaire du bénéficiaire ou du prestataire de services d'initiation de paiement.

6. La procédure pour donner la permission fait l'objet d'un accord entre le payeur et le prestataire de services de paiement concerné.

7. L'utilisateur de services de paiement peut retirer à tout moment la permission d'exécuter une opération de paiement ou d'accéder à un compte de paiement aux fins de services d'initiation de paiement ou de services d'information sur les comptes. L'utilisateur de services de paiement peut également retirer la permission d'exécuter une série d'opérations de paiement, auquel cas toute opération de paiement postérieure est réputée non autorisée.

Article 50

Divergences entre le nom du bénéficiaire et son identifiant unique dans le cas de virements

1. Dans le cas de virements, le prestataire de services de paiement du bénéficiaire vérifie gratuitement, à la demande du prestataire de services de paiement du payeur, la concordance entre l'identifiant unique et le nom du bénéficiaire fournis par le payeur et communique le résultat de cette vérification au prestataire de services de paiement du payeur. Si l'identifiant unique et le nom du bénéficiaire ne concordent pas, le prestataire de services de paiement du payeur notifie au payeur toute divergence détectée et l'informe du degré de cette divergence.

2. Les prestataires de services de paiement fournissent le service visé au paragraphe 1 immédiatement après que le payeur a communiqué à son prestataire de services de paiement l'identifiant unique et le nom du bénéficiaire, et avant que le payeur n'ait la possibilité d'autoriser le virement.

3. Les prestataires de services de paiement veillent à ce que la détection et la notification d'une divergence mentionnées au paragraphe 1 n'empêchent pas les payeurs d'autoriser le virement concerné. Si le payeur, après avoir été informé d'une divergence détectée, autorise le virement et que l'opération est exécutée conformément à l'identifiant unique communiqué par le payeur, cette opération est réputée être correctement exécutée.

4. Les prestataires de services de paiement veillent à ce que les utilisateurs de services de paiement aient le droit de renoncer à ce que le service mentionné au paragraphe 1 leur soit proposé et informent leurs utilisateurs de la manière d'exercer ce droit. Les prestataires de services de paiement veillent à ce que les utilisateurs de services de paiement qui ont initialement choisi de renoncer à recevoir le service mentionné au paragraphe 1 aient le droit de choisir de le recevoir à nouveau.

5. Les prestataires de services de paiement informent leurs utilisateurs de services de paiement que l'autorisation d'une opération malgré la détection et la notification d'une divergence ou le choix de renoncer à recevoir le service mentionné au paragraphe 1 peuvent conduire à ce que les fonds soient virés sur un compte de paiement non détenu par le bénéficiaire indiqué par le payeur. Les prestataires de services de paiement fournissent cette information en même temps que la notification de divergences ou au moment où l'utilisateur de services de paiement choisit de renoncer à recevoir le service mentionné au paragraphe 1.

6. Le service mentionné au paragraphe 1 est fourni pour les ordres de paiement passés par l'intermédiaire de canaux d'initiation de paiement électroniques et par l'intermédiaire d'ordres de paiement non électroniques nécessitant une interaction en temps réel entre le payeur et le prestataire de services de paiement du payeur.

7. Le service de vérification de la concordance mentionné au paragraphe 1 n'est pas exigé lorsque le payeur n'a pas saisi lui-même l'identifiant unique et le nom du bénéficiaire.

8. Le présent article ne s'applique pas aux virements instantanés libellés en euros relevant du champ d'application du règlement XXX (règlement sur les paiements instantanés).

Article 51

Limitation et blocage de l'utilisation des instruments de paiement

1. Lorsqu'un instrument de paiement spécifique est utilisé aux fins de donner une permission, le payeur et le prestataire de services de paiement peuvent convenir de limites de dépenses pour les opérations de paiement exécutées au moyen dudit instrument de paiement. Les prestataires de services de paiement n'augmentent pas unilatéralement les limites de dépenses convenues avec leurs utilisateurs de services de paiement.

2. Si le contrat-cadre le prévoit, le prestataire de services de paiement peut se réserver le droit de bloquer l'instrument de paiement, pour des raisons objectivement motivées ayant trait à la sécurité de l'instrument de paiement, à des soupçons d'utilisation non autorisée ou frauduleuse de l'instrument de paiement ou, s'il s'agit d'un instrument de paiement doté d'une ligne de crédit, au risque sensiblement accru que le payeur soit dans l'incapacité de s'acquitter de son obligation de paiement.

3. Dans ces cas, le prestataire de services de paiement informe le payeur, de la manière convenue, du blocage de l'instrument de paiement et des raisons de ce blocage, si possible avant que l'instrument de paiement ne soit bloqué et au plus tard immédiatement après, à moins que le fait de fournir cette information ne soit pas acceptable pour des raisons de sécurité objectivement justifiées ou soit interdit en vertu d'une autre disposition du droit de l'Union ou de droit national pertinente.

4. Le prestataire de services de paiement débloque l'instrument de paiement ou remplace celui-ci par un nouvel instrument de paiement dès lors que les raisons justifiant le blocage n'existent plus.

Article 52

Obligations de l'utilisateur de services de paiement liées aux instruments de paiement et aux données de sécurité personnalisées

L'utilisateur de services de paiement habilité à utiliser un instrument de paiement:

a) utilise l'instrument de paiement conformément aux conditions régissant l'émission et l'utilisation de cet instrument de paiement, qui sont objectives, non discriminatoires et proportionnées;

b) lorsqu'il a connaissance de la perte, du vol, du détournement ou de toute utilisation non autorisée de l'instrument de paiement, en informe dans les meilleurs délais le prestataire de services de paiement ou l'entité désignée par celui-ci.

Aux fins du point a), dès qu'il reçoit un instrument de paiement, l'utilisateur de services de paiement prend toute mesure raisonnable pour préserver la sécurité de ses données de sécurité personnalisées.

Article 53

Obligations du prestataire de services de paiement liées aux instruments de paiement

1. Le prestataire de services de paiement qui émet un instrument de paiement:

a) s'assure que les données de sécurité personnalisées ne sont pas accessibles à d'autres parties que l'utilisateur de services de paiement qui est autorisé à utiliser cet instrument, sans préjudice des obligations de l'utilisateur de services de paiement énoncées à l'article 52;

b) s'abstient d'envoyer tout instrument de paiement non sollicité, sauf dans le cas où un instrument de paiement déjà donné à l'utilisateur de services de paiement doit être remplacé;

c) veille à la disponibilité, à tout moment, de moyens appropriés permettant à l'utilisateur de services de paiement de procéder à la notification prévue à l'article 52, point b), ou de demander le déblocage de l'instrument de paiement conformément à l'article 51, paragraphe 4;

d) fournit à l'utilisateur de services de paiement la possibilité de procéder à la notification prévue à l'article 52, point b), à titre gratuit et facture uniquement les coûts de remplacement éventuels directement imputables à cet instrument de paiement;

e) empêche toute utilisation de l'instrument de paiement après une notification effectuée en application de l'article 52, point b).

f) Aux fins du point c), le prestataire de services de paiement fournit sur demande à l'utilisateur de services de paiement, pendant 18 mois à compter de la notification, les moyens de prouver que ce dernier a bien procédé à cette notification.

2. Le prestataire de services de paiement supporte le risque lié à l'envoi à l'utilisateur de services de paiement d'un instrument de paiement ou de toute donnée de sécurité personnalisée relative à celui-ci.

Article 54

Notification et correction des opérations de paiement non autorisées, autorisées ou mal exécutées

1. Le prestataire de services de paiement ne corrige une opération de paiement non autorisée, mal exécutée ou une opération de paiement autorisée que si l'utilisateur de services de paiement informe le prestataire de services de paiement conformément

aux articles 57 et 59 dans les meilleurs délais à partir du moment où il constate une telle opération donnant lieu à une réclamation, y compris à une réclamation au titre de l'article 75, et au plus tard dans un délai de 13 mois suivant la date de débit.

Les délais de notification fixés au premier alinéa ne s'appliquent pas lorsque le prestataire de services de paiement n'a pas fourni ou mis à disposition les informations relatives à l'opération de paiement conformément au titre II.

2. Lorsqu'un prestataire de services d'initiation de paiement intervient, l'utilisateur de services de paiement obtient la correction par le prestataire de services de paiement gestionnaire du compte dans les conditions prévues au paragraphe 1 du présent article, sans préjudice de l'article 56, paragraphe 4, et de l'article 75, paragraphe 1.

Article 55

Preuve de l'autorisation et de l'exécution des opérations de paiement

1. Lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée ou affirme que l'opération de paiement n'a pas été exécutée correctement, c'est au prestataire de services de paiement qu'incombe la charge de prouver que l'opération en question a été autorisée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre du service fourni par le prestataire de services de paiement.

Si l'opération de paiement est initiée par l'intermédiaire d'un prestataire de services d'initiation de paiement, c'est à ce dernier qu'incombe la charge de prouver que, pour ce qui le concerne, l'opération en question a été autorisée et dûment enregistrée et qu'elle n'a pas été affectée par une déficience technique ou autre en relation avec le service de paiement qu'il doit assurer.

2. Lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, l'utilisation d'un instrument de paiement, telle qu'enregistrée par le prestataire de services de paiement, y compris le prestataire de services d'initiation de paiement le cas échéant, ne suffit pas en tant que telle à prouver que l'opération de paiement a été autorisée par le payeur ou que celui-ci a agi frauduleusement ou n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou à plusieurs des obligations qui lui incombent en vertu de l'article 52. Le prestataire de services de paiement, y compris, le cas échéant, le prestataire de services d'initiation de paiement, fournit des éléments afin de prouver la fraude ou la négligence grave commise par l'utilisateur de services de paiement.

Article 56

Responsabilité du prestataire de services de paiement en cas d'opérations de paiement non autorisées

1. Sans préjudice de l'article 54, en cas d'opération de paiement non autorisée, le prestataire de services de paiement du payeur rembourse au payeur le montant de cette opération immédiatement après avoir pris connaissance de l'opération non autorisée ou après en avoir été informé, et en tout état de cause au plus tard à la fin du premier jour ouvrable suivant, sauf si le prestataire de services de paiement du

payeur a des motifs raisonnables de soupçonner que le payeur a commis une fraude et s'il communique ces motifs par écrit à l'autorité nationale concernée.

2. Lorsqu'il a des motifs raisonnables de soupçonner que la fraude a été commise par le payeur, le prestataire de services de paiement du payeur, dans un délai de dix jours ouvrables après avoir pris connaissance de l'opération ou après en avoir été informé:

   a) soit rembourse au payeur le montant de l'opération de paiement non autorisée s'il a conclu, après enquête complémentaire, qu'aucune fraude n'a été commise par le payeur;

   b) soit justifie son refus de remboursement, en indiquant les organismes que le payeur peut alors saisir conformément aux articles 90, 91, 93, 94 et 95 si le payeur n'accepte pas les raisons données.

3. Le cas échéant, le prestataire de services de paiement du payeur rétablit le compte de paiement débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu. Le prestataire de services de paiement du payeur veille par ailleurs à ce que la date de valeur à laquelle le compte de paiement du payeur est crédité ne soit pas postérieure à la date à laquelle il a été débité.

4. Lorsque l'opération de paiement est initiée par l'intermédiaire d'un prestataire de services d'initiation de paiement, le prestataire de services de paiement gestionnaire du compte rembourse immédiatement, et en tout état de cause au plus tard à la fin du premier jour ouvrable suivant, le montant de l'opération de paiement non autorisée et, le cas échéant, rétablit le compte de paiement débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu.

5. Si le prestataire de services d'initiation de paiement est responsable de l'opération de paiement non autorisée, il indemnise immédiatement le prestataire de services de paiement gestionnaire du compte, à sa demande, pour les pertes subies ou les sommes payées en raison du remboursement du payeur, y compris le montant de l'opération de paiement non autorisée. Conformément à l'article 55, paragraphe 1, c'est au prestataire de services d'initiation de paiement qu'incombe la charge de prouver que, pour ce qui le concerne, l'opération de paiement en question a été autorisée et dûment enregistrée et qu'elle n'a pas été affectée par une déficience technique ou autre en relation avec le service de paiement qu'il doit assurer.

6. Le payeur peut avoir droit à une indemnisation financière complémentaire de la part du prestataire de services de paiement conformément à la loi applicable au contrat conclu entre le payeur et le prestataire de services de paiement ou, le cas échéant, au contrat conclu entre le payeur et le prestataire de services d'initiation de paiement.

Article 57

Responsabilité du prestataire de services de paiement en cas d'application incorrecte du service de vérification de la concordance

1. Le payeur ne supporte aucune perte financière pour un virement autorisé lorsque le prestataire de services de paiement du payeur n'a pas notifié au payeur, en violation de l'article 50, paragraphe 1, une divergence détectée entre l'identifiant unique et le nom du bénéficiaire communiqués par le payeur.

2. Dans un délai de dix jours ouvrables après avoir pris connaissance ou après avoir été informé d'une opération de virement exécutée dans les circonstances figurant au paragraphe 1, le prestataire de services de paiement:

   a) soit rembourse au payeur le montant du virement autorisé;

   b) soit justifie son refus de remboursement, en indiquant les organismes que le payeur peut alors saisir conformément aux articles 90, 91, 93, 94 et 95 si le payeur n'accepte pas les raisons données.

3. Lorsqu'il est responsable de la violation de l'article 50, paragraphe 1, commise par le prestataire de services de paiement du payeur, le prestataire de services de paiement du bénéficiaire rembourse le préjudice financier subi par le prestataire de services de paiement du payeur.

4. Il incombe au prestataire de services de paiement du payeur ou, dans le cas visé au paragraphe 3, à celui du bénéficiaire de prouver qu'il n'y a pas eu violation de l'article 50, paragraphe 1.

5. Les paragraphes 1 à 4 ne s'appliquent pas si le payeur a agi de manière frauduleuse ou s'il a choisi de renoncer à recevoir le service de vérification en application de l'article 50, paragraphe 4.

6. Le présent article ne s'applique pas aux virements instantanés libellés en euros relevant du champ d'application du règlement XXX (règlement sur les paiements instantanés).

Article 58

Responsabilité des prestataires de services techniques et des opérateurs de schémas de paiement lorsqu'ils ne prennent pas en charge l'application d'une authentification forte du client

Les prestataires de services techniques et les opérateurs de schémas de paiement qui fournissent des services au bénéficiaire ou au prestataire de services de paiement du bénéficiaire ou du payeur sont responsables de tout préjudice financier causé au bénéficiaire ou au prestataire de services de paiement du bénéficiaire ou du payeur par le fait qu'ils ont omis, dans le cadre de leur relation contractuelle, de fournir les services nécessaires pour permettre l'application d'une authentification forte du client.

Article 59

Responsabilité du prestataire de services de paiement en cas d'usurpation d'identité

1. Lorsqu'un utilisateur de services de paiement qui est un consommateur a été manipulé par un tiers prétendant être un employé du prestataire de services de paiement du consommateur en utilisant illégalement le nom, l'adresse électronique ou le numéro de téléphone de ce prestataire de services de paiement et que cette manipulation a donné lieu ultérieurement à des opérations de paiement autorisées de façon frauduleuse, le prestataire de services de paiement rembourse au consommateur le montant total de l'opération de paiement autorisée de façon frauduleuse, à condition que le consommateur ait, sans tarder, signalé la fraude à la police et informé son prestataire de services de paiement.

2. Dans un délai de dix jours ouvrables après avoir pris connaissance ou après avoir été informé de l'opération de paiement autorisée de façon frauduleuse, le prestataire de services de paiement:

a) soit rembourse au consommateur le montant de l'opération de paiement autorisée de façon frauduleuse;

b) soit, s'il a des motifs raisonnables de soupçonner que le consommateur a commis une fraude ou une négligence grave, justifie son refus de remboursement, en indiquant au consommateur les organismes que ce dernier peut alors saisir conformément aux articles 90, 91, 93, 94 et 95 s'il n'accepte pas les raisons données.

3. Le paragraphe 1 ne s'applique pas en cas d'agissement frauduleux ou de négligence grave du consommateur.

4. Il incombe au prestataire de services de paiement du consommateur de prouver que ce dernier a agi frauduleusement ou a commis une négligence grave.

5. Lorsqu'ils sont informés par un prestataire de services de paiement qu'une fraude du type mentionné au paragraphe 1 a été commise, les prestataires de services de communications électroniques coopèrent étroitement avec les prestataires de services de paiement et agissent rapidement pour veiller à ce que des mesures organisationnelles et techniques appropriées soient mises en place pour préserver la sécurité et la confidentialité des communications conformément à la directive 2002/58/CE, y compris en ce qui concerne l'identification de la ligne appelante et l'adresse de courrier électronique.

Article 60

Responsabilité du payeur en cas d'opérations de paiement non autorisées

1. Par dérogation à l'article 56, le payeur peut être tenu de supporter, jusqu'à concurrence de 50 EUR, les pertes liées à toute opération de paiement non autorisée consécutive à l'utilisation d'un instrument de paiement perdu ou volé ou au détournement d'un instrument de paiement.

Le premier alinéa ne s'applique pas:

a) si la perte, le vol ou le détournement d'un instrument de paiement ne pouvait être détecté par le payeur avant le paiement, sauf si le payeur a agi frauduleusement; ou

b) si la perte est due à des actes ou à une carence d'un salarié, d'un agent ou d'une succursale d'un prestataire de services de paiement ou d'une entité vers laquelle ses activités ont été externalisées.

Le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de la part du payeur ou du fait qu'il n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou à plusieurs des obligations qui lui incombent en vertu de l'article 52. Dans ces cas, le montant maximal visé au premier alinéa ne s'applique pas.

Lorsque le payeur n'a pas agi de manière frauduleuse ni n'a manqué intentionnellement aux obligations qui lui incombent en vertu de l'article 52, les autorités compétentes nationales ou les prestataires de services de paiement peuvent

limiter la responsabilité mentionnée au présent paragraphe en tenant compte, notamment, de la nature des données de sécurité personnalisées et des circonstances particulières dans lesquelles l'instrument de paiement a été perdu, volé ou détourné.

2. Lorsque le prestataire de services de paiement du payeur ne satisfait pas à l'obligation d'exiger une authentification forte du client prévue à l'article 85, le payeur ne supporte aucune perte financière éventuelle à moins qu'il ait agi frauduleusement. Il en va de même lorsque le prestataire de services de paiement du payeur ou du bénéficiaire applique une dérogation à l'utilisation de l'authentification forte du client. Lorsque le bénéficiaire ou son prestataire de services de paiement omet de mettre au point ou de modifier les systèmes, matériels informatiques et logiciels qui sont nécessaires pour appliquer une authentification forte du client, le bénéficiaire ou son prestataire de services de paiement rembourse le préjudice financier causé au prestataire de services de paiement du payeur.

3. Lorsqu'il applique une dérogation à l'utilisation de l'authentification forte du client, le prestataire de services de paiement du bénéficiaire est responsable à l'égard du prestataire de services de paiement du payeur de toute perte financière subie par ce dernier.

4. Sauf agissement frauduleux de sa part, le payeur ne supporte aucune conséquence financière résultant de l'utilisation d'un instrument de paiement perdu, volé ou détourné, survenue après la notification prévue à l'article 52, point b).

Si le prestataire de services de paiement ne fournit pas de moyens appropriés permettant, à tout moment, la notification de la perte, du vol ou du détournement d'un instrument de paiement, conformément à l'article 53, paragraphe 1, point c), le payeur n'est pas tenu, sauf agissement frauduleux de sa part, de supporter les conséquences financières résultant de l'utilisation de cet instrument de paiement.

Article 61

Opérations de paiement dont le montant n'est pas connu à l'avance

1. Lorsqu'une opération de paiement est initiée par le bénéficiaire ou par son intermédiaire dans le cadre d'une opération de paiement liée à une carte et que le montant futur exact n'est pas connu au moment où le payeur autorise l'exécution de l'opération de paiement, le prestataire de services de paiement du payeur peut bloquer des fonds sur le compte de paiement du payeur uniquement si celui-ci a donné sa permission concernant le montant exact des fonds à bloquer.

2. Le montant des fonds bloqués par le prestataire de services de paiement du payeur est proportionné au montant de l'opération de paiement auquel le payeur peut raisonnablement s'attendre.

3. Le bénéficiaire informe son prestataire de services de paiement du montant exact de l'opération de paiement immédiatement après la livraison du service ou des biens au payeur.

4. Le prestataire de services de paiement du payeur débloque les fonds bloqués sur le compte de paiement du payeur immédiatement après réception des informations sur le montant exact de l'opération de paiement.

Article 62

Remboursement d'opérations de paiement initiées par le bénéficiaire ou par son intermédiaire

1. Un payeur a droit au remboursement par son prestataire de services de paiement d'une opération de paiement autorisée qui a été initiée par le payeur par l'intermédiaire d'un bénéficiaire et qui a déjà été exécutée, pour autant que les deux conditions suivantes soient remplies:

   a) l'autorisation n'indiquait pas le montant exact de l'opération de paiement lorsqu'elle a été donnée;

   b) le montant de l'opération de paiement dépassait le montant auquel le payeur pouvait raisonnablement s'attendre en tenant compte du profil de ses dépenses passées, des conditions prévues par son contrat-cadre et des circonstances pertinentes dans ce cas.

   À la demande du prestataire de services de paiement, le payeur a la charge de prouver que ces conditions sont remplies.

   Le remboursement correspond au montant total de l'opération de paiement exécutée. La date de valeur à laquelle le compte de paiement du payeur est crédité n'est pas postérieure à la date à laquelle il a été débité.

   Sans préjudice du paragraphe 3 du présent article, outre le droit mentionné au premier alinéa du présent paragraphe, en cas d'opérations de paiement autorisées ayant été initiées par un bénéficiaire, y compris les prélèvements mentionnés à l'article 1er du règlement (UE) nº 260/2012, le payeur jouit d'un droit au remboursement inconditionnel dans les délais fixés à l'article 63 du présent règlement.

2. Aux fins du paragraphe 1, premier alinéa, point b), le payeur ne peut invoquer des raisons liées à d'éventuels frais de change si le taux de change de référence convenu avec son prestataire de services de paiement conformément à l'article 13, paragraphe 1, point e), et à l'article 20, point c) iii), a été appliqué.

3. Le payeur et le prestataire de services de paiement peuvent convenir, dans un contrat-cadre, que le payeur n'a pas droit à un remboursement lorsque:

   a) le payeur a donné son autorisation à l'exécution de l'opération de paiement directement au prestataire de services de paiement;

   b) le cas échéant, les informations relatives à la future opération de paiement ont été fournies au payeur ou mises à sa disposition de la manière convenue, quatre semaines au moins avant l'échéance, par le prestataire de services de paiement ou par le bénéficiaire.

4. Pour les prélèvements dans des devises autres que l'euro, les prestataires de services de paiement peuvent offrir des droits au remboursement plus favorables conformément à leurs schémas de prélèvement, à condition qu'ils soient plus avantageux pour le payeur.

Article 63

Demandes de remboursement d'opérations de paiement initiées par le bénéficiaire ou par son intermédiaire

1. Le payeur peut demander le remboursement, mentionné à l'article 62, d'une opération de paiement autorisée initiée par le bénéficiaire ou par son intermédiaire pendant une période de huit semaines à compter de la date à laquelle les fonds ont été débités.

2. Dans un délai de dix jours ouvrables suivant la réception d'une demande de remboursement, le prestataire de services de paiement:

   a) soit rembourse le montant total de l'opération de paiement;

   b) soit justifie son refus de remboursement, en indiquant les organismes que le payeur peut alors saisir conformément aux articles 90, 91, 93, 94 et 95 si le payeur n'accepte pas les raisons données.

   Le droit du prestataire de services de paiement, au titre du premier alinéa du présent paragraphe, de refuser le remboursement ne s'applique pas dans le cas énoncé à l'article 62, paragraphe 1, quatrième alinéa.

CHAPITRE 5

Exécution des opérations de paiement

SECTION 1

ORDRES DE PAIEMENT ET MONTANTS TRANSFERES

Article 64

Réception des ordres de paiement

1. Le moment de réception est le moment où l'ordre de paiement est reçu par le prestataire de services de paiement du payeur.

   Le compte du payeur n'est pas débité avant réception de l'ordre de paiement. Si le moment de réception n'est pas un jour ouvrable pour le prestataire de services de paiement du payeur, l'ordre de paiement est réputé avoir été reçu le jour ouvrable suivant. Le prestataire de services de paiement peut établir une heure limite proche de la fin d'un jour ouvrable au-delà de laquelle tout ordre de paiement reçu est réputé avoir été reçu le jour ouvrable suivant.

2. Si l'utilisateur de services de paiement qui passe un ordre de paiement et le prestataire de services de paiement conviennent que l'exécution de l'ordre de paiement commencera un jour donné, ou à l'issue d'une période déterminée, ou le jour où le payeur a mis les fonds à la disposition du prestataire de services de paiement, le moment de réception aux fins de l'article 69 est réputé être le jour convenu. Si le jour convenu n'est pas un jour ouvrable pour le prestataire de services de paiement, l'ordre de paiement est réputé avoir été reçu le jour ouvrable suivant.

3. Le présent article ne s'applique pas aux virements instantanés libellés en euros qui relèvent du règlement XXX (règlement sur les paiements instantanés).

Article 65

Refus d'un ordre de paiement

1. Lorsqu'il refuse d'exécuter un ordre de paiement ou d'initier une opération de paiement, le prestataire de services de paiement notifie à l'utilisateur de services de paiement le refus et, si possible, les motifs de ce refus ainsi que la procédure à suivre pour corriger toute erreur factuelle l'ayant entraîné, à moins d'une interdiction en vertu d'une autre disposition du droit de l'Union ou de droit national pertinente.

   Le prestataire de services de paiement fournit la notification ou la met à disposition selon les modalités convenues, dès que possible et, en tout cas, dans les délais prévus à l'article 69.

   Le contrat-cadre peut prévoir la possibilité pour le prestataire de services de paiement d'imputer des frais raisonnables pour un tel refus si celui-ci est objectivement justifié.

2. Lorsque toutes les conditions énoncées dans le contrat-cadre du payeur sont réunies, le prestataire de services de paiement gestionnaire du compte du payeur ne refuse pas d'exécuter une opération de paiement autorisée, que l'ordre de paiement soit passé par un payeur, y compris par un prestataire de services d'initiation de paiement, ou par un bénéficiaire ou par son intermédiaire, à moins d'une interdiction en vertu d'une autre disposition du droit de l'Union ou de droit national pertinente.

3. Aux fins des articles 69 et 75, un ordre de paiement dont l'exécution a été refusée est réputé non reçu.

Article 66

Irrévocabilité d'un ordre de paiement

1. L'utilisateur de services de paiement ne révoque pas un ordre de paiement une fois que celui-ci a été reçu par le prestataire de services de paiement du payeur, sauf disposition contraire du présent article.

2. Lorsque l'opération de paiement est initiée par un prestataire de services d'initiation de paiement ou par le bénéficiaire ou par son intermédiaire, le payeur ne révoque pas l'ordre de paiement après avoir donné sa permission à ce que le prestataire de services d'initiation de paiement initie l'opération de paiement ou après avoir donné sa permission à l'exécution de l'opération de paiement en faveur du bénéficiaire.

3. En cas de prélèvement et sans préjudice du droit au remboursement, le payeur peut révoquer l'ordre de paiement au plus tard à la fin du jour ouvrable précédant le jour convenu pour le débit des fonds.

4. Dans le cas visé à l'article 64, paragraphe 2, l'utilisateur de services de paiement peut révoquer un ordre de paiement au plus tard à la fin du jour ouvrable précédant le jour convenu.

5. Après expiration des délais fixés aux paragraphes 1 à 4, l'ordre de paiement ne peut être révoqué que si l'utilisateur de services de paiement et les prestataires de services

de paiement concernés en sont convenus ainsi. Dans les cas visés aux paragraphes 2 et 3, le consentement du bénéficiaire est également requis. Si le contrat-cadre le prévoit, le prestataire de services de paiement concerné peut imputer des frais pour la révocation.

Article 67

Montants transférés et montants reçus

1. Le prestataire de services de paiement du payeur, le ou les prestataires de services de paiement du bénéficiaire et les intermédiaires des prestataires de services de paiement transfèrent le montant total de l'opération de paiement et s'abstiennent de prélever des frais sur le montant transféré.

2. Le bénéficiaire et le prestataire de services de paiement peuvent convenir que le prestataire concerné déduit ses frais du montant transféré avant d'en créditer le bénéficiaire. Dans ce cas, le montant total de l'opération de paiement et les frais sont séparés dans l'information donnée au bénéficiaire.

3. Si des frais autres que ceux visés au paragraphe 2 sont déduits du montant transféré, le prestataire de services de paiement du payeur veille à ce que le bénéficiaire reçoive le montant total de l'opération de paiement initiée par le payeur. Au cas où l'opération de paiement est initiée par le bénéficiaire ou par son intermédiaire, le prestataire de services de paiement du bénéficiaire veille à ce que le bénéficiaire reçoive le montant total de l'opération de paiement.

SECTION 2

DELAI D'EXECUTION ET DATE DE VALEUR

Article 68

Champ d'application

1. La présente section s'applique:

   a) aux opérations de paiement effectuées en euros;

   b) aux opérations de paiement nationales effectuées dans la devise d'un État membre n'appartenant pas à la zone euro;

   c) aux opérations de paiement entraînant une seule conversion entre l'euro et la devise d'un État membre n'appartenant pas à la zone euro, à condition que la conversion requise soit effectuée dans l'État membre n'appartenant pas à la zone euro concerné et que, en cas d'opérations de paiement transfrontières, le transfert transfrontière s'effectue en euros.

2. La présente section s'applique aux opérations de paiement non mentionnées au paragraphe 1, à moins que l'utilisateur de services de paiement et le prestataire de services de paiement en soient convenus autrement, à l'exception de l'article 73, auquel les parties ne peuvent déroger. Cependant, si l'utilisateur de services de paiement et le prestataire de services de paiement conviennent d'un délai plus long que celui fixé à l'article 69 pour des opérations de paiement à l'intérieur de l'Union,

ce délai plus long ne peut pas dépasser quatre jours ouvrables à compter de la réception mentionnée à l'article 64.

Article 69

Opérations de paiement effectuées vers un compte de paiement

1. Sans préjudice de l'article 2, paragraphe 1, point c), du règlement (UE) nº 260/2012, le prestataire de services de paiement du payeur veille à ce que, après la réception mentionnée à l'article 64, le montant de l'opération de paiement soit crédité sur le compte du prestataire de services de paiement du bénéficiaire au plus tard à la fin du premier jour ouvrable suivant. Ce délai peut être prolongé d'un jour ouvrable supplémentaire dans le cas des opérations de paiement initiées sur support papier.
2. Le prestataire de services de paiement du bénéficiaire attribue une date de valeur à l'opération de paiement et en met le montant à la disposition sur le compte de paiement du bénéficiaire après que le prestataire de services de paiement a reçu les fonds conformément à l'article 73.
3. Le prestataire de services de paiement du bénéficiaire transmet un ordre de paiement passé par le bénéficiaire ou par son intermédiaire au prestataire de services de paiement du payeur dans les délais convenus entre le bénéficiaire et le prestataire de services de paiement, de manière à permettre le règlement à la date convenue en cas de prélèvement.

Article 70

Cas dans lequel le bénéficiaire n'est pas titulaire d'un compte de paiement auprès du prestataire de services de paiement

Lorsque le bénéficiaire n'est pas titulaire d'un compte de paiement auprès du prestataire de services de paiement, le prestataire de services de paiement qui reçoit les fonds destinés au bénéficiaire les met à la disposition de ce dernier dans le délai fixé à l'article 69, paragraphe 1.

Article 71

Espèces déposées sur un compte de paiement

Lorsqu'un consommateur verse des espèces sur un compte de paiement auprès du prestataire de services de paiement, dans la devise de ce compte de paiement, le prestataire de services de paiement veille à ce que le montant versé soit mis à disposition et reçoive une date de valeur immédiatement après la réception de ces fonds. Lorsque l'utilisateur de services de paiement n'est pas un consommateur, le montant est mis à disposition et reçoit une date de valeur au plus tard le jour ouvrable suivant celui de la réception des fonds.

Article 72

Opérations de paiement nationales

Pour les opérations de paiement nationales, les États membres peuvent prévoir des délais maximaux d'exécution plus courts que ceux prévus dans la présente section.

Article 73

Date de valeur et disponibilité des fonds

1. Pour le compte de paiement du bénéficiaire, la date de valeur du crédit n'est pas postérieure à celle du jour ouvrable au cours duquel le montant de l'opération de paiement est crédité sur le compte du prestataire de services de paiement du bénéficiaire.

2. Le prestataire de services de paiement du bénéficiaire veille à ce que le montant de l'opération de paiement soit à la disposition du bénéficiaire immédiatement après que ce montant a été crédité sur le compte du prestataire de services de paiement du bénéficiaire lorsque, pour sa part:

   a) soit il n'y a pas de conversion;

   b) soit il y a conversion entre l'euro et la devise d'un État membre ou entre les devises de deux États membres.

   L'obligation énoncée au présent paragraphe vaut également pour les opérations de paiement qui se déroulent au sein d'un seul et même prestataire de services de paiement.

3. Pour le compte de paiement du payeur, la date de valeur du débit n'est pas antérieure au moment où le montant de l'opération de paiement est débité de ce compte de paiement.

Article 74

Identifiants uniques inexacts

1. Une opération de paiement exécutée conformément à l'identifiant unique est réputée être correctement exécutée pour ce qui concerne le bénéficiaire indiqué par l'identifiant unique.

2. Si l'identifiant unique fourni par l'utilisateur de services de paiement est inexact, le prestataire de services de paiement n'est pas responsable au titre de l'article 75 de l'inexécution ou de la mauvaise exécution de l'opération de paiement.

3. Le prestataire de services de paiement du payeur s'efforce, dans la mesure du raisonnable, de récupérer les fonds engagés dans l'opération de paiement. Le prestataire de services de paiement du bénéficiaire coopère à ces efforts également en communiquant au prestataire de services de paiement du payeur toutes les informations utiles pour récupérer les fonds.

   Lorsqu'il n'est pas possible de récupérer les fonds comme prévu au premier alinéa, le prestataire de services de paiement du payeur fournit au payeur, sur demande écrite, toutes les informations dont il dispose et qui présentent un intérêt pour le payeur afin

que celui-ci puisse introduire un recours devant une juridiction pour récupérer les fonds.

4. Lorsque le contrat-cadre le prévoit, le prestataire de services de paiement peut imputer des frais de recouvrement à l'utilisateur de services de paiement.

5. Si l'utilisateur de services de paiement fournit des informations en sus de celles prévues à l'article 13, paragraphe 1, point a), ou à l'article 20, point b) ii), le prestataire de services de paiement n'est responsable que de l'exécution de l'opération de paiement conformément à l'identifiant unique fourni par l'utilisateur de services de paiement.

6. Lorsque l'identifiant unique fourni par le prestataire de services d'initiation de paiement est inexact, les prestataires de services de paiement sont responsables conformément à l'article 76.

Article 75

Responsabilité des prestataires de services de paiement en cas de non-exécution, de mauvaise exécution ou d'exécution tardive d'opérations de paiement

1. Lorsqu'un ordre de paiement est passé directement par le payeur, le prestataire de services de paiement du payeur est, sans préjudice de l'article 54, de l'article 74, paragraphes 2 et 3, et de l'article 79, responsable de la bonne exécution de l'opération de paiement à l'égard du payeur, à moins qu'il ne puisse démontrer au payeur et, le cas échéant, au prestataire de services de paiement du bénéficiaire que le prestataire de services de paiement du bénéficiaire a reçu le montant de l'opération de paiement conformément à l'article 69, paragraphe 1. Dans ce cas, c'est le prestataire de services de paiement du bénéficiaire qui est responsable de la bonne exécution de l'opération de paiement à l'égard du bénéficiaire.

   Lorsque le prestataire de services de paiement du payeur est responsable au titre du premier alinéa, il rembourse immédiatement au payeur le montant de l'opération de paiement non exécutée ou mal exécutée et, le cas échéant, rétablit le compte de paiement débité dans l'état où il se serait trouvé si l'opération de paiement mal exécutée n'avait pas eu lieu.

   La date de valeur à laquelle le compte de paiement du payeur est crédité n'est pas postérieure à la date à laquelle il a été débité.

   Lorsque le prestataire de services de paiement du bénéficiaire est responsable au titre du premier alinéa, il met immédiatement le montant de l'opération de paiement à la disposition du bénéficiaire et, si besoin est, crédite le compte de paiement du bénéficiaire du montant correspondant.

   La date de valeur à laquelle le compte de paiement du bénéficiaire a été crédité n'est pas postérieure à la date de valeur qui lui aurait été attribuée si l'opération avait été correctement exécutée, conformément à l'article 73.

   Lorsqu'une opération de paiement est exécutée tardivement, le prestataire de services de paiement du bénéficiaire veille, à la demande du prestataire de services de paiement du payeur agissant pour le compte du payeur, à ce que la date de valeur à laquelle le compte de paiement du bénéficiaire a été crédité ne soit pas postérieure à la date de valeur qui lui aurait été attribuée si l'opération avait été correctement exécutée.

Dans le cas d'une opération de paiement non exécutée ou mal exécutée où l'ordre de paiement est passé par le payeur, le prestataire de services de paiement de celui-ci s'efforce immédiatement, sur demande et sans frais pour le payeur, quelle que soit la responsabilité déterminée au titre du présent paragraphe, de retrouver la trace de l'opération de paiement et notifie le résultat de sa recherche au payeur.

2. Lorsqu'un ordre de paiement est passé par le bénéficiaire ou par son intermédiaire, le prestataire de services de paiement du bénéficiaire est, sans préjudice de l'article 54, de l'article 74, paragraphes 2 et 3, et de l'article 79, responsable à l'égard du bénéficiaire de la bonne transmission de l'ordre de paiement au prestataire de services de paiement du payeur, conformément à l'article 69, paragraphe 3. Lorsque le prestataire de services de paiement du bénéficiaire est responsable au titre du présent alinéa, il retransmet immédiatement l'ordre de paiement en question au prestataire de services de paiement du payeur.

En cas de transmission tardive de l'ordre de paiement, la date de valeur attribuée au montant de l'opération sur le compte de paiement du bénéficiaire n'est pas postérieure à la date de valeur qui lui aurait été attribuée si l'opération avait été correctement exécutée.

Sans préjudice de l'article 54, de l'article 74, paragraphes 2 et 3, et de l'article 79, le prestataire de services de paiement du bénéficiaire est responsable à l'égard du bénéficiaire du traitement de l'opération de paiement conformément aux obligations qui lui incombent au titre de l'article 73. Lorsque le prestataire de services de paiement du bénéficiaire est responsable au titre du présent alinéa, il veille à ce que le montant de l'opération de paiement soit mis à la disposition du bénéficiaire immédiatement après que ce montant a été crédité sur son propre compte. La date de valeur attribuée au montant de cette opération sur le compte de paiement du bénéficiaire n'est pas postérieure à la date de valeur qui lui aurait été attribuée si l'opération avait été correctement exécutée.

Dans le cas d'une opération de paiement non exécutée ou mal exécutée pour laquelle le prestataire de services de paiement du bénéficiaire n'est pas responsable au titre des premier et troisième alinéas, c'est le prestataire de services de paiement du payeur qui est responsable à l'égard du payeur. Le prestataire de services de paiement du payeur dont la responsabilité est ainsi engagée rembourse au payeur, le cas échéant et dans les meilleurs délais, le montant de l'opération de paiement non exécutée ou mal exécutée et rétablit le compte de paiement débité dans l'état où il se serait trouvé si l'opération de paiement mal exécutée n'avait pas eu lieu. La date de valeur à laquelle le compte de paiement du payeur est crédité n'est pas postérieure à la date à laquelle il a été débité.

L'obligation au titre du quatrième alinéa ne s'applique pas au prestataire de services de paiement du payeur lorsqu'il prouve que le prestataire de services de paiement du bénéficiaire a reçu le montant de l'opération de paiement même si l'exécution de l'opération de paiement est simplement retardée. Dans ce cas, le prestataire de services de paiement du bénéficiaire attribue une date de valeur au montant de cette opération sur le compte de paiement du bénéficiaire qui n'est pas postérieure à la date de valeur qui lui aurait été attribuée si l'opération avait été correctement exécutée.

Dans le cas d'une opération de paiement non exécutée ou mal exécutée où l'ordre de paiement est passé par le bénéficiaire ou par son intermédiaire, le prestataire de services de paiement de celui-ci s'efforce immédiatement, sur demande et sans frais

pour le payeur, quelle que soit la responsabilité déterminée au titre du présent paragraphe, de retrouver la trace de l'opération de paiement et notifie le résultat de sa recherche au bénéficiaire.

3. Les prestataires de services de paiement sont redevables, à l'égard de leurs utilisateurs de services de paiement respectifs, des frais dont ils sont responsables et des intérêts supportés par ces utilisateurs du fait de la non-exécution ou de la mauvaise exécution, y compris l'exécution tardive, d'une opération de paiement.

Article 76

Responsabilité en cas de services d'initiation de paiement pour la non-exécution, la mauvaise exécution ou l'exécution tardive d'opérations de paiement

1. Lorsqu'un ordre de paiement est passé par le payeur ou par le bénéficiaire par l'intermédiaire d'un prestataire de services d'initiation de paiement, le prestataire de services de paiement gestionnaire du compte, sans préjudice de l'article 54 et de l'article 74, paragraphes 2 et 3, rembourse au payeur le montant de l'opération de paiement non exécutée ou mal exécutée et, le cas échéant, rétablit le compte de paiement débité dans l'état où il se serait trouvé si l'opération de paiement mal exécutée n'avait pas eu lieu.

   C'est au prestataire de services d'initiation de paiement qu'incombe la charge de prouver que l'ordre de paiement a été reçu par le prestataire de services de paiement gestionnaire du compte du payeur conformément à l'article 64 et que, pour ce qui le concerne, l'opération de paiement a été authentifiée et dûment enregistrée et qu'elle n'a pas été affectée par une déficience technique ou autre en relation avec la non-exécution, la mauvaise exécution ou l'exécution tardive de l'opération.

2. Si le prestataire de services d'initiation de paiement est responsable de la non-exécution, de la mauvaise exécution ou de l'exécution tardive de l'opération de paiement, il indemnise immédiatement le prestataire de services de paiement gestionnaire du compte, à sa demande, pour les pertes subies ou les sommes payées en raison du remboursement du payeur.

Article 77

Indemnisation financière complémentaire

Toute indemnisation financière complémentaire par rapport à celle prévue dans la présente section peut être fixée conformément à la loi applicable au contrat conclu entre l'utilisateur de services de paiement et le prestataire de services de paiement.

Article 78

Droit de recours

1. Lorsque la responsabilité d'un prestataire de services de paiement au titre des articles 56, 57, 59, 75 et 76 est imputable à un autre prestataire de services de paiement ou à un intermédiaire, ledit prestataire de services de paiement ou intermédiaire indemnise le premier prestataire de services de paiement pour toute perte subie ou toute somme payée au titre des articles 56, 57, 59, 75 et 76. Cette

indemnisation s'applique au cas où l'un des prestataires de services de paiement n'applique pas l'authentification forte du client.

2. Des indemnisations financières complémentaires peuvent être fixées conformément aux conventions existant entre les prestataires de services de paiement ou les intermédiaires et conformément à la loi applicable à la convention qu'ils ont conclue.

Article 79

Circonstances anormales et imprévisibles

Aucune responsabilité au titre des chapitres 4 ou 5 n'est engagée en cas de circonstances anormales et imprévisibles échappant au contrôle de la partie qui fait valoir ces circonstances, dont les suites auraient été inévitables malgré tous les efforts déployés, ni lorsque le prestataire de services de paiement est lié par d'autres obligations juridiques prévues par le droit de l'Union ou le droit national.

CHAPITRE 6

Protection des données

Article 80

Protection des données

Les systèmes de paiement et les prestataires de services de paiement sont autorisés à traiter les catégories particulières de données à caractère personnel visées à l'article 9, paragraphe 1, du règlement (UE) 2016/679 et à l'article 10, paragraphe 1, du règlement (UE) 2018/1725 dans la mesure nécessaire à la prestation de services de paiement et au respect des obligations au titre du présent règlement, dans l'intérêt public du bon fonctionnement du marché intérieur des services de paiement, sous réserve de garanties appropriées pour les libertés et droits fondamentaux des personnes physiques, notamment:

a) des mesures techniques visant à garantir le respect des principes de limitation de la finalité, de minimisation des données et de limitation de la conservation, tels qu'énoncés dans le règlement (UE) 2016/679, y compris des limitations techniques applicables à la réutilisation des données et à l'utilisation de mesures de pointe en matière de sécurité et de protection de la vie privée, y compris la pseudonymisation ou le chiffrement;

b) des mesures organisationnelles, notamment la formation au traitement de catégories particulières de données, la limitation de l'accès à des catégories particulières de données et l'enregistrement de cet accès.

CHAPITRE 7

Risques opérationnels et de sécurité et authentification

Article 81

Gestion des risques opérationnels et de sécurité

1. Les prestataires de services de paiement établissent un cadre prévoyant des mesures d'atténuation et des mécanismes de contrôle appropriés en vue de gérer les risques opérationnels et de sécurité liés aux services de paiement qu'ils fournissent. Ce cadre prévoit que les prestataires de services de paiement établissent et maintiennent des procédures efficaces de gestion des incidents, y compris pour la détection et la classification des incidents opérationnels et de sécurité majeurs.

   Le premier alinéa est sans préjudice de l'application du chapitre II du règlement (UE) 2022/2554 du Parlement européen et du Conseil[65]:

   a) aux prestataires de services de paiement mentionnés à l'article 2, paragraphe 1, points a), b) et d), du présent règlement;

   b) aux prestataires de services d'information sur les comptes mentionnés à l'article 36, paragraphe 1, de la directive (UE) XXX (DSP3); et

   c) aux établissements de paiement exemptés en vertu de l'article 34, paragraphe 1, de la directive (UE) XXX (DSP3);

   Les prestataires de services de paiement fournissent à l'autorité compétente désignée en application de la directive (UE) XXX (DSP3), chaque année ou à des intervalles plus rapprochés fixés par l'autorité compétente, une évaluation à jour et exhaustive des risques opérationnels et de sécurité liés aux services de paiement qu'ils fournissent et des informations sur le caractère adéquat des mesures d'atténuation et des mécanismes de contrôle mis en œuvre pour faire face à ces risques.

2. L'ABE encourage la coopération, y compris l'échange d'informations, dans le domaine des risques opérationnels et de sécurité associés aux services de paiement entre les autorités compétentes, entre les autorités compétentes et la BCE et, le cas échéant, l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information.

[65] 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 (JO L 333 du 27.12.2022, p. 1).

Article 82

Signalement de la fraude

1. Les prestataires de services de paiement fournissent à leurs autorités compétentes, au moins chaque année, des données statistiques relatives à la fraude liée aux différents moyens de paiement. Les autorités compétentes en question fournissent ces données sous forme agrégée à l'ABE et à la BCE.

2. L'ABE élabore, en étroite coopération avec la BCE, des projets de normes techniques de réglementation portant sur les données statistiques à fournir conformément au paragraphe 1 au titre des exigences en matière de signalement de la fraude mentionnées au paragraphe 1.

   L'ABE soumet les projets de normes techniques de réglementation mentionnés au premier alinéa à la Commission au plus tard le [OP: veuillez insérer la date correspondant à un an après la date d'entrée en vigueur du présent règlement]. La Commission est habilitée à adopter les normes techniques de réglementation visées au premier alinéa, conformément aux articles 10 à 14 du règlement (UE) nº 1093/2010.

3. L'ABE élabore des projets de normes techniques d'exécution établissant des formulaires et modèles types à utiliser pour la communication à l'ABE par les autorités compétentes des données relatives à la fraude en matière de paiements, conformément au paragraphe 1.

   L'ABE soumet les projets de normes techniques d'exécution mentionnés au premier alinéa à la Commission au plus tard le [OP: veuillez insérer la date correspondant à un an après la date d'entrée en vigueur du présent règlement]. La Commission est habilitée à adopter les normes techniques de réglementation mentionnées au premier alinéa, conformément à l'article 15 du règlement (UE) nº 1093/2010.

Article 83

Mécanismes de contrôle des opérations et partage des données relatives à la fraude

1. Les prestataires de services de paiement mettent en place des mécanismes de contrôle des opérations qui:

   a) prennent en charge l'application de la procédure d'authentification forte du client conformément à l'article 85;

   b) dérogent à l'application de l'authentification forte du client sur la base des critères énoncés à l'article 85, paragraphe 11, sous réserve du respect de conditions précises et limitées fondées sur le niveau de risque encouru et sur les types et les détails des données évaluées par le prestataire de services de paiement;

   c) permettent aux prestataires de services de paiement de prévenir et de détecter les opérations de paiement potentiellement frauduleuses, y compris les opérations impliquant des services d'initiation de paiement.

2. Les mécanismes de contrôle des opérations sont fondés sur l'analyse des opérations de paiement antérieures et de l'accès aux comptes de paiement en ligne. Le traitement est limité aux données suivantes, nécessaires aux fins mentionnées au paragraphe 1:

a) les informations sur l'utilisateur de services de paiement, notamment les caractéristiques de son environnement et de son comportement qui sont typiques d'une utilisation normale des données de sécurité personnalisées;

b) les informations sur le compte de paiement, notamment l'historique des opérations de paiement;

c) les informations relatives à l'opération, notamment le montant de l'opération et l'identifiant unique du bénéficiaire;

d) les données de la session, notamment la plage d'adresses ip de l'appareil à partir duquel le compte de paiement a été consulté.

Les prestataires de services de paiement ne stockent pas les données mentionnées au présent paragraphe plus longtemps que nécessaire aux fins énoncées au paragraphe 1, ni après la cessation de la relation avec le client. Les prestataires de services de paiement veillent à ce que les mécanismes de contrôle des opérations tiennent au moins compte de chacun des facteurs suivants liés aux risques:

a) les listes d'éléments d'authentification volés ou détournés;

b) le montant de chaque opération de paiement;

c) les scénarios connus de fraude lors de la prestation de services de paiement;

d) les signes d'infection par un logiciel malveillant lors de sessions d'application de la procédure d'authentification;

e) si le dispositif d'accès ou le logiciel est fourni par le prestataire de services de paiement, un registre d'utilisation du dispositif d'accès ou du logiciel fourni à l'utilisateur de services de paiement, et l'utilisation anormale du dispositif ou du logiciel.

3. Dans la mesure nécessaire pour se conformer au paragraphe 1, point c), les prestataires de services de paiement peuvent échanger l'identifiant unique d'un bénéficiaire avec d'autres prestataires de services de paiement adhérant à des dispositifs de partage d'informations au sens du paragraphe 5 lorsque le prestataire de services de paiement dispose d'éléments suffisants pour présumer qu'une opération de paiement frauduleuse a eu lieu. L'existence d'éléments suffisants pour partager des identifiants uniques est présumée lorsqu'au moins deux utilisateurs différents de services de paiement qui sont des clients du même prestataire de services de paiement ont informé qu'un identifiant unique d'un bénéficiaire a été utilisé pour effectuer un virement frauduleux. Les prestataires de services de paiement ne conservent pas les identifiants uniques obtenus à la suite de l'échange d'informations mentionné au présent paragraphe et au paragraphe 5 plus longtemps que nécessaire aux fins prévues au paragraphe 1, point c).

4. Les dispositifs de partage d'informations définissent les modalités de participation et les détails des éléments opérationnels, y compris de l'utilisation de plates-formes informatiques spécialisées. Avant d'adopter de tels dispositifs, les prestataires de services de paiement procèdent conjointement à une analyse d'impact relative à la protection des données au sens de l'article 35 du règlement (UE) 2016/679 et, le cas

échéant, procèdent à la consultation préalable de l'autorité de contrôle conformément à l'article 36 dudit règlement.

5. Les prestataires de services de paiement notifient aux autorités compétentes leur participation aux dispositifs de partage d'informations mentionnés au paragraphe 5 lors de la validation de leur adhésion ou, le cas échéant, la cessation de leur adhésion, lorsque celle-ci prend effet.

6. Le traitement des données à caractère personnel conformément au paragraphe 4 n'entraîne pas la résiliation de la relation contractuelle avec le client par le prestataire de services de paiement ni n'affecte l'enregistrement futur de ces données par un autre prestataire de services de paiement.

Article 84

Tendances et risques de fraude en matière de paiements

1. Les prestataires de services de paiement alertent leurs clients par tous les moyens et médias appropriés lorsque de nouvelles formes de fraude en matière de paiements apparaissent, en tenant compte des besoins de leurs groupes de clients les plus vulnérables. Les prestataires de services de paiement donnent à leurs clients des indications claires sur la manière d'identifier les tentatives frauduleuses et les avertissent des mesures nécessaires et des précautions à prendre pour éviter d'être victimes d'actions frauduleuses pouvant les viser. Les prestataires de services de paiement indiquent à leurs clients où ils peuvent signaler des actes frauduleux et obtenir rapidement des informations relatives à la fraude.

2. Les prestataires de services de paiement organisent au moins une fois par an des programmes de formation sur les tendances et risques de fraude en matière de paiements à l'intention de leurs employés et veillent à ce que leurs employés soient correctement formés à l'accomplissement de leurs tâches et responsabilités conformément aux politiques et procédures de sécurité pertinentes afin d'atténuer et de gérer les risques de fraude aux paiements.

3. Au plus tard le [OP: veuillez insérer la date correspondant à 18 mois après la date d'entrée en vigueur du présent règlement], l'ABE émet des orientations conformément à l'article 16 du règlement (UE) nº 1093/2010 concernant les programmes relatifs aux risques de fraude aux paiements mentionnés aux paragraphes 1 et 2 du présent article.

Article 85

Authentification forte du client

1. Un prestataire de services de paiement applique l'authentification forte du client lorsque le payeur:

   a) accède à son compte de paiement en ligne;

   b) accède aux informations sur les comptes de paiement;

   c) passe un ordre de paiement pour une opération de paiement électronique;

d) exécute une action, grâce à un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiements ou de toute autre utilisation frauduleuse.

2. Les opérations de paiement qui ne sont pas initiées par le payeur mais uniquement par le bénéficiaire ne sont pas soumises à une authentification forte du client dans la mesure où ces opérations sont initiées sans aucune interaction ou intervention du payeur.

3. Lorsque le payeur a donné mandat au bénéficiaire de passer un ordre de paiement pour une opération de paiement ou une série d'opérations de paiement au moyen d'un instrument de paiement particulier qui est émis pour être utilisé par le payeur afin de passer des ordres de paiement pour les opérations de paiement, et que ce mandat est fondé sur un accord entre le payeur et le bénéficiaire pour la fourniture de produits ou de services, les opérations de paiement initiées ensuite par le bénéficiaire sur la base d'un tel mandat peuvent être qualifiées d'opérations initiées par le bénéficiaire, à condition que ces opérations n'aient pas besoin d'être précédées d'une action spécifique du payeur pour déclencher leur initiation par le bénéficiaire.

4. Les opérations de paiement pour lesquelles des ordres de paiement sont passés par le bénéficiaire sur la base du mandat donné par le payeur sont soumises aux dispositions générales applicables aux opérations initiées par le bénéficiaire mentionnées aux articles 61, 62 et 63.

5. Lorsque le mandat du payeur au bénéficiaire pour passer des ordres de paiement concernant des opérations mentionnées au paragraphe 3 est donné grâce à un moyen de communication à distance avec la participation du prestataire de services de paiement, la mise en place d'un tel mandat est soumise à une authentification forte du client.

6. En ce qui concerne les prélèvements, lorsque le mandat donné par le payeur au bénéficiaire pour initier un ou plusieurs prélèvements est fourni grâce à un moyen de communication à distance avec la participation directe d'un prestataire de services de paiement à la mise en place d'un tel mandat, une authentification forte du client est appliquée.

7. Les opérations de paiement pour lesquelles des ordres de paiement sont passés par le payeur selon des modalités autres que l'utilisation de plates-formes ou de dispositifs électroniques, tels que les ordres de paiement sur support papier, les ordres de paiement passés par courrier ou par téléphone, ne sont pas soumises à une authentification forte du client, que l'opération soit ou non exécutée par voie électronique, à condition que des exigences de sécurité et des vérifications permettant une forme d'authentification de l'opération de paiement soient appliquées par le prestataire de services de paiement du payeur.

8. Pour la passation à distance d'un ordre de paiement mentionnée au paragraphe 1, point c), les prestataires de services de paiement appliquent l'authentification forte du client comprenant des éléments qui établissent un lien dynamique entre l'opération, d'une part, et le montant et le bénéficiaire donnés, d'autre part.

9. Pour la passation d'un ordre de paiement mentionnée au paragraphe 1, point c), au moyen d'un dispositif du payeur utilisant une technologie de proximité pour l'échange d'informations avec l'infrastructure du bénéficiaire, dont l'authentification nécessite l'utilisation de l'internet sur le dispositif du payeur, les prestataires de services de paiement appliquent l'authentification forte du client comprenant des

éléments qui établissent un lien dynamique entre l'opération, d'une part, et le montant et le bénéficiaire donnés, d'autre part, ou des mesures de sécurité harmonisées d'effet identique, qui garantissent la confidentialité, l'authenticité et l'intégrité du montant de l'opération et du bénéficiaire durant l'ensemble des phases de l'initiation.

10. Aux fins du paragraphe 1, les prestataires de services de paiement mettent en place des mesures de sécurité adéquates afin de protéger la confidentialité et l'intégrité des données de sécurité personnalisées des utilisateurs de services de paiement.

11. Toute dérogation à l'application de l'authentification forte du client qui doit être prévue par l'ABE en vertu de l'article 89 repose sur un ou plusieurs des critères suivants:

a) le niveau de risque lié au service fourni;

b) le montant, le caractère récurrent de l'opération ou les deux;

c) le moyen utilisé pour exécuter l'opération.

12. Les deux éléments ou plus mentionnés à l'article 3, point 35), sur lesquels repose l'authentification forte du client ne doivent pas nécessairement appartenir à des catégories différentes, pour autant que leur indépendance soit totalement préservée.

Article 86

Authentification forte du client en ce qui concerne les services d'initiation de paiement et d'information sur les comptes

1. L'article 85, paragraphe 9, s'applique également lorsque les paiements sont initiés par l'intermédiaire d'un prestataire de services d'initiation de paiement. L'article 85, paragraphe 10, s'applique également lorsque les paiements sont initiés par l'intermédiaire d'un prestataire de services d'initiation de paiement et lorsque les informations sont demandées par l'intermédiaire d'un prestataire de services d'information sur les comptes.

2. Les prestataires de services de paiement gestionnaires de comptes autorisent les prestataires de services d'initiation de paiement et les prestataires de services d'information sur les comptes à se fonder sur les procédures d'authentification prévues par le prestataire de services de paiement gestionnaire du compte à l'intention de l'utilisateur de services de paiement conformément à l'article 85, paragraphes 1 et 10, et, lorsque le prestataire de services d'initiation de paiement intervient, conformément à l'article 85, paragraphes 1, 8, 9, 10 et 11.

3. Sans préjudice du paragraphe 2, lorsque les informations sur les comptes de paiement sont consultées par un prestataire de services d'information sur les comptes, le prestataire de services de paiement gestionnaire du compte n'applique l'authentification forte du client que pour le premier accès d'un prestataire de services d'information sur les comptes donné aux données d'un compte de paiement, sauf si le prestataire de services de paiement gestionnaire du compte a des motifs raisonnables de soupçonner une fraude, mais pas pour les accès ultérieurs de ce prestataire de services d'information sur les comptes à ce compte de paiement.

4. À moins que le prestataire de services de paiement gestionnaire du compte n'ait des motifs raisonnables de soupçonner une fraude, les prestataires de services d'information sur les comptes appliquent leur propre authentification forte du client lorsque l'utilisateur de services de paiement accède aux informations sur les comptes de paiement extraites par un tel prestataire de services d'information sur les comptes au moins 180 jours après la dernière application de l'authentification forte du client.

Article 87

Accords d'externalisation pour l'application de l'authentification forte du client

Le prestataire de services de paiement du payeur conclut un accord d'externalisation avec son prestataire de services techniques dans le cas où ce dernier fournit et vérifie les éléments de l'authentification forte du client. En vertu d'un tel accord, le prestataire de services de paiement d'un payeur reste entièrement responsable de tout défaut d'application de l'authentification forte du client et a le droit d'auditer et de contrôler les mesures de sécurité.

Article 88

Exigences en matière d'accessibilité concernant l'authentification forte du client

1. Sans préjudice des exigences en matière d'accessibilité prévues par la directive (UE) 2019/882, les prestataires de services de paiement veillent à ce que tous leurs clients, y compris les personnes handicapées, les personnes âgées, les personnes ayant de faibles compétences numériques et celles qui n'ont pas accès aux canaux ou instruments de paiement numériques, disposent au moins d'un moyen, adapté à leur situation spécifique, leur permettant de procéder à une authentification forte du client.

2. Les prestataires de services de paiement ne subordonnent pas l'exécution de l'authentification forte du client à l'utilisation exclusive d'un moyen unique d'authentification et ne font pas dépendre l'exécution de l'authentification forte du client, explicitement ou implicitement, de la possession d'un téléphone intelligent. Les prestataires de services de paiement mettent au point divers moyens d'application de l'authentification forte du client afin de tenir compte de la situation spécifique de tous leurs clients.

Article 89

Normes techniques de réglementation concernant l'authentification, la communication et les mécanismes de contrôle des opérations

1. L'ABE élabore des projets de normes techniques de réglementation qui précisent:

a) les exigences relatives à l'authentification forte du client mentionnée à l'article 85;

b) les dérogations à l'application de l'article 85, paragraphes 1, 8 et 9, sur la base des critères énoncés à l'article 85, paragraphe 11;

c) les exigences auxquelles doivent satisfaire les mesures de sécurité, conformément à l'article 85, paragraphe 10, afin de protéger la confidentialité et l'intégrité des données de sécurité personnalisées des utilisateurs de services de paiement;

d) les exigences applicables, conformément à l'article 87, aux accords d'externalisation conclus entre les prestataires de services de paiement des payeurs et les prestataires de services techniques en ce qui concerne la fourniture et la vérification des éléments d'authentification forte du client par les prestataires de services techniques;

e) les exigences en vertu du titre III, chapitre 3, applicables aux normes ouvertes communes et sécurisées de communication aux fins de l'identification, de l'authentification, de la notification et de l'information, ainsi que pour la mise en œuvre des mesures de sécurité, entre les prestataires de services de paiement gestionnaires de comptes, les prestataires de services d'initiation de paiement, les prestataires de services d'information sur les comptes, les payeurs, les bénéficiaires et d'autres prestataires de services de paiement;

f) des dispositions supplémentaires relatives aux normes ouvertes sécurisées de communication utilisant des interfaces spécifiques;

g) les exigences techniques applicables aux mécanismes de contrôle des opérations mentionnés à l'article 83.

Aux fins du point b), en ce qui concerne la dérogation à l'application de l'authentification forte du client pour les opérations de paiement, sur la base d'une analyse des risques liés à l'opération, les projets de normes techniques de réglementation précisent, entre autres:

i) les conditions qui doivent être remplies pour qu'une opération de paiement électronique à distance soit considérée comme présentant un faible niveau de risque;

ii) les méthodes et modèles de mise en œuvre de l'analyse des risques liés à l'opération;

iii) les critères de calcul des taux de fraude, y compris en ce qui concerne la répartition des taux de fraude entre les prestataires de services de paiement fournissant des services d'émission et d'acquisition, ou au sein des prestataires de services de paiement fournissant des services d'émission et d'acquisition par l'intermédiaire d'une entité juridique unique;

iv) des exigences détaillées et proportionnées en matière de communication d'informations et d'audit.

2. Lorsqu'elle élabore les projets de normes techniques de réglementation mentionnés au paragraphe 1, l'ABE tient compte des éléments suivants:

a) la nécessité de garantir un niveau de sécurité approprié pour les utilisateurs de services de paiement et les prestataires de services de paiement par l'adoption d'exigences efficaces et fondées sur les risques;

b) la nécessité de garantir la sécurité des fonds et des données à caractère personnel des utilisateurs de services de paiement;

c) la nécessité de garantir et de maintenir une concurrence équitable entre l'ensemble des prestataires de services de paiement;

d) la nécessité de garantir la neutralité du modèle commercial et des technologies;

e) la nécessité de permettre le développement de moyens de paiement innovants, accessibles et faciles à utiliser.

L'ABE soumet les projets de normes techniques de réglementation mentionnés au paragraphe 1 à la Commission au plus tard le [OP: veuillez insérer la date correspondant à un an après la date d'entrée en vigueur du présent règlement]. La Commission est habilitée à adopter les normes techniques de réglementation mentionnées au premier alinéa, conformément aux articles 10 à 14 du règlement (UE) nº 1093/2010.

3. Conformément à l'article 10 du règlement (UE) nº 1093/2010, l'ABE réexamine et, le cas échéant, met à jour les normes techniques de réglementation à intervalles réguliers, afin notamment de tenir compte de l'innovation et des progrès technologiques, ainsi que des dispositions du chapitre II du règlement (UE) 2022/2554, et des portefeuilles européens d'identité numérique mis en œuvre en vertu du règlement (UE) nº 910/2014.

CHAPITRE 8

Procédures d'exécution, autorités compétentes et pénalités

SECTION 1

PROCEDURES DE RECLAMATION

Article 90

Réclamations

1. Les États membres mettent en place des procédures permettant aux utilisateurs de services de paiement et aux autres parties intéressées, y compris les associations de consommateurs, de soumettre des réclamations aux autorités compétentes désignées pour faire appliquer le présent règlement en cas de violation alléguée des dispositions du présent règlement par des prestataires de services de paiement.

2. Le cas échéant et sans préjudice du droit de recours devant une juridiction prévu par le droit procédural national, la réponse des autorités compétentes aux réclamations mentionnées au paragraphe 1 informe l'auteur de la réclamation de l'existence des procédures de règlement extrajudiciaire des litiges instituées conformément à l'article 95.

Article 91

Autorités compétentes et pouvoirs d'enquête

1. Les autorités compétentes exercent leurs pouvoirs d'enquête sur les infractions potentielles au présent règlement et imposent les sanctions et mesures administratives prévues par leur cadre juridique national conformément au présent règlement, selon l'une ou l'autre des modalités suivantes:

   a) directement;

   b) en collaboration avec d'autres autorités;

   c) en déléguant des pouvoirs à d'autres autorités ou organes, tout en conservant la responsabilité de la surveillance de l'autorité ou de l'organisme délégataire;

   d) par saisine des autorités judiciaires compétentes.

   Lorsque les autorités compétentes délèguent l'exercice de leurs pouvoirs à d'autres autorités ou organes conformément au point c), la délégation de pouvoir précise les tâches déléguées, les conditions dans lesquelles elles doivent être exécutées et les conditions dans lesquelles la délégation de pouvoir peut être révoquée. Les autorités ou organes auxquels les pouvoirs sont délégués sont organisés de manière à veiller à éviter les conflits d'intérêts. Les autorités compétentes surveillent l'activité des autorités ou organes auxquels les pouvoirs sont délégués.

2. Les États membres désignent des autorités compétentes chargées de garantir et de contrôler le respect effectif du présent règlement. Ces autorités compétentes prennent toutes les mesures appropriées pour assurer ce respect.

   Les autorités compétentes sont:

   a) soit des autorités publiques,

   b) soit des organismes reconnus par le droit national ou par des autorités publiques expressément habilitées à cette fin par le droit national, notamment les banques centrales nationales.

   Les autorités compétentes sont indépendantes des instances économiques et ne présentent aucun conflit d'intérêts. Sans préjudice du paragraphe 2, point b), les établissements de paiement, les établissements de crédit ou les offices de chèques postaux ne peuvent être désignés comme autorités compétentes.

3. Les autorités compétentes visées au paragraphe 2 sont dotées de tous les pouvoirs d'enquête et des ressources nécessaires à l'exercice de leurs tâches.

   Ces pouvoirs comprennent:

   a) dans le cadre des procédures d'enquête sur les infractions potentielles au présent règlement, le pouvoir d'exiger, notamment des personnes physiques ou morales suivantes, toutes les informations nécessaires pour mener à bien une telle enquête:

      i) les prestataires de services de paiement;

      ii) les prestataires de services techniques et les opérateurs de systèmes de paiement;

      iii) les fournisseurs de distributeurs automatiques de billets qui ne gèrent pas de comptes de paiement;

iv) les prestataires de services de communications électroniques;

v) les personnes physiques appartenant aux entités mentionnées aux points i), ii) et iii);

vi) les tiers auprès desquels les entités mentionnées aux points i), ii) et iii) ont externalisé des fonctions ou des activités opérationnelles;

vii) les agents et distributeurs des entités mentionnées aux points i), ii) et iii) et leurs succursales établies dans l'État membre concerné;

b) le pouvoir de mener toutes les enquêtes nécessaires auprès de toute personne mentionnée au point a), i) à vi), établie ou située sur le territoire de l'État membre de l'autorité compétente ou y fournissant des services, lorsque cela est nécessaire à l'accomplissement des tâches confiées aux autorités compétentes, y compris le pouvoir:

i) d'exiger la production de documents;

ii) d'examiner les livres et les enregistrements des personnes mentionnées au point a), i) à vii), et d'en prendre des copies ou d'en prélever des extraits;

iii) de demander des explications écrites ou orales à toute personne mentionnée au point a), i) à vii), ou à ses représentants ou à son personnel, le cas échéant;

iv) d'interroger toute autre personne physique qui accepte d'être interrogée aux fins de recueillir des informations concernant l'objet d'une enquête;

c) le pouvoir de procéder à tous les contrôles nécessaires dans les locaux professionnels des personnes morales ou des personnes physiques mentionnées au point a), i) à vii), sous réserve de notification préalable par les autorités compétentes concernées.

4. Lorsque la législation d'un État membre prévoit des sanctions pénales applicables aux infractions au présent règlement conformément à l'article 96, paragraphe 2, cet État membre met en place des dispositions législatives, réglementaires et administratives nécessaires pour permettre aux autorités compétentes:

a) d'assurer la liaison avec les autorités judiciaires compétentes afin de recevoir des informations précises concernant les enquêtes pénales portant sur des infractions alléguées au présent règlement, les procédures pénales engagées pour de telles infractions alléguées et l'issue de ces procédures, y compris le jugement définitif;

b) de fournir ces informations aux autres autorités compétentes et à l'ABE afin de satisfaire à leur obligation de coopérer entre elles et avec l'ABE aux fins du présent règlement.

5. La mise en œuvre et l'exercice des pouvoirs énoncés au présent article sont proportionnés et conformes au droit de l'Union et au droit national, y compris aux garanties procédurales applicables et aux principes de la charte des droits fondamentaux de l'Union européenne. Les mesures d'enquête et d'exécution adoptées en application du présent règlement sont adaptées à la nature de l'infraction et au préjudice global réel ou potentiel qui en découle.

6. Au plus tard le [OP: veuillez insérer la date d'entrée en vigueur du présent règlement], l'ABE émet, conformément à l'article 16 du règlement (UE)

nº 1093/2010, des orientations sur les procédures de réclamation, notamment concernant les canaux de dépôt des réclamations, les informations demandées aux auteurs des réclamations et la publication de l'analyse agrégée des réclamations mentionnées à l'article 90, paragraphe 1.

Article 92

Secret professionnel

1. Sans préjudice des cas relevant du droit pénal national, toutes les personnes qui travaillent ou ont travaillé pour des autorités compétentes ainsi que tous les experts mandatés par les autorités compétentes sont tenus au secret professionnel concernant les informations relatives aux enquêtes effectuées par les autorités compétentes.
2. Les informations échangées conformément à l'article 93 sont soumises au secret professionnel tant au sein de l'autorité communiquant les informations qu'au sein de l'autorité destinataire.

Article 93

Compétence et coopération entre les autorités compétentes

1. En cas de violation ou de violation présumée des titres II et III, les autorités compétentes sont celles de l'État membre d'origine du prestataire de services de paiement, sauf dans le cas des agents et succursales exerçant une activité en vertu du droit d'établissement où les autorités compétentes sont celles de l'État membre d'accueil.
2. En cas de violations ou de violations présumées des titres II et III de la part de prestataires de services techniques, d'opérateurs de systèmes de paiement, de fournisseurs de distributeurs automatiques de billets qui ne gèrent pas de comptes de paiement, de prestataires de services de communications électroniques ou de la part de leurs agents ou succursales, les autorités compétentes sont celles de l'État membre dans lequel le service concerné est fourni.
3. Dans l'exercice de leurs pouvoirs d'enquête et de sanction, y compris dans les affaires transfrontières, les autorités compétentes coopèrent entre elles et avec les autres autorités de tout secteur concerné, selon le cas et conformément au droit de l'Union et au droit national, en échangeant des informations et en assurant l'assistance mutuelle aux autres autorités compétentes concernées, dans la mesure nécessaire à l'application effective des sanctions et mesures administratives.
4. Les autorités des autres secteurs concernés mentionnées au paragraphe 3 coopèrent avec les autorités compétentes en vue de l'application effective des sanctions et mesures administratives.

SECTION 2

PROCEDURES DE REGLEMENT DES LITIGES ET SANCTIONS

Article 94

Règlement des litiges

1. Les prestataires de services de paiement mettent en place et appliquent des procédures appropriées et efficaces pour le règlement des réclamations des utilisateurs de services de paiement concernant les droits et obligations découlant des titres II et III de la présente directive. Les autorités compétentes contrôlent l'application de ces procédures.

   Ces procédures sont appliquées dans chaque État membre où le prestataire de services de paiement propose les services de paiement et dans une des langues officielles de l'État membre concerné ou dans une autre langue si le prestataire de services de paiement et l'utilisateur de services de paiement en sont convenus ainsi.

2. Les prestataires de services de paiement mettent tout en œuvre pour répondre, sur support papier ou, si le prestataire de services de paiement et l'utilisateur de services de paiement en sont convenus ainsi, sur un autre support durable, aux réclamations des utilisateurs de services de paiement. Cette réponse aborde tous les points soulevés dans la réclamation et est transmise dans un délai approprié et au plus tard dans les 15 jours ouvrables suivant la réception de la réclamation. Dans des situations exceptionnelles, si une réponse ne peut être donnée dans les 15 jours ouvrables pour des raisons échappant au contrôle du prestataire de services de paiement, celui-ci envoie une réponse d'attente motivant clairement le délai complémentaire nécessaire pour répondre à la réclamation et précisant la date ultime à laquelle l'utilisateur de services de paiement recevra une réponse définitive. En tout état de cause, le délai pour recevoir une réponse définitive ne dépasse pas 35 jours ouvrables supplémentaires.

   Les États membres peuvent introduire ou maintenir des règles en matière de procédures de règlement des différends qui sont plus avantageuses pour l'utilisateur de services de paiement que celles prévues au premier alinéa. Lorsque les États membres procèdent de la sorte, ce sont ces règles qui s'appliquent.

3. Le prestataire de services de paiement informe l'utilisateur de services de paiement d'au moins une instance de règlement extrajudiciaire compétente pour connaître des litiges concernant les droits et obligations découlant des titres II et III.

4. Les informations mentionnées au paragraphe 3 sont mentionnées de manière claire, complète et aisément accessible sur le site internet du prestataire de services de paiement et sur l'application mobile correspondante, quand il en existe, auprès de la succursale et dans les conditions générales du contrat conclu entre le prestataire de services de paiement et l'utilisateur de services de paiement. Le prestataire de services de paiement précise comment de plus amples informations sur l'instance de règlement extrajudiciaire concernée et sur les conditions d'un tel recours peuvent être obtenues.

Article 95

Procédures de règlement extrajudiciaire

1. Les États membres mettent en place, conformément au droit de l'Union et au droit national applicables ainsi qu'aux exigences de qualité énoncées dans la directive 2013/11/UE du Parlement européen et du Conseil[66], des procédures indépendantes, impartiales, transparentes et efficaces de règlement extrajudiciaire aux fins du règlement des litiges opposant les utilisateurs de services de paiement aux prestataires de services de paiement quant aux droits et obligations découlant des titres II et III, en recourant, le cas échéant, aux organismes compétents existants. Les procédures de règlement extrajudiciaire sont applicables aux prestataires de services de paiement.

2. Les organismes mentionnés au paragraphe 1 du présent article coopèrent efficacement à la résolution des litiges transfrontières concernant les droits et obligations découlant des titres II et III.

3. Les États membres désignent une autorité compétente chargée d'accréditer, de contrôler et de publier le niveau de qualité de l'instance ou des instances de règlement extrajudiciaire sur leur territoire pour régler les litiges relatifs aux droits et obligations découlant des titres II et III, conformément à l'article 18 de la directive 2013/11/UE.

4. Les autorités compétentes mentionnées au paragraphe 3 notifient à la Commission, conformément à l'article 20 de la directive 2013/11/UE, l'instance ou les instances de règlement extrajudiciaire compétentes sur leur territoire pour régler les litiges relatifs aux droits et obligations découlant des titres II et III.

5. La Commission publie une liste des instances de règlement extrajudiciaire qui lui ont été notifiées conformément au paragraphe 4 et met à jour cette liste chaque fois que des changements lui sont communiqués.

Article 96

Sanctions et mesures administratives

1. Sans préjudice des pouvoirs de surveillance des autorités compétentes désignées en vertu de la directive (UE) XXX (DSP3), conformément au titre II, chapitre 1, section 3, de ladite directive, et du droit des États membres de prévoir des sanctions pénales, les États membres déterminent le régime des sanctions et mesures administratives applicables aux infractions au présent règlement et veillent à ce qu'il soit mis en œuvre. Les sanctions et mesures administratives sont effectives, proportionnées et dissuasives.

2. Les États membres peuvent décider de ne pas fixer de régime de sanctions et mesures administratives applicable aux infractions au présent règlement qui sont passibles de

[66] Directive 2013/11/UE du Parlement européen et du Conseil du 21 mai 2013 relative au règlement extrajudiciaire des litiges de consommation et modifiant le règlement (CE) nº 2006/2004 et la directive 2009/22/CE (directive relative au RELC) (JO L 165 du 18.6.2013, p. 63).

sanctions pénales en vertu du droit pénal national. Dans ce cas, les États membres notifient à la Commission les dispositions de droit pénal pertinentes et leurs modifications ultérieures conformément à l'article 103.

3. Lorsque le régime national mentionné au paragraphe 1 s'applique aux prestataires de services de paiement et aux autres personnes morales, en cas d'infraction et sous réserve des conditions prévues par le droit national, des sanctions et mesures administratives sont applicables aux membres de l'organe de direction de ces prestataires de services de paiement et de ces personnes morales ainsi qu'aux autres personnes physiques reconnues responsables d'une infraction au présent règlement.

4. Les États membres peuvent établir, conformément à leur droit national, des règles permettant à leurs autorités compétentes de clore une enquête concernant une infraction alléguée au présent règlement à la suite d'un accord de règlement ou d'une procédure d'exécution accélérée.

Le fait que les autorités compétentes soient habilitées à transiger ou à ouvrir des procédures d'exécution accélérées est sans incidence sur les obligations qui incombent aux États membres en vertu du paragraphe 1.

Article 97

Sanctions administratives et autres mesures administratives pour des infractions spécifiques

1. Sans préjudice de l'article 96, paragraphe 2, les dispositions législatives, réglementaires et administratives nationales fixent les sanctions administratives et autres mesures administratives mentionnées au paragraphe 2 du présent article applicables en cas de violation ou de contournement des dispositions suivantes:

   a) les règles d'accès aux comptes détenus auprès d'un établissement de crédit prévues à l'article 32;

   b) les règles d'accès sécurisé aux données de la part du prestataire de services de paiement gestionnaire du compte ou des prestataires de services d'information sur les comptes et des prestataires de services d'initiation de paiement énoncées au titre III, chapitre 3, sans préjudice de l'article 45;

   c) l'obligation d'organiser ou de mettre en œuvre des mécanismes de prévention de la fraude, y compris l'authentification forte du client, conformément aux articles 85, 86 et 87;

   d) l'obligation de respecter les exigences de transparence en matière de frais incombant aux opérateurs de DAB ou autres distributeurs d'espèces, conformément à l'article 20, point c) ii);

   e) le non-respect, par les prestataires de services de paiement, du délai d'indemnisation des utilisateurs de services de paiement fixé à l'article 56, paragraphe 2, à l'article 57, paragraphe 2, et à l'article 59, paragraphe 2.

2. Dans les cas mentionnés au paragraphe 1, les sanctions et mesures administratives applicables consistent notamment en:

   a) des amendes administratives;

i) dans le cas d'une personne morale, une amende administrative maximale d'au moins 10 % de son chiffre d'affaires annuel total tel que défini au paragraphe 3;

ii) dans le cas d'une personne physique, une amende administrative maximale d'au moins 5 000 000 EUR ou, dans les États membres dont la monnaie n'est pas l'euro, la valeur correspondante dans la monnaie nationale à la date d'entrée en vigueur du présent règlement;

iii) une amende administrative d'un montant maximal d'au moins deux fois le montant de l'avantage retiré de l'infraction, s'il peut être déterminé;

b) une déclaration publique précisant l'identité de la personne morale ou physique responsable de l'infraction et la nature de l'infraction;

c) une injonction ordonnant à la personne morale ou physique responsable de l'infraction de mettre un terme au comportement illicite et lui interdisant de le réitérer;

d) l'interdiction provisoire, pour tout membre de l'organe de direction de la personne physique ou toute autre personne physique tenue pour responsable de la violation, d'exercer des fonctions de direction.

3. Le chiffre d'affaires annuel total mentionné au paragraphe 2, point a) i), du présent article et à l'article 98, paragraphe 1, du présent règlement est égal au chiffre d'affaires net tel que défini à l'article 2, point 5), de la directive 2013/34/UE, selon les états financiers annuels disponibles à la dernière date de clôture du bilan, adoptés sous la responsabilité des membres des organes d'administration, de direction et de surveillance de la personne morale.

Lorsque la personne morale est une entreprise mère ou une filiale d'une entreprise mère qui est tenue d'établir des états financiers consolidés conformément à l'article 22 de la directive 2013/34/UE, le chiffre d'affaires annuel total à prendre en considération est le chiffre d'affaires net ou le revenu déterminé selon les normes comptables applicables, tel qu'il ressort des états financiers consolidés de l'entreprise mère ultime arrêtés à la dernière date de clôture du bilan et adoptés sous la responsabilité des organes d'administration, de direction et de surveillance.

4. Les États membres peuvent habiliter les autorités compétentes, conformément à leur droit national, à imposer d'autres types de sanctions et d'autres types de pouvoirs de sanction en plus de ceux mentionnés au paragraphe 2 du présent article et à l'article 98 en ce qui concerne les astreintes.

Article 98

Astreintes

1. Les autorités compétentes sont habilitées à infliger des astreintes aux personnes physiques ou morales pour non-respect de toute décision, injonction, mesure provisoire, demande, obligation ou autre mesure adoptée conformément au présent règlement.

L'astreinte visée au premier alinéa est effective et proportionnée et consiste en un montant journalier à payer jusqu'au rétablissement de la conformité. Les astreintes

sont infligées pour une durée n'excédant pas six mois à compter de la date indiquée dans la décision infligeant l'astreinte.

Les autorités compétentes sont habilitées à infliger des astreintes d'un montant maximal d'au moins:

a) 3 % du chiffre d'affaires journalier moyen dans le cas d'une personne morale;

b) 30 000 EUR dans le cas d'une personne physique.

Le chiffre d'affaires journalier moyen est le chiffre d'affaires annuel total mentionné à l'article 97, paragraphe 3, divisé par 365.

2. Les États membres peuvent prévoir des montants de sanctions pécuniaires plus élevés que ceux prévus au paragraphe 1.

Article 99

Éléments à prendre en considération pour déterminer les sanctions administratives et autres mesures administratives

1. Les autorités compétentes tiennent compte, au moment de déterminer le type et le niveau des sanctions administratives ou autres mesures administratives, de l'ensemble des éléments et circonstances pertinents pour appliquer des sanctions proportionnées, y compris:

a) de la gravité et de la durée de l'infraction;

b) du degré de responsabilité de la personne physique ou morale responsable de l'infraction;

c) de l'assise financière de la personne physique ou morale responsable de l'infraction, telle qu'elle ressort, entre autres, du chiffre d'affaires annuel total de la personne morale ou des revenus annuels de la personne physique responsable de l'infraction;

d) de l'ampleur de l'avantage retiré ou des pertes évitées par la personne physique ou morale responsable de l'infraction, dans la mesure où ils peuvent être déterminés;

e) des préjudices subis par des tiers du fait de l'infraction, dans la mesure où ils peuvent être déterminés;

f) du préjudice résultant pour la personne morale ou physique responsable de l'infraction du cumul de poursuites de nature administrative et de nature pénale et de sanctions pénales et administratives pour le même comportement;

g) de l'incidence de l'infraction sur les intérêts des consommateurs et des autres utilisateurs de services de paiement;

h) des conséquences systémiques négatives réelles ou potentielles de l'infraction;

i) de la complicité ou de la participation de plus d'une personne physique ou morale à l'infraction;

j) des infractions antérieures commises par la personne physique ou morale responsable de l'infraction;

k) du degré de coopération avec les autorités compétentes dont a fait preuve la personne physique ou morale responsable de l'infraction;

l) de toute mesure corrective prise par la personne morale ou physique responsable de l'infraction pour éviter qu'elle ne se reproduise.

2. Les autorités compétentes qui recourent à des accords de règlement ou à des procédures d'exécution accélérées conformément à l'article 96, paragraphe 4, adaptent les sanctions et mesures administratives pertinentes prévues aux articles 96, 97 et 98 au cas concerné afin de garantir leur proportionnalité.

Article 100

Droit de recours

1. Les décisions prises par les autorités compétentes en application du présent règlement peuvent faire l'objet d'un recours juridictionnel.

2. Le paragraphe 1 s'applique également en cas de carence.

Article 101

Publication des sanctions et mesures administratives

1. Les autorités compétentes publient sur leur site internet toutes les décisions imposant une sanction ou une mesure administrative à des personnes physiques et morales pour infraction au présent règlement et, le cas échéant, tous les accords de règlement. La publication comprend une brève description de l'infraction, de la sanction administrative ou de toute autre mesure administrative imposée ou, le cas échéant, une déclaration relative à l'accord de règlement. L'identité de la personne physique faisant l'objet de la décision imposant une sanction ou une mesure administrative n'est pas publiée.

   Les autorités compétentes publient la décision et la déclaration visées au premier alinéa immédiatement après que la personne morale ou physique faisant l'objet de la décision a été informée de cette décision ou que l'accord de règlement a été signé.

2. Par dérogation au paragraphe 1, lorsque la publication de l'identité ou d'autres données à caractère personnel concernant des personnes physiques est jugée nécessaire par l'autorité compétente nationale pour protéger la stabilité des marchés financiers ou garantir l'application effective du présent règlement, notamment dans le cas des déclarations publiques visées à l'article 97, paragraphe 2, point b), ou des interdictions temporaires visées à l'article 97, paragraphe 2, point d), l'autorité compétente nationale peut également publier l'identité des personnes ou des données à caractère personnel à condition qu'elle justifie une telle décision et que la publication soit limitée aux données à caractère personnel strictement nécessaires pour protéger la stabilité des marchés financiers ou garantir l'application effective du présent règlement.

3. Lorsque la décision imposant une sanction administrative ou une autre mesure administrative fait l'objet d'un recours devant l'autorité judiciaire ou une autre autorité compétente, les autorités compétentes publient également sans tarder sur leur

site internet officiel des informations sur le recours ainsi que toute information ultérieure sur le résultat dudit recours dans la mesure où il concerne des personnes morales. Lorsque la décision attaquée concerne une personne physique et que la dérogation prévue au paragraphe 2 n'est pas appliquée, les autorités compétentes ne publient les informations relatives au recours que dans une version anonymisée.

4. Les autorités compétentes veillent à ce que toute publication effectuée conformément au présent article demeure sur leur site internet officiel pendant cinq ans au plus. Les données à caractère personnel contenues dans la publication ne sont conservées sur le site internet officiel de l'autorité compétente que si un réexamen annuel montre qu'il est toujours nécessaire de publier ces données pour protéger la stabilité des marchés financiers ou garantir l'application effective du présent règlement, et en tout état de cause pendant une durée maximale de cinq ans.

Article 102

Surveillance des procédures, sanctions et mesures

1. Les autorités compétentes communiquent régulièrement à l'ABE, sous une forme anonymisée et agrégée:

   a) les procédures administratives formelles engagées, suspendues ou closes conduisant à l'imposition de sanctions ou de mesures administratives;

   b) les astreintes infligées conformément à l'article 98 pour des infractions en cours au présent règlement;

   c) le cas échéant, les accords de règlement et les procédures d'exécution accélérées, et leur issue, indépendamment de leur publication, conformément à l'article 96, paragraphe 4;

   d) les procédures pénales donnant lieu à une condamnation et les sanctions correspondantes signalées par les autorités judiciaires conformément à l'article 91, paragraphe 4, point a);

   e) tout recours contre les décisions d'imposer des sanctions pénales ou administratives ou des mesures administratives et l'issue de ce recours.

2. Lorsque l'autorité compétente rend publique une sanction ou mesure administrative, elle la notifie simultanément à l'ABE.

3. Dans un délai de deux ans à compter de la date d'application du présent règlement, puis tous les deux ans, l'ABE présente à la Commission un rapport sur l'application par les autorités compétentes des sanctions en vue de garantir le respect du présent règlement.

Article 103

Notification des mesures de mise en œuvre

Les États membres notifient à la Commission les dispositions législatives, réglementaires et administratives adoptées conformément au présent chapitre, y compris toute disposition de droit pénal pertinente, au plus tard le [OP: veuillez insérer la date d'entrée en vigueur du

présent règlement]. Les États membres notifient dans les meilleurs délais à la Commission toute modification ultérieure qui y est apportée.

CHAPITRE 9

Pouvoirs d'intervention de l'ABE en matière de produits

Article 104

Pouvoirs d'intervention temporaire de l'ABE

1. Conformément à l'article 9, paragraphe 5, du règlement (UE) nº 1093/2010, l'ABE peut, si les conditions énoncées aux paragraphes 2 et 3 du présent article sont remplies, interdire ou restreindre temporairement dans l'Union un certain type ou une fonctionnalité spécifique d'un service ou instrument de paiement ou d'un service ou instrument de monnaie électronique. Une interdiction ou une restriction peut s'appliquer dans des circonstances précises ou admettre des exceptions définies par l'ABE.

2. L'ABE ne prend de décision en vertu du paragraphe 1 que si toutes les conditions suivantes sont remplies:

   a) la mesure proposée concerne un nombre important d'utilisateurs de services de paiement ou d'utilisateurs de services de monnaie électronique ou vise à faire face à une menace pour le bon fonctionnement des marchés des paiements ou des marchés de monnaie électronique et pour l'intégrité de ces marchés, ou pour la stabilité de tout ou partie de ces marchés dans l'Union;

   b) les exigences réglementaires déjà applicables, en vertu du droit de l'Union, au service de paiement ou au service de monnaie électronique concerné ne parent pas à cette menace;

   c) la ou les autorités compétentes n'ont pas pris de mesures pour faire face à la menace ou les mesures qui ont été prises ne sont pas suffisantes à cet effet.

   Si les conditions énoncées à l'alinéa premier sont remplies, l'ABE peut, par mesure de précaution, imposer l'interdiction ou la restriction prévue au paragraphe 1 avant qu'un service de paiement ou un service de monnaie électronique n'ait été fourni ou distribué aux utilisateurs de services de paiement.

3. Lorsqu'elle prend une mesure au titre du présent article, l'ABE s'assure:

   a) que la mesure n'a pas une incidence négative sur l'efficacité du marché des paiements ou du marché des services de monnaie électronique ou sur les prestataires de services de paiement ou de services de monnaie électronique, qui serait disproportionnée par rapport aux bénéfices apportés par la mesure;

   b) que la mesure ne suscite pas de risque d'arbitrage réglementaire; et

   c) que la mesure a été prise après consultation de l'autorité compétente nationale concernée.

4. Avant de décider d'intervenir au titre du présent article, l'ABE informe les autorités compétentes de la mesure qu'elle propose.

5. L'ABE publie un avis sur son site internet chaque fois qu'elle décide d'intervenir en vertu du présent article. L'avis décrit de façon détaillée l'interdiction ou la restriction et précise le moment après la publication de l'avis à partir duquel les mesures prendront effet, tout en veillant à ce que les avis relatifs à de telles décisions concernant des personnes physiques ne soient publiés que dans une version anonymisée. L'interdiction ou la restriction n'est applicable qu'aux actes postérieurs à la prise d'effet des mesures.

6. L'ABE examine les interdictions ou les restrictions imposées en application du paragraphe 1 à intervalles réguliers et au moins tous les trois mois. Si l'interdiction ou la restriction n'est pas renouvelée après cette période de trois mois, elle expire.

7. Les mesures adoptées par l'ABE au titre du présent article prévalent sur toute mesure précédente prise par une autorité compétente.

8. La Commission adopte, conformément à l'article 106, des actes délégués précisant les critères et les facteurs que doit prendre en compte l'ABE pour déterminer quand il existe, au sens du paragraphe 2, point a), un nombre important d'utilisateurs de services de paiement ou d'utilisateurs de services de monnaie électronique ou une menace pour le bon fonctionnement des marchés des paiements ou des services de monnaie électronique et pour l'intégrité de ces marchés, ou pour la stabilité de tout ou partie de ces marchés dans l'Union.

   Ces critères et facteurs sont notamment les suivants:

   a) le degré de complexité d'un service ou instrument de paiement, ou d'un service ou instrument de monnaie électronique et la relation avec le type d'utilisateurs, y compris les consommateurs, auxquels ils sont proposés;

   b) le degré de risque, pour les consommateurs, d'un service ou instrument de paiement, ou d'un service ou instrument de monnaie électronique;

   c) l'utilisation éventuelle par les fraudeurs du service ou instrument de paiement, ou du service ou instrument de monnaie électronique;

   d) la taille ou le niveau d'utilisation du service ou instrument de paiement, ou du service ou instrument de monnaie électronique;

   e) le degré d'innovation d'un service ou instrument de paiement, ou d'un service ou instrument de monnaie électronique.

TITRE IV

ACTES DÉLÉGUÉS

Article 105

Actes délégués

La Commission est habilitée à adopter des actes délégués conformément à l'article 106 afin de modifier le présent règlement en mettant à jour les montants visés à l'article 58, paragraphe 1.

Article 106

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.
2. Le pouvoir d'adopter les actes délégués visés à l'article 105 est conféré à la Commission pour une durée indéterminée à compter de la date d'entrée en vigueur du présent règlement.
3. La délégation de pouvoir visée à l'article 105 peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.
4. Avant d'adopter un acte délégué, la Commission consulte les experts désignés par les États membres, conformément aux principes définis dans l'accord interinstitutionnel «Mieux légiférer» du 13 avril 2016.
5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.
6. Un acte délégué adopté en vertu de l'article 105 n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de trois mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de trois mois à l'initiative du Parlement européen ou du Conseil.

TITRE V

DISPOSITIONS FINALES

Article 107

Droits au remboursement plus favorables et mesures de prévention de la fraude plus strictes

1. Les États membres ou les prestataires de services de paiement peuvent accorder aux utilisateurs de services de paiement des droits au remboursement plus favorables en ce qui concerne les virements autorisés visés aux articles 57 et 59, et prévoir des mesures de prévention de la fraude plus strictes que celles prévues à l'article 83, paragraphe 1, et à l'article 84.
2. Les États membres notifient à la Commission, au plus tard le [OP: veuillez insérer la date d'entrée en vigueur du présent règlement], les dispositions adoptées en vertu du paragraphe 1. Ils notifient sans retard à la Commission toute modification ultérieure.

Article 108

Clause de réexamen

1. La Commission soumet, au plus tard cinq ans après la date d'application du présent règlement, au Parlement européen, au Conseil, à la BCE et au Comité économique et social européen, un rapport sur l'application et l'impact du présent règlement, et en particulier sur:

   a) l'adéquation et l'incidence sur la concurrence et l'utilisation du système de banque ouverte des règles relatives à l'accès aux données des comptes de paiement pour l'activité des services d'information sur les comptes et des services d'initiation de paiement, et en particulier des règles relatives aux interfaces spécifiques et de leurs dérogations respectivement prévues aux articles 38 et 39;

   b) l'incidence des règles relatives à l'absence d'accords contractuels et d'indemnisation obligatoires pour l'accès des prestataires de services d'information sur les comptes et de services d'initiation de paiement aux interfaces mentionnées à l'article 34;

   c) l'adéquation et l'impact des règles relatives aux frais, y compris des règles relatives à la surfacturation énoncées à l'article 28;

   d) l'adéquation et l'impact des règles en matière de prévention et de réparation de la fraude sur les opérations non autorisées et autorisées.

   Le cas échéant, la Commission accompagne son rapport d'une proposition législative.

2. La Commission soumet, au plus tard le[OP: veuillez insérer la date correspondant à trois ans après la date d'entrée en vigueur du présent règlement], au Parlement européen, au Conseil, à la BCE et au Comité économique et social européen, un rapport sur le champ d'application du présent règlement, notamment en ce qui concerne les systèmes de paiement, les schémas de paiement et les prestataires de services techniques. Le cas échéant, la Commission accompagne ce rapport d'une proposition législative.

Article 109

Modifications du règlement (UE) nº 1093/2010

Le règlement (UE) nº 1093/2010 est modifié comme suit:

1. À l'article 1er, paragraphe 2, la première phrase est remplacée par la phrase suivante:

«L'Autorité agit selon les pouvoirs que le présent règlement lui confère et dans le champ d'application de la directive 2002/87/CE, de la directive 2008/48/CE ([1]), de la directive 2009/110/CE, du règlement (UE) nº 575/2013 ([2]), de la directive 2013/36/UE ([3]), de la directive 2014/49/UE ([4]), de la directive 2014/92/UE ([5]), de la directive (UE) […] (DSP3), du règlement (UE) […] (règlement sur les services de paiement) du Parlement européen et du Conseil ainsi que, dans la mesure où ces actes s'appliquent aux établissements de crédit, aux établissements financiers et aux autorités compétentes chargées de leur surveillance, des

parties pertinentes de la directive 2002/65/CE, y compris l'ensemble des directives, règlements et décisions fondés sur ces actes, ainsi que de tout autre acte juridiquement contraignant de l'Union conférant des tâches à l'Autorité.»

2. L'article 4, point 2, est modifié comme suit:

a) le point i) est remplacé par le texte suivant:

«les autorités compétentes ou les autorités de surveillance relevant du champ d'application des actes sectoriels mentionnées à l'article 1er, paragraphe 2, y compris la Banque centrale européenne en ce qui concerne les questions liées aux tâches qui lui sont confiées par le règlement (UE) nº 1024/2013;»;

b) les points iii), vi) et viii) sont supprimés.

Article 110

Modification du règlement (UE) 2017/2394

À l'annexe du règlement (UE) 2017/2394, le point suivant est ajouté:

«29. Règlement (UE) xxxx du Parlement européen et du Conseil du xxxx concernant les services de paiement dans le marché intérieur et modifiant le règlement (UE) nº 1093/2010.»

Article 111

Tableau de correspondance

Toute référence faite à la directive (UE) 2015/2366 et à la directive 2009/110/CE s'entend comme faite à la directive (UE) (DSP3) ou au présent règlement et est à lire selon le tableau de correspondance figurant à l'annexe III du présent règlement.

Article 112

Entrée en vigueur et application

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

Il est applicable à partir du [OP: veuillez insérer la date correspondant à 18 mois après la date d'entrée en vigueur du présent règlement].

Toutefois, les articles 50 et 57 s'appliquent à partir du [OP: veuillez insérer la date correspondant à 24 mois après la date d'entrée en vigueur du présent règlement].

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tous les États membres.

Fait à Bruxelles, le

Par le Parlement européen	*Par le Conseil*[2]
La présidente	*Le président*