Conseil de
l'Union européenne

Bruxelles, le 21 octobre 2026
(OR. en)

8543/26

Dossier interinstitutionnel:
2023/0210(COD)

EF 129
ECOFIN 524
CODEC 759
ECB

ACTES LÉGISLATIFS ET AUTRES INSTRUMENTS

Objet:	Position du Conseil en première lecture en vue de l'adoption du RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL concernant les services de paiement dans le marché intérieur et modifiant les règlements (UE) nº 1093/2010, (UE) nº 260/2012, (UE) 2017/2394 et (UE) 2021/1230

RÈGLEMENT (UE) 2026/...
DU PARLEMENT EUROPÉEN ET DU CONSEIL

du ...

concernant les services de paiement dans le marché intérieur
et modifiant les règlements (UE) nº 1093/2010, (UE) nº 260/2012,
(UE) 2017/2394 et (UE) 2021/1230

(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 de la Banque centrale européenne[1],

vu l'avis du Comité économique et social européen[2],

statuant conformément à la procédure législative ordinaire[3],

---

1 JO C, C/2024/3869, 19.6.2024, ELI: http://data.europa.eu/eli/C/2024/3869/oj.
2 JO C, C/2024/1594, 5.3.2024, ELI: http://data.europa.eu/eli/C/2024/1594/oj.
3 Position du Parlement européen du 23 avril 2024 (JO C, C/2025/3725, 17.9.2025, ELI: http://data.europa.eu/eli/C/2025/3725/oj) et position du Conseil en première lecture du … (non encore parue au Journal officiel). Position du Parlement européen du …(non encore parue au Journal officiel).

considérant ce qui suit:

(1) Depuis l'adoption de la directive (UE) 2015/2366 du Parlement européen et du Conseil[4], 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, y compris 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 du 24 septembre 2020 sur une stratégie en matière de paiements de détail pour l'UE, la Commission a annoncé le lancement d'un réexamen complet de l'application et des effets de la directive (UE) 2015/2366, qui devait inclure une évaluation globale de sa pertinence, en tenant compte de l'évolution du marché.

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

(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 des effets et de l'application de la directive (UE) 2015/2366 a révélé que celle-ci avait en grande partie réussi à réaliser bon nombre de ses objectifs, mais elle a également recensé certains domaines dans lesquels les objectifs de cette directive n'ont pas été 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 («open bankin»), à savoir les services d'information sur les comptes et les 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. Cette 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 de l'incidence et de l'application de la directive (UE) 2015/2366 a également recensé des problèmes liés à des divergences dans la mise en œuvre et le contrôle de l'application de ladite directive, qui ont eu une incidence directe sur la concurrence entre les prestataires de services de paiement en créant des conditions réglementaires effectivement différentes selon les États membres, ce qui a encouragé un arbitrage réglementaire. Il convient de ne pas laisser de place à l'élection de juridiction («forum shopping»), dans le cadre de laquelle un prestataire de services de paiement choisirait, comme pays d'origine, un État membre dans lequel l'application des règles de l'Union en matière de services de paiement lui est plus avantageuse, alors qu'il fournit des services transfrontières dans des États membres qui adoptent une interprétation plus stricte des règles ou des politiques plus actives de contrôle de l'application de ces règles à l'égard des 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 des activités de service de paiement, notamment les droits et obligations des parties concernées. Ces règles, à l'exclusion de celles relatives à l'agrément et à la surveillance des établissements de paiement, qui devraient rester dans une directive, devraient être plus claires et plus détaillées, afin de réduire au minimum la marge d'interprétation.

(5) Si l'émission de monnaie électronique est régie par la directive 2009/110/CE du Parlement européen et du Conseil[5], l'utilisation de la monnaie électronique pour financer des opérations de paiement est quant à elle, 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, 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 des directives 2009/110/CE et (UE) 2015/2366. Étant donné que la directive 2009/110/CE est abrogée par la directive (UE) 2026/... du Parlement européen et du Conseil[6+], ses règles, à l'exception des règles relatives à l'agrément et à la surveillance, qui ont été intégrées dans la directive (UE) 2026/...[++], devraient être reprises dans un cadre unifié au sein du présent règlement, moyennant les adaptations appropriées.

---

5 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, ELI: http://data.europa.eu/eli/dir/2009/110/oj).

6 Directive (UE) 2026/… du Parlement européen et du Conseil du … concernant les services de paiement dans le marché intérieur, modifiant la directive 98/26/CE et le règlement (UE) 2023/1114 et abrogeant les directives (UE) 2009/110/CE et 2015/2366 (JO L, …, ELI: …).

\+ JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209 (COD)) et ajouter les informations correspondantes dans la note de bas de page.

++ JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

(6) Pour assurer la sécurité juridique et un champ d'application clair des règles applicables à la 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 la 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[7]. Les établissements de paiement ne sont pas autorisés à recevoir des 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) 2026/…[+]. 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.

---

7 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, 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, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

+ JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

(8) L'exclusion du champ d'application de la directive (UE) 2015/2366 de certaines catégories d'opérateurs de distributeurs automatiques de billets s'est révélée difficile à mettre en pratique. Il convient, par conséquent, de remplacer la catégorie des fournisseurs de distributeurs automatiques de billets, qui était exclue de l'obligation d'agrément en tant que prestataire de services de paiement en vertu de la directive (UE) 2015/2366, par une nouvelle catégorie de fournisseurs de distributeurs automatiques de billets qui ne gèrent pas de comptes de paiement. Ces fournisseurs de distributeurs automatiques de billets, qui sont soumis à l'enregistrement en vertu de la directive (UE) 2026/...[+], devraient être soumis à des exigences en matière de transparence des frais dans les cas où ils en perçoivent pour les retraits d'espèces.

(9) Afin d'améliorer encore l'accès aux espèces, les détaillants devraient être autorisés à proposer, dans les magasins physiques, des services de retrait d'espèces, même lorsqu'un client n'effectue aucun achat, sans devoir obtenir d'agrément en tant que prestataire de services de paiement, sans enregistrement ou sans devoir être un agent d'un établissement de paiement. Ces services de retrait d'espèces devraient toutefois être soumis à l'obligation de communiquer les éventuels frais facturés au client. Les détaillants devraient fournir ces services sur une base volontaire et en fonction des espèces dont ils disposent.

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

(10) 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 été appliquée de manière très différente 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 la notion d'agent commercial aux fins de cette exclusion. 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 cette fin, les agents commerciaux devraient être autorisés, en vertu d'un accord 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 qu'aucune des parties ne dispose d'une véritable marge ou autonomie 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 européenne de surveillance (Autorité bancaire européenne – ABE), instituée par le règlement (UE) nº 1093/2010 du Parlement européen et du Conseil[8], devrait élaborer des orientations sur l'exclusion des opérations de paiement allant du payeur au bénéficiaire effectuées par l'intermédiaire d'un agent commercial, afin d'apporter davantage de clarté et de convergence entre les autorités compétentes. Ces orientations pourraient inclure un référentiel des cas d'utilisation qui relèvent généralement de l'exclusion applicable aux agents commerciaux.

---

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

(11) 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, même si les prestataires de services dont les instruments relevaient de cette exclusion étaient tenus de notifier leur activité aux autorités compétentes. L'ABE a fourni des orientations supplémentaires dans ses orientations du 24 février 2022. Malgré ces tentatives visant à clarifier l'application de l'exclusion relative aux instruments à finalité spécifique, des prestataires de services cherchent encore à bénéficier de cette exclusion tout en fournissant 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.

(12) Pour déterminer si un réseau limité est exclu du champ d'application du présent règlement, il convient de prendre en considération la localisation géographique et le nombre de points d'acceptation de ce réseau. Les instruments à finalité spécifique devraient permettre au détenteur d'acquérir des biens ou des services uniquement dans les locaux physiques ou les commerces en ligne 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, susceptibles de 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. En parallèle, l'environnement réglementaire des États membres pour ces titres devrait garantir l'acceptabilité de ces derniers. Les instruments à finalité spécifique devraient également inclure les instruments fondés sur la monnaie électronique lorsqu'ils satisfont aux exigences liées à l'exclusion. Il n'y a pas lieu d'exclure les instruments de paiement pouvant être utilisés pour réaliser des achats dans des magasins de commerçants enregistrés sur une liste, lesdits instruments étant, en principe, conçus pour un réseau de prestataires de services qui ne cesse de s'étendre.

(13) 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 sites, 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 également être exclues. Cette exclusion ne devrait s'appliquer que lorsque la valeur des opérations de paiement est inférieure à un seuil déterminé. Pour que l'exclusion s'applique, l'opérateur de télécommunications devrait fournir les services de paiement en plus des services de communications électroniques qu'il fournit à ses abonnés. Cela implique qu'il existe un accord contractuel direct entre l'opérateur de télécommunications et l'abonné pour la fourniture des services de communications électroniques et que le service de paiement constitue un service additionnel à ces services. Il existe des situations dans lesquelles un fournisseur de contenus numériques ou le fournisseur de services, pour lesquels l'abonné a payé par l'intermédiaire de son propre opérateur de télécommunications, fait appel à d'autres fournisseurs de services (ci-après dénommés "intermédiaires") pour la collecte et le transfert des fonds. Bien que ces intermédiaires, y compris les opérateurs bénéficiaires, les opérateurs d'encaissement et les opérateurs de transit, puissent également fournir des services de communications électroniques, ils ne peuvent pas bénéficier de l'exclusion, étant donné qu'ils n'ont pas de relation contractuelle directe avec l'abonné en ce qui concerne la fourniture de services de communications électroniques.

(14) 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 et les services connexes entre une entreprise mère et sa filiale, ou entre filiales d'une même entreprise mère, qui sont assurés par un prestataire de services de paiement faisant partie du même groupe devraient être exclus du champ d'application du présent règlement, y compris la redistribution, au moyen d'opérations de paiement intragroupe, de fonds reçus de tiers externes pour le compte d'entités du groupe, ainsi que la centralisation des ordres de paiement et des fonds de paiement pour le compte d'un groupe par une entreprise mère ou sa filiale pour transmission ultérieure, en vue de leur traitement, à un prestataire de services de paiement fournissant des services de paiement au groupe. Dans la mesure où les opérateurs de service public au sens du règlement (CE) nº 1370/2007 du Parlement européen et du Conseil[9] gèrent les paiements d'égalisation et le partage des recettes au sein d'un système fermé de traitement des paiements des opérateurs de transport ou par l'intermédiaire de leurs centres de compensation ou d'organisations ou associations tarifaires, ces opérations de paiement devraient également être exclues du champ d'application du présent règlement. Ces exclusions ne devraient pas être utilisées pour contourner ou éluder le droit de l'Union ou le droit national dans le domaine de la lutte contre le blanchiment de capitaux et le financement du terrorisme ou les règles relatives à l'agrément et à la surveillance des établissements de paiement.

[9] Règlement (CE) nº 1370/2007 du Parlement européen et du Conseil du 23 octobre 2007 relatif aux services publics de transport de voyageurs par chemin de fer et par route, et abrogeant les règlements (CEE) nº 1191/69 et (CEE) nº 1107/70 du Conseil (JO L 315 du 3.12.2007, p. 1, ELI: http://data.europa.eu/eli/reg/2007/1370/oj).

(15) 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, les services de protection de la vie privée, l'authentification des données et des entités, la fourniture de technologies de l'information et de la communication (TIC) et de réseaux de communication, ainsi que 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.

(16) Les services techniques ne sont pas des services de paiement dans la mesure où 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, qui devrait être limitée au préjudice financier direct et ne devrait pas excéder le montant de l'opération concernée, ou à l'obligation de conclure des accords d'externalisation avec des prestataires de services de paiement lorsque les prestataires de services techniques doivent fournir et vérifier les éléments d'authentification forte du client. Il convient 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.

(17) 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.

(18) 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 du payeur, 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.

(19) 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'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 pouvant être 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 de services d'information sur les comptes. Dans certains cas, tels que celui d'un compte de carte de crédit ou lorsqu'un compte n'est utilisé que pour l'exécution d'une seule opération, il convient de procéder à une analyse au cas par cas afin de déterminer si ce compte présente ces caractéristiques. 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, qui ne peuvent pas être utilisés pour envoyer ou recevoir des fonds à destination ou en provenance d'un tiers, sont par conséquent exclus de la définition d'un compte de paiement.

(20) La transmission de fonds («money remittance») est un service de paiement généralement fondé 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 proposent 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 donc être traités comme des services de transmission de fonds («money remittance»).

(21) Compte tenu de l'apparition de nouveaux types d'instruments de paiement, des solutions technologiques en évolution constante qui offrent de tels instruments et des incertitudes qui existent sur le marché en ce qui concerne la qualification juridique de tels instruments, il convient de préciser davantage la définition d'un "instrument de paiement" en fournissant des 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 certaines 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 le régime de responsabilité du prestataire de services de paiement. Aussi la NFC devrait-elle être considérée comme un élément d'un instrument de paiement et non comme un instrument de paiement en tant que tel.

(23) La définition d’un "instrument de paiement" figurant dans 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 les cartes de ce type 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, afin de 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 à transfert direct (ci-après dénommés "portefeuilles numériques pass-through") qui impliquent soit la tokenisation d'un instrument de paiement existant, par exemple une carte de paiement, soit un virement à partir d'un compte de paiement, doivent être considérés comme des services techniques et devraient dès lors être exclus des définitions d'instrument de paiement et de service d'initiation de paiement énoncées dans le présent règlement, à condition qu'aucun fonds ne soit stocké dans le portefeuille numérique, que le fournisseur de portefeuille numérique n'entre jamais en possession de tels fonds et que le fournisseur de portefeuille fonctionne selon des accords contractuels dans le cadre d'un système fermé avec les prestataires de services de paiement qui gèrent le compte de paiement du payeur ou émettent l'instrument de paiement du payeur. Un jeton ne peut pas être considéré, en tant que tel, comme un instrument de paiement, mais constitue plutôt une application de paiement, telle que définie à l'article 2, point 21), du règlement (UE) 2015/751 du Parlement européen et du Conseil[10]. Toutefois, d'autres catégories de portefeuilles numériques, à savoir les portefeuilles électroniques préfinancés tels que les portefeuilles fonctionnant par étapes ("staged-wallets"), qui se caractérisent par une étape de financement et une étape de paiement, devraient être considérées comme des instruments de paiement et leur émission comme un service de paiement. Cela inclut à la fois les portefeuilles dans lesquels les utilisateurs stockent des fonds à l'avance pour de futures opérations et les portefeuilles dans lesquels la phase de financement et la phase de paiement interviennent simultanément au moment de l'opération, y compris lorsque le portefeuille est automatiquement financé, en tout ou en partie, à partir d'un instrument ou d'un compte de paiement lié.

---

[10] 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, ELI: http://data.europa.eu/eli/reg/2015/751/oj).

(25) Les évolutions technologiques intervenues 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 peuvent ainsi avoir un aperçu complet et structuré de leurs comptes de paiement immédiatement et à tout moment.

(26) Le réexamen auquel la Commission a procédé a mis en évidence le fait qu'il arrive parfois que les prestataires agréés de services d'information sur les comptes agrègent et fournissent des données relatives aux comptes de paiement, non pas au consommateur dont ils ont reçu le consentement pour accéder aux données et les agréger, mais à une autre partie, afin de permettre à cette dernière de fournir d'autres services au consommateur en utilisant les données. Il existe toutefois des divergences de vues quant à la question de savoir si cette activité relève du champ des services réglementés d'information sur les comptes. Cette évolution du modèle économique de la banque ouverte («open banking») 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 des services de paiement, y compris en matière de prêts, de comptabilité et de services 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. Cette évolution du modèle économique de la banque ouverte («open banking») 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 le consentement 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.

(27) La définition des "fonds" devrait couvrir la monnaie de banque centrale émise 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, y compris les jetons de 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.

(28) Le règlement (UE) 2023/1114 du Parlement européen et du Conseil[11] prévoit que les jetons de monnaie électronique, tels qu'ils sont définis dans ledit règlement, sont réputés être de la monnaie électronique, et cela indépendamment de la question de savoir si les jetons de monnaie électronique répondent ou non à la définition de monnaie électronique au sens du présent règlement. En conséquence, les références à la monnaie électronique dans le présent règlement devraient s'entendre comme incluant les jetons de monnaie électronique, sauf si le présent règlement en dispose autrement, et les jetons de monnaie électronique devraient être inclus, en tant que monnaie électronique, dans la définition de "fonds". De même, la fourniture de services de transfert de crypto-actifs pour le compte de clients, au sens du règlement (UE) 2023/1114, liés aux jetons de monnaie électronique, pourrait être considérée comme un service de paiement d'exécution d'opérations de paiement, y compris lorsque ces services de transfert sont fournis dans le cadre d'autres services sur crypto-actifs, à moins que ces transferts ne soient couverts par une exclusion spécifique du champ d'application du présent règlement et de la directive (UE) 2026/…[+].

---

[11] Règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs, et modifiant les règlements (UE) nº 1093/2010 et (UE) nº 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937 (JO L 150 du 9.6.2023, p. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

(29) Compte tenu de l'évolution du marché depuis l'adoption de la directive (UE) 2015/2366, et afin d'éviter d'appliquer des exigences disproportionnées aux prestataires de services sur crypto-actifs qui fournissent des services liés aux jetons de monnaie électronique conformément au règlement (UE) 2023/1114, ainsi que de garantir la clarté juridique en ce qui concerne le champ d'application du présent règlement et de la directive (UE) 2026/...[+] à l'égard des services liés aux jetons de monnaie électronique, il convient d'exclure du champ d'application du présent règlement et de la directive (UE) 2026/...[+] certains types d'opérations de paiement liées aux jetons de monnaie électronique, lorsque des jetons de monnaie électronique sont utilisés dans le cadre d'activités commerciales ou d'investissement. Cela concerne en particulier l'échange par des prestataires de services sur crypto-actifs de jetons de monnaie électronique contre des fonds ou des crypto-actifs, lorsque le prestataire de services sur crypto-actifs agit en son nom propre en tant qu'acheteur ou vendeur de ces jetons de monnaie électronique, ainsi que l'échange de jetons de monnaie électronique contre des jetons de monnaie électronique ou des crypto-actifs effectué par un prestataire de services sur crypto-actifs qui sert d'intermédiaire entre acheteurs et vendeurs. Cette exclusion devrait couvrir en particulier les échanges de jetons de monnaie électronique dans le cadre de la fourniture d'un service d'échange de crypto-actifs contre des fonds, d'échange de crypto-actifs contre d'autres crypto-actifs, d'exploitation d'une plate-forme de négociation de crypto-actifs, de réception et transmission d'ordres sur crypto-actifs pour le compte de clients ou d'exécution d'ordres sur crypto-actifs pour le compte de clients, au sens du règlement (UE) 2023/1114. Toutefois, l'exclusion ne devrait pas inclure les services de transfert fournis par un prestataire de services sur crypto-actifs lorsque des jetons de monnaie électronique sont utilisés pour payer des biens ou des services.

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

(30) Compte tenu de l'exclusion spécifique prévue par la directive (UE) 2015/2366 en ce qui concerne les opérations de paiement effectuées exclusivement en espèces et allant directement du payeur au bénéficiaire, sans aucune intervention d'un intermédiaire, il convient de prévoir une exclusion similaire dans le présent règlement en ce qui concerne les opérations effectuées avec des jetons de monnaie électronique sans intervention d'un intermédiaire. Cette exclusion devrait s'appliquer, entre autres, aux transferts de jetons de monnaie électronique entre deux adresses autohébergées lorsqu'aucun intermédiaire n'intervient, que ce soit du côté du payeur ou du côté du bénéficiaire, et ne devrait pas couvrir les opérations de paiement entre un portefeuille de conservation et une adresse autohébergée.

(31) 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. 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 nationales ou de l'Union 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 spécifique liée à la prévention des infractions et aux enquêtes en la matière.

(32) Les prestataires de services de paiement ont besoin d'avoir accès à des systèmes de paiement et à des schémas de paiement pour pouvoir fournir des services de paiement aux utilisateurs. En général, ces systèmes de paiement comprennent les principaux systèmes permettant de traiter des virements et des prélèvements, tandis que les schémas de paiement comprennent généralement des schémas de cartes faisant intervenir quatre parties. Pour assurer l'égalité de traitement dans l'ensemble de l'Union entre les différentes catégories de prestataires de services de paiement agréés, il convient de clarifier les règles régissant l'accès aux systèmes et schémas de paiement. Cet accès peut être direct ou indirect par l'intermédiaire d'un autre participant à ce système ou schéma de paiement. L'accès devrait être soumis à des exigences qui garantissent l'intégrité et la stabilité de ces systèmes et schémas de paiement. À cette fin, l'opérateur de système de paiement ou l'opérateur de schéma de paiement, selon le cas, 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 ou schéma de paiement devrait supporter le risque lié à son propre choix de système ou de schéma et apporter la preuve au système ou schéma de paiement que son organisation interne est suffisamment solide pour gérer ces types de risques. Les opérateurs de systèmes de paiement et les opérateurs de schémas 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 du schéma ou présente un niveau de risque inacceptable.

(33) Les prestataires de services de paiement et les prestataires de services techniques qui fournissent des services aux prestataires de services de paiement devraient être en mesure d'assurer l'interopérabilité avec les fonctionnalités matérielles et logicielles fournies ou contrôlées par les fabricants d'équipements d'origine d'appareils mobiles ou les prestataires de services de communications électroniques, qui sont nécessaires pour traiter et exécuter les opérations de paiement en ligne ou hors ligne de manière concurrentielle, et d'avoir accès à des fins d'opérabilité à ces fonctionnalités. Ces caractéristiques techniques comprennent le matériel et les logiciels nécessaires pour gérer le flux d'opérations entre le mode de paiement et le dispositif d'acceptation, tels que la NFC sur les appareils mobiles et le noyau de paiement, ou pour faire en sorte que les applications de paiement mobile fonctionnent dans un environnement sécurisé qui protège les clés et algorithmes cryptographiques, le code PIN client ou les données biométriques, telles que les éléments dits sécurisés des appareils mobiles, y compris la carte à circuit intégré universelle (UICC), l'élément sécurisé intégré (eSE) et la microSD. Les fabricants d'équipements d'origine d'appareils mobiles et les prestataires de services de communications électroniques devraient être tenus de permettre l'interopérabilité avec toutes les fonctionnalités matérielles et logicielles nécessaires au traitement et à l'exécution d'opérations en ligne et hors ligne, et d'y donner accès, à des conditions équitables, raisonnables et non discriminatoires. Cette obligation devrait être sans préjudice de l'article 6, paragraphe 7, du règlement (UE) 2022/1925 du Parlement européen et du Conseil[12], qui oblige les contrôleurs d'accès à fournir, gratuitement, une interopérabilité effective avec les fonctionnalités du système d'exploitation, du matériel informatique ou des logiciels des appareils mobiles, ainsi qu'un accès à des fins d'opérabilité à ces fonctionnalités, ces dispositions étant applicables aux moyens de paiement numériques existants et nouveaux.

---

[12] Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques) (JO L 265 du 12.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).

(34) Les opérateurs de systèmes de paiement et les opérateurs de schémas 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 et les opérateurs de schémas de paiement ne devraient pas opérer de discrimination à l'égard des établissements de paiement en ce qui concerne leur participation, à condition que les règles du système ou du schéma puissent être respectées et qu'il n'y ait pas de risque inacceptable pour le système ou le schéma. Ces systèmes comprennent, entre autres, ceux désignés au titre de la directive 98/26/CE du Parlement européen et du Conseil[13]. 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) 2025/1355 de la Banque centrale européenne[14], la ou les banques centrales qui exercent cette surveillance devraient contrôler le respect de ces règles dans le cadre de leur surveillance. Pour les autres systèmes ou schémas de paiement, les États membres devraient désigner des autorités compétentes nationales chargées de veiller à ce que les opérateurs de systèmes de paiement et les opérateurs de schémas de paiement se conforment à ces exigences, si lesdites exigences ne sont pas appliquées sous la surveillance du fonctionnement de ces autres systèmes ou schémas de paiement par l'Eurosystème ou les banques centrales des États membres dont la monnaie n'est pas l'euro.

---

13 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, ELI: http://data.europa.eu/eli/dir/1998/26/oj).

14 Règlement (UE) 2025/1355 de la Banque centrale européenne du 2 juillet 2025 concernant les exigences de surveillance applicables aux systèmes de paiement d'importance systémique (BCE/2025/22) (JO L, 2025/1355, 14.7.2025, ELI: http://data.europa.eu/eli/reg/2025/1355/oj).

(35) Les coûts plus élevés pour les prestataires de services de paiement qui fournissent des services d'acquisition d'opérations de paiement liées à une carte et pour les commerçants résultent du manque de transparence des prix appliqués par les opérateurs de schémas de cartes de paiement et les entités de traitement. Cela pourrait, par exemple, s'expliquer par le fait que les prestataires de services d'acquisition d'opérations de paiement et les commerçants n'ont pas connaissance des mesures à prendre pour éviter les frais comportementaux, ne savent pas quel service est optionnel ou comment renoncer à un service optionnel. Cela porte finalement préjudice aux consommateurs en raison de la répercussion par les commerçants de l'augmentation de leurs coûts d'acceptation des cartes, entraînant une hausse des prix de détail. Étant donné que les consommateurs sont alors susceptibles de réduire leur consommation, cela a des répercussions négatives sur le chiffre d'affaires des commerçants, à moins que ceux-ci n'absorbent ces coûts, ce qui a pour effet de diminuer leurs marges bénéficiaires. Les frais de schéma et les frais de traitement devraient donc être transparents, mais aussi comparables, afin de permettre aux prestataires de services d'acquisition d'opérations de paiement de maximiser l'efficacité des services de schéma et de traitement qu'ils se procurent et fournissent, en créant les conditions permettant de réaliser des gains d'efficacité jusqu'aux commerçants, grâce à des commissions de service moins élevées pour l'acceptation des paiements liés à une carte, et jusqu'aux consommateurs, grâce à des prix de détail plus bas. Dans le même temps, les prestataires de services d'acquisition d'opérations de paiement et les commerçants ne peuvent faire des choix véritablement éclairés en matière de services de schéma et de traitement que s'ils sont rapidement informés de tous nouveaux frais de schéma et de traitement ou de toute modification de ces frais. Le règlement (UE) 2015/751 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte établit des exigences de transparence auxquelles les prestataires de services d'acquisition d'opérations de paiement sont soumis à l'égard des bénéficiaires avec lesquels ils concluent un contrat.

Les prestataires de services d'acquisition d'opérations de paiement devraient veiller à ce que les informations qu'ils fournissent aux commerçants lorsqu'ils s'acquittent des obligations qui leur incombent au titre du règlement (UE) 2015/751 présentent le même niveau de transparence que les informations qui leur ont été communiquées en ce qui concerne les services de schéma et de traitement et les frais correspondants. En raison de la nature complexe des systèmes de facturation des schémas de cartes de paiement et des entités de traitement, et pour que les exigences de transparence soient efficaces et proportionnées, 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 afin de préciser davantage les informations à communiquer aux prestataires de services de paiement qui fournissent des services d'acquisition d'opérations de paiement en ce qui concerne les services de schéma et de traitement et les frais correspondants.

(36) Pour assurer 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.

(37) Les dispositions relatives à l'accès aux systèmes et schémas de paiement ne devraient pas s'appliquer aux systèmes et schémas dont un seul prestataire de services de paiement assure la mise en œuvre et le fonctionnement. Ces systèmes et schémas de paiement peuvent fonctionner soit en concurrence directe avec d'autres systèmes ou schémas de paiement, soit, de manière plus courante, dans une niche du marché qui n'est pas couverte par d'autres systèmes ou schémas de paiement. Ces schémas incluent 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, y compris en faisant appel à des titulaires d'agrément, 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, 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 et schémas de paiement fermés peuvent apporter par rapport aux systèmes et schémas de paiement ordinaires en place, il convient de ne pas exiger d'accorder à des tiers l'accès à ces systèmes et schémas de paiement fermés exclusifs. Néanmoins, ces systèmes et schémas fermés devraient continuer d'être soumis aux éventuelles règles nationales et de l'Union en matière de concurrence exigeant d'accorder l'accès à ces systèmes ou schémas pour maintenir une concurrence effective sur les marchés de paiement.

(38) 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 exigences en matière d'agrément en ce qui concerne la protection des fonds des utilisateurs de services de paiement. Les établissements de paiement devraient également s'efforcer de ne pas protéger tous les fonds des utilisateurs de services de paiement auprès d'un seul établissement de crédit afin d'éviter, le cas échéant, un risque de concentration. Toutefois, comme l'a notamment montré l'ABE dans son avis du 5 janvier 2022, 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.

(39) Les établissements de crédit devraient donc fournir, sur une base objective, non discriminatoire et proportionnée, l'accès à un compte de paiement aux établissements de paiement et aux établissements de paiement demandeurs, ainsi qu'à leurs agents. Il est nécessaire d'inclure dans cette disposition les établissements de paiement demandeurs, étant donné qu'un compte auprès d'un établissement de crédit sur lequel les fonds des clients peuvent être protégés est une condition préalable à l'obtention d'un agrément en tant qu'établissement de paiement. Les établissements de crédit ne devraient pouvoir refuser l'accès à un compte de paiement que dans des cas exceptionnels, lorsqu'il existe des motifs sérieux de le faire. Les établissements de crédit devraient pouvoir refuser d'ouvrir un compte de paiement, ou clôturer un compte de paiement, pour un établissement de paiement, ses agents ou un établissement de paiement demandeur lorsque l'ouverture ou la gestion d'un tel compte entraînerait une violation du règlement (UE) 2024/1624 du Parlement européen et du Conseil[15]. Les établissements de crédit devraient également pouvoir refuser cet accès dans les cas où le demandeur n'a pas fourni d'informations ou de documents pertinents pour ouvrir un compte, car cela pourrait entraver, entre autres, leur capacité à s'acquitter de leurs obligations de vigilance à l'égard de la clientèle. Un établissement de paiement, ses agents ou un établissement de paiement demandeur 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.

---

15 Règlement (UE) 2024/1624 du Parlement européen et du Conseil du 31 mai 2024 relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme (JO L, 2024/1624, 19.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1624/oj).

Afin de faciliter l'exercice de ce droit de recours, les établissements de crédit devraient communiquer par écrit et de manière détaillée les motifs de tout refus de fournir un compte ou de toute clôture ultérieure d'un compte. Ces motifs devraient faire mention d'éléments particuliers relatifs à l'établissement de paiement concerné, et non de considérations générales ou génériques. Lorsque le compte de paiement fait l'objet d'un refus au motif que l'ouverture ou la gestion d'un tel compte entraînerait une violation du règlement (UE) 2024/1624, la justification fournie au client ou au demandeur ne devrait pas entraîner la divulgation d'informations protégées en vertu de l'article 73 dudit règlement. 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 les motifs de l'une ou de l'autre décision, l'ABE devrait élaborer des projets de normes techniques de réglementation harmonisant la présentation de ces motifs.

(40) Pour pouvoir faire des choix éclairés et choisir facilement leur prestataire de services de paiement au sein de l'Union, les utilisateurs de services de paiement devraient recevoir des informations comparables sur les services de paiement d'une manière claire, neutre et compréhensible. Afin que les utilisateurs de services de paiement reçoivent de telles informations 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.

(41) Lorsqu'ils fournissent les informations requises aux utilisateurs de services de paiement, les prestataires de services de paiement devraient tenir compte des besoins desdits utilisateurs ainsi que des aspects pratiques et du rapport coût-efficacité en fonction du contrat de services de paiement spécifique. 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 doivent prendre des mesures concrètes pour obtenir les informations, y compris en les réclamant expressément auprès des prestataires de services de paiement, en consultant leur compte bancaire en ligne ou en introduisant leur carte bancaire dans un appareil imprimant les relevés 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.

(42) Étant donné que les consommateurs et les entreprises ne se trouvent pas dans la même situation de vulnérabilité, ils 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 raisonnable de laisser les entreprises et les organisations en convenir autrement lorsqu'elles n'ont pas affaire à des consommateurs. Sous réserve des normes techniques de réglementation adoptées par la Commission, les accords ainsi conclus avec des entreprises et des organisations qui ne sont pas des consommateurs pourraient déterminer si l'authentification forte du client s'applique ou non. Les microentreprises, au sens de la recommandation 2003/361/CE de la Commission[16], pourraient être traitées de la même manière que les consommateurs. Certaines règles devraient toujours s'appliquer, indépendamment du statut de l'utilisateur.

---

16 Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

(43) Les prestataires de services de paiement, y compris les fournisseurs de distributeurs automatiques de billets, devraient afficher à l'intention de leurs clients, de manière claire, neutre et compréhensible, des informations sur les frais éventuels, aussi bien avant que le client n'initie le retrait qu'au moment de procéder au retrait, par exemple en affichant de manière numérique sur le terminal les frais prélevés. Une fois l'opération terminée, les informations sur les frais devraient être documentées, à la simple demande du client, sur support papier ou sur un autre support durable.

(44) 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 ou sur un autre support durable, sans frais et à tout moment au cours de la relation contractuelle.

(45) 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 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.

(46) Les instruments de paiement pour des opérations de faible valeur devraient constituer un moyen simple et bon marché pour l'acquisition de biens et de 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, qui tiennent compte des capacités techniques que l'on est en droit d'attendre d'instruments spécialisés dans les paiements de faible valeur. Malgré cette charge réglementaire allégée, 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.

(47) 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 passent un ordre de paiement, il ne devrait pas toujours être nécessaire de fournir les informations 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 convient également d'indiquer, y compris sur le site internet, où il est possible de trouver d'autres informations plus détaillées. 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.

(48) 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.

(49) 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 avec ceux pratiqués par d'autres prestataires. Afin d'accroître la transparence des frais de distributeurs automatiques de billets facturés aux utilisateurs de services de paiement, les prestataires de services de paiement devraient fournir à ces utilisateurs des informations, sur support papier ou sur un autre support durable, sur tous les frais applicables aux retraits effectués aux distributeurs automatiques de billets nationaux dans différentes situations, en fonction du distributeur automatique de billets auquel les utilisateurs de services de paiement retirent des espèces. Pour les retraits aux distributeurs automatiques de billets libellés en euros, tous les frais payables par les utilisateurs de services de paiement à leur prestataire de services de paiement, y compris lorsque les retraits sont effectués à des distributeurs automatiques de billets gérés par des fournisseurs de distributeurs automatiques de billets indépendants, devraient être soumis au principe de l'égalité des frais, tel qu'il est énoncé à l'article 3 du règlement (UE) 2021/1230 du Parlement européen et du Conseil[17]. Il convient, dès lors, de modifier ledit règlement en conséquence.

(50) 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 convenir, dans le contrat-cadre, des modalités de la transmission des informations fournies par la suite sur les opérations de paiement effectuées.

---

17 Règlement (UE) 2021/1230 du Parlement européen et du Conseil du 14 juillet 2021 concernant les paiements transfrontaliers dans l'Union (JO L 274 du 30.7.2021, p. 20, ELI: http://data.europa.eu/eli/reg/2021/1230/oj).

(51) 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 justifiées, 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.

(52) 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 trois 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 trois 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'autres dispositions pertinentes du droit de l'Union ou de droit national, par exemple en matière de 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.

(53) 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 sous la forme d'un montant monétaire dans la monnaie du compte du payeur et d'une marge de pourcentage sur un taux de change moyen du marché agrégé qui reflète fidèlement le marché. Afin de garantir que le taux de change utilisé est fiable et reflète fidèlement le marché, il devrait être fourni par un administrateur de confiance qui satisfait aux exigences applicables en matière de gouvernance et de contrôle, telles que les principes sur les indices de référence financiers publiés par l'Organisation internationale des commissions de valeurs (OICV). Un prestataire de services de paiement devrait utiliser le même indice de référence de manière cohérente et pour les échanges effectués dans les deux sens. 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.

(54) Le prestataire de services de paiement du payeur devrait fournir une estimation du temps nécessaire 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. Le prestataire de services de paiement du payeur devrait informer le payeur qu'il ne s'agit pas d'un délai exact, étant donné que le moment de réception est susceptible de dépendre de différents facteurs, parfois hors du contrôle du prestataire de services de paiement du payeur.

(55) Étant donné qu'un prestataire de services de paiement ne peut fournir le nom du bénéficiaire au payeur, ou le mettre à sa disposition, que s'il dispose de ces informations, cette exigence ne peut s'appliquer dans les cas où il n'est pas possible de le faire. C'est généralement le cas pour les transmissions de fonds effectuées en tant qu'opération de paiement isolée, lorsque le prestataire de services de paiement du payeur n'a pas accès au nom du bénéficiaire sauf s'il est fourni par le payeur. Il convient donc que, dans de tels cas, le prestataire de services de paiement du payeur ne soit pas tenu de fournir le nom du bénéficiaire au payeur ou de le mettre à sa disposition.

(56) 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 convient 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 pourrait 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 prélève aucuns frais auprès du payeur ou du bénéficiaire. De même, sans préjudice des règles de concurrence de l'Union et du règlement (UE) 2015/751, et en fonction des clauses du contrat, le prestataire de services de paiement du bénéficiaire pourrait ne facturer l'utilisation du service de paiement qu'au bénéficiaire lorsque ces frais comprennent une compensation en faveur du prestataire de services de paiement du payeur et que le prestataire de services de paiement du payeur n'impute pas de frais 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 ou la compensation entre les prestataires de services de paiement ou les autres intermédiaires.

(57) 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[18], 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.

[18] 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, ELI: http://data.europa.eu/eli/reg/2012/260/oj).

(58) Les éléments recueillis lors 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 du 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.

(59) Les services de banque ouverte («open banking») sont des services de paiement qui supposent l'accès aux données relatives aux comptes de paiement 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 prestataires de services d'information sur les comptes fournissent un service visant à permettre, 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. Le prestataire de services d'information sur les comptes pourrait également transmettre les données relatives aux comptes de paiement obtenues à un tiers qui, à son tour, fournirait un service à l'utilisateur de services de paiement en tirant parti de ces données, éventuellement avec des services à valeur ajoutée supplémentaires. Les services d'initiation de paiement permettent d'initier un paiement à partir du compte de l'utilisateur, tel qu'un virement, d'une manière pratique pour l'utilisateur et le bénéficiaire, sans recourir à un instrument tel qu'une carte de paiement. Un service d'initiation de paiement nécessite d'obtenir le consentement du payeur pour accéder au compte de paiement. Conformément au constat qui est fait dans le règlement (UE) 2024/1624, certains services d'initiation de paiement établissent une relation d'affaires avec le bénéficiaire. Par conséquent, la définition du service d'initiation de paiement reflète le fait que les prestataires de ces services peuvent proposer des services d'initiation de paiement au payeur et au bénéficiaire. La fourniture d'un portefeuille numérique "pass-through" permettant à l'utilisateur d'initier un paiement à partir de son compte de paiement, à condition qu'aucun fonds ne soit stocké dans le portefeuille numérique, que le fournisseur de portefeuille numérique n'entre jamais en possession de tels fonds et que le fournisseur de portefeuille fonctionne selon des accords contractuels avec les prestataires de services de paiement qui gèrent le compte du payeur, ne devrait pas être considérée comme un service d'initiation de paiement.

(60) Les prestataires de services de paiement gestionnaires de comptes devraient permettre aux prestataires de services d'information sur les comptes et aux prestataires de services d'initiation de 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 donné son consentement 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 la date d'application de la directive (UE) 2015/2366, l'accès aux données dans le cadre de la banque ouverte («open banking») s'effectue sur une telle base non contractuelle, et gratuitement. Si les services réglementés d'accès aux données devaient être soumis à des frais, alors qu'il n'y en avait pas précédemment, l'incidence sur la poursuite de la prestation de ces services et, 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 du règlement (UE) 2023/2854 du Parlement européen et du Conseil[19], en particulier à l'article 9, paragraphe 3, dudit règlement, que le présent règlement ne remet pas en cause.

[19] Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données) (JO L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

(61) Les prestataires de services de paiement gestionnaires de comptes et les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement peuvent établir une relation contractuelle, y compris dans le cadre d'un accord contractuel multilatéral tel qu'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 («open banking») 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 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 du règlement (UE) 2023/2854, notamment en ce qui concerne l'article 9, paragraphes 1 et 2, dudit règlement, sur la compensation. Il devrait toujours être possible, pour les prestataires de services d'information sur les comptes et les prestataires 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 tel qu'un schéma existe et où les mêmes données sont également disponibles dans le cadre dudit accord.

(62) 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 être accordé aux prestataires de services d'information sur les comptes et aux prestataires de services d'initiation de paiement par l'intermédiaire d'une interface conçue et dédiée à des fins de banque ouverte («open banking»), telle qu'une interface de programmation d'applications. 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 les prestataires 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 dédiée devrait permettre aux prestataires de services d'information sur les comptes et aux prestataires 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 les prestataires de services d'initiation de paiement devraient pouvoir choisir la méthode d'authentification qu'ils proposent à l'utilisateur de services de paiement, afin de proposer l'option la moins contraignante. Les prestataires de services d'information sur les comptes et de services d'initiation de paiement devraient utiliser l'interface dédiée pour accéder aux données. En cas de défaillance ou d'indisponibilité imprévue de l'interface dédiée, la continuité des activités de ces prestataires de services serait compromise par l'impossibilité d'accéder aux données pour lesquelles ils ont obtenu un consentement. Il est essentiel que les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement soient en mesure d'accéder à tout moment aux données qui sont indispensables à la fourniture de services aux clients. Par conséquent, une indisponibilité prévue de l'interface dédiée, afin de permettre aux prestataires de services de paiement gestionnaires de comptes de mettre à jour l'interface dédiée ou d'y apporter des modifications, devrait normalement avoir lieu entre minuit et six heures. Si la maintenance des systèmes prévoit généralement la mise à niveau du système pendant la nuit, entre minuit et six heures à l'heure locale du prestataire de services de paiement gestionnaire de comptes, une procédure de maintenance approfondie peut prendre plus que quelques heures. En règle générale, le prestataire de services de paiement gestionnaire de comptes devrait également, sauf en cas de modification d'urgence, dûment informer les prestataires de services de paiement utilisant l'interface dédiée, au moins un mois à l'avance, de toute indisponibilité prévue et de sa durée.

(63) Afin de faciliter l'utilisation de l'interface dédiée, ses spécifications techniques devraient être documentées, en précisant les procédures, protocoles et outils requis, 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 («open banking») 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 aux prestataires 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 les prestataires 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), ou d'autres normes largement reconnues offrant un niveau de sécurité équivalent, qui permettraient aux prestataires de services de paiement gestionnaires de comptes de bénéficier d'un large éventail de solutions technologiques sans compromettre la sécurité ni s'appuyer sur des normes de niche qui seraient difficiles à mettre en œuvre pour les prestataires tiers.

(64) Afin que les prestataires de services d'information sur les comptes et les prestataires 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 dédiée qu'ils sont tenus d'utiliser devrait permettre une expérience utilisateur simple et fluide en satisfaisant 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 dédiée devrait permettre non seulement l'initiation d'opérations de paiement isolées, mais aussi d'ordres permanents. Des exigences plus détaillées relatives aux interfaces dédiées devraient être définies dans les normes techniques de réglementation élaborées par l'ABE.

(65) Aux fins d'une vérification efficace avant l'initiation d'un paiement, les prestataires de services de paiement gestionnaires de comptes devraient veiller à ce que les prestataires de services d'initiation de paiement puissent vérifier le nom complet du titulaire du compte par l'intermédiaire de l'interface dédiée et ne devraient donc pas fournir de noms partiels ou abrégés.

(66) Compte tenu de l'incidence considérable que l'indisponibilité imprévue prolongée d'une interface dédiée aurait sur la continuité des activités des prestataires de services d'information sur les comptes et des prestataires de services d'initiation de paiement, les prestataires de services de paiement gestionnaires de comptes devraient tout mettre en œuvre pour prévenir toute indisponibilité imprévue ou toute sous-performance de cette interface. Une sous-performance devrait être comprise comme une performance inférieure à celle de l'interface utilisée par le prestataire de services de paiement gestionnaire de comptes pour l'authentification et la communication avec ses utilisateurs de services de paiement. Les prestataires de services de paiement gestionnaires de comptes devraient remédier à une telle indisponibilité ou sous-performance sans retard injustifié et garantir un délai de rétablissement optimal pour l'interface dédiée. 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 les prestataires de services d'initiation de paiement de toute indisponibilité de leur interface dédiée et des mesures prises pour y remédier. Compte tenu de l'importance capitale que revêtent la disponibilité et la fonctionnalité complètes de l'interface dédiée pour les modèles économiques des prestataires de services d'information sur les comptes et des prestataires de services d'initiation de paiement, l'interface dédiée devrait garantir une disponibilité et des performances au moins égales à celles de l'interface que le prestataire de services de paiement gestionnaire de comptes utilise pour l'authentification et la communication avec ses utilisateurs. L'ABE devrait être chargée de préciser, dans des projets de normes techniques de réglementation, les exigences relatives aux statistiques trimestrielles sur la disponibilité et les performances des interfaces dédiées et, à des fins de comparaison, des interfaces que le prestataire de services de paiement gestionnaire de comptes met à la disposition de ses utilisateurs de services de paiement pour accéder directement à leur compte de paiement en ligne, et à la publication de ces statistiques sur le site internet du prestataire de services de paiement gestionnaire de comptes, ainsi que les normes établissant un délai de rétablissement optimal en cas d'indisponibilité imprévue d'une interface dédiée, en fonction de la gravité de l'incident. Cette gravité devrait tenir compte, entre autres, du nombre de clients touchés et des types de fonctionnalités des prestataires de services d'information sur les comptes et des prestataires de services d'initiation de paiement concernés par l'incident.

(67) Les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement devraient toujours dûment s'identifier et respecter leurs obligations, telles que les limites du consentement qui leur a été accordé, et ne devraient notamment accéder qu'aux données dont ils ont besoin pour satisfaire à leurs obligations contractuelles et fournir le service réglementé. Il convient de ne jamais pratiquer la "capture de données d'écran" ("screen scraping"), c'est-à-dire d'accéder aux données relatives aux comptes de paiement, sans identification conforme, ce quelles que soient les circonstances.

(68) Étant donné que la mise en place ou la maintenance d'une interface dédiée 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 dédiée d'accès aux données, et d'autoriser le prestataire de services de paiement gestionnaire de comptes soit à ne proposer un accès aux données de paiement que par l'intermédiaire de son "interface client", à condition que cette interface soit déjà un point de terminaison d'interface de programmation d'application, c'est-à-dire un point de connexion numérique spécifique et sécurisé permettant une communication automatisée de machine à machine et l'échange de données, soit à ne proposer aucune interface d'accès aux données de banque ouverte («open banking»). Le cas échéant, compte tenu des spécificités de l'État membre, les banques centrales nationales qui n'agissent pas en leur qualité d'autorité monétaire ou d'autres autorités publiques peuvent se voir accorder par l'État membre une exemption à l'obligation de disposer d'une interface dédiée. L'accès aux données par l'intermédiaire de l'interface client, lorsqu'il n'existe pas d'interface dédiée, peut être approprié lorsque cette interface est déjà une interface de programmation d'application, par exemple dans les cas de relations entre entreprises où aucune application mobile ni interface internet n'est utilisée entre le prestataire de services de paiement gestionnaire du compte et son client, ou lorsqu'une interface dédiée représenterait une charge financière et une charge en ressources importantes pour le prestataire de services de paiement gestionnaire du compte, comme c'est le cas pour les prestataires de services de paiement de très petite taille. Le fait d'être exempté de l'obligation de maintenir une interface d'accès aux données nécessaires à la banque ouverte («open banking») 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 («open banking») n'auraient aucun intérêt pour ses clients. Des critères détaillés concernant l'octroi de ces décisions d'exemption devraient être définis dans les normes techniques de réglementation élaborées par l'ABE, en tenant compte, entre autres, de la taille, du chiffre d'affaires annuel et du volume des paiements du prestataire de services de paiement gestionnaire du compte. Une fois accordées, ces exemptions ne devraient pas être maintenues si les circonstances qui ont conduit à leur octroi changent de manière significative.

(69) Pour exploiter pleinement le potentiel de la banque ouverte («open banking») dans l'Union, il est essentiel d'empêcher tout traitement discriminatoire des prestataires de services d'information sur les comptes et des prestataires de services d'initiation de paiement par les prestataires de services de paiement gestionnaires de comptes. Lorsqu'un 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 l'interface client de ce prestataire, 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.

(70) 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, et ce de manière continue, à la demande du prestataire de services d'initiation 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 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 avoir accès aux 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 d'une qualité comparable à celle d'autres moyens de paiement électronique mis à la disposition du bénéficiaire, dont les cartes de paiement.

(71) Pour renforcer la confiance dans la banque ouverte («open banking»), il est essentiel que les utilisateurs de services de paiement qui utilisent les services d'information sur les comptes et les services d'initiation de paiement aient la pleine maîtrise de leurs données et accès à des informations claires sur les consentements à l'accès aux données qu'ils ont accordées aux prestataires de services de paiement, notamment la finalité du consentement et les catégories de données relatives aux comptes de paiement qui sont concernées, telles que les données d'identité du compte, de l'opération, ainsi que 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 («open banking»). Les tableaux de bord ne devraient pas comporter de formulations dissuasives ou décourageantes susceptibles d'inciter un utilisateur de services de paiement à ne pas recourir aux services d'un prestataire de services d'initiation de paiement ou d'un prestataire de services d'information sur les comptes. Le consentement à l'initiation de paiements isolés ne devrait pas figurer sur ce tableau de bord. Un tableau de bord ne devrait pas permettre à un utilisateur de services de paiement d'établir de nouveaux consentements à l'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 rapidement mettre des informations à la disposition des prestataires de services d'information sur les comptes et des prestataires 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 rapidement informer les prestataires de services de paiement gestionnaires de comptes des consentements à l'accès aux données, nouvelles ou rétablies, accordées par les utilisateurs de services de paiement, y compris de la durée de validité du consentement 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 consentements qu'il a accordés à des prestataires de services d'information sur les comptes et des prestataires 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 («open banking»), étant donné que le tableau de bord ne gère pas la relation contractuelle entre l'utilisateur et un prestataire de services de banque ouverte («open banking») mais qu'il appartient à l'utilisateur de services de paiement de vérifier ce risque. Un tableau de bord des consentements devrait donner aux clients les moyens de gérer, de manière éclairée et impartiale, les consentements 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 consentements 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[20].

(72) Les prestataires de services d'information sur les comptes devraient pouvoir accéder aux informations sur les comptes de paiement désignés et les 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 spontanément ces informations ou pas. Lorsqu'un prestataire de services d'information sur les comptes a l'intention d'accéder à des informations et que l'utilisateur de services de paiement ne demande pas spontanément ces informations, le prestataire de services d'information sur les comptes devrait informer l'utilisateur de services de paiement de son intention. Dans ce cas, l'obligation d'information ne doit pas nécessairement être remplie à chaque accès, mais peut l'être en incluant ces informations dans le contrat-cadre conclu entre le prestataire de services d'information sur les comptes et l'utilisateur de services de paiement.

---

20 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, ELI: http://data.europa.eu/eli/dir/2019/882/oj).

(73) Le réexamen de la directive (UE) 2015/2366 a révélé que les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement se heurtent encore 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[21]. Ces obstacles continuent d'entraver considérablement l'exploitation du plein potentiel de la banque ouverte («open banking») dans l'Union. Ces obstacles sont régulièrement signalés par les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement aux autorités de surveillance et de régulation et à la Commission. Le 4 juin 2020, l'ABE a publié un avis dans lequel elle analyse ces obstacles. Malgré des efforts de clarification, 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 banque ouverte («open banking») réglementés. Il est donc indispensable de fournir une liste claire et non exhaustive de ces entraves interdites à la banque ouverte («open banking»), en s'appuyant notamment sur les travaux menés par l'ABE.

[21] 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, ELI: http://data.europa.eu/eli/reg_del/2018/389/oj).

(74) Les motifs liés à la prévention de la fraude ou au respect du règlement (UE) 2016/679 du Parlement européen et du Conseil[22] ne devraient pas servir de base générale pour refuser, restreindre ou retarder l'accès aux données par des prestataires tiers. Les mesures prises pour ces motifs pourraient, à titre exceptionnel, restreindre l'accès aux services de banque ouverte («open banking»), mais ne devraient être autorisées qu'au cas par cas, lorsqu'elles sont dûment justifiées, sur la base d'éléments objectifs et vérifiables laissant soupçonner une fraude ou d'une obligation spécifique au titre du règlement (UE) 2016/679, et devraient rester strictement nécessaires, proportionnées et limitées dans leur portée et leur durée. Elles ne devraient pas entraîner de restrictions systématiques ou générales à la banque ouverte («open banking»), ni légitimer des obstacles à l'accès aux données qui sont interdits par le présent règlement. Si les prestataires de services de paiement gestionnaire de comptes peuvent légitimement prendre des mesures pour lutter contre la fraude, ces mesures ne devraient pas entraîner de discrimination à l'égard des services fournis par les prestataires de services d'initiation de paiement et les prestataires de services d'information sur les comptes. À ce titre, elles devraient s'appliquer à ces services de la même manière qu'aux services de paiement fournis directement ou indirectement par le prestataire de services de paiement gestionnaire du compte lui-même, y compris les services de paiement par carte ou virement qui sont à la disposition des bénéficiaires dans le commerce. Ce principe devrait s'appliquer à la fois à l'expérience d'authentification du payeur et au degré de certitude qu'un paiement initié sera exécuté par le prestataire de services de paiement gestionnaire du compte.

---

[22] 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(75) 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 ou 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 formulées de manière à empêcher les utilisateurs de services de paiement 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) 2026/…[+]. 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 l'identifiant unique ne constituent pas des données de paiement sensibles.

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

(76) Pour atteindre entièrement ses objectifs, la banque ouverte («open banking») 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 («open banking»), les autorités compétentes nationales sont les chargées du contrôle de premier niveau en matière de banque ouverte («open banking»). Il est donc essentiel que les autorités compétentes nationales mettent tout en œuvre pour garantir le respect du cadre réglementé de l'Union en matière de banque ouverte («open banking»). 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 faciliter un dialogue fluide et régulier entre les différents acteurs de l'écosystème de la banque ouverte («open banking»). Il faut en particulier veiller à ce que les prestataires de services de paiement gestionnaires de comptes respectent à tout moment leurs obligations en ce qui concerne l'interface dédiée. Les prestataires de services de paiement gestionnaires de comptes, les prestataires de services d'information sur les comptes et les prestataires 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 («open banking») dans l'Union par les autorités nationales 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 («open banking») devrait combler une lacune dans les données qui existe actuellement et qui empêche de mesurer efficacement l'adoption effective de la banque ouverte («open banking») dans l'Union. Les prestataires de services de paiement gestionnaires de comptes, les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement devraient avoir accès aux organismes de règlement des litiges, conformément à l'article 10 du règlement (UE) 2023/2854.

(77) L'interface dédiée devrait constituer le principal point d'accès aux services d'information sur les comptes et aux services d'initiation de paiement. Toutefois, certains prestataires de services de paiement gestionnaires de comptes pourraient disposer d'interfaces supplémentaires destinées à d'autres contextes d'application, qui sont techniquement en mesure de fournir aux prestataires de services d'information sur les comptes et aux prestataires de services d'initiation de paiement les mêmes services que l'interface dédiée. Les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement devraient pouvoir utiliser ces interfaces supplémentaires avec le consentement du prestataire de services de paiement gestionnaire du compte. Toutefois, cette possibilité ne doit pas être interprétée comme une obligation pour le prestataire de services de paiement gestionnaire du compte d'accorder l'accès par un autre moyen que l'interface dédiée, et elle ne confère pas non plus aux prestataires de services d'information sur les comptes, aux prestataires de services d'initiation de paiement ou à d'autres entités non réglementées le droit d'exiger un tel accès. Les interfaces supplémentaires ne peuvent être utilisées que si les participants le souhaitent de leur propre initiative, avec l'accord des prestataires de services de paiement gestionnaires des comptes, et dans le respect des mêmes conditions de sécurité en matière d'identification et de communication sécurisée que celles qui s'appliquent à l'interface dédiée, et à condition que ces interfaces supplémentaires utilisent des normes largement acceptées et interopérables.

(78) La notion de consentement au sens du présent règlement s'applique sans préjudice des règles relatives au traitement licite des données à caractère personnel, y compris les dispositions relatives au consentement et au consentement explicite, prévues par le règlement (UE) 2016/679. Lorsqu'il s'agit d'un traitement de données à caractère personnel, il incombe au responsable du traitement d'évaluer la base juridique appropriée au titre du règlement (UE) 2016/679 et de veiller à ce que toutes les conditions relatives à cette base juridique, telles qu'énoncées dans ledit règlement, soient remplies.

(79) Une opération de paiement ou une série d'opérations de paiement ne devrait être considérée comme autorisée que si le payeur a donné son consentement à l'exécution de l'opération de paiement selon les modalités convenues entre ledit payeur et le prestataire de services de paiement gestionnaire du compte. Elle ne devrait pas être considérée comme autorisée lorsque l'opération a été initiée ou modifiée par un tiers agissant sans le consentement de l'utilisateur de services de paiement. Les cas d'opérations de paiement initiées ou modifiées par un tiers agissant sans le consentement de l'utilisateur de services de paiement comprennent les situations dans lesquelles ce tiers utilise des données de sécurité personnalisées de l'utilisateur de services de paiement obtenues de manière frauduleuse.

(80) Pour maintenir 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 serait possible 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 qui vérifie si l'identifiant unique du bénéficiaire et le nom de celui-ci, tels qu'ils ont été fournis par le payeur, concordent, et dans le cas où une divergence est détectée, le notifie à ce payeur. Lorsque le bénéficiaire est une personne morale, ce service pourrait être assuré en vérifiant la concordance entre l'identifiant unique du bénéficiaire et un autre élément de données, tel qu'un numéro fiscal, un identifiant unique européen tel qu'il est visé à l'article 16, paragraphe 1, deuxième alinéa, de la directive (UE) 2017/1132 du Parlement européen et du Conseil[23], ou un identifiant d'entité juridique (IEJ), qui identifie sans ambiguïté le bénéficiaire, si le payeur est autorisé à transmettre cet élément de données via un canal d'initiation de paiement de son prestataire de services de paiement et si cet élément de données est disponible dans les systèmes internes du prestataire de services de paiement du bénéficiaire. Lorsque le compte de paiement du bénéficiaire n'est pas identifié par un identifiant international de compte bancaire (IBAN), un autre type d'identifiant unique devrait être utilisé pour identifier sans ambiguïté le compte de paiement du bénéficiaire. Ces services, dans les pays où ils existent, ont eu une incidence positive considérable sur la réduction du 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 utilisateurs de services de paiement.

---

[23] Directive (UE) 2017/1132 du Parlement européen et du Conseil du 14 juin 2017 relative à certains aspects du droit des sociétés (JO L 169 du 30.6.2017, p. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

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. Afin de permettre au payeur de décider s'il procède ou non à l'opération envisagée, le prestataire de services de paiement du payeur devrait donner notification au payeur avant que ce dernier n'autorise l'opération. Certaines solutions d'initiation de virement pourraient être mises à la disposition des payeurs pour leur permettre de passer un ordre de paiement sans qu'ils aient à saisir eux-mêmes à la fois l'identifiant unique et le nom du bénéficiaire. En pareil cas, le prestataire de services de paiement devrait s'assurer que le bénéficiaire auquel le payeur a l'intention d'envoyer un virement est correctement identifié.

(81) Le règlement (UE) nº 260/2012 prévoit qu'un service de vérification de la concordance entre l'identifiant unique et le nom du bénéficiaire ou un autre élément de données doit être proposé aux utilisateurs de virements en euros, y compris les virements instantanés en euros. Afin d'obtenir un cadre cohérent pour l'ensemble des virements tout en évitant tout 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) nº 260/2012 et devrait être alignée sur le service de vérification prévu par le règlement (UE) nº 260/2012.

(82) Certaines caractéristiques du nom du bénéficiaire sur le compte duquel le payeur souhaite faire un virement pourraient accroître la probabilité que le prestataire de services de paiement détecte une divergence. Ces divergences comprennent 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 toute friction inutile dans les situations où le nom du bénéficiaire fourni par le payeur et le nom associé à l'IBAN ou, lorsque l'IBAN n'est pas utilisé pour identifier le compte de paiement, à un autre type d'identifiant unique fourni par le payeur, ne correspondent pas exactement mais sont néanmoins presque identiques, et afin de faciliter la décision du payeur de procéder ou non à l'opération envisagée, les prestataires de services de paiement devraient indiquer au payeur le nom du bénéficiaire associé à l'IBAN ou à tout autre type d'identifiant unique fourni par le payeur, d'une manière qui garantisse la conformité au règlement (UE) 2016/679.

(83) Le fait d'autoriser une opération de paiement alors que le service de vérification de la concordance a détecté une divergence et l'a 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 décision s'ils choisissent de ne pas tenir compte de la divergence notifiée et de procéder à l'exécution de l'opération. Les utilisateurs de services de paiement qui ne sont pas des consommateurs devraient avoir la possibilité de renoncer à bénéficier du service garantissant la vérification du bénéficiaire lorsqu'ils transmettent des ordres de paiement via des canaux d'initiation de paiement reposant sur des processus ou protocoles automatisés dédiés et qui sont uniquement mis à la disposition des utilisateurs de services de paiement qui ne sont pas des consommateurs. Après avoir renoncé à ce service, ces utilisateurs de services de paiement devraient avoir la possibilité d'y avoir de nouveau recours. En outre, afin de permettre une intégration plus harmonieuse du service assurant la vérification dans les processus de gestion des paiements de ces utilisateurs de services de paiement, les prestataires de services de paiement devraient leur offrir la possibilité de convenir, dans le contrat-cadre, que le service assurant la vérification des ordres de paiement passés via ces canaux d'initiation de paiement soit fourni après l'autorisation de ces ordres et que, en cas d'aboutissement à certains résultats spécifiques par le service assurant la vérification, le prestataire de services de paiement du payeur exécute ces ordres sans autre intervention de la part de l'utilisateur de services de paiement. Il convient, dès lors, de modifier le règlement (UE) n° 260/2012 en conséquence.

(84) Afin de permettre à l'utilisateur de services de paiement de se protéger, le prestataire de services de paiement devrait lui offrir la possibilité de fixer, dans le contrat-cadre, une limite correspondant au montant maximal pouvant être transféré via un moyen de paiement ou un instrument de paiement. En outre, l'utilisateur de services de paiement devrait pouvoir fixer des limites différentes pour chaque moyen de paiement et chaque instrument de paiement, exprimées, à la seule discrétion dudit utilisateur de services de paiement, soit par opération, soit dans un délai déterminé, telle qu'une journée ou une semaine. Lorsque le prestataire de services de paiement propose que l'utilisateur de services de paiement fixe une limite pour les virements, cette limite devrait être la même pour les différents types de virements, afin que l'utilisateur de services de paiement ne soit pas privé, à son insu, d'un accès aux virements instantanés équivalent à celui dont il bénéficie pour les autres types de virements. Les utilisateurs de services de paiement devraient également pouvoir modifier les limites fixées précédemment dans le contrat-cadre.

(85) Afin de garantir l'efficacité des limites de dépenses, il importe que toute augmentation de ces limites demandée par l'utilisateur de services de paiement par l'intermédiaire d'un canal à distance ne prenne effet qu'après un certain délai. En l'absence d'un tel délai, un fraudeur pourrait convaincre une victime de modifier ses limites de dépenses et serait alors en mesure de la dépouiller immédiatement d'un montant bien plus important. Un délai permettrait à l'utilisateur de services de paiement de se rendre compte qu'il a été contacté et manipulé par un fraudeur. Le délai devrait être fixé par défaut à quatre heures par le prestataire de services de paiement. L'utilisateur de services de paiement devrait pouvoir ajuster le délai à la hausse ou à la baisse, ou choisir de ne pas appliquer ce délai, ces actions étant soumises au délai en vigueur. La mise en œuvre d'une authentification forte du client devrait être obligatoire lorsque l'utilisateur du service de paiement demande une augmentation de ses limites de dépenses par l'intermédiaire d'un canal à distance.

(86) La décision du prestataire de services de paiement de bloquer un instrument de paiement devrait reposer sur des raisons objectivement justifiées, fondées sur les données recueillies grâce au mécanisme de surveillance des opérations, et devrait tenir compte des risques de fraude susceptibles de compromettre la sécurité de l'instrument de paiement et les intérêts de l'utilisateur de services de paiement. Parmi les raisons objectivement justifiées, on peut citer le soupçon d'une utilisation non autorisée, le soupçon d'opérations frauduleuses, la sécurité de l'instrument de paiement, le risque de manipulation concernant une activité financière et les opérations effectuées à grande distance les unes des autres dans un délai court non justifiable.

(87) À mesure que les services de paiement se numérisent de plus en plus, de nombreux prestataires de services de paiement proposent aux utilisateurs de recourir à des applications mobiles pour effectuer des opérations de paiement. Si ces applications mobiles sont utiles et avantageuses pour les utilisateurs de services de paiement, elles présentent également un risque de fraude. Pour prévenir ce risque, le processus d'activation d'une application mobile sur un appareil devrait nécessiter l'utilisation de différents canaux de communication, lorsqu'il existe une relation client entre l'utilisateur de service de paiement et le prestataire de services de paiement, ainsi que la mise en œuvre d'une authentification forte du client. Lors de l'établissement de la relation client, le prestataire de services de paiement et l'utilisateur de services de paiement devraient convenir d'un délai avant que l'activation d'une application mobile ne prenne effet, afin de permettre à l'utilisateur de services de paiement d'intervenir s'il n'a pas lui-même activé l'application mobile. Afin de faciliter le processus d'établissement d'une relation client, également appelé entrée en relation, le délai ne devrait pas s'appliquer précisément lorsque l'application mobile est utilisée pour établir la relation client entre l'utilisateur de services de paiement et le prestataire de services de paiement. Le prestataire de services de paiement devrait fixer un délai de quatre heures. Par la suite, l'utilisateur de services de paiement devrait avoir le droit d'ajuster ce délai ou de renoncer à son application, auquel cas la mise en œuvre d'une authentification forte du client devrait être requise. Tout ajustement de la durée du délai demandé par l'utilisateur de services de paiement devrait lui-même être soumis au délai proposé par le prestataire de services de paiement, et pourrait consister en une prolongation ou une réduction du délai de quatre heures.

Le prestataire de services de paiement devrait également notifier à l'utilisateur de services de paiement, de manière sécurisée et par différents canaux de communication, l'activation d'une application mobile liée à son compte de paiement sur un appareil, s'il existe une relation client entre le prestataire de services de paiement et l'utilisateur de services de paiement. Cette notification a pour but de renforcer la vigilance de l'utilisateur de services de paiement et devrait donc permettre à celui-ci d'alerter le prestataire de services de paiement si cet utilisateur n'a pas installé l'application mobile. Dans ce cas, le prestataire de services de paiement devrait veiller à ce que l'application mobile ne permette pas d'accéder au compte de paiement de l'utilisateur de services de paiement ni d'initier des opérations de paiement. Cette obligation de notification ne devrait pas s'appliquer à l'activation d'une application mobile sur un appareil de l'utilisateur de services de paiement, si celle-ci est effectuée par le prestataire de services de paiement dans ses locaux physiques, ni à l'établissement initial de la relation client entre le prestataire de services de paiement et l'utilisateur de services de paiement, car aucun fonds ni compte de paiement de l'utilisateur de services de paiement n'est accessible par l'intermédiaire du prestataire de services de paiement au moment de l'établissement de la relation client et parce qu'il serait impossible pour le prestataire de services de paiement de contacter l'utilisateur de services de paiement concerné, étant donné qu'au moment de l'entrée en relation, le prestataire de services de paiement n'a pas encore vérifié les coordonnées de l'utilisateur de services de paiement.

(88) Les prestataires de services de paiement devraient veiller, dans leurs communications avec leurs clients, à ce que toute information susceptible, si elle était interceptée de manière illicite, de compromettre la sécurité de l'instrument de paiement ou des données de paiement sécurisés, soit transmise au client par des canaux de communication sûrs et efficaces.

(89) 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.

(90) 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.

(91) Lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée ou fait valoir que ladite opération de paiement n'a pas été correctement exécutée, l'utilisation d'un instrument de paiement sous la forme convenue entre le prestataire de services de paiement et l'utilisateur de services de paiement ne devrait pas nécessairement suffire en tant que telle à prouver que l'opération de paiement a été autorisée par le payeur. L'authentification ou le recours à l'authentification forte du client enregistrée par le prestataire de services de paiement, y compris, le cas échéant, le prestataire de services d'initiation de paiement, ne devrait pas nécessairement constituer à lui seul une preuve suffisante que l'opération de paiement a été autorisée par le payeur ou que celui-ci a agi frauduleusement ou n'a pas satisfait, de manière intentionnelle ou à la suite d'une négligence grave, à une ou à plusieurs des obligations qui incombent à l'utilisateur de services de paiement en ce qui concerne les instruments de paiement et les données de sécurité personnalisées.

(92) Pour que l'utilisateur de services de paiement puisse avoir plus facilement accès au prestataire de services de paiement, ce dernier devrait créer et fournir un canal de communication pour permettre à l'utilisateur de services de paiement de procéder à une notification ou de demander le déblocage de l'instrument de paiement conformément au présent règlement. Ce canal devrait également permettre à l'utilisateur de services de paiement de procéder à une notification à propos d'une opération frauduleuse. Les prestataires de services de paiement pourraient utiliser ce canal pour offrir des conseils à un client qui pense être victime d'une attaque frauduleuse et pour permettre aux utilisateurs de services de paiement de signaler les problèmes concernant les opérations de paiement effectuées, tels que des erreurs commises par les machines de paiement lors d’opérations de paiement.

(93) Compte tenu de la complexité croissante et de l'évolution rapide des schémas de fraude, il convient de veiller à ce que, avant qu'un prestataire de services de paiement ne conclue qu'un utilisateur de services de paiement a agi frauduleusement, de façon intentionnelle ou à la suite d'une négligence grave, et qu'il refuse par conséquent d'accorder un remboursement à cet utilisateur de services de paiement conformément au présent règlement, ledit utilisateur de services de paiement ait la possibilité de fournir à son prestataire de services de paiement, à l'appui de sa demande, toute information ou preuve pertinente concernant les circonstances de l'opération de paiement ou de la série d'opérations de paiement contestées. Dans ce contexte, lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement ou une série d'opérations de paiement, ou lorsqu'un utilisateur de services de paiement qui est un consommateur affirme qu'une opération de paiement ou une série d'opérations de paiement est le résultat d'une fraude impliquant l'usurpation d'identité du prestataire de services de paiement au sens du présent règlement, ledit prestataire de services de paiement ne devrait pas conclure que cet utilisateur de services de paiement, ou le consommateur, selon le cas, a agi frauduleusement, de façon intentionnelle ou à la suite d'une négligence grave, sans avoir au préalable invité de manière proactive et sans ambiguïté ledit utilisateur de services de paiement à fournir de telles informations ou preuves, et sans en avoir dûment tenu compte dans son évaluation. L'obligation qui incombe au prestataire de services de paiement de permettre à l'utilisateur de services de paiement de fournir les preuves ou informations pertinentes à l'appui de ses demandes devrait être interprétée comme un droit de l'utilisateur de services de paiement de voir toutes les informations pertinentes concernant les circonstances de l'opération de paiement ou de la série d'opérations de paiement contestées dûment examinées par le prestataire de services de paiement. Ce droit de l'utilisateur de services de paiement ne devrait pas être interprété comme un motif permettant au prestataire de services de paiement de conclure que l'utilisateur de services de paiement a agi frauduleusement, de manière intentionnelle ou à la suite d'une négligence grave, lorsque l’utilisateur de services de paiement ne fournit pas de preuve qu'il ne peut raisonnablement être tenu de détenir, comme des enregistrements d'appels téléphoniques, ou lorsque cet utilisateur de services de paiement ne fournit aucune preuve ni aucune information.

(94) 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, lorsque le prestataire de services de paiement soupçonne qu'une telle opération non autorisée résulte d'un manquement du payeur, qu'il soit intentionnel ou dû à une négligence grave, à une ou plusieurs de ses obligations en matière de sécurité des instruments de paiement et des données de sécurité personnalisées, ou d'un comportement frauduleux du payeur, et que ces soupçons reposent sur des raisons objectivement justifiées, le prestataire de services de paiement devrait être en mesure de mener une enquête avant de rembourser le payeur. Le prestataire de services de paiement devrait, dans un délai de quinze jours ouvrables à compter de la date à laquelle il a constaté ou été informé de l'opération, 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. Lorsque le prestataire de services de paiement refuse le remboursement après avoir conclu, à l'issue de son enquête, que le payeur a agi frauduleusement, le prestataire de services de paiement devrait communiquer les motifs de cette conclusion à l'autorité nationale compétente. Les États membres devraient indiquer clairement au public à quelle autorité nationale compétente cette communication du prestataire de services de paiement doit être adressée. 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 notifier sans retard injustifié au prestataire de services de paiement le vol, la perte ou le détournement d'un instrument de paiement ou de données de sécurité personnalisées, 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, à la date d'adoption du présent règlement, un montant de 50 EUR est 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 ou de données de sécurité personnalisées. En outre, une fois qu'il a informé le prestataire de services de paiement du risque d'utilisation frauduleuse de son instrument de paiement ou de ses données de sécurité personnalisées, l'utilisateur de services de paiement ne devrait pas être tenu de couvrir toute autre perte pouvant résulter de l'utilisation frauduleuse de cet instrument de paiement ou de ces données de sécurité personnalisées. Les prestataires de services de paiement devraient être responsables de la sécurité technique de leurs propres produits.

(95) Des dispositions en matière de responsabilité dans le cas de virements autorisés pour lesquelles il y a eu une erreur dans la prestation ou un dysfonctionnement du service chargé de vérifier la concordance 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 des informations erronées. Le prestataire de services de paiement du payeur devrait être tenu pour responsable et rembourser sans retard au payeur le montant total d'un virement mal exécuté qui a résulté de l'incapacité dudit prestataire de services de paiement à fournir, ou à fournir correctement, au payeur le service assurant la vérification du bénéficiaire. Lorsque la responsabilité du prestataire de services de paiement du payeur est imputable au prestataire de services de paiement du bénéficiaire ou du prestataire de services d'initiation de paiement, le prestataire de services de paiement du bénéficiaire ou, le cas échéant, le prestataire de services d'initiation de paiement devrait indemniser le prestataire de services de paiement du payeur pour le préjudice financier subi.

(96) Les prestataires de services de paiement devraient coopérer avec les utilisateurs de services de paiement et les autorités compétentes lorsque la bonne exécution du service assurant la vérification du bénéficiaire est remise en cause.

(97) Les utilisateurs de services de paiement devraient être protégés de manière adéquate contre ce qui est connu sous le nom de fraude par l'ingénierie sociale, dans laquelle le fraudeur manipule l'utilisateur de services de paiement pour l'amener à exécuter une certaine action, comme l'initiation d'une opération de paiement ou la transmission des données de sécurité de l'utilisateur de services de paiement aux fraudeurs. Le nombre de cas d'ingénierie sociale de ce type a considérablement augmenté ces dernières années. Ces nouveaux types de fraude rendent plus floue la distinction établie par la directive (UE) 2015/2366 entre les opérations autorisées et les opérations non autorisées. Les moyens permettant de présumer que le consentement a 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 son consentement devraient être dûment prises en considération, y compris par les tribunaux, lorsqu'il s'agit de déterminer si l'opération concernée a été autorisée ou non. L'opération concernée pourrait en effet avoir été autorisée dans des circonstances telles que l'autorisation accordée a reposé sur des prémisses viciées qui compromettent l'intégrité du consentement donné. 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 vigilance moindre du client. Il est donc nécessaire de définir les conditions dans lesquelles un utilisateur de services de paiement a droit à un remboursement.

(98) Les fraudeurs ont souvent recours à des outils et des techniques tels que l'usurpation de l'identifiant de l'appelant, l'usurpation d'adresse de courrier électronique ou l'usurpation d'adresse IP. Ces cas de fraude sont complexes et impliquent souvent différents acteurs tout au long de la chaîne de la fraude. Les prestataires de services de paiement disposent de plus de moyens que les utilisateurs de services de paiement pour mettre fin à ces cas de fraude. Tant les prestataires de services de paiement que les fournisseurs de services de communications électroniques peuvent jouer un rôle essentiel dans la prévention de la fraude grâce à des mesures préventives adéquates et à des dispositions techniques efficaces. Les prestataires de services de paiement ont soumis à des obligations spécifiques en vertu du règlement (UE) 2022/2554 du Parlement européen et du Conseil[24], qui visent à atténuer les risques liés aux TIC. Le règlement (UE) 2022/2554 soumet les prestataires de services de paiement à un ensemble complet de règles relatives au cadre de gestion des risques liés aux TIC, comprenant des outils, des politiques et des procédures visant à protéger la confidentialité, l'intégrité et la disponibilité des données, qu'elles soient au repos, en cours d'utilisation ou en transit. Afin de se conformer à ces obligations, les prestataires de services de paiement devraient avoir mis en place des mesures techniques et des outils adéquats pour empêcher la reproduction frauduleuse et l'utilisation abusive du nom de domaine du prestataire de services de paiement ainsi que des canaux de communication utilisés pour les échanges entre le prestataire de services de paiement et l'utilisateur de services de paiement, y compris l'adresse de courrier électronique du prestataire de services de paiement et l'identification de la ligne appelante.

---

[24] 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, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

(99) L'usurpation d'identité d'un prestataire de services de paiement, ou "spoofing", consiste pour des fraudeurs à se faire passer pour le prestataire de services de paiement du consommateur et à utiliser de manière abusive le nom de domaine ou les canaux de communication attribués au prestataire de services de paiement du consommateur, par exemple son adresse de courrier électronique, son numéro de téléphone, son site internet ou son application mobile. La fraude par usurpation d'identité nuit à la réputation du prestataire de services de paiement et du secteur financier dans son ensemble et peut causer des préjudices financiers importants aux consommateurs de l'Union et saper leur confiance dans les paiements électroniques et dans le système financier. Un consommateur qui a été victime d'une telle fraude par usurpation d'identité 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 consommateur. Lorsque la fraude concerne le site internet ou l'application mobile du prestataire de services de paiement, le droit au remboursement devrait s'étendre aux cas où le fraudeur s'est approprié ces canaux, ainsi qu'aux cas où il a créé de fausses versions du site internet ou de l'application mobile qui reproduisent le contenu du site ou de l'application authentique. Dès que le consommateur se rend compte qu'il a été victime de ce type de manipulation frauduleuse par usurpation d'identité, il devrait signaler l'incident à son prestataire de services de paiement et aux forces de l’ordre sans retard injustifié, de préférence au moyen de procédures de réclamation en ligne, lorsqu'elles sont mises à disposition par les forces de l’ordre. Étant donné que les consommateurs particulièrement vulnérables peuvent avoir des difficultés à signaler la fraude aux forces de l’ordre dans les meilleurs délais, les prestataires de services de paiement sont encouragés à aider le consommateur à effectuer ce signalement, si nécessaire.

(100) La fraude aux paiements, y compris l'initiation ou la modification d'ordres de paiement sans le consentement du payeur, le vol de données de paiement sensibles, y compris les données de sécurité personnalisées, ou la manipulation du payeur, notamment par usurpation d'identité, implique souvent des activités frauduleuses de la part d'utilisateurs de services tels que les services de communications interpersonnelles ou les services d'hébergement, qui permettent le stockage et, le cas échéant, la diffusion au public de contenus en ligne. En fonction des caractéristiques techniques du service fourni, les prestataires de ces services ont accès à différentes données et, par conséquent, à différents types d'indices d'activités potentiellement frauduleuses. À ce titre, ces prestataires ont la capacité de contribuer à la lutte collective contre la fraude, y compris celle liée à l'usurpation d'identité, en échangeant des informations pertinentes avec les prestataires de services de paiement, dans le but de prévenir et de détecter les utilisations frauduleuses des services de communications interpersonnelles ou d'hébergement. À titre d'exemple, les informations pertinentes peuvent inclure les coordonnées des comptes de paiement des professionnels obtenues par les prestataires de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec ces professionnels, conformément à l'article 30 du règlement (UE) 2022/2065 du Parlement européen et du Conseil[25], concernant des éléments d'information identifiés comme des contenus illicites par ces prestataires, ou encore des informations relatives aux instruments de paiement signalés comme volés par les utilisateurs de services de paiement auprès de leurs prestataires de services de paiement.

[25] Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (JO L 277 du 27.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj).

Le traitement des données à caractère personnel strictement nécessaires à la prévention de la fraude relève d'un intérêt légitime des prestataires de services de communications interpersonnelles, des prestataires de services d'hébergement, des prestataires de services de paiement et de leurs clients. Les prestataires de services de communications interpersonnelles et de services d'hébergement devraient pouvoir échanger des données à caractère personnel avec les prestataires de services de paiement afin d'identifier les acteurs et comportements frauduleux, pour autant que toutes les conditions prévues à l'article 6, paragraphe 1, point f), du règlement (UE) 2016/679 soient remplies. De plus, les prestataires de services de communications interpersonnelles et de services d'hébergement devraient également contribuer à la lutte contre la fraude en échangeant des informations avec les prestataires de services de paiement concernant les scénarios de fraude, les tendances et les menaces identifiées en lien avec l'utilisation de leurs services. Ce faisant, ils peuvent aider à améliorer l'efficacité des mécanismes de surveillance des opérations ainsi que des campagnes de sensibilisation et des formations en matière de prévention de la fraude mises en œuvre conformément au présent règlement.

(101) Lorsque les conditions pertinentes, y compris les exigences du règlement (UE) 2016/679, relatives à l'échange, sur une base volontaire, des informations nécessaires à la prévention et à la détection de la fraude sont remplies, les prestataires de services de communications interpersonnelles et les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient disposer de canaux de communication spécifiques ou conclure des accords ou systèmes de partage d'informations permettant une communication efficace avec les prestataires de services de paiement, tels que les accords de partage d'informations établis en vertu de l'article 29 de la directive (UE) 2022/2555 du Parlement européen et du Conseil[26]. Ces mécanismes devraient comporter de solides garanties en matière de confidentialité, de protection des données et d'utilisation des informations, conformément au règlement (UE) 2016/679.

[26] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(102) La directive (UE) 2022/2555 impose aux prestataires de services de communications interpersonnelles accessibles au public de prendre des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées afin de garantir la disponibilité, l'authenticité, l'intégrité et la confidentialité de leurs services. Dans la mesure où la manipulation frauduleuse de l'identification de la ligne appelante ou de l'adresse de courrier électronique peut être considérée comme compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité de ces services, ces prestataires devraient déjà être tenus, en vertu de la directive (UE) 2022/2555, de mettre en œuvre des mesures visant à pallier ce risque. Sans préjudice de ces obligations, les prestataires de services de communications interpersonnelles accessibles au public devraient prendre les mesures organisationnelles et techniques appropriées pour détecter et prévenir l'utilisation de leurs services à des fins de fraude par usurpation d'identité, notamment par la manipulation de l'identification de la ligne appelante ou de l'adresse de courrier électronique, lorsque cette utilisation vise à inciter les utilisateurs de services de paiement à effectuer un paiement ou à prendre une mesure susceptible de compromettre la sécurité du compte de paiement. Toute mesure prise dans le but de prévenir ou de détecter l'utilisation de ces services à des fins de fraude par usurpation d'identité doit être conforme aux règles énoncées dans le règlement (UE) 2016/679 et la directive 2002/58/CE du Parlement européen et du Conseil[27]. En particulier, ces mesures ne devraient pas impliquer une surveillance généralisée et indifférenciée du contenu des communications ou de l'ensemble des données relatives au trafic.

[27] 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 (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(103) Le règlement (UE) 2022/2065 établit des règles pleinement harmonisées concernant la prestation de services intermédiaires au sein du marché intérieur, ainsi que des obligations de diligence spécifiques adaptées à certaines catégories particulières de fournisseurs de services intermédiaires, à savoir les services dits de "simple transport", de "mise en cache" et d'"hébergement". En particulier, il impose des obligations de diligence spécifiques aux plateformes en ligne et aux moteurs de recherche en ligne, y compris lorsqu'ils sont désignés comme de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne. Ces obligations de diligence jouent un rôle important dans la prévention de la prolifération de contenus illicites en ligne, tels que les escroqueries financières. Par exemple, les prestataires de services d'hébergement sont tenus de mettre en place des mécanismes de signalement et d'action conviviaux permettant de signaler le contenu illicite, tel que des offres illégales de services financiers ou des tentatives de fraude, au prestataire de services d'hébergement. Les fournisseurs de plateformes en ligne sont également tenus de traiter en priorité les signalements émanant de signaleurs de confiance. Lorsque, sur la base des informations fournies par le payeur au prestataire de services de paiement ou d'autres informations dont dispose ledit prestataire de services de paiement, il est possible de considérer qu'une opération de paiement frauduleuse trouve son origine dans un élément d'information en ligne, les prestataires de services de paiement devraient recourir aux mécanismes de notification visés à l'article 16 du règlement (UE) 2022/2065 afin de notifier aux fournisseurs de services d'hébergement la présence sur leur service de cet élément d'information spécifique. Lorsque les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne se conforment à l'article 16 du règlement (UE) 2022/2065, notamment en mettant en place des mécanismes de signalement et d'action faciles d'accès et conviviaux, ils devraient être considérés comme respectant l'obligation prévue par le présent règlement d'informer les destinataires de leurs services de la procédure à suivre pour signaler toute activité frauduleuse présente au niveau de leurs services. Les prestataires de services de paiement devraient également pouvoir demander le statut de "signaleur de confiance" conformément à l'article 22 du règlement (UE) 2022/2065.

(104) Le règlement (UE) 2022/2065 encourage et facilite l'élaboration de codes de conduite volontaires au niveau de l'Union afin de contribuer à la bonne application dudit règlement, en tenant compte notamment des défis spécifiques liés à la lutte contre différents types de contenus illicites et aux risques systémiques, tout en promouvant la prévention, en renforçant la sécurité et en luttant contre la fraude aux paiements et les escroqueries financières. Il convient également de faciliter l'élaboration d'un code de conduite volontaire au niveau de l'Union dans les domaines couverts par le présent règlement.

(105) La promotion et l'offre frauduleuses de services financiers, telles que la publicité pour des produits et services de crédit, d'assurance et d'investissement, y compris les crypto-actifs, fournis par ou pour le compte d'entités qui ne sont ni agréées ni enregistrées conformément au droit de l'Union ou au droit national pour fournir de tels produits et services, peuvent être liées à la fraude aux paiements résultant de la tromperie et de la manipulation du consentement des utilisateurs de services de paiement afin qu'ils initient une opération de paiement ou une série d'opérations de paiement, ou du vol de données de paiement sensibles, y compris les données de sécurité personnalisées. Afin de réduire ce type de promotion et d'offre frauduleuses de services financiers, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient demander aux annonceurs de services financiers réglementés qu'ils fournissent des informations, telles que les numéros d'agrément ou d'enregistrement, attestant que le prestataire du service financier réglementé faisant l'objet de la publicité a été agréé ou enregistré pour fournir de tels services dans un État membre ou au niveau de l'Union. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient veiller à ce que leurs services ne soient pas proposés à des fins publicitaires tant que l'annonceur n'a pas fourni les informations relatives à l'enregistrement ou à l'agrément de l'entité pour le compte de laquelle la publicité est diffusée en tant que prestataire de services financiers réglementé.

Cette exigence ne devrait pas équivaloir à une obligation pour les fournisseurs des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne concernés de surveiller de manière générale les produits ou services proposés par les professionnels par l'intermédiaire de leurs services, ni à une obligation générale de recherche de faits visant à évaluer l'exactitude des informations fournies par les annonceurs. Toutefois, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne concernés devraient, dès réception des informations fournies par les annonceurs concernant l'agrément ou l'enregistrement du prestataire des services financiers réglementés faisant l'objet de la publicité, et avant d'autoriser l'annonceur à utiliser leur service aux fins de la publicité de ces services financiers réglementés, tout mettre en œuvre pour évaluer si ces informations, dont l'exactitude relève de la responsabilité des annonceurs aux fins du présent règlement, sont fiables et complètes, à condition que cette évaluation puisse être effectuée de manière proportionnée à l'aide d'outils automatisés. Les autorités européennes de surveillance, à savoir l'ABE, l'Autorité européenne de surveillance (Autorité européenne des marchés financiers) (AEMF) instituée par le règlement (UE) n° 1095/2010 du Parlement européen et du Conseil[28] et l'Autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles) (AEAPP) instituée par le règlement (UE) n° 1094/2010 du Parlement européen et du Conseil[29], tiennent déjà à jour des registres publics des prestataires de services financiers en vertu de la législation applicable. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne pourraient avoir recours à ces registres dans le cadre de leurs efforts visant à s'assurer que les informations fournies par l'annonceur potentiel sont fiables et complètes.

---

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

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

(106) Alors que les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne sont soumis à des obligations de transparence et de diligence en matière de publicité en ligne au titre du règlement (UE) 2022/2065, le présent règlement précise davantage les modalités d'application de ces obligations dans le cas particulier de la publicité pour des services financiers réglementés. Afin de se conformer à leur obligation de déployer des efforts raisonnables pour garantir l'exactitude et l'exhaustivité des informations contenues dans leurs registres établis conformément à l'article 39 du règlement (UE) 2022/2065, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne pourraient avoir recours aux registres des prestataires agréés ou enregistrés de services financiers réglementés mis à disposition conformément au droit de l'Union applicable, notamment la directive (UE) 2026/…[+], y compris aux registres publics tenus par les autorités européennes de surveillance.

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

(107) Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne sont tenus, dans le cadre du règlement (UE) 2022/2065, d'identifier, d'analyser et d'évaluer avec diligence tout risque systémique découlant de la conception ou du fonctionnement de leur service, y compris la diffusion de contenus illicites par l'intermédiaire de leurs services, tels que les contenus en ligne malveillants ou frauduleux au sens du présent règlement. Le cas échéant, à la suite de cette évaluation, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient mettre en place des mesures d'atténuation raisonnables, proportionnées et efficaces, conformément à l'article 35 du règlement (UE) 2022/2065, afin de faire face à ces risques, sous la supervision directe de la Commission. Lorsque, en vertu de l'article 35 du règlement (UE) 2022/2065, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne doivent mettre en place des mesures d'atténuation relatives au risque de publicité frauduleuse concernant des services financiers réglementés qu'ils ont identifié conformément à l'article 34 dudit règlement, les mesures mises en place conformément aux obligations énoncées dans le présent règlement pourraient être considérées comme un moyen possible de garantir le respect par ces fournisseurs de l'article 35, paragraphe 1, point e), du règlement (UE) 2022/2065. Toutefois, le respect des obligations prévues par le présent règlement ne devrait pas nécessairement être considéré comme suffisant en soi pour garantir le respect par ces fournisseurs de l'article 35, paragraphe 1, point e), du règlement (UE) 2022/2065, et devrait donc être sans préjudice d'autres mesures d'atténuation que ces fournisseurs pourraient être tenus de mettre en place.

(108) Afin d'évaluer la possibilité 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 particulières propres à chaque cas. Les preuves et le degré de négligence allégué devraient en général être évalués conformément au droit national. Toutefois, si la notion de 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, par exemple, 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. Lors de l'évaluation de la possibilité d'une négligence grave de la part de l'utilisateur de services de paiement, l'ensemble des circonstances factuelles devraient être prises compte, comme par exemple le caractère novateur et la complexité de la fraude; les moyens ou stratégies utilisés par des tiers pour s'emparer illégalement des données de sécurité personnalisées de l'utilisateur de services de paiement; le fait que l'utilisateur de services de paiement ait déjà été victime du même type de fraude; dans le cas d'un nouveau type de fraude, le respect par les prestataires de services de paiement des obligations qui leur incombent en vertu du présent règlement, y compris en ce qui concerne leurs groupes de clients les plus vulnérables; le fait que l'utilisateur de services de paiement ait pris les mesures adéquates pour garantir de manière appropriée la confidentialité de ses données de sécurité personnalisées; toute caractéristique connue de l'utilisateur de services de paiement susceptible de l'exposer davantage au risque d'être victime d'une fraude; le fait que les prestataires de services de paiement ait fourni au payeur des avertissements clairs, spécifiques et adaptés à sa situation, et le fait que l'utilisateur de services de paiement n'ait pas tenu compte des interventions spécifiques et ciblées de son prestataire de services de paiement. Cette liste n'est ni exhaustive, ni cumulative, ni contraignante, et ne porte pas atteinte au pouvoir d'appréciation des juridictions de l'Union ou des juridictions nationales, ni à celui des instances de règlement des litiges.

(109) Compte tenu du fait que la notion de "négligence grave" fait l'objet d'interprétations très divergentes au sein de l'Union, l'ABE est encouragée à publier des orientations visant à préciser davantage les circonstances factuelles à prendre en considération lors de l'évaluation de la possibilité d'une négligence grave de la part de l'utilisateur de services de paiement.

(110) 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.

(111) Les consommateurs sont particulièrement vulnérables dans le cas d'opérations de paiement où le montant exact de l'opération n'est pas connu au moment où le payeur donne son consentement à 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 raisonnablement s'attendre, et uniquement si le payeur a donné son consentement à ce 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.

(112) 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 bénéficie d'une autre forme de protection. Cela pourrait être le cas soit parce que le payeur a donné son consentement à l'exécution d'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.

(113) Afin de pouvoir établir leur programmation financière et remplir leurs obligations de paiement dans les délais, 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, y compris les vérifications de la sécurité et de la disponibilité des fonds, les informations sur l'utilisation du numéro d'identification personnel 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 de la transmission par un bénéficiaire 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 de l'octroi au bénéficiaire d'une avance sur les montants concernés par le prestataire de services de paiement, sous la forme d'une somme créditée de manière conditionnelle sur le compte, ne devrait aucunement entrer en ligne de compte à cet égard.

(114) Les utilisateurs de services de paiement devraient également pouvoir être assurés de la bonne exécution d'un ordre de paiement dûment complété et valide si le prestataire de services de paiement n'a aucun motif contractuel ou légal justifiant un refus ou tout autre forme de non-exécution, tel que les obligations découlant du présent règlement ou du règlement (UE) 2024/1624.

(115) Étant donné que la fraude constitue une activité criminelle au sens de l'article 2, point 1), de la directive (UE) 2018/1673 du Parlement européen et du Conseil[30], elle est considérée comme une infraction sous-jacente aux fins du règlement (UE) 2024/1624. Pour cette raison, les obligations prévues par ledit règlement en matière de signalement des opérations suspectes, conformément à son article 69, ainsi que l'obligation de s'abstenir d'exécuter ces opérations suspectes, conformément à son article 71, s'appliquent également dans les cas où un prestataire de services de paiement sait ou soupçonne qu'une opération de paiement est frauduleuse. Ces obligations s'appliquent également lorsque le prestataire de services de paiement a des motifs raisonnables de soupçonner qu'une opération de paiement est liée à une activité criminelle, par exemple lorsque le prestataire de services de paiement du payeur a des motifs raisonnables de soupçonner qu'une opération de paiement initiée par le payeur pourrait résulter d'une fraude ou que, avant de mettre les fonds à la disposition du bénéficiaire, le prestataire de services de paiement du payeur a des motifs raisonnables de soupçonner qu'une opération de paiement qui a été ou sera créditée sur son compte pourrait résulter d'une fraude.

[30] Directive (UE) 2018/1673 du Parlement européen et du Conseil du 23 octobre 2018 visant à lutter contre le blanchiment de capitaux au moyen du droit pénal (JO L 284 du 12.11.2018, p. 22, ELI: http://data.europa.eu/eli/dir/2018/1673/oj).

(116) Il est nécessaire de veiller à la cohérence entre les objectifs visant à empêcher que les utilisateurs de services de paiement ne soient victimes de fraudes, à garantir le respect du règlement (UE) 2024/1624 en ce qui concerne les opérations suspectes, et à atténuer l'impact sur les utilisateurs de services de paiement résultant de retards dans l'exécution d'opérations de paiement légitimes ou du refus de telles opérations. C'est pourquoi, lorsqu'un prestataire de services de paiement refuse d'exécuter une opération de paiement conformément au présent règlement, ce refus devrait être sans préjudice des autres obligations qui incombent à ce prestataire de services de paiement au titre du règlement (UE) 2024/1624 en ce qui concerne ladite opération de paiement, telles que l'obligation de déclaration de soupçons auprès de la cellule de renseignement financier conformément à l'article 69 dudit règlement. Dans le cas des virements, bien que le résultat du service assurant la vérification du bénéficiaire, mis en œuvre conformément au règlement (UE) n° 260/2012 et au présent règlement puisse constituer un élément pertinent dans le cadre de la surveillance des opérations de paiement effectuée par le prestataire de services de paiement en vue de détecter la fraude, ce résultat ne devrait pas, en soi, constituer le seul motif justifiant la décision du prestataire de services de paiement de refuser l'exécution de l'opération de paiement, afin de garantir le droit du payeur de procéder à l'autorisation de l'opération de paiement concernée conformément à l'article 5 *quater* du règlement (UE) n° 260/2012 et au présent règlement.

(117) Afin de permettre au prestataire de services de paiement d'évaluer s'il existe ou non des raisons objectivement justifiées de soupçonner qu'une opération de paiement est frauduleuse et donc de refuser l'exécution de cette opération de paiement, et afin de limiter l'incidence sur les utilisateurs de services de paiement en ce qui concerne les opérations de paiement légitimes, le prestataire de services de paiement du payeur devrait contacter le payeur pour obtenir les informations nécessaires aux fins de cette évaluation, tout en respectant pleinement les règles relatives à l'interdiction de divulguer des soupçons prévues par le règlement (UE) 2024/1624. Le prestataire de services de paiement du payeur devrait notifier au payeur toute information ou mesure requise de la part du payeur aux fins de son évaluation, tout en fournissant des informations suffisantes pour permettre au payeur de comprendre les risques identifiés par le prestataire de services de paiement. Le prestataire de services de paiement du payeur devrait veiller à ce que le payeur dispose à tout moment de moyens appropriés pour contacter le prestataire de services de paiement afin de lui fournir les informations ou d'effectuer l'action demandée dans ladite notification, et devrait mettre tout en œuvre pour contacter le payeur avant de créditer les fonds sur le compte du prestataire de services de paiement du bénéficiaire. Conformément à l'article 73 du règlement (UE) 2024/1624, de telles communications entre le prestataire de services de paiement du payeur et le payeur ne devraient à aucun moment révéler au payeur ou, le cas échéant, au prestataire de services d'initiation de paiement, que des opérations ou activités de paiement font l'objet ou ont fait l'objet d'une évaluation conformément à l'article 69 du règlement (UE) 2024/1624, que des informations sont, seront ou ont été transmises conformément à l'article 69 ou 70 du règlement (UE) 2024/1624 ou qu'une analyse à cet effet est en cours ou pourrait être ouverte.

(118) Étant donné que, conformément au règlement (UE) n° 260/2012, le montant d'un virement instantané en euros devrait mis à disponible sur le compte de paiement du bénéficiaire dans un délai de dix secondes à compter de la réception de l'ordre de paiement par le prestataire de services de paiement du payeur, les règles imposant au prestataire de services de paiement du payeur d'informer et de contacter le payeur s'il suspend l'exécution d'une opération de paiement en raison d'un soupçon de fraude, ne devraient pas s'appliquer dans le cas des virements instantanés. En pareils cas, et dans les cas où le prestataire de services de paiement du payeur, après avoir notifié et contacté le payeur, n'a toutefois pas pu obtenir les informations requises avant l'expiration du délai réglementaire prévu pour créditer les fonds sur le compte du prestataire de services de paiement du bénéficiaire, ce dernier devrait déterminer s'il existe ou non des raisons objectivement justifiées de soupçonner une fraude et décider s'il convient ou non de refuser l'exécution de l'opération de paiement, en s'appuyant sur le mécanisme de surveillance des opérations et sur toute autre information pertinente dont dispose le prestataire de services de paiement, mais sans se fonder uniquement sur les résultats du service assurant la vérification du bénéficiaire.

(119) Aux fins du présent règlement, le fait qu'un ordre de paiement ou une opération de paiement soit inhabituel ne devrait pas constituer automatiquement des motifs de soupçonner que l'opération de paiement est frauduleuse, ni constituer, en soi, des raisons objectivement justifiées de soupçonner une fraude. Toutefois, tout ordre de paiement ou opération de paiement inhabituel pourrait constituer un premier indice de fraude, ce qui devrait alerter le prestataire de services de paiement et pourrait justifier une enquête plus approfondie. Pour déterminer s'il existe des raisons objectivement justifiées de soupçonner une fraude concernant un ordre de paiement ou une opération de paiement, le prestataire de services de paiement devrait tenir compte des circonstances spécifiques de chaque opération, ainsi que de son évaluation plus large de l'évolution du risque de fraude, sur la base de la surveillance des opérations effectuée par le prestataire de services de paiement ou de toute information pertinente dont il dispose. Lorsqu'une décision de refuser ou de suspendre l'exécution d'une opération de paiement repose exclusivement sur un traitement automatisé, cette décision n'est admissible que si des mesures appropriées ont été mises en œuvre afin de protéger les droits, les libertés et les intérêts légitimes de l'utilisateur de services de paiement.

(120) Lorsque le prestataires de services de paiement refuse d'exécuter une opération de paiement, le refus et le motif de ce refus devraient être communiqués sans retard injustifié au payeur, au prestataires de services de paiement du payeur et, le cas échéant, au prestataire de services d'initiation de paiement, ou, dans le cas des virements instantanés, dans un délai de dix secondes à compter de la réception de l'ordre de paiement par le prestataire de services de paiement du payeur, dans le respect des exigences du droit de l'Union et du droit national. En outre, le prestataire de services de paiement du payeur devrait informer le payeur de la procédure lui permettant de corriger l'évaluation ayant conduit au refus, ou de revenir sur cette décision. 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. Le prestataire de services de paiement du payeur ne devrait pas imputer de frais lorsqu'il refuse d'exécuter l'opération de paiement en raison d'une suspicion de fraude.

(121) 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.

(122) 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, en ce qui concerne le remboursement au payeur du 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.

(123) 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. Les bénéficiaires devraient cependant avoir la faculté de conclure un accord avec leur prestataire de services de paiement 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.

(124) Les obligations prévues par le présent règlement concernant les interfaces de banque ouverte («open banking») et la vérification du bénéficiaire ne devraient pas s'appliquer aux opérations de paiement effectuées au moyen de jetons de monnaie électronique. L'extension de l'application de ces exigences aux opérations de paiement effectuées au moyen de jetons de monnaie électronique peut entraîner l'imposition d'exigences considérables en matière d'investissement et des charges excessives aux entités fournissant ces services, compte tenu des coûts élevés liés à la mise en œuvre de ces exigences. De plus, eu égard au fait que les opérations effectuées au moyen de jetons de monnaie électronique ne sont pas encore aussi courantes que les opérations de paiement classiques, il y a moins d'urgence et d'intérêt à imposer de telles exigences en ce qui concerne les opérations de paiement effectuées au moyen de jetons de monnaie électronique.

(125) Afin d'améliorer l'efficience des paiements dans toute l'Union, il convient 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, sauf disposition contraire pertinente du droit national ou du droit de l'Union en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme. 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, et 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.

(126) Afin de permettre aux payeurs de récupérer rapidement leurs fonds chaque fois qu'il existe un risque élevé qu'une ou plusieurs opérations de paiement soient frauduleuses, il convient de préciser dans le présent règlement que, lorsque le prestataire de services de paiement du bénéficiaire a des raisons objectivement justifiées de soupçonner qu'une opération de paiement ou une série d'opérations de paiement créditées ou devant être créditées sur son compte pourrait résulter d'une fraude, et que le prestataire de services de paiement s'abstient de mettre ces fonds à disposition sur le compte de paiement du bénéficiaire conformément à son obligation de s'abstenir d'exécuter une opération suspecte en vertu de l'article 71 du règlement (UE) 2024/1624, ledit prestataire de services de paiement est en mesure de restituer les fonds crédités sur son compte au prestataire de services de paiement du payeur, ou de refuser l'opération de paiement ou la série d'opérations de paiement devant être créditées sur son compte par le prestataire de services de paiement du payeur, selon le cas. Afin d'améliorer la protection des payeurs, il convient d'exiger que, dans certains cas où il existe des indices de fraude plus solides, le prestataire de services de paiement du bénéficiaire restitue les fonds au prestataire de services de paiement du payeur ou refuse l'opération de paiement ou la série d'opérations de paiement devant être créditées sur le compte de celui-ci par le prestataire de services de paiement du payeur, selon le cas. Pour éviter des pratiques de réduction des risques excessives, il convient de fixer un niveau de preuve plus élevé à partir duquel cette obligation et la responsabilité correspondante devraient s'appliquer, lorsque le prestataire de services de paiement du bénéficiaire dispose de preuves ou d'indices solides, cohérents et irréfutables lui permettant de conclure, en l'absence d'autre explication plausible, que l'opération de paiement ou la série d'opérations de paiement résulte d'une fraude.

(127) Afin de préserver la confiance des utilisateurs de services de paiement dans la fiabilité de ces services, il importe de veiller à ce que les mesures de prévention de la fraude qui interfèrent avec l'exécution des opérations de paiement soient suffisamment communiquées au payeur, à son prestataire de services de paiement et, le cas échéant, au prestataire de services d'initiation de paiement, dans les délais applicables à l'exécution de ces opérations de paiement fixés dans le présent règlement et dans le règlement (UE) nº 260/2012, tout en restant pleinement conformes aux règles relatives à l'interdiction de divulgation énoncées dans le règlement (UE) 2024/1624. Afin d'éviter une application inégale de ces mesures de protection et de transparence dans le cas des virements instantanés libellés en euros et dans le cas des virements instantanés libellés dans d'autres monnaies, il convient d'établir dans le présent règlement que, pour tout virement instantané, lorsque, conformément au présent règlement, le prestataire de services de paiement du bénéficiaire refuse de mettre les fonds à la disposition du bénéficiaire et, le cas échéant, restitue ces fonds au prestataire de services de paiement du payeur ou rejette l'opération ou la série d'opérations de paiement devant être créditées sur son compte par le prestataire de services de paiement du payeur, le prestataire de services de paiement du bénéficiaire devrait notifier ce refus au prestataire de services de paiement du payeur dans un délai de dix secondes à compter du moment de la réception de l'ordre de paiement pour ce virement instantané ou cette série de virements instantanés par le prestataire de services de paiement du payeur. Dès réception de cette notification, le prestataire de services de paiement du payeur devrait immédiatement rétablir le compte de paiement du payeur dans l'état dans lequel il se serait trouvé si l'opération n'avait pas eu lieu et informer, sans frais, le payeur et, le cas échéant, le prestataire de services d'initiation de paiement de la restitution des fonds et du fait que les fonds n'ont pas été mis à disposition sur le compte de paiement du bénéficiaire en raison de mesures de prévention de la fraude. Conformément à l'article 73 du règlement (UE) 2024/1624, ces communications ne devraient à aucun moment révéler au payeur ou, le cas échéant, au prestataire de services d'initiation de paiement, que des opérations ou activités de paiement font l'objet ou ont fait l'objet d'une évaluation conformément à l'article 69 du règlement (UE) 2024/1624, que des informations sont, seront ou ont été transmises conformément à l'article 69 ou 70 du règlement (UE) 2024/1624 ou qu'une analyse à cet effet est en cours ou pourrait être ouverte.

(128) 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.

(129) 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.

(130) Le prestataire de services de paiement devrait avoir la possibilité de préciser clairement les informations exigées aux fins de l'exécution correcte d'une opération de paiement. Sans préjudice de son obligation de fournir le service assurant la vérification du bénéficiaire, le prestataire de services de paiement du payeur devrait agir avec toute la diligence requise et vérifier la cohérence de l'identifiant unique, et, s'il apparaît que cet identifiant unique n'est pas cohérent et que, par conséquent, l'ordre de paiement en question est impossible à exécuter, refuser cette opération de paiement et en informer le payeur.

(131) 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 le prestataire de services de paiement qui exécute l'opération 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 cette exécution. Eu égard à l'ensemble de ces considérations, il convient que, sauf en cas de situations anormales et imprévisibles, et sauf disposition contraire du présent règlement ou d'autres dispositions pertinentes du droit de l'Union, 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 de ce prestataire de services de paiement que la somme soit créditée sur le compte du bénéficiaire.

(132) 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 sans retard injustifié 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.

(133) Le bon fonctionnement des virements et des autres services de paiement requiert que les prestataires de services de paiement et leurs intermédiaires, y compris 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, il est nécessaire de garantir la sécurité juridique quant au fait qu'un prestataire de services de paiement qui n'est pas responsable obtiendra, 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.

(134) Aux fins du règlement (UE) 2022/2065, la notion de contenu illicite devrait être comprise comme se référant à des informations, quelle que soit leur forme, qui, en vertu du droit de l'Union ou du droit national applicables, sont soit elles-mêmes illicites, soit rendues illicites par les règles applicables en raison du fait qu'elles se rapportent à des activités illégales. Il peut s'agir, par exemple, de toute offre de services financiers, y compris de services de paiement, qui n'est pas conforme aux exigences applicables à l'offre de tels services en vertu du présent règlement, de la directive (UE) 2026/...[+] ou d'autres dispositions du droit de l'Union ou du droit national, ou tout contenu rendu illicite au regard du droit national en matière de fraude, y compris les infractions prévues par le droit national adopté en vertu de la directive (UE) 2019/713 du Parlement européen et du Conseil[31].

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

[31] Directive (UE) 2019/713 du Parlement européen et du Conseil du 17 avril 2019 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision-cadre 2001/413/JAI du Conseil (JO L 123 du 10.5.2019, p. 18, ELI: http://data.europa.eu/eli/dir/2019/713/oj).

(135) Toute réclamation d'un prestataire de services de paiement contre d'autres prestataires, tels que des fournisseurs de services de communications électroniques ou des fournisseurs de services intermédiaires, portant sur un préjudice financier causé dans le cadre d'une fraude devrait être introduite conformément au droit national.

(136) En ce qui concerne les fournisseurs de services intermédiaires, le règlement (UE) 2022/2065 établit un cadre pleinement harmonisé pour l'exemption conditionnelle de responsabilité de ces fournisseurs, sous certaines conditions et conformément à l'interprétation donnée par la Cour de justice de l'Union européenne. Afin de bénéficier de l'exemption de responsabilité relative aux services d'hébergement en vertu du règlement (UE) 2022/2065, les fournisseurs de services d'hébergement, y compris les plateformes en ligne, devraient agir rapidement pour retirer le contenu illicite ou rendre l'accès à ce contenu impossible, dès qu'ils ont effectivement connaissance de ce contenu ou, en cas de demande en dommages et intérêts, dès qu'ils ont conscience dudit contenu, en particulier dans les cas où le fournisseur de services d'hébergement a été informé de faits ou de circonstances sur la base desquels un opérateur économique diligent aurait dû identifier l'illicéité en question. En ce qui concerne tout particulièrement les fournisseurs de services d'hébergement définis à l'article 3, point g), iii), du règlement (UE) 2022/2065, lorsque les conditions d'exemption de responsabilité au titre de l'article 6, paragraphe 1, dudit règlement ne sont pas remplies et que les fournisseurs de services d'hébergement deviennent responsables d'un contenu stocké dans leurs services, et que ce contenu a donné lieu à une ou plusieurs opérations de paiement non autorisées ou opérations de paiement autorisées de façon frauduleuse au sens du présent règlement, les prestataires de services de paiement devraient pouvoir obtenir une indemnisation de la part des fournisseurs de services d'hébergement pour le montant remboursé à leurs clients pour ces opérations au titre du présent règlement.

(137) Aucune disposition du présent règlement ne saurait être interprétée comme une obligation générale faite aux fournisseurs de services d'hébergement de surveiller les informations qu'ils transmettent ou stockent, ou comme exigeant de ces fournisseurs qu'ils recherchent activement des faits ou des circonstances indiquant une activité illégale, telle que l'usurpation d'identité d'un prestataire de services de paiement.

(138) La prestation de services de paiement par des 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[32], 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 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 de l'application du présent règlement.

---

[32] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(139) Comme le reconnaît la Commission dans sa communication sur une stratégie en matière de paiements de détail pour l'UE, le bon fonctionnement des marchés des paiements de l'Union, y compris la sécurité des paiements et la protection des utilisateurs de services de paiement contre la fraude, revêt un intérêt public important. C'est pourquoi, 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, les opérateurs de systèmes de paiement et les opérateurs de schémas 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, conformément à l'article 9, paragraphe 2, point g), et à l'article 10, paragraphe 2, point g), desdits règlements, respectivement. 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 organisationnelles 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.

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

(141) 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 la surveillance des opérations joue un rôle important dans cette détection. Il convient donc d'exiger à la fois du prestataire de services de paiement du payeur et du prestataire de services de paiement du bénéficiaire qu'ils disposent de mécanismes de surveillance 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. Le prestataire de services de paiement du payeur devrait effectuer cette surveillance des opérations avant l'exécution d'une opération de paiement, ce qui, dans le cas des virements instantanés, signifie en temps réel. Le prestataire de services de paiement du bénéficiaire devrait effectuer cette surveillance des opérations avant de mettre les fonds à la disposition du bénéficiaire. Lorsqu'un prestataire de services de paiement ne respecte pas les obligations qui lui incombent en ce qui concerne l'application de la surveillance des opérations à une opération ou série d'opérations de paiement, et que cette opération ou série d'opérations de paiement a été initiée par des moyens frauduleux, ou à la suite d'une fraude, le montant total de cette opération ou série d'opérations de paiement devrait être remboursé au payeur par son prestataire de services de paiement. Lorsque le prestataire de services de paiement qui n'a pas appliqué la surveillance des opérations est le prestataire de services de paiement du bénéficiaire, il devrait rembourser au prestataire de services de paiement du payeur le montant remboursé par ce dernier au payeur.

(142) L'ABE devrait élaborer des projets de normes techniques de réglementation relatives aux exigences techniques particulières liées aux mécanismes de surveillance 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.

(143) 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 dans la mesure nécessaire pour garantir que les mécanismes de surveillance des opérations fonctionnent efficacement de manière à permettre auxdits prestataires de détecter et de prévenir les fraudes, notamment en détectant un comportement atypique de l'utilisateur de services de paiement qui pourrait indiquer une opération potentiellement frauduleuse ou une utilisation potentiellement frauduleuse du compte de paiement. La surveillance des opérations effectuée par les prestataires de services de paiement pourrait, dans la mesure nécessaire à la détection de la fraude, inclure le traitement des informations échangées au moyen du service assurant la vérification du bénéficiaire ou dans le cadre de dispositifs de partage d'informations établis conformément au présent règlement ou à d'autres dispositions pertinentes du droit de l'Union.

(144) Les prestataires de services de paiement ne devraient conserver les données traitées aux fins du respect de leurs obligations en matière de surveillance des opérations et de partage d'informations sur la fraude que pendant la durée nécessaire à ces fins et, en tout état de cause, pendant une période maximale de cinq ans après la cessation de la relation avec le client. Les recommandations révisées du Groupe d'action financière démontrent que, pour être en mesure de coopérer pleinement et de se conformer rapidement aux demandes d'informations des autorités compétentes afin de prévenir ou de détecter des actes de blanchiment de capitaux ou de financement du terrorisme ou d'enquêter à cet égard, les entités assujetties devraient conserver, pendant au moins cinq ans, les informations nécessaires obtenues par l'intermédiaire des mesures de vigilance à l'égard de la clientèle et les documents relatifs aux opérations. En conséquence, le règlement (UE) 2024/1624 établit que la durée de conservation applicable aux données à caractère personnel traitées conformément audit règlement, y compris en ce qui concerne les informations traitées dans le cadre des partenariats en matière de partage d'informations établis en vertu de l'article 75 dudit règlement, devrait être de cinq ans après la fin de la relation d'affaires ou après la transaction à titre occasionnel. Étant donné que la fraude est considérée comme une infraction sous-jacente aux fins du règlement (UE) 2024/1624, il convient d’établir une durée maximale de conservation applicable aux données à caractère personnel traitées conformément au présent règlement, durée qui devrait également être fixée à cinq ans après la fin d'une relation d'affaires ou d'une opération à titre occasionnel, afin de garantir la sécurité juridique et la cohérence entre les mesures de prévention et de détection de la criminalité financière.

(145) La fraude 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 convient d'améliorer constamment la surveillance des opérations en tirant pleinement parti de technologies telles que l'intelligence artificielle ainsi que de renseignements sur la fraude qui soient aussi exhaustifs et à jour que possible. Un prestataire de services de paiement ne dispose souvent pas d'une vue d'ensemble complète de tous les éléments et indicateurs susceptibles de conduire à une détection rapide d'activités potentiellement frauduleuses dans une opération de paiement donnée. L'échange d'informations entre prestataires de services de paiement peut accroître les possibilités de mieux détecter les fraudes potentielles et de mieux protéger les utilisateurs de services de paiement. C'est pourquoi les prestataires de services de paiement devraient, aux fins de la surveillance des opérations, exploiter les données relatives à la fraude aux paiements partagées par d'autres prestataires de services de paiement, et partager les données relatives à la fraude aux paiements avec d'autres prestataires de services de paiement de manière multilatérale, dans le cadre de dispositifs de partage d'informations. Lorsque le partage d'informations implique le traitement de données à caractère personnel, ce partage devrait être limité aux types de données à caractère personnel que les prestataires de services de paiement peuvent traiter aux fins du contrôle des opérations conformément au présent règlement. Toutefois, les caractéristiques environnementales et comportementales, qui sont propres à l'utilisateur de services de paiement dans des conditions d'utilisation normale des données de sécurité personnalisées, ne devraient pas être partagées. Les données partagées devraient porter sur des opérations de paiement spécifiques pour lesquelles le prestataire de services de paiement a des soupçons de fraude, et non sur des opérations antérieures ou ultérieures liées. Les prestataires de services de paiement devraient également partager les raisons objectivement justifiées qui ont conduit à soupçonner une activité frauduleuse en ce qui concerne cette opération de paiement particulière et, lorsque cette opération de paiement est associée à un élément d'information potentiellement frauduleux stocké par un fournisseur de services d'hébergement, les informations concernant la notification faite à ce fournisseur.

(146) Le partage d'informations devrait être soumis à des garanties solides à la pointe de la technologie en matière de confidentialité, de protection des données et d'utilisation des informations, telles que la pseudonymisation et le chiffrement, l'accès et le contrôle exercé par les utilisateurs, et devrait être conforme au règlement (UE) 2016/679. 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 dudit règlement. 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 également définir les rôles et les responsabilités de tous les prestataires de services de paiement concernés conformément aux règles en matière de protection des données, y compris en cas de responsabilité conjointe du traitement.

(147) Les prestataires de services de paiement sont en mesure d'échanger des données relatives à des opérations de paiement, lorsqu'il y a suspicion de fraude, avec d'autres participants à des partenariats en matière de partage d'informations établis conformément à l'article 75 du règlement (UE) 2024/1624, y compris des autorités compétentes telles que les cellules de renseignement financier, les autorités de surveillance et toute autorité publique chargée de mener des enquêtes ou des poursuites pénales concernant le blanchiment de capitaux, les infractions sous-jacentes ou le financement du terrorisme, ou de procéder au dépistage, à la saisie ou au gel et à la confiscation des avoirs d'origine criminelle, en conformité avec les droits fondamentaux et les garanties procédurales juridictionnelles. Les prestataires de services de paiement sont également en mesure de partager avec d'autres prestataires de services de paiement et d'autres participants, y compris les autorités publiques, des données relatives aux menaces pesant sur la sécurité de leurs systèmes de TIC, y compris lorsque l'usurpation d'identité, l'hameçonnage et les logiciels malveillants sont utilisés pour commettre une fraude à l'encontre d'utilisateurs de services de paiement, dans le cadre de dispositifs de partage d'informations et de renseignements sur les cybermenaces établis en vertu de l'article 45 du règlement (UE) 2022/2554. Étant donné que ces partenariats ou dispositifs fournissent déjà des cadres adéquats pour la participation des autorités publiques, y compris les autorités répressives, au partage volontaire de données relatives à la fraude, sous réserve de garanties suffisantes, il n'est pas jugé nécessaire de créer un régime supplémentaire pour cet échange au titre du présent règlement.

(148) Lorsqu'un prestataire de services de paiement participe à des partenariats ou à des dispositifs de partage d'informations établis conformément à l'article 75 du règlement (UE) 2024/1624 et à l'article 45 du règlement (UE) 2022/2554, et lorsque ces partenariats ou dispositifs de partage d'informations permettent au prestataire de services de paiement d'échanger les données nécessaires afin de détecter et de prévenir les fraudes conformément au présent règlement, le partage de données dans le cadre de ces partenariats en matière de partage d'informations devrait être considéré comme suffisant pour garantir le respect par le prestataire de services de paiement des obligations qui lui incombent au titre du présent règlement en ce qui concerne le partage de données relatives à la fraude aux paiements dans le cadre de dispositifs de partage d'informations. Lorsque les prestataires de services de paiement participent à ces partenariats ou dispositifs de partage d'informations afin de respecter leurs obligations au titre du présent règlement, ils devraient être autorisés à traiter les données à caractère personnel échangées dans le cadre de ces partenariats ou dispositifs aux fins du respect des obligations en matière de surveillance des opérations énoncées dans le présent règlement.

(149) 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 pourrait entraîner la divulgation de données à caractère personnel, y compris d'identifiants uniques de bénéficiaires potentiellement impliqués dans des virements frauduleux, ne devraient être utilisées par les prestataires de services de paiement qu'aux fins de l'amélioration de la surveillance 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 de comptes de paiement sans enquête approfondie.

(150) Lors de l'élaboration de mesures visant à lutter contre la fraude dans le domaine des services de paiement, il est particulièrement important de mener des consultations appropriées avec les parties prenantes concernées afin d'échanger les bonnes pratiques et de partager les expériences. Ces consultations devraient s'appuyer sur les contributions d'experts des secteurs public et privé ayant des connaissances et une expérience avérées dans les domaines concernés. À cette fin, la Commission devrait mettre en place une plateforme de lutte contre la fraude. La plateforme de lutte contre la fraude devrait être composée d'experts et peut comprendre, par exemple, des représentants des organes compétents de l'Union, des autorités nationales compétentes, des prestataires de services de paiement, des prestataires de services techniques, des fournisseurs de plateformes en ligne, des opérateurs de télécommunications, des fournisseurs de services Internet, des experts représentant différents systèmes ou schémas de paiement, des commerçants, des organisations de consommateurs et des organismes de résolution des litiges.

(151) La plateforme de lutte contre la fraude devrait être constituée dans le respect des règles horizontales applicables à la création et au fonctionnement des groupes d'experts de la Commission, y compris en ce qui concerne le processus de sélection. Ce dernier devrait avoir pour objet d'assurer un niveau élevé d'expertise, un équilibre géographique et un équilibre entre les hommes et les femmes, ainsi qu'une représentation équilibrée du savoir-faire et de l'expérience pertinents, compte tenu des tâches spécifiques de la plateforme de lutte contre la fraude. Lors du processus de sélection, il convient que la Commission procède à une évaluation, conformément à ces règles horizontales, pour déterminer la présence éventuelle de conflits d'intérêts chez les candidats à la sélection, et qu'elle prenne les mesures appropriées pour les résoudre.

(152) La plateforme de lutte contre la fraude devrait conseiller la Commission sur l'élaboration et le suivi de la mise en œuvre d'actes juridiques visant à lutter contre la fraude dans le domaine des services de paiement. Aux fins de l'élaboration d'un code de conduite volontaire visant à favoriser la prévention, renforcer la sécurité et lutter contre la fraude aux paiements et les escroqueries financières, la plateforme de lutte contre la fraude devrait adresser des recommandations à la Commission et au comité européen des services numériques. La plateforme de lutte contre la fraude devrait également partager des informations et analyser les tendances en matière de fraude dans le domaine des services de paiement, et partager des informations sur les mesures de lutte contre la fraude dans le domaine des services de paiement, y compris les mesures d'atténuation, ainsi que sur la manière d'améliorer la coopération transfrontière et intersectorielle relative aux moyens de lutter contre la fraude dans le domaine des services de paiement. La plateforme de lutte contre la fraude devrait s'acquitter de ses tâches dans le respect du principe de transparence. Elle devrait également tenir compte des travaux des initiatives existantes visant à lutter contre la fraude aux paiements, en évitant les doubles emplois, et travailler en étroite collaboration avec elles.

(153) 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 appropriées sur la fraude, en 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 être encouragée à élaborer des orientations sur les différents programmes que les prestataires de services de paiement doivent mettre au point concernant les risques de fraude aux paiements, en tenant compte de l'évolution constante de la nature des risques liés à la fraude, lorsqu'elle le juge nécessaire pour assurer la cohérence de ces programmes dans l'ensemble de l'Union.

(154) La sensibilisation aux menaces de fraude est essentielle pour renforcer le niveau de protection des utilisateurs de services de paiement contre ces menaces, et donc leur niveau de confiance dans l'utilisation des services de paiement dans l'ensemble de l'Union, compte tenu notamment de l'évolution rapide des techniques et des stratégies déployées par les fraudeurs. Les États membres peuvent jouer un rôle crucial pour développer, au niveau collectif, la sensibilisation et la préparation des citoyens à cet égard, au-delà des informations individuelles fournies par les prestataires de services à leurs clients. La directive (UE) 2022/2555 impose déjà aux États membres d'élaborer des stratégies nationales en matière de cybersécurité, dans le cadre desquelles des politiques spécifiques devraient être adoptées dans le but de promouvoir et de développer l'éducation et la formation en matière de cybersécurité, les compétences en matière de cybersécurité, les initiatives de sensibilisation et de recherche et développement en matière de cybersécurité, ainsi que d'orientations sur les bonnes pratiques de cyberhygiène et les contrôles en la matière, visant à renforcer le niveau de sensibilisation et de préparation des citoyens, des parties prenantes et des entités face aux risques en matière de cybersécurité, y compris les techniques utilisées pour commettre des fraudes, telles que l'hameçonnage, l'usurpation d'identité, les logiciels malveillants et d'autres formes d'ingénierie sociale. En outre, la directive (UE) 2019/713 impose aux États membres d'adopter ou de renforcer un ensemble de mesures destinées à prévenir la fraude et la contrefaçon des moyens de paiement autres que les espèces, et des initiatives visant à réduire le risque que de telles infractions se produisent, y compris des tentatives de fraude au moyen, par exemple, de l'hameçonnage et de la copie, par des campagnes d'information et de sensibilisation et des programmes d'éducation. Conformément aux obligations qui leur incombent en vertu de ces directives, les États membres devraient élaborer et tenir à jour des mesures permanentes et adéquates pour sensibiliser davantage le public aux schémas existants et émergents de fraude aux paiements, aux procédures à suivre conformément au présent règlement afin de détecter et de signaler les tentatives de fraude et aux droits et obligations des utilisateurs de services de paiement en ce qui concerne la fraude au titre du présent règlement. Les États membres devraient informer la Commission des mesures adoptées.

(155) Les États membres devraient veiller à ce qu'un financement suffisant soit disponible pour ces mesures de sensibilisation et d'éducation, et à ce qu'elles soient correctement ciblées, en particulier pour répondre aux besoins et aux intérêts des groupes de consommateurs vulnérables, y compris les jeunes, les personnes âgées et les personnes ayant des compétences numériques limitées. Les prestataires de services de paiement, les fournisseurs de services de communications interpersonnelles au sens de la directive (UE) 2018/1972 du Parlement européen et du Conseil[33] et les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient coopérer avec les États membres à l'élaboration et à la mise à jour de ces campagnes de sensibilisation à la fraude, y compris en fournissant des informations sur les menaces et les schémas de fraude recensés dans leurs services, ainsi que de bonnes pratiques en matière de sensibilisation des utilisateurs. Cette coopération devrait être gratuite, dans des conditions raisonnables et proportionnées.

(156) 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.

---

33 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, ELI: http://data.europa.eu/eli/dir/2018/1972/oj).

(157) Les exigences relatives à l'authentification forte du client ne devraient pas être modifiées de manière substantielle par rapport aux exigences existantes au titre de la directive (UE) 2015/2366. L'authentification forte du client continuera de reposer sur deux éléments ou plus, appartenant aux catégories "connaissance", "possession" et "inhérence" et indépendants les uns des autres. La catégorie "inhérence" concerne les propriétés physiques des parties du corps, les caractéristiques physiologiques et les processus comportementaux créés par le corps, ainsi que toute combinaison de ceux-ci. Au moins deux des éléments utilisés doivent provenir de catégories différentes. Afin de permettre des innovations dans les technologies d'authentification, une exception à ce principe permet l'utilisation de deux éléments de la catégorie "inhérence", lorsque cela ne diminue pas le niveau de sécurité. Afin de garantir un niveau élevé de sécurité et l'application uniforme de cette exception par les autorités nationales compétentes, l'ABE devrait élaborer des orientations sur la manière d'évaluer l'indépendance des deux éléments dans de tels cas.

(158) L'authentification forte du client ne devrait pas être contournée, en particulier 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 opérations fondées sur 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 de 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 opérations fondées sur des ordres de paiement passés par courrier ou par téléphone, seule la passation de l'ordre de paiement, et non son authentification ni son exécution, devrait être non numérique pour qu'une opération soit considérée comme fondée sur 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. En ce sens, une opération de paiement liée à une carte pourrait être considérée comme une opération fondée sur un ordre de paiement passé par courrier ou par téléphone si la passation de l'ordre de paiement a lieu de manière non électronique, par exemple lorsque les données de paiement sont transmises par le titulaire de la carte à un commerçant par des canaux non électroniques. 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 prestataire de services d'acquisition d'opérations de paiement établi en dehors de l'Union en vue d'échapper aux exigences en matière d'authentification forte du client.

(159) 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, à l'exclusion du droit inconditionnel au remboursement, qui devrait s'appliquer uniquement aux prélèvements.

(160) Afin d'établir des conditions de concurrence équitables entre les différents instruments de paiement, il devrait être possible d'initier un ou plusieurs virements récurrents, y compris de montants variables, sans obligation d'authentification forte du client lorsque ces virements sont initiés par le prestataire de services de paiement du payeur à la suite d'une demande du bénéficiaire, pour autant que certaines conditions cumulatives soient remplies. En particulier, cela devrait être possible lorsque la demande du bénéficiaire est fondée sur l'accord du bénéficiaire avec le payeur qui fixe les conditions relatives à la fréquence des paiements et aux montants à payer, lorsque le payeur conclut avec son prestataire de services de paiement un accord qui est soumis à une authentification forte du client et qui donne pour instruction au prestataire d'exécuter les virements respectifs conformément à l'accord du payeur avec le bénéficiaire, et lorsque l'initiation des virements respectifs par le prestataire de services de paiement du payeur ne nécessite aucune action supplémentaire de la part du payeur. Afin d'assurer des garanties équivalentes, les dispositions relatives aux remboursements et aux demandes de remboursement applicables aux opérations de paiement initiées par un bénéficiaire ou par son intermédiaire devraient s'appliquer aux virements relevant du présent cadre dans les mêmes conditions que celles applicables aux opérations initiées par des commerçants. En outre, afin de promouvoir une innovation sans entrave et d'accélérer l'accroissement de la disponibilité de modes de paiement efficaces pour les payeurs et les bénéficiaires au point d'interaction, il est nécessaire de permettre l'initiation d'un ou plusieurs virements récurrents au titre de ce cadre à compter de la date d'entrée en vigueur du présent règlement.

(161) Afin d'améliorer l'inclusion financière, et conformément à la directive (UE) 2019/882, tous les utilisateurs de services de paiement, y compris les personnes handicapées, les personnes âgées, les personnes ayant des compétences numériques limitées 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 parce qu'ils n'étaient pas en mesure 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 soient adaptées à leurs besoins et à leur situation. Ces méthodes devraient être gratuites et ne devraient pas imposer l'utilisation d'une seule technologie, d'un seul dispositif ou mécanisme, ni la possession d'un téléphone intelligent (smartphone) ou d'un autre dispositif intelligent.

(162) Les portefeuilles européens d'identité numérique mis en œuvre dans le cadre du règlement (UE) nº 910/2014 du Parlement européen et du Conseil[34] 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 vise à rendre encore plus aisées l'identification et l'authentification numériques transfrontières pour les paiements numériques sécurisés et à faciliter le développement d'un paysage paneuropéen des paiements numériques. Conformément à l'article 5 *septies*, paragraphe 2, du règlement (UE) nº 910/2014, les prestataires de services de paiement seront dans l'obligation d'accepter l'utilisation des portefeuilles européens d'identité numérique pour permettre le respect des exigences en matière d'authentification forte du client pour l'identification en ligne à des fins de connexion au compte et d'initiation d'opérations dans le domaine des services de paiement. L'ABE devrait être chargée d'élaborer des normes techniques de réglementation qui devraient tenir spécifiquement compte de l'utilisation des portefeuilles européens d'identité numérique pour permettre le respect des exigences en matière d'authentification forte du client aux fins susmentionnées.

(163) La croissance du commerce électronique et des paiements par téléphone mobile devrait aller de pair avec un renforcement généralisé des mesures de sécurité. Dans les cas d'initiation à distance d'une opération de paiement, à savoir 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 de services de paiement soit à tout moment conscient du montant du paiement et du bénéficiaire de l'opération que l'utilisateur de services de paiement autorise.

---

[34] 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, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(164) 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 les opérations, 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.

(165) L'établissement d'un lien dynamique permet de parer au risque de falsification du nom du bénéficiaire et du montant donné de l'opération entre le moment où un ordre de paiement est passé et l'authentification du paiement, 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. Par conséquent, les prestataires de services de paiement devraient également appliquer des éléments qui établissent un lien dynamique entre, d'une part, les opérations et, d'autre part, un montant et un bénéficiaire donnés 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.

(166) 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 surveillance 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, fournissant davantage de détails et de meilleures définitions concernant les exigences en matière de suivi des risques et les données à partager, et 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 par conséquent élaborer des projets de normes techniques de réglementation établissant des règles relatives à l'analyse des risques liés aux opérations.

(167) 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 ou les opérations de paiement initiées par des personnes morales, que ces paiements soient ou non effectués par 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 est nécessaire afin de limiter les risques d'usurpation d'identité, d'hameçonnage 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.

(168) 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.

(169) Les acteurs du marché des différents États membres ne comprennent pas tous 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 en matière de paiements ou de toute autre utilisation frauduleuse. 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 pertinent.

(170) Les opérateurs de portefeuilles numériques "pass-through" 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 de pouvoir continuer à effectuer ces vérifications, tout en étant tenus de se conformer aux obligations 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 numériques "pass-through", 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.

(171) 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 du préjudice financier direct causé aux bénéficiaires ou aux prestataires de services de paiement des bénéficiaires ou des payeurs pour ne pas avoir fourni, dans le cadre de leur relation contractuelle, les services nécessaires pour permettre l'application d'une authentification forte du client, de façon proportionnée à ce manquement et pour un montant n'excédant pas le montant de l'opération en question.

(172) Les États membres devraient veiller à ce que les autorités compétentes désignées par les États membres en vertu de l'article 18 de la directive 2013/11/UE du Parlement européen et du Conseil[35] exercent les fonctions énoncées aux articles 19 et 20 de ladite directive en ce qui concerne les entités de règlement des litiges établies sur leur territoire, qui entendent prétendre à la qualité d'entités de règlement extrajudiciaire des litiges pour le règlement des litiges concernant les droits et obligations prévus par le présent règlement.

(173) Les autorités compétentes devraient avoir le pouvoir de demander des informations aux fournisseurs de services intermédiaires au sens du règlement (UE) 2022/2065 qui contribuent au fonctionnement de services de paiement non autorisés, ainsi que de leur donner pour instruction de bloquer ou de restreindre l'accès aux sites internet hébergés par des opérateurs de services de paiement non autorisés. Afin de protéger temporairement les fonds et autres actifs des clients, ce pouvoir devrait déjà être disponible au stade de l'enquête lorsqu'il existe une suspicion raisonnable fondée sur des faits justifiant l'hypothèse selon laquelle des opérations commerciales non autorisées ont lieu.

---

[35] 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, ELI: http://data.europa.eu/eli/dir/2013/11/oj).

(174) Sans préjudice du droit de recours juridictionnel des consommateurs, les États membres devraient veiller à ce qu'il existe des procédures de règlement extrajudiciaire des litiges aisément accessibles, adéquates, indépendantes, impartiales, transparentes et efficaces entre les prestataires de services de paiement et les utilisateurs de services de paiement. Le règlement (CE) nº 593/2008 du Parlement européen et du Conseil[36] 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, pour régler les litiges avant la saisine d'une juridiction. Pour les litiges contractuels entre consommateurs et entreprises concernant l'achat de biens ou de services, la directive 2013/11/UE garantit l'accès, pour les consommateurs et les entreprises de l'Union, à des entités de règlement extrajudiciaire des litiges dont la qualité est certifiée et qui respectent les exigences de qualité énoncées dans la directive 2013/11/UE. La participation à des procédures de règlement extrajudiciaire des litiges pour le règlement des litiges entre prestataires de services de paiement et consommateurs concernant les droits et obligations prévus par le présent règlement devrait être obligatoire pour les prestataires de services de paiement. Cela permettrait aux consommateurs, qui ne disposent pas des mêmes moyens et ressources que les personnes morales pour faire valoir leurs droits au titre du présent règlement, d'avoir accès à des moyens de mise en œuvre plus rapides et moins coûteux. Toutefois, les consommateurs ne devraient pas être contraints de participer à de telles procédures de règlement extrajudiciaire des litiges.

---

[36] Règlement (CE) nº 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome I) (JO L 177 du 4.7.2008, p. 6, ELI: http://data.europa.eu/eli/reg/2008/593/oj).

(175) Le droit à un recours effectif et le droit à un procès équitable sont des droits fondamentaux prévus à l'article 47 de la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée "Charte"). C'est pourquoi les procédures de règlement extrajudiciaire des litiges ne devraient pas être conçues pour se substituer aux procédures juridictionnelles et ne sauraient priver les consommateurs ou les professionnels de leur droit à former un recours devant les tribunaux. Le présent règlement ne saurait empêcher les parties d'exercer leur droit d'accès au système judiciaire. Dans les cas où un litige n'a pas pu être résolu en passant par une procédure de règlement extrajudiciaire des litiges donnée dont l'issue n'est pas contraignante, il convient de ne pas empêcher les parties d'engager par la suite une action en justice en rapport avec ce litige. Les États membres devraient être libres de choisir les moyens appropriés pour atteindre cet objectif. Ils devraient avoir la possibilité de prévoir, entre autres, que les délais de prescription n'expirent pas pendant une procédure de règlement extrajudiciaire des litiges.

(176) Les consommateurs devraient être autorisés à faire respecter leurs droits en lien avec les obligations imposées aux prestataires de services de paiement dans le cadre du présent règlement, au moyen d'actions représentatives conformément à la directive (UE) 2020/1828 du Parlement européen et du Conseil[37].

[37] Directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 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, ELI: http://data.europa.eu/eli/dir/2020/1828/oj).

(177) Il convient d'instaurer des procédures appropriées pour donner suite aux réclamations introduites contre 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 appropriées, effectives, proportionnées et dissuasives soient infligées. Afin de garantir le respect effectif du présent règlement, les États membres devraient désigner des autorités compétentes qui remplissent les conditions fixées par le règlement (UE) nº 1093/2010 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 notamment lui communiquer une description précise des missions de ces autorités.

(178) Étant donné que certaines dispositions de la directive (UE) 2015/2366, telles que celles relatives à la transparence ex ante des coûts et au délai d'exécution, ont été conçues en gardant à l'esprit les paiements électroniques traditionnels et ne tenaient pas compte des caractéristiques spécifiques de l'utilisation de la technologie des registres distribués ou d'une technologie similaire pour les opérations de paiement effectuées au moyen de jetons de monnaie électronique, il importe de préciser si ces exigences s'appliquent aux opérations de paiement effectuées au moyen de jetons de monnaie électronique, et d'introduire des dispositions transitoires à cet égard.

(179) Il est nécessaire de faire converger davantage les pouvoirs dont disposent les autorités compétentes, en vue de tendre vers une intensité équivalente de l'exécution des règles à l'intérieur du marché des paiements intégré. Les autorités compétentes devraient se voir attribuer tous les pouvoirs de surveillance, d'enquête et de sanction nécessaires pour garantir le respect du présent règlement. Le présent règlement devrait donc établir un ensemble minimal commun de pouvoirs que les autorités compétentes devraient se voir confier, assorti de ressources suffisantes pour garantir l'efficacité de la surveillance. Afin de protéger les consommateurs et de garantir une information adéquate du marché à tout moment, les autorités compétentes devraient être habilitées à adopter des mesures de surveillance en temps utile, telles que la suspension ou l'interdiction de la fourniture, de la commercialisation et de la publicité de services, ou la publication d'avis au public pour avertir ce dernier d'une infraction réelle ou présumée au présent règlement. Les autorités compétentes devraient faire usage de ces pouvoirs en particulier lorsque l'infraction prend la forme de services de paiement non autorisés, d'informations fausses ou trompeuses diffusées par l'intermédiaire du marché des paiements et, plus généralement, lorsqu'un prestataire de services de paiement ou un tiers participant à la fourniture de services de paiement a manqué aux obligations qui lui incombent au titre du présent règlement. Lorsque des informations publiées par les autorités compétentes au moyen d'avis au public semblent erronées ou incomplètes ou que leurs circonstances sous-jacentes sont inexactes, les autorités compétentes devraient les rectifier rapidement par les mêmes canaux de communication que ceux utilisés pour informer le public.

(180) Dans l'environnement numérique, les autorités compétentes devraient être en mesure de mettre fin rapidement et efficacement aux infractions au présent règlement, notamment lorsque l'auteur de l'infraction dissimule son identité ou se déplace à l'intérieur de l'Union ou dans un pays tiers afin d'échapper à la loi. En cas de risque de préjudice grave pour les intérêts des consommateurs, les autorités compétentes devraient pouvoir adopter des mesures provisoires, y compris retirer un contenu d'une interface en ligne ou ordonner qu'un message d'avertissement s'affiche clairement lorsque les consommateurs accèdent à une interface en ligne. Lesdites mesures ne devraient pas excéder ce qui est nécessaire pour atteindre l'objectif consistant à faire cesser ou interdire l'infraction au présent règlement.

(181) 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 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.

(182) Les États membres devraient être tenus de prévoir des sanctions administratives et des 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.

(183) 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.

(184) Lorsqu'elles imposent des sanctions administratives et des mesures administratives, les autorités compétentes devraient tenir compte de toute sanction pénale antérieure 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. Le but est de faire en sorte que la sévérité des sanctions et autres mesures administratives imposées à des fins punitives, en cas de cumul de poursuites administratives et de poursuites pénales, soit limitée à ce qui est nécessaire au regard de la gravité de l'infraction en question.

(185) Un système de surveillance efficace exige que les autorités de surveillance soient conscientes de toute lacune dans le respect des règles énoncées dans le présent règlement par les prestataires de services de paiement. Il importe donc que les autorités de surveillance puissent s'informer mutuellement des sanctions administratives et mesures administratives imposées aux prestataires de services de paiement lorsque ces informations sont également utiles à d'autres autorités de surveillance.

(186) 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 et d'autres autorités chargées de faire respecter la loi. Les États membres devraient veiller à ce que leurs cadres juridiques permettent et facilitent 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 des échanges d'informations ainsi qu'une assistance mutuelle en vue de l'application effective des sanctions administratives et des mesures administratives, en particulier dans le cadre du recouvrement transfrontalier des sanctions pécuniaires.

(187) Indépendamment de leur désignation en droit national, des formes de procédures d'exécution accélérées ou d'accords transactionnels existent dans de nombreux États membres et sont utilisées comme alternative à une procédure formelle en vue de parvenir à une adoption plus rapide d'une décision imposant une sanction administrative ou une mesure administrative ou pour mettre fin à l'infraction alléguée en question et à ses conséquences avant qu'une procédure formelle de sanction soit engagée. En raison des approches juridiques très variées adoptées au niveau national, 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 les États membres. Néanmoins, il convient de reconnaître que ces méthodes permettent aux autorités compétentes qui peuvent les mettre en œuvre de traiter les dossiers d'infraction de manière plus rapide, moins coûteuse et globalement plus 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 d'exécution dans leurs cadres juridiques ni de contraindre les autorités compétentes à y recourir si elles ne le jugent pas approprié.

(188) Les États membres ont mis en place et prévoient actuellement tout un éventail de sanctions administratives et de mesures administratives en cas d'infraction aux principales dispositions du droit de l'Union régissant la prestation de services de paiement, d'où un manque de cohérence entre les approches choisies en ce qui concerne les enquêtes sur les violations de ces dispositions et les sanctions en la matière. Le fait de ne pas définir plus clairement quelles dispositions essentielles doivent déclencher des mesures d'exécution suffisamment dissuasives dans chaque État membre irait à l'encontre de la réalisation du marché unique des services de paiement et risque d'encourager le "forum shopping" dans la mesure où les autorités compétentes sont inégalement équipées pour réprimer rapidement et avec le même effet dissuasif les infractions à ces dispositions.

(189) Étant donné que l'objet des astreintes, qui sont appliquées conformément au droit national, est de contraindre les personnes physiques ou morales qui sont identifiées comme responsables d'une infraction au droit de l'Union en cours ou qui se voient imposer de se conformer à une injonction d'une 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 ou d'autres mesures administratives en raison de la même infraction.

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

(191) Les autorités compétentes devraient être habilitées par les États membres à imposer des sanctions administratives et des mesures administratives aux prestataires de services de paiement ou à d'autres personnes physiques ou morales, s'il y a lieu, afin de remédier aux infractions au présent règlement. L'éventail des sanctions et mesures dont disposent les autorités compétentes 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.

(192) La publication d'une sanction administrative ou d'une mesure administrative pour infraction aux dispositions du présent règlement peut avoir un effet très dissuasif sur la récidive. La publication permet en outre 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, et 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 exerce ses activités sur leur territoire dans un contexte transfrontalier. Pour ces raisons, la publication des décisions relatives aux sanctions administratives et aux mesures administratives, ainsi que des informations sur le droit de recours contre celles-ci et l'issue d'un tel recours, devrait être autorisée pour autant qu'elle concerne des personnes morales. Lorsqu'elles décident de publier ou non 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, lorsqu'une publication de ce type fait référence à des personnes physiques, elle peut empiéter de manière disproportionnée sur leurs droits découlant de la Charte 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 que la publication de décisions contenant des données à caractère personnel est nécessaire 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.

(193) 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 convient 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.

(194) 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 ce qui est de compléter le présent règlement en précisant davantage les informations relatives aux frais devant être communiquées par les schémas de cartes de paiement et les entités de traitement aux prestataires de services d'acquisition d'opérations de paiement; de mettre à jour le montant à concurrence duquel un payeur peut être tenu de supporter des pertes liées à une opération de paiement non autorisée résultant d'une perte, d'un vol ou du détournement d'un instrument de paiement ou de données de sécurité personnalisées; d'adapter les règles applicables aux opérations de paiement effectuées au moyen de jetons de monnaie électronique en tenant compte de l'évolution des technologies et des marchés; et de préciser les critères et facteurs que l'ABE doit prendre en compte pour déterminer certaines conditions liées aux pouvoirs d'intervention temporaire. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 "Mieux légiférer"[38]. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

---

38 JO L 123 du 12.5.2016, p. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

(195) 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.

(196) 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 dont il est établi qu'il est susceptible de léser les consommateurs, menaçant ainsi le bon fonctionnement et l'intégrité des marchés financiers. Il y a donc lieu de modifier le règlement (UE) nº 1093/2010 en conséquence.

(197) Afin de faciliter la coopération transfrontalière pour ce qui concerne l'exécution du présent règlement, il convient de modifier l'annexe du règlement (UE) 2017/2394 du Parlement européen et du Conseil[39] pour y insérer une référence au présent règlement.

---

[39] 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, ELI: http://data.europa.eu/eli/reg/2017/2394/oj).

(198) 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 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.

(199) Étant donné que le présent règlement et la directive (UE) 2026/...[+] fixent le cadre juridique régissant la prestation de services de paiement 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) 2026/...[+]. 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 du ... [27 mois à compter de la date d'entrée en vigueur du présent règlement], laissant ainsi 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.

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

(200) 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 sept 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 («open banking»), la proposition de solutions supplémentaires pour lutter contre la fraude et l'adéquation et l'impact des règles sur l'étendue des situations dans lesquelles un consommateur dispose d'un droit au remboursement pour des opérations autorisées. Toutefois, en ce qui concerne d'autres questions, à savoir les pratiques tarifaires pour les services de paiement, les obligations imposées aux fournisseurs de services de communications électroniques et aux fournisseurs de services d'hébergement en matière de prévention de la fraude aux paiements, le champ d'application du présent règlement, ainsi que l'adéquation et l'impact des règles énoncées dans le présent règlement en ce qui concerne les opérations de paiement effectuées au moyen de jetons de monnaie électronique, il convient qu'un réexamen ait lieu avant le... [sept ans après la date d'entrée en vigueur du présent règlement], compte tenu de l'importance fondamentale que revêtent ces questions pour le fonctionnement d'un marché des paiements compétitif, innovant et sûr au sein de l'Union. 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.

(201) Compte tenu de l'importance croissante des IBAN virtuels utilisés à des fins commerciales légitimes au sein de l'Union, il est essentiel de renforcer la sécurité juridique et de garantir le respect du règlement (UE) nº 260/2012. Il est donc nécessaire de préciser que les IBAN virtuels sont soumis aux mêmes règles que les IBAN, qui contiennent les éléments indiqués par l'ISO. Il convient, dès lors, de modifier le règlement (UE) nº 260/2012 en conséquence. De plus, les IBAN virtuels sont autorisés en tant qu'identifiants de compte de paiement valides lorsque l'utilisation d'un IBAN est requise. Compte tenu, d'une part, des risques et des défis posés par les IBAN virtuels, y compris du point de vue de la lutte contre le blanchiment de capitaux et le financement du terrorisme, et, d'autre part, de leurs avantages, la Commission devrait présenter au Parlement européen, au Conseil, à la BCE et au Comité économique et social européen un rapport examinant la nécessité d'introduire de nouvelles mesures réglementant les IBAN virtuels au niveau de l'Union et, le cas échéant, accompagner ce rapport d'une proposition législative.

(202) Conformément aux principes d'amélioration de la réglementation, le présent règlement devrait être réexaminé du point de vue de l'adéquation et de l'incidence des règles énoncées aux titres II et III du présent règlement en ce qui concerne les opérations de paiement effectuées au moyen de jetons de monnaie électronique. Dans le cadre de son réexamen, la Commission devrait évaluer si, compte tenu de l'évolution de la situation, il serait souhaitable d'étendre les exigences du présent règlement relatives à la vérification du bénéficiaire et à la banque ouverte («open banking») aux opérations de paiement effectuées en jetons de monnaie électronique.

(203) Le présent règlement respecte les droits fondamentaux et observe les principes reconnus par la Charte, y compris 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.

(204) Les références à des montants en euros faites dans le présent règlement s'entendent comme la contre-valeur en monnaie nationale définie par chaque État membre dont la monnaie n'est pas l'euro. Les références à des opérations de paiement en euros ou dans d'autres monnaies s'entendent comme des opérations de paiement avec des fonds libellés en euros ou dans d'autres monnaies, y compris des jetons de monnaie électronique libellés en euros ou dans d'autres monnaies.

(205) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 et a rendu un avis le 22 août 2023[40],

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

[40] JO C, C/2023/1019, 16.11.2023, ELI: http://data.europa.eu/eli/C/2023/1019/oj.

TITRE I

OBJET, CHAMP D'APPLICATION ET DÉFINITIONS

Article premier

Objet

1. Le présent règlement établit des règles uniformes applicables à la prestation de services de paiement en ce qui concerne:

   a) la transparence des conditions et des exigences en matière d'information;

   b) les droits et obligations respectifs des utilisateurs de services de paiement et des prestataires de services de paiement.

2. Sauf indication contraire, toute référence aux services de paiement faite dans le présent règlement s'entend comme désignant tout service de paiement visé à l'annexe I de la directive (UE) 2026/...[+].

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

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 tels qu'ils sont définis à l'article 4, paragraphe 1, point 1), du règlement (UE) nº 575/2013 du Parlement européen et du Conseil[41], y compris leurs succursales lorsque celles-ci sont situées dans l'Union, que l'administration centrale de ces succursales 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;

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 et leurs autorités régionales ou locales lorsqu'ils n'agissent pas en qualité d'autorités publiques.

---

41 Règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et modifiant le règlement (UE) n° 648/2012 (JO L 176 du 27.6.2013, p. 1, ELI: http://data.europa.eu/eli/reg/2013/575/oj).

2. Le présent règlement s'applique également aux services fournis au sein de l'Union par les entités suivantes:

a) les prestataires de services techniques, aux fins de l'article 23, paragraphe 2, et des articles 59, 94, 96, 97, 101 et 103;

b) les opérateurs de systèmes de paiement et les opérateurs de schémas de paiement, aux fins des articles 31, 84, 101 et 103, les opérateurs de schémas de paiement, y compris les schémas de cartes de paiement, aux fins de l'article 59 et les opérateurs de schémas de cartes de paiement et les entités de traitement aux fins de l'article 32;

c) les fournisseurs de services de communications interpersonnelles, aux fins des articles 61, 90, 96, 101 et 103;

d) les fournisseurs de services de communications électroniques, aux fins de l'article 96;

e) les fournisseurs de services d'hébergement, aux fins des articles 61, 82 et 101;

f) les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne, aux fins des articles 61, 62, 90 et 98;

g) les fabricants d'équipements d'origine d'appareils mobiles, aux fins de l'article 96.

3. Le présent règlement ne s'applique pas:

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

b) aux opérations de paiement effectuées exclusivement en jetons de monnaie électronique et allant directement du payeur au bénéficiaire, sans l'intervention d'un intermédiaire;

c) aux opérations de paiement allant du payeur au bénéficiaire, par l'intermédiaire d'un agent commercial, sous réserve que 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 uniquement pour le compte du payeur ou uniquement pour le compte du bénéficiaire, mais pas des deux; et

   ii) cet accord confère à l'agent commercial la possibilité concrète de négocier avec le payeur ou le bénéficiaire ou de conclure la vente ou l'achat de biens ou de services;

d) 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;

e) aux services pour lesquels des espèces sont fournies par le bénéficiaire au 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 ladite opération de paiement;

f) aux services pour lesquels des commerces de détail acceptent de fournir des espèces 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 ou de services;

g) 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 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 qui n'est pas partie à la convention de Genève du 19 mars 1931 portant loi uniforme sur les chèques;

iii) une traite sur support papier visée dans 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 qui n'est pas 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 ou des bons physiques de nature similaire;

vi) un chèque de voyage sur support papier;

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

h) 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, des banques centrales ou d'autres participants au système, et des prestataires de services de paiement, sans préjudice de l'article 31;

i) aux opérations de paiement liées au service d'actifs et de titres, y compris la distribution de dividendes, de revenus ou autres, le remboursement ou la vente, effectuées par les personnes visées au point h) 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;

j) aux opérations de paiement effectuées par un prestataire de services sur crypto-actifs qui sert d'intermédiaire entre un acheteur et un vendeur lorsque des jetons de monnaie électronique sont échangés contre d'autres jetons de monnaie électronique ou contre d'autres crypto-actifs, ou à l'échange de jetons de monnaie électronique contre des fonds, y compris des jetons de monnaie électronique, ou contre des crypto-actifs, effectuées par un prestataire de services sur crypto-actifs agissant en son nom propre en tant qu'acheteur ou vendeur de ces jetons de monnaie électronique;

k) aux services reposant sur des instruments de paiement spécifiques, y compris des instruments basés sur la monnaie électronique, qui satisfont à l'une des conditions suivantes:

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

   ii) des instruments ne pouvant être utilisés que pour acquérir un éventail très limité de biens ou de services, y compris des instruments dont l'utilisation est limitée aux opérations entre utilisateurs de services de paiement qui ne sont pas des consommateurs;

iii) des 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 et qui ne peuvent être convertis en espèces;

l) aux opérations de paiement proposées par un fournisseur de réseaux de communications électroniques tels qu'ils sont définis à l'article 2, point 1), de la directive (UE) 2018/1972, ou de services en plus des services de communications électroniques tels qu'ils sont 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

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 60 EUR et que:

– la valeur cumulée des opérations de paiement pour un même abonné ne dépasse pas 360 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 360 EUR par mois;

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

n) aux opérations de paiement effectuées entre des prestataires de services sur crypto-actifs ou leurs succursales pour leur propre compte;

o) 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 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;

p) au transport physique de billets de banque et de pièces à titre professionnel, y compris leur collecte, leur traitement et leur remise;

q) aux opérations de change espèces contre espèces pour lesquelles les fonds ne sont pas détenus sur un compte de paiement.

4. 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.

5. Le titre II, à l'exception de l'article 13, paragraphe 1, point b), de l'article 20, paragraphe 2, point e), et de l'article 24, point a), et le titre III, à l'exception des articles 70 à 76, 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.

6. Le titre II, à l'exception de l'article 13, paragraphe 1, point b), de l'article 20, paragraphe 2, point e), de l'article 20, paragraphe 5, point 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 51, 58, 65, 66 et 70, de l'article 73, paragraphe 1, et des articles 79 et 82, 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.

7. Les États membres peuvent exempter les établissements visés 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.

8. Au plus tard le ... [12 mois à compter de 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 sur l'exclusion du champ d'application du présent règlement des opérations de paiement allant du payeur au bénéficiaire par l'intermédiaire d'un agent commercial visées au paragraphe 3, point c), du présent article.

9. L'ABE élabore des projets de normes techniques de réglementation pour préciser les conditions d'exclusion du champ d'application du présent règlement des services fondés sur des instruments de paiement spécifiques visés au paragraphe 3, point k), du présent article. Lorsqu'elle élabore ces projets de normes techniques de réglementation, l'ABE tient compte de l'expérience acquise dans l'application de ses orientations du 24 février 2022 concernant l'exclusion des réseaux limités du champ d'application de la directive (UE) 2015/2366.

L'ABE soumet les projets de normes techniques de réglementation visées au premier alinéa à la Commission au plus tard le … [12 mois à compter de la date d'entrée en vigueur du présent règlement].

La Commission est habilitée à adopter ces normes techniques de réglementation conformément aux articles 10 à 14 du règlement (UE) nº 1093/2010.

10. Au plus tard le ... [21 mois à compter de la date d'entrée en vigueur du présent règlement], les États membres notifient à la Commission les dispositions législatives qu'ils adoptent en vertu du paragraphe 7. Ils notifient sans retard injustifié à la Commission toute modification ultérieure qui y est apportée et toute disposition législative qu'ils adoptent en vertu du paragraphe 7 à une date ultérieure.

Article 3

Définitions

Aux fins du présent règlement, on entend par:

1) "service de paiement", une ou plusieurs des activités énumérées à l'annexe I de la directive (UE) 2026/...[+] exercées à titre professionnel;

2) "prestataire de services de paiement", une entité visée à l'article 2, paragraphe 1, du présent règlement ou une personne physique ou morale bénéficiant d'une exemption en vertu de l'article 33, ou visé à l'article 35, paragraphe 1, ou à l'article 36, paragraphe 1, de la directive (UE) 2026/…[+];

3) "utilisateur de services de paiement", une personne physique ou morale qui utilise un service de paiement en qualité de payeur ou de bénéficiaire, ou les deux;

4) "consommateur", une personne physique qui, dans le cadre des contrats de services de paiement régis par le présent règlement, agit à des fins qui n'entrent pas dans le cadre de son activité commerciale ou professionnelle;

5) "payeur", une personne physique ou morale qui est titulaire d'un compte de paiement et qui passe ou autorise 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;

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

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

7) "fonds", la monnaie de banque centrale émise pour une utilisation de détail, la monnaie scripturale et la monnaie électronique, y compris les jetons de monnaie électronique;

8) "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;

9) "initiation d'une opération de paiement", les étapes nécessaires pour préparer l'exécution d'une opération de paiement, y compris la passation d'un ordre de paiement et l'achèvement du processus d'authentification;

10) "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;

11) "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;

12) "passation à distance d'un ordre de paiement", la passation d'un ordre de paiement par l'internet;

13) "établissement de paiement", une personne morale qui, conformément à l'article 13 de la directive (UE) 2026/…[+], a obtenu un agrément l'autorisant à fournir des services de paiement dans toute l'Union;

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

14) "établissement de paiement demandeur", une entreprise qui a demandé un agrément conformément à l'article 3 de la directive (UE) 2026/...[+] et à l'égard de laquelle la décision est en attente;

15) "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;

16) "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 détient une succursale, ou fournit des services de paiement;

17) "agent", une personne physique ou morale qui agit au nom et pour le compte d'un établissement de paiement pour la fourniture des services de paiement et qui, soit entre en possession de fonds pour le compte de l'établissement de paiement, soit participe directement à la fourniture de services de paiement par l'établissement de paiement;

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

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

19) "groupe", un groupe d'entreprises qui sont liées entre elles par une relation au sens de l'article 22, paragraphe 1, 2 ou 7, de la directive 2013/34/UE du Parlement européen et du Conseil[42] ou d'établissements visés aux articles 4, 5, 6 et 7 du règlement délégué (UE) nº 241/2014 de la Commission[43] 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;

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

21) "opérateur de système de paiement", l'entité juridique légalement responsable de l'exploitation d'un système de paiement;

22) "prestataire de services techniques", un prestataire fournissant des services qui, sans être des services de paiement, sont à l'appui de la prestation de services de paiement, sans entrer à aucun moment en possession des fonds à transférer;

---

[42] 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, 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, ELI: http://data.europa.eu/eli/dir/2013/34/oj).

[43] Règlement délégué (UE) n° 241/2014 de la Commission du 7 janvier 2014 complétant le règlement (UE) n° 575/2013 du Parlement européen et du Conseil par des normes techniques de réglementation concernant les exigences de fonds propres et d'engagements éligibles applicables aux établissements (JO L 74 du 14.3.2014, p. 8, ELI: http://data.europa.eu/eli/reg_del/2014/241/oj).

23) "fournisseur de services de communications électroniques", un fournisseur de services de communications électroniques tel qu'il est défini à l'article 2, point 4), de la directive (UE) 2018/1972;

24) "fournisseur de services de communications interpersonnelles", un fournisseur de services de communications interpersonnelles tel qu'il est défini à l'article 2, point 5), de la directive (UE) 2018/1972;

25) "fournisseur de services d'hébergement", un fournisseur de services d'hébergement au sens de l'article 3, point g), iii), du règlement (UE) 2022/2065;

26) "fournisseur de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne", un fournisseur de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne au sens de l'article 33 du règlement (UE) 2022/2065;

27) "prestataire de services sur crypto-actifs", un prestataire de services sur crypto-actifs tel qu'il est défini à l'article 3, paragraphe 1, point 15), du règlement (UE) 2023/1114;

28) "service sur crypto-actifs", un service sur crypto-actifs tel qu'il est défini à l'article 3, paragraphe 1, point 16), du règlement (UE) 2023/1114;

29) "jeton de monnaie électronique", un jeton de monnaie électronique tel qu'il est défini à l'article 3, paragraphe 1, point 7), du règlement (UE) nº 2023/1114;

30) "monnaie électronique", une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, 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;

31) "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 ou de services physiques;

32) "microentreprise", une entreprise qui, au moment de la conclusion du contrat de service de paiement, est une entreprise telle qu'elle est définie à l'article 1er et à l'article 2, paragraphes 1 et 3, de l'annexe de la recommandation 2003/361/CE;

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

34) "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;

35) "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 peut être 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;

36) "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;

37) "prestataire de services de paiement gestionnaire du compte", un prestataire de services de paiement qui fournit et gère un compte de paiement pour un utilisateur de services de paiement;

38) "fournisseur de distributeurs automatiques de billets", une personne physique ou morale qui fournit des services de retrait d'espèces visés au point 1 de l'annexe I de la directive (UE) 2026/...[+] et qui n'est pas un prestataire de services de paiement gestionnaire du compte et ne fournit aucun autre service de paiement visé à l'annexe I de ladite directive;

39) "support durable", tout instrument permettant à l'utilisateur de services de paiement de stocker les informations qui lui sont adressées personnellement d'une manière permettant de s'y reporter ultérieurement pendant un laps de temps adapté aux fins auxquelles les informations sont destinées et qui permet la reproduction à l'identique des informations stockées;

40) "dénomination commerciale", le nom communément utilisé par le bénéficiaire, dans le cadre des échanges commerciaux et de la publicité de son entreprise, pour s'identifier auprès du payeur;

41) "transmission de fonds" (money remittance), un service de paiement pour lequel les fonds sont reçus 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;

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

42) "instrument de paiement", un ou plusieurs dispositifs individualisés 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;

43) "service d'initiation de paiement", un service consistant à passer un ordre de paiement à la demande de l'utilisateur de services de paiement concernant un compte de paiement détenu auprès d'un autre prestataire de services de paiement;

44) "service d'information sur les comptes", un service en ligne par lequel un prestataire accède à un ou plusieurs comptes de paiement accessibles en ligne et détenus par un utilisateur de services de paiement auprès d'un ou de plusieurs prestataires de services de paiement gestionnaires de comptes, afin de fournir un service d'agrégation ou de consolidation des données relatives aux comptes de paiement à l'utilisateur de services de paiement ou de transmettre les données à une autre entité qui fournira ce service à l'utilisateur de services de paiement;

45) "prestataire de services d'initiation de paiement", un prestataire de services de paiement fournissant des services d'initiation de paiement;

46) "prestataire de services d'information sur les comptes", un prestataire de services de paiement fournissant des services d'information sur les comptes;

47) "schéma de cartes de paiement", un schéma de cartes de paiement tel qu'il est défini à l'article 2, point 16), du règlement (UE) 2015/751;

48) "traitement", dans le cadre d'opérations de paiement, le traitement tel qu'il est défini à l'article 2, point 27), du règlement (UE) 2015/751;

49) "entité de traitement", une entité de traitement telle qu'elle est définie à l'article 2, point 28), du règlement (UE) 2015/751;

50) "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;

51) "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;

52) "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;

53) "virement", un service de paiement 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;

54) "virement instantané", un virement qui est exécuté immédiatement, 24 heures sur 24 et quel que soit le jour civil;

55) "date de valeur", la date de référence utilisée par un prestataire de services de paiement pour le calcul des intérêts applicables aux fonds débités d'un compte de paiement ou crédités sur un compte de paiement;

56) "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;

57) "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;

58) "taux de change moyen du marché agrégé", un taux qui représente le point médian entre les prix d'achat et de vente d'une paire de devises sur le marché des changes et qui est calculé en combinant des données provenant de sources multiples afin de refléter de manière précise et en temps réel les conditions du marché;

59) "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;

60) "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), lesquels sont indépendants les uns des autres 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;

61) "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;

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

63) "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;

64) "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 autres que des virements instantanés;

65) "adresse auto-hébergée", une adresse auto-hébergée au sens de l'article 3, point 20), du règlement (UE) 2023/1113;

66) "portefeuille de conservation", une adresse de portefeuille de crypto-actifs où un prestataire de services sur crypto-actifs assure la conservation ou le contrôle, pour le compte de son client, de ces crypto-actifs ou des moyens d'accès à ces crypto-actifs, le cas échéant sous la forme de clés cryptographiques privées;

67) "opération initiée par un commerçant", une opération de paiement pour laquelle le payeur a donné mandat au bénéficiaire de passer un ordre de paiement pour une opération 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, pour laquelle ce mandat est fondé sur un accord entre le payeur et le bénéficiaire pour la fourniture de produits ou de services, et pour laquelle ces opérations n'ont pas besoin d'être précédées d'une action spécifique du payeur pour déclencher leur initiation par le bénéficiaire;

68) "opération de passation d'ordre par correspondance ou par téléphone", une opération de paiement pour laquelle des ordres de paiement sont passés par le payeur en utilisant des moyens autres que des plateformes ou des dispositifs électroniques, tels que des ordres de paiement sur support papier, des ordres de paiement par correspondance ou par téléphone, que l'exécution de l'opération soit ou non effectuée par voie électronique;

69) "astreintes", des mesures d'exécution pécuniaires périodiques visant à mettre fin aux infractions continues au présent règlement ou à toute décision rendue par une autorité compétente en vertu du présent règlement et contraignant une personne physique ou morale à se remettre en conformité avec les dispositions ou les décisions qu’elle a enfreintes.

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

Chapitre 1
Règles générales

Article 4

Champ d'application

1. Le présent titre s'applique aux opérations de paiement isolées et aux contrats-cadres, ainsi qu'aux opérations de paiement qui relèvent de ces contrats. Les parties à ces opérations de paiement isolées et à ces contrats-cadres ainsi qu'aux opérations de paiement qui relèvent de ces contrats 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. Au plus tard le... [21 mois à compter de la date d'entrée en vigueur du présent règlement], les États membres notifient à la Commission les dispositions législatives qu'ils adoptent en vertu du paragraphe 2. Ils notifient sans retard injustifié à la Commission toute modification ultérieure qui y est apportée et toute disposition législative qu'ils adoptent en vertu du paragraphe 2 à une date ultérieure.

Article 5

Devise et conversion monétaire

1. Les opérations de paiement sont effectuées 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. Aux fins du paragraphe 2 du présent article, ainsi que de l'article 7, de l'article 13, paragraphe 1, point f), et de l'article 20, paragraphe 3, point e), le taux de change moyen du marché agrégé utilisé reflète fidèlement le marché, avec un retard maximal de 10 minutes ou, pour les monnaies pour lesquelles cela n'est pas possible, il reflète le dernier prix négocié sur une plate-forme de négociation réputée. Il est fourni par un administrateur de confiance qui respecte les principes de l'OICV sur les indices de référence financiers.

4. Le payeur a la possibilité d'accepter le service de conversion monétaire sur la base des informations fournies conformément au paragraphe 2.

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, de manière claire, neutre et compréhensible.

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, de manière claire, neutre et compréhensible, 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 des services de retrait d'espèces, y compris celles visées à l'article 36 de la directive (UE) 2026/...[+], affichent, pour leurs clients au distributeur automatique de billets, des informations sur les frais de retrait éventuels à payer par le client, y compris, le cas échéant, les frais de conversion conformément à l'article 5, paragraphe 2, du présent règlement. Les informations sont présentées de manière claire, neutre et compréhensible avant l'initiation de l'opération de paiement. Sur demande du client, les informations sur les frais éventuels sont également mises à disposition sur un support durable 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 dans le cadre du présent titre.

2. Les prestataires de services de paiement et les utilisateurs de services de paiement peuvent, d'un commun accord, convenir de frais liés à la fourniture d'informations supplémentaires, ou communiquées de manière plus fréquente, ou transmises par d'autres moyens de communication que ceux prévus par le contrat-cadre, et communiquées 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.

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

Article 9

Charge de la preuve en matière d'obligations d'information

Il incombe aux prestataires de services de paiement de prouver qu'ils se sont conformés aux obligations d'information prévues au présent titre.

Article 10

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

1. 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 n'excédant pas 300 EUR, soit stockent des fonds dont le montant n'excède à aucun moment 300 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 aisément accessibles;

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; en pareils cas, le prestataire de services de paiement fournit au payeur la possibilité de vérifier le montant des fonds stockés.

2. Dans le cas des instruments de paiement prépayés, les limites de dépenses et de stockage visées au paragraphe 1 ne dépassent pas 500 EUR.

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 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 de manière claire, neutre 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 qui lui incombent au titre dudit paragraphe immédiatement après l'exécution de l'opération de paiement.

3. Les prestataires de services de paiement peuvent s'acquitter des obligations qui leur incombent au titre 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) lorsque le prestataire de services de paiement du bénéficiaire est situé en dehors de l'Union, le délai estimé pour que les fonds des virements et des opérations de transmission de fonds soient reçus par ce prestataire de services de paiement;

   d) tous les frais payables par l'utilisateur de services de paiement au 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 montant monétaire dans la monnaie du compte du payeur et en marge de pourcentage sur un taux de change moyen du marché agrégé, tel qu'il est visé à l'article 5, paragraphe 3;

g) les procédures de règlement extrajudiciaire des litiges à la disposition de l'utilisateur de services de paiement conformément aux articles 100, 104 et 105.

Les informations visées au premier alinéa, point f), sont communiquées au payeur avant l'initiation de l'opération de paiement.

2. Avant d'initier l'opération de paiement, les prestataires de services d'initiation de paiement fournissent au payeur, ou mettent à sa disposition, des informations claires et complètes sur ce qui suit:

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 sans ambiguïté du bénéficiaire, y compris une référence à sa dénomination commerciale et, si le prestataire de services de paiement en dispose et si elle est différente de la dénomination commerciale, la dénomination légale du bénéficiaire;

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 conditions mentionnées à l'article 20. Ces informations et conditions sont fournies dans des termes aisément compréhensibles et de manière claire, neutre 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 qui lui incombent au titre dudit paragraphe immédiatement après la conclusion du contrat-cadre.

3. Les prestataires de services de paiement peuvent s'acquitter des obligations qui leur incombent au titre 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

1. Le prestataire de services de paiement fournit à l'utilisateur de services de paiement les informations et conditions ci-après concernant le prestataire de services de paiement:

   a) 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 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;

b) les coordonnées des autorités de contrôle compétentes désignées en vertu de la directive (UE) 2026/...[+] et les coordonnées des registres prévus 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.

2. Le prestataire de services de paiement fournit à l'utilisateur de services de paiement les informations et conditions ci-après concernant l'utilisation du service de paiement:

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

b) 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;

c) la forme et la procédure pour passer un ordre de paiement ou donner son consentement à l'exécution d'une opération de paiement et pour retirer ce consentement, conformément aux articles 50 et 69;

d) une référence au moment de réception de l'ordre de paiement conformément à l'article 67 et l'éventuel délai limite établi par le prestataire de services de paiement;

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

f) 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;

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

g) la fixation de limites de dépenses pour l'utilisation d'instruments de paiement et de moyens de paiement par l'utilisateur de services de paiement conformément à l'article 52, paragraphe 1, avec des informations sur la durée du délai nécessaire pour que toute augmentation des limites de dépenses qui en résulte prenne effet et la manière dont l'utilisateur de services de paiement peut modifier ces limites de dépenses et ajuster ce délai ou y déroger;

h) dans le cas d'instruments de paiement liés à une carte co-badgés, les droits de l'utilisateur de services de paiement au titre de l'article 8 du règlement (UE) 2015/751.

3. Le prestataire de services de paiement fournit à l'utilisateur de services de paiement les informations et conditions ci-après concernant les frais, les taux d'intérêt et les taux de change:

a) 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;

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

i) de leur prestataire de services de paiement;

ii) d'un prestataire de services de paiement appartenant au même réseau de distributeurs automatiques de billets que le prestataire de services de paiement de l'utilisateur;

iii) d'un prestataire de services de paiement appartenant à un réseau de distributeurs automatiques de billets avec lequel le prestataire de services de paiement de l'utilisateur a une relation contractuelle;

iv) d'un fournisseur de distributeurs automatiques de billets;

c) 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 taux de change de référence;

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

e) le cas échéant, les frais estimés des services de conversion monétaire liés à un virement, exprimés en montant monétaire dans la monnaie du compte du payeur et en marge de pourcentage sur un taux de change moyen du marché agrégé, tel qu'il est visé à l'article 5, paragraphe 3.

Les informations visées au premier alinéa, point e), sont communiquées au payeur avant l'initiation de chaque opération de paiement.

4. Le prestataire de services de paiement fournit à l'utilisateur de services de paiement les informations et conditions ci-après concernant la communication:

a) 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;

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

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

d) 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.

5. Le prestataire de services de paiement fournit à l'utilisateur de services de paiement les informations et conditions ci-après concernant les mesures de protection et les mesures correctives:

a) 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 53, premier alinéa, point b);

b) 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;

c) les conditions dans lesquelles le prestataire de services de paiement se réserve le droit de bloquer un instrument de paiement, conformément à l'article 52;

d) la responsabilité du payeur conformément à l'article 60, paragraphe 4, et à l'article 63, y compris des informations sur le montant concerné;

e) la manière dont l'utilisateur de services de paiement doit adresser une notification au prestataire de services de paiement en cas d'opération de paiement non autorisée ou mal initiée ou mal exécutée, et le délai dont il dispose pour le faire, conformément à l'article 55, ainsi que les forces de l'ordre en cas de fraude par usurpation d'identité visée à l'article 60;

f) la responsabilité du prestataire de services de paiement en cas d'opérations de paiement non autorisées conformément à l'article 57, d'application incorrecte du service de vérification de la concordance entre le nom et l'identifiant unique conformément à l'article 58, et de fraude par usurpation d'identité conformément à l'article 60;

g) la responsabilité du prestataire de services de paiement liée à l'initiation ou à l'exécution d'opérations de paiement, conformément aux articles 79 et 80;

h) les conditions de remboursement conformément aux articles 65 et 66.

6. Le prestataire de services de paiement fournit à l'utilisateur de services de paiement les informations et conditions ci-après concernant les modifications et la résiliation du contrat-cadre:

a) lorsqu'il en est convenu ainsi, l'information selon laquelle l'utilisateur de services de paiement sera réputé avoir accepté les modifications 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 qu'il n'acceptait pas ces modifications avant la date proposée pour l'entrée en vigueur de celles-ci;

b) la durée du contrat-cadre;

c) 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.

7. Le prestataire de services de paiement fournit à l'utilisateur de services de paiement les informations et conditions ci-après concernant les recours:

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

b) les procédures de règlement extrajudiciaire des litiges à la disposition de l'utilisateur de services de paiement conformément aux articles 100, 104 et 105.

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 clauses contractuelles du contrat-cadre ainsi que les informations et conditions mentionnées à l'article 20, sur support papier ou un autre support durable.

Article 22

Modifications du contrat-cadre

1. Le prestataire de services de paiement propose des modifications du contrat-cadre, y compris 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 leur entrée en vigueur. L'utilisateur de services de paiement peut accepter ou rejeter les modifications avant la date proposée pour leur entrée en vigueur.

2. Le cas échéant, conformément à l'article 20, paragraphe 6, point a), le prestataire de services de paiement informe l'utilisateur de services de paiement que ce dernier est réputé avoir accepté ces modifications s'il n'a pas notifié au prestataire de services de paiement, avant la date proposée pour leur entrée en vigueur, qu'il ne les acceptait pas. Le prestataire de services de paiement informe également l'utilisateur de services de paiement que, si ledit utilisateur rejette ces modifications, ce dernier a le droit de résilier le contrat-cadre sans frais et avec effet à tout moment avant la date à laquelle ces modifications auraient été appliquées.

3. Les modifications du taux d'intérêt ou du taux 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 du taux d'intérêt ou du taux de change se fondent sur le taux d'intérêt ou le taux de change de référence convenus conformément à l'article 20, paragraphe 3, points c) et d). 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 du taux d'intérêt ou du taux 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 du taux d'intérêt ou du taux de change appliqués aux opérations de paiement d'une manière neutre qui ne crée 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. Un tel délai ne peut être 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 trois 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 trois 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 non-exécutoire ou nul.

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

7. Au plus tard le... [21 mois à compter de la date d'entrée en vigueur du présent règlement], les États membres notifient à la Commission les dispositions législatives qu'ils adoptent en vertu du paragraphe 6. Ils notifient sans retard injustifié à la Commission toute modification ultérieure qui y est apportée et toute disposition législative qu'ils adoptent en vertu du paragraphe 6 à une date ultérieure.

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 et avant l'initiation de l'opération de paiement, pour cette opération de paiement spécifique, des informations explicites sur les points suivants:

a) le délai d'exécution maximal;

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

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, sans retard injustifié et selon les modalités prévues à l'article 19, paragraphe 1, les informations suivantes:

   a) une référence permettant au payeur d'identifier chaque opération de paiement et les informations nécessaires pour permettre l'identification sans ambiguïté du bénéficiaire, y compris une référence à sa dénomination commerciale et, si le prestataire de services de paiement en dispose et si elle est différente de la dénomination commerciale, la dénomination légale 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 pour 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 exiger que les informations visées au paragraphe 1 soient fournies ou mises à disposition périodiquement, à une fréquence à déterminer par le payeur, gratuitement et selon des modalités convenues qui permettent au payeur de les stocker et de les reproduire à l'identique. Le payeur est habilité à exiger la fourniture ou la mise à disposition de ces informations au minimum une fois par mois.

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. Au plus tard le... [21 mois à compter de la date d'entrée en vigueur du présent règlement], les États membres notifient à la Commission les dispositions législatives qu'ils adoptent en vertu du paragraphe 3. Ils notifient sans retard injustifié à la Commission toute modification ultérieure qui y est apportée et toute disposition législative qu'ils adoptent en vertu du paragraphe 3 à une date ultérieure.

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, sans retard injustifié et selon les modalités prévues à l'article 19, paragraphe 1, les 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, à une fréquence d'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. Au plus tard le ... [21 mois à compter de la date d'entrée en vigueur du présent règlement], les États membres notifient à la Commission les dispositions législatives qu'ils adoptent en vertu du paragraphe 3. Ils notifient sans retard injustifié à la Commission toute modification ultérieure qui y est apportée et toute disposition législative qu'ils adoptent en vertu du paragraphe 3 à une date ultérieure.

TITRE III
DROITS ET OBLIGATIONS LIÉS À LA PRESTATIONET À L'UTILISATION DE SERVICES DE PAIEMENT

Chapitre 1
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 50, paragraphe 7, ainsi que les articles 56, 63, 65, 66, 69, 79 et 80 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 55.

2. Les États membres peuvent prévoir que l'article 105 ne s'applique pas lorsque l'utilisateur de services de paiement n'est pas un consommateur.

3. Les États membres peuvent appliquer le présent titre aux microentreprises de la même manière qu'aux consommateurs.

4. Au plus tard le … [21 mois à compter de la date d'entrée en vigueur du présent règlement], les États membres notifient à la Commission les dispositions législatives qu'ils adoptent en vertu des paragraphes 2 et 3. Ils notifient sans retard injustifié à la Commission toute modification ultérieure qui y est apportée et toute disposition législative qu'ils adoptent en vertu des paragraphes 2 et 3 à une date ultérieure.

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 68, paragraphe 3, de l'article 69, paragraphe 5, et de l'article 78, paragraphe 3. 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 le prestataire de services de paiement du bénéficiaire et le payeur paie les frais prélevés par le prestataire de services de paiement du payeur.

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 interdire aux bénéficiaires ou limiter le droit de ces derniers 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. Le prestataire de services de paiement n’empêche pas le bénéficiaire d’offrir au payeur une réduction ou d'orienter ce dernier d'une autre manière vers l'utilisation d'un instrument de paiement donné. 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. Les frais appliqués ne dépassent pas les coûts directs supportés par le bénéficiaire pour l'utilisation de cet instrument de paiement.

6. Au plus tard le … [21 mois à compter de la date d'entrée en vigueur du présent règlement], les États membres notifient à la Commission les dispositions législatives qu'ils adoptent en vertu du paragraphe 4. Ils notifient sans retard injustifié à la Commission toute modification ultérieure qui y est apportée et toute disposition législative qu'ils adoptent en vertu du paragraphe 4 à une date ultérieure.

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 ne dépassant pas 300 EUR, soit stockent des fonds dont le montant n'excède à aucun moment 300 EUR, les prestataires de services de paiement peuvent convenir avec leurs utilisateurs de services de paiement que:

   a) l'article 53, premier alinéa, point b), l'article 54, paragraphe 1, premier alinéa, points c) et d), et l'article 63, paragraphe 5, 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 56 et 57 et l'article 63, paragraphes 1 et 5, 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 68, 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 69, 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 73 et 74, d'autres délais d'exécution s'appliquent.

2. Dans le cas des instruments de paiement prépayés, les limites de dépenses et de stockage visées au paragraphe 1 ne dépassent pas 500 EUR.

3. Les articles 57 et 63 s'appliquent 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.

4. Au plus tard le … [21 mois à compter de la date d'entrée en vigueur du présent règlement], les États membres notifient à la Commission les dispositions législatives qu'ils adoptent en vertu du paragraphe 3. Ils notifient sans retard injustifié à la Commission toute modification ultérieure qui y est apportée et toute disposition législative qu'ils adoptent en vertu du paragraphe 3 à une date ultérieure.

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 que le contrat ne prenne fin;

   b) le contrat stipule une date de fin 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 de fin du contrat.

   Le montant des frais est 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 de la monnaie électronique avant l'expiration du contrat, il peut s'agir d'une demande de remboursement en tout ou en partie.

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

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

   b) soit rembourse tous les fonds dont le remboursement est demandé par le détenteur de monnaie électronique lorsque l'établissement de paiement exerce d'autres activités commerciales mentionnées à l'article 10, paragraphe 1, point c), de la directive (UE) 2026/....[+] 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 l'émetteur de monnaie électronique et ces personnes.

8. Un établissement de paiement qui émet de la monnaie électronique n'octroie pas au détenteur de monnaie électronique d'intérêts ni aucun autre avantage liés à la durée pendant laquelle ce détenteur détient de la monnaie électronique.

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

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 les règles et procédures d'admission à la participation à son système de paiement ainsi que les critères et méthodes qu'il applique pour évaluer le risque 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 des risques pour le système, comme indiqué 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 justifie dûment tout refus.

4. Les opérateurs de systèmes de paiement n'imposent pas:

a) des règles restrictives en ce qui concerne la participation 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.

5. Les paragraphes 1 à 4 s'appliquent aux opérateurs de schémas de paiement. Ces paragraphes ne s'appliquent pas aux opérateurs de systèmes de paiement ni aux opérateurs de schémas de paiement composés exclusivement de prestataires de services de paiement appartenant au même groupe.

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 au système de paiement communique les raisons d'un tel refus à tout prestataire de services de paiement demandeur.

7. Les États membres désignent une autorité compétente chargée de veiller au respect des paragraphes 1 à 4 et du paragraphe 6, selon le cas, par les systèmes de paiement et les schémas de paiement régis par leur droit national, sauf dans les cas où ces exigences sont appliquées ou mises en œuvre par l'Eurosystème ou les banques centrales des États membres dont la monnaie n'est pas l'euro dans le cadre de la surveillance des opérations de ces systèmes ou schémas de paiement, tels que les systèmes de paiement relevant du règlement (UE) 2025/1355.

Article 32

Pratiques transparentes des schémas de cartes de paiement, des entités de traitement et des prestataires de services d'acquisition d'opérations de paiement

1. Les opérateurs de schémas de cartes de paiement et les entités de traitement veillent à ce que les frais imposés aux prestataires de services de paiement fournissant des services d'acquisition d'opérations de paiement soient classés par catégories et communiqués d'une manière claire et cohérente afin de permettre la comparabilité des catégories de facturation entre les schémas et les entités de traitement sur la base, au moins, des catégories de frais suivantes:

   a) commissions d'interchange;

   b) frais de traitement; et

   c) frais des schémas de paiement, dont:

      i) les frais obligatoires;

      ii) les frais liés à un comportement spécifique ou à l'utilisation ou non d'une technologie; et

      iii) les frais liés aux services optionnels.

   Les catégories de frais sont clairement définies.

Les informations visées au premier alinéa sont communiquées aux prestataires de services de paiement fournissant des services d'acquisition d'opérations de paiement d'une manière à ce qu'apparaisse très clairement quels frais correspondent à quels services.

Les informations visées au premier alinéa sont aussi précises que possible et font, dans la mesure du possible, une distinction entre les frais appliqués en fonction de la catégorie de carte, du canal de vente, du volume et de la valeur des transactions du commerçant et de la localisation géographique.

2. Les prestataires de services de paiement fournissant des services d'acquisition d'opérations de paiement utilisent les informations communiquées en vertu du paragraphe 1 du présent article lorsqu'ils s'acquittent des obligations qui leur incombent au titre des articles 9 et 12 du règlement (UE) 2015/751.

3. Aux fins du paragraphe 1, les opérateurs de schémas de cartes de paiement et les entités de traitement:

   a) communiquent au plus tard six mois avant leur mise en œuvre aux prestataires de services de paiement fournissant des services d'acquisition d'opérations de paiement, sans ambiguïté et de manière transparente et cohérente, tout nouveau frais et toute modification concernant les frais de schéma et les frais de traitement;

   b) tiennent un répertoire public unique de l'Union de leur schéma et des règles et frais en matière de traitement, conformément aux catégories de frais visées au paragraphe 1.

4. Au plus tard le ... [15 mois à compter de la date d'entrée en vigueur du présent règlement], la Commission adopte un acte délégué conformément à l'article 115 afin de compléter le présent règlement en précisant davantage les informations à communiquer aux prestataires de services de paiement fournissant des services d'acquisition d'opérations de paiement au titre du paragraphe 1.

Article 33

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

1. Les établissements de crédit donnent accès aux comptes de paiement aux établissements de paiement, à leurs agents et aux établissements de paiement demandeurs sur une base objective, non discriminatoire et proportionnée. Cet accès est suffisamment étendu pour permettre aux établissements de paiement de fournir des services de paiement de manière efficace et sans entraves.

2. Un établissement de crédit peut refuser d'ouvrir un compte de paiement pour un établissement de paiement, pour ses agents ou pour un établissement de paiement demandeur ou peut clôturer un tel compte uniquement dans l'hypothèse où:

   a) l'ouverture ou la gestion d'un tel compte de paiement entraînerait une infraction au règlement (UE) 2024/1624;

   b) une violation substantielle du contrat est ou a été commise par l'établissement de paiement, ses agents ou l'établissement de paiement demandeur;

   c) des informations ou des documents pertinents n'ont pas été reçus de la part du demandeur de compte;

d) l'autorité compétente a refusé de délivrer un agrément en tant qu'établissement de paiement ou l'a retiré.

3. L’accès accordé à un agent en vertu du paragraphe 1 est accordé exclusivement pour la prestation de services de paiement pour le compte d'un établissement de paiement.

4. Sans retard injustifié, et au plus tard un mois après avoir reçu une demande complète, un établissement de crédit notifie à l'établissement de paiement, à ses agents ou à l'établissement de paiement demandeur, ainsi qu'à l'autorité compétente, toute décision de refuser d'ouvrir un compte de paiement pour un établissement de paiement, ses agents ou un établissement de paiement demandeur. Une telle décision fournit des raisons dûment justifiées, précise les risques que représente l'activité ou l'activité prévue de cet établissement de paiement ou de ses agents ou de cet établissement de paiement demandeur, tels qu'ils sont évalués par l'établissement de crédit, sur la base des motifs visés au paragraphe 2, et ne revêt pas un caractère générique.

L'établissement de crédit notifie à l'établissement de paiement, à ses agents ou à l'établissement de paiement demandeur, ainsi qu'à l'autorité compétente, une décision de clôture du compte de paiement au moins quatre mois avant de le clôturer. Toute décision de clôture d'un compte de paiement fournit des raisons dûment justifiées, est spécifique et fondée sur les motifs visés au paragraphe 2 du présent article, et tient compte de la capacité de l'établissement de paiement à se conformer à l'exigence en matière de protection énoncée à l'article 9 de la directive (UE) 2026/...[+].

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

Par dérogation aux premier et deuxième alinéas du présent paragraphe, dans les cas visés au paragraphe 2, point a), les établissements de crédit:

a) notifient à l'établissement de paiement, à ses agents ou à l'établissement de paiement demandeur uniquement le fait que l'ouverture ou la gestion d'un compte de paiement entraînerait une infraction au règlement (UE) 2024/1624 et ne communiquent aucun détail sur la nature de cette infraction;

b) sont autorisés à clôturer le compte de paiement à l'issue d'un délai de préavis plus court.

5. L'autorité compétente peut publier des données agrégées relatives aux refus et aux clôtures de comptes de paiement.

6. Un établissement de paiement ou ses agents ou un établissement de paiement demandeur qui fait l'objet d'une décision d'un établissement de crédit de refuser d'ouvrir un compte de paiement ou de clôturer un tel compte peuvent former un recours auprès de l’autorité compétente.

7. L'ABE élabore des projets de normes techniques de réglementation précisant le format harmonisé de la notification et de la décision mentionnées au paragraphe 4 du présent article ainsi que les informations harmonisées qu'elles doivent contenir.

L'ABE soumet les projets de normes techniques de réglementation visées au premier alinéa à la Commission au plus tard le … [12 mois à compter de la date d'entrée en vigueur du présent règlement].

La Commission est habilitée à adopter ces normes techniques de réglementation 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 34

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. Cette obligation 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. Cette obligation s'applique à tous les comptes de paiement détenus par l'utilisateur de services de paiement qui sont accessibles en ligne.

Article 35

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 des prestataires 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 36

Fourniture d'interfaces d'accès dédiées

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 dédiée aux fins de l'échange de données avec les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement.

2. Un prestataire de services de paiement gestionnaire du compte met en place l'interface dédiée visée au paragraphe 1 dans un délai de trois mois à compter de l'obtention de son agrément. Afin que l'interface dédiée puisse être utilisée dès que possible, le prestataire de services de paiement gestionnaire du compte fournit sans retard injustifié la documentation technique pertinente concernant l'interface dédiée, à la demande des prestataires agréés de services d'initiation de paiement, des prestataires de services d'information sur les comptes ou des entreprises qui ont demandé l'agrément nécessaire à leurs autorités compétentes.

Les prestataires de services de paiement gestionnaires de comptes autorisent toujours l'accès à l'interface dédiée visée au paragraphe 1 afin de permettre la continuité des activités des prestataires de services d'initiation de paiement et des prestataires de services d'information sur les comptes.

3. Un prestataire de services de paiement gestionnaire du compte veille à ce que l'interface dédiée mentionnée au paragraphe 1 utilise 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) ou d'autres normes pertinentes largement reconnues offrant un niveau de sécurité équivalent. Un prestataire de services de paiement gestionnaire du compte veille également à ce que les spécifications techniques d'une interface dédiée telle que mentionnée au paragraphe 1 fassent l'objet d'une documentation, précisant la 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 du 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 injustifié, la documentation relative aux spécifications techniques de leurs interfaces dédiées 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. Un prestataire de services de paiement gestionnaire du compte veille à ce que, sauf en cas d'urgence l'empêchant de satisfaire à cette exigence, toute modification des spécifications techniques de l'interface dédiée mentionnée au paragraphe 1 soit mise à la disposition, à l'avance et au minimum par voie de publication sur son site internet, des prestataires agréés de services d'initiation de paiement et de services d'information sur les comptes ou des établissements de paiement demandeurs concernés, dans les plus brefs délais et au moins deux mois avant la mise en œuvre de cette 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 communication préalable des informations pertinentes et mettent cette documentation à la disposition des autorités compétentes sur demande.

5. Les prestataires de services de paiement gestionnaires de comptes publient sur leurs sites internet des statistiques trimestrielles relatives à la disponibilité, à l'indisponibilité imprévue et aux performances de leurs interfaces dédiées et, à des fins de comparaison, des interfaces qu'ils mettent à la disposition de leurs utilisateurs de services de paiement afin qu'ils aient un accès direct aux comptes de paiement en ligne. Les performances des interfaces dédiées 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. Un prestataire de services de paiement gestionnaire du compte met à disposition un dispositif d'essai, comprenant une assistance et permettant des tests de connectivité et de fonctionnement des interfaces dédiées, afin que les prestataires agréés de services d'initiation de paiement et les prestataires de services d'information sur les comptes, ou les établissements de paiement de paiement demandeurs concernés, puissent tester les logiciels et les 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 de données au moyen de son interface dédiée, 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 des messages de notification expliquant les raisons de l'erreur ou de l'événement imprévu.

Article 37

Exigences relatives aux interfaces dédiées d'accès aux données

1. Un prestataire de services de paiement gestionnaire du compte veille à ce que l'interface dédiée qu'il met en place en vertu de l'article 36, paragraphe 1, satisfasse aux exigences de sécurité et de performance suivantes:

   a) l'interface dédiée 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 dédiée 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 dédiée 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. Un prestataire de services de paiement gestionnaire du compte veille à ce que l'interface dédiée mentionnée au paragraphe 1 permette 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 du consentement donné 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 conformément à l'article 50, paragraphe 3;

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.

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 dédiée visée au paragraphe 1, afin de demander et de recevoir des informations concernant un ou plusieurs comptes de paiement désignés et les opérations de paiement associées. Ces informations comprennent l'identifiant unique du compte, les noms associés des titulaires du compte, les devises, le solde du compte et les opérations de paiement initiées au moyen d'un instrument de paiement qui n'ont pas encore été imputées sur le compte de paiement, lorsque ces opérations sont déjà visibles sur l'interface client.

4. Les prestataires de services de paiement gestionnaires de comptes veillent à ce que l'interface dédiée visée au paragraphe 1 permette aux prestataires de services d'initiation de paiement, au minimum:

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

b) d'initier une opération de paiement isolée;

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

d) d'initier des opérations de paiement en faveur de plusieurs bénéficiaires;

e) d'initier des opérations de paiement, que le bénéficiaire figure ou non sur la liste des bénéficiaires du payeur, à moins que l'utilisateur de services de paiement ne soit dans l'incapacité d'effectuer ces opérations de paiement par l'intermédiaire de l'interface client;

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 l'opération de paiement ne soit initiée, que le nom du titulaire du compte soit ou non disponible par l'intermédiaire de l'interface directe;

h) dans les cas où le prestataire de services de paiement gestionnaire du compte propose plusieurs procédures d'authentification, de choisir celle qui doit être présentée au payeur;

i) avant l'initiation de l'opération de paiement, de voir l'identifiant unique du compte, les noms associés des titulaires du compte et, le cas échéant, les devises dont dispose l'utilisateur de services de paiement.

5. Les prestataires de services de paiement gestionnaires de comptes veillent à ce que l'interface dédiée visée au paragraphe 1 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, le plus tôt possible, que l'opération de paiement a été ou sera exécutée sur la base des informations dont celui-ci dispose, en tenant compte de tout ordre de paiement préexistant susceptible d'affecter l'exécution intégrale de l'ordre de paiement passé.

Les informations mentionnées au premier alinéa, 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.

6. Aux fins des 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 l'identifiant unique du compte ne constituent pas des données de paiement sensibles.

Article 38

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

1. Sans préjudice de l'article 37, un prestataire de services de paiement gestionnaire du compte veille à ce que l'interface dédiée mentionnée à l'article 36, 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'il met à la disposition de l'utilisateur de services de paiement pour qu'il accède directement à son compte de paiement en ligne.

2. Un prestataire de services de paiement gestionnaire du compte fournit 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. Un prestataire de services de paiement gestionnaire du compte fournit 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 dès réception de l'ordre de paiement. Toute mise à jour de ces informations, y compris du statut du paiement, est mise à la disposition du prestataire de services d'initiation de paiement par l'intermédiaire de l'interface dédiée et en continu jusqu'à ce que l'opération de paiement ait été exécutée ou rejetée.

Article 39

Exigences en matière de disponibilité et de performance de l'interface dédiée

1. Un prestataire de services de paiement gestionnaire du compte prend toutes les mesures en son pouvoir pour limiter toute indisponibilité prévue de l'interface dédiée à ce qui est strictement nécessaire et pour éviter l'indisponibilité imprévue et la sous-performance de l'interface dédiée. Une indisponibilité est 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 reçoivent des messages d'erreur du serveur ou n'obtiennent pas de réponse de l'interface dédiée du prestataire de services de paiement gestionnaire du compte dans les 30 secondes.

2. En cas d'indisponibilité prévue de l'interface dédiée, les prestataires de services de paiement gestionnaires de comptes informent au moins un mois à l'avance, sauf en cas de modifications dues à des situations d'urgence, les prestataires de services de paiement utilisant cette interface de l'indisponibilité prévue et de sa durée. Les indisponibilités prévues se situent habituellement entre 00 h 00 et 6 h 00.

3. En cas d'indisponibilité imprévue de l'interface dédiée, les prestataires de services de paiement gestionnaires de comptes informent en temps utile les prestataires de services d'initiation de paiement et les prestataires de services d'information sur les comptes, au moyen de l'interface dédiée, des mesures prises pour rétablir l'interface et du délai considéré comme nécessaire pour résoudre le problème. Les prestataires de services de paiement gestionnaires de comptes veillent à ce que l'interface dédiée soit rétablie dans un délai optimal.

4. Un prestataire de services de paiement gestionnaire du compte veille à ce que la disponibilité et les performances de l'interface dédiée soient au moins égales à celles de l'interface qu'il utilise pour l'authentification et la communication avec ses utilisateurs de services de paiement.

5. L'ABE élabore des projets de normes techniques de réglementation précisant:

a) les exigences relatives aux statistiques trimestrielles sur la disponibilité et les performances des interfaces visées à l'article 36, paragraphe 5, et leur publication;

b) les normes fixant un délai de rétablissement optimal en cas d'indisponibilité imprévue d'une interface dédiée conformément au paragraphe 3, en fonction de la gravité de l'incident.

Aux fins du premier alinéa, point b), une évaluation de la gravité tient compte, entre autres, du nombre de clients touchés et des types de fonctionnalités des prestataires de services d'information sur les comptes et des prestataires de services de services d'initiation de paiement concernés par l'incident.

L'ABE soumet les projets de normes techniques de réglementation visées au premier alinéa à la Commission au plus tard le … [9 mois à compter de la date d'entrée en vigueur du présent règlement].

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

Article 40

Dérogation à l'obligation de disposer d'une interface dédiée pour l'accès aux données

1. Par dérogation à l'article 36, 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 dédiée et l'autoriser:

   a) 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, à condition que cette interface offre des fonctionnalités équivalentes pour faciliter l'accès des prestataires de services d'initiation de paiement et des prestataires de services d'information sur les comptes et utilise des normes largement acceptées et interopérables;

   b) soit, lorsque cela se justifie, à ne proposer aucune interface pour l'échange sécurisé de données.

   Le cas échéant, les États membres peuvent exempter les banques centrales nationales qui n'agissent pas en leur qualité d'autorité monétaire ou d'autres autorités publiques visées à l'article 2, paragraphe 1, point d), de l'obligation de disposer d'une interface dédiée.

2. L'ABE élabore des projets de normes techniques de réglementation qui précisent les critères sur la base desquels, conformément au paragraphe 1, il est justifié qu'un prestataire de services de paiement gestionnaire du compte ne propose pas d'interface pour l'échange sécurisé de données. En précisant ces critères, l'ABE tient compte, entre autres, de la taille, du chiffre d'affaires annuel et du volume des paiements du prestataire de services de paiement gestionnaire du compte.

L'ABE soumet les projets de normes techniques de réglementation visées au premier alinéa à la Commission au plus tard le … [12 mois à compter de la date d'entrée en vigueur du présent règlement].

La Commission est habilitée à adopter lesdites normes techniques de réglementation 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 41

Obligations des 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 de l'utilisateur du service de paiement 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, et de manière continue, à la demande de celui-ci, il met à la disposition du prestataire de services d'initiation de paiement 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 premier alinéa, 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'opération de paiement, y compris toute mise à jour du statut de paiement, soit mise à la disposition du prestataire de services d'initiation de paiement dès qu'il dispose de ces informations.

Article 42

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. Le prestataire de services de paiement gestionnaire du compte permet 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 ce prestataire de services de paiement gestionnaire du compte 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.

3. Lorsque le prestataire de services d'information sur les comptes a l'intention d'accéder aux informations visées au paragraphe 2 alors que l'utilisateur de services de paiement ne demande pas spontanément ces informations, il veille à ce que l'utilisateur de services de paiement soit dûment informé de cette intention avant d'utiliser cette fonctionnalité.

Article 43

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 au compte de paiement par ce prestataire de services d'information sur les comptes ou ce prestataire de services d'initiation de paiement qui est réputé non autorisé en vertu de l'article 50, paragraphe 4, ou frauduleux, y compris à l'initiation non autorisée ou frauduleuse d'une opération de paiement. En pareils 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, fournie 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 motivées ou soit interdit en vertu d'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 une situation et les raisons justifiant les mesures prises. L'autorité compétente évalue cette situation et prend au besoin des mesures appropriées.

Article 44

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 consentements que celui-ci a accordés 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, à tout moment et dans un format facile à comprendre, une vue d'ensemble de chaque consentement en cours accordé aux fins de services d'information sur les comptes ou de services d'initiation de paiement, comprenant notamment:

      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 du consentement;

      iv) la durée de validité du consentement, y compris la date à laquelle l'utilisateur de services de paiement a donné ce consentement;

      v) les catégories de données partagées;

      vi) les dates de l'accès aux données relatives aux comptes de paiement.

b) permet à l'utilisateur de services de paiement de retirer, à tout moment et gratuitement, l'accès aux données à tous les prestataires de services d'information sur les comptes ou à tous les prestataires de services d'initiation de paiement ou à un prestataire de services d'information sur les comptes ou à un prestataire de services d'initiation de paiement donné;

c) dans les 48 heures suivant le retrait d'un consentement, permet à l'utilisateur de services de paiement de rétablir tout accès aux données retiré;

d) comporte un registre des consentements à l'accès aux données qui ont été retirés ou qui ont expiré sur une durée de deux ans.

3. Lorsque, par application du paragraphe 2, point b), un utilisateur de services de paiement décide de retirer l'accès aux données, le prestataire de services d'initiation de paiement ou le prestataire de services d'information sur les comptes concerné:

a) cesse d'accéder aux données et de les utiliser; et

b) supprime sans retard injustifié, mais pas avant un délai de 48 heures après le retrait d'un consentement, les données reçues à la suite du consentement à l'accès aux données accordé par l'utilisateur de services de paiement.

Par dérogation au premier alinéa, point b), le prestataire de services de paiement concerné peut conserver les données si l'utilisateur de services de paiement en décide explicitement ainsi.

4. 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, à ce que les informations qui s'affichent sur le tableau de bord soient claires, neutres, précises et facilement compréhensibles pour l'utilisateur de services de paiement et à ce qu'elles ne comportent aucune formulation dissuasive ou décourageante susceptible de dissuader l'utilisateur de services de paiement de recourir aux services d'un prestataire de services d'initiation de paiement ou d'un prestataire de services d'information sur les comptes.

Le prestataire de services de paiement gestionnaire du compte:

a) n'incite pas l'utilisateur de services de paiement à retirer un consentement donné aux fins de services d'information sur les comptes ou de services d'initiation de paiement;

b) ne conçoit, n'organise ni n'exploite son tableau de bord d'une manière qui induit l'utilisateur de services de paiement en erreur, le manipule ou l'enjoint à accorder des consentements qui ne sont pas dans l'intérêt supérieur de l'utilisateur, ou d'une manière qui altère ou entrave sensiblement la capacité de l'utilisateur à prendre des décisions libres et éclairées.

5. Le prestataire de services d'information sur les comptes ou le prestataire de services d'initiation de paiement auquel le consentement a été accordé fournit sans retard injustifié les informations visées au paragraphe 2, point a), au prestataire de services de paiement gestionnaire du compte. Le prestataire de services de paiement gestionnaire du compte ne fournit ces informations que dans la mesure où elles lui ont été fournies par le prestataire de services d'information sur les comptes ou par le prestataire de services d'initiation de paiement auquel le consentement a été accordé.

6. Le prestataire de services de paiement gestionnaire du compte et le prestataire de services d'information sur les comptes ou le prestataire de services d'initiation de paiement auquel le consentement a été accordé coopèrent pour mettre les informations à la disposition de l'utilisateur de services de paiement sur le tableau de bord sans retard injustifié.

Le prestataire de services de paiement gestionnaire du compte met les informations à la disposition du prestataire de services d'information sur les comptes ou du prestataire de services d'initiation de paiement, sans retard injustifié, toute modification apportée par l'utilisateur de services de paiement à un consentement au moyen du tableau de bord, y compris le retrait d'un consentement.

Un prestataire de services d'information sur les comptes ou un prestataire de services d'initiation de paiement informe sans retard injustifié le prestataire de services de paiement gestionnaire du compte de tout nouveau consentement accordé par un utilisateur de services de paiement concernant un compte de paiement fourni par ce prestataire de services de paiement gestionnaire du compte, y compris les informations visées au paragraphe 2, points a), i) à v).

7. Le prestataire de services de paiement gestionnaire du compte n'est pas responsable des actions visées au paragraphe 2, points b) et c), entreprises par l'utilisateur de services de paiement.

Article 45

Entraves interdites à l'accès aux données

1. Les prestataires de services de paiement gestionnaires de comptes veillent à ce que leurs interfaces dédiées n'entravent pas la prestation de services d'initiation de paiement et de services d'information sur les comptes.

Constituent notamment 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 personnalisées 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 les services d'initiation de paiement;

c) le fait de demander des vérifications du consentement donné 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 des prestataires 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 dédiée;

e) le fait d'exiger, sauf si cela est nécessaire 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 les prestataires de services d'information sur les comptes en liaison, en particulier, avec la mise à jour du tableau de bord visé à l'article 44, que les prestataires de services d'initiation de paiement et les prestataires de services d'information sur les comptes enregistrent au préalable 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, à moins que l'utilisateur de services de paiement ne soit dans l'incapacité d'effectuer ces paiements par l'intermédiaire de l'interface client;

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 une authentification forte du client plus fréquemment que ne l'exige 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 dédiée 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 inclue 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 des paiements à l'aide du prestataire de services de paiement gestionnaire du compte;

k) le fait d'imposer une redirection automatique d'un utilisateur, au stade de l'authentification, vers la page internet du prestataire de services de paiement gestionnaire du compte lorsque l'interface dédiée ne prend pas en charge toutes les procédures d'authentification mises à la disposition de ses utilisateurs de services de paiement par le prestataire de services de paiement gestionnaire du compte;

l) le fait d'exiger à deux reprises une authentification forte 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" ou par "Non" et une deuxième authentification forte du client pour l'initiation du paiement.

2. Les mesures prises par les prestataires de services de paiement gestionnaires de comptes qui sont nécessaires pour lutter contre les soupçons de fraude au titre du présent règlement ou pour se conformer au règlement (UE) 2016/679 ne sont pas réputées constituer des entraves à l'accès aux données, à moins que ces mesures ne constituent des entraves interdites visées au paragraphe 1, points a) à l), du présent article.

SECTION 4

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

Article 46

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 dédiée mentionnée à l'article 36, sauf dans les circonstances énoncées à l'article 40, paragraphe 1, ou, exceptionnellement, au moyen d'une autre interface sûre et efficace.

2. Lorsque seule l'interface visée à l'article 40, paragraphe 1, point a), est accessible à un prestataire de services d'initiation de paiement ou à un prestataire de services d'information sur les comptes, 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) fournit des informations conformément à l'article 44, paragraphe 2, points a), ii) à v);

   c) 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;

d) 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;

e) enregistre, en vue de permettre à l'autorité compétente d'enquêter sur la conformité avec la présente section, 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 sans retard injustifié, à l'autorité compétente.

Aux fins du premier alinéa, point e), les registres sont effacés trois ans après leur création. Les registres peuvent être conservés plus longtemps dans la mesure où ils sont nécessaires à des procédures de contrôle déjà en cours.

Article 47

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 du consentement de l'utilisateur de services de paiement, conformément à l'article 50;

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 du service 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 du service de paiement obtenue lors de la prestation de services d'initiation de paiement ne soit communiquée qu'au bénéficiaire et uniquement avec le consentement de l'utilisateur du service de paiement;

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

g) sont en mesure de refuser d'initier une opération de paiement pour des raisons objectivement justifiées.

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

a) sans préjudice de l'article 46, paragraphe 2, point e), ne conservent 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 procèdent pas au traitement de données à caractère personnel ou non personnel, y compris l'utilisation, la consultation ou la conservation 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 de paiement.

Article 48

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 du consentement de l'utilisateur de services de paiement, conformément à l'article 50;

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 de manière sécurisée avec le prestataire de services de paiement gestionnaire du compte et l'utilisateur de services de paiement;

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 au consentement de l'utilisateur de services de paiement.

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

a) n'accède pas à des données de paiement sensibles liées à des comptes de paiement;

b) ne traite pas de données à des fins autres que la prestation du service d'information sur les comptes autorisée par l'utilisateur de services de paiement.

3. Les articles 4 à 8, les articles 10, 11 et 12, les articles 14 à 19, les articles 21 à 29, les articles 51 et 52, les articles 54 à 83 et les articles 87 et 90 ne s'appliquent pas aux prestataires de services d'information sur les comptes.

SECTION 5

MISE EN ŒUVRE

Article 49

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 dédiée mentionnée à l'article 36, paragraphe 1, et à l'article 39 et à ce que toute entrave interdite mentionnée à l'article 45 soit immédiatement levée par le prestataire de services de paiement gestionnaire du compte concerné. Lorsqu'elles constatent que les interfaces dédiées ne sont pas conformes au présent règlement ou qu'il existe des entraves interdites, y compris sur la base des informations transmises par les prestataires de services d'initiation de paiement ou de services d'information sur les comptes, les autorités compétentes prennent sans retard injustifié les mesures d'application nécessaires et adéquates et imposent toute sanction appropriée.

2. Les autorités compétentes prennent sans tarder toutes les mesures d’exécution requises lorsque cela est nécessaire pour préserver les droits d'accès des prestataires de services d'initiation de paiement et des prestataires de services d'information sur les comptes. Les mesures d’exécution peuvent comprendre des sanctions appropriées.

3. Les autorités compétentes veillent à ce que les prestataires de services d'initiation de paiement et les prestataires de services d'information sur les comptes respectent leurs obligations relatives à l'utilisation des interfaces d'accès aux données.

4. Les autorités compétentes disposent des ressources nécessaires, en particulier en ce qui concerne le personnel spécialisé, pour accomplir leurs missions à tout moment.

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, de leur propre initiative, des réunions conjointes avec les prestataires de services de paiement gestionnaires de comptes et les prestataires de services d'initiation de paiement et les prestataires de services d'information sur les comptes aux fins du paragraphe 7.

7. Les autorités compétentes 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, les prestataires de services d'initiation de paiement et les prestataires de services d'information sur les comptes soient résolus rapidement et durablement.

8. 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, paragraphe 1, point b), de l'article 31 et de l'article 35, paragraphe 2, du règlement (UE) nº 1093/2010, l'ABE coordonne l'activité de surveillance visée au premier alinéa du présent paragraphe, 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 peuvent, le cas échéant, contenir des recommandations.

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

L'ABE soumet les projets de normes techniques de réglementation visés au premier alinéa à la Commission au plus tard le … [18 mois à compter de la date d'entrée en vigueur du présent règlement].

La Commission est habilitée à adopter lesdites normes techniques de réglementation conformément aux articles 10 à 14 du règlement (UE) nº 1093/2010.

Chapitre 4
Autorisation des opérations de paiement

Article 50

Autorisation

1. Une opération de paiement ou une série d'opérations de paiement n'est autorisée que si le payeur a donné son consentement 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 en ont convenu ainsi, après son exécution.

2. Une opération de paiement est réputée non autorisée lorsqu'elle a été initiée ou modifiée par un tiers agissant sans le consentement du payeur, y compris en utilisant les données de sécurité personnalisées du payeur obtenues frauduleusement.

3. 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 son consentement à ce que celui-ci accède au compte de paiement et aux données pertinentes de ce compte.

4. En l'absence de consentement, 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.

5. Les prestataires de services de paiement gestionnaires de comptes ne vérifient pas le consentement donné 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.

6. Le consentement visé aux paragraphes 1 et 3 est exprimé sous la forme convenue entre l'utilisateur de services de paiement et le prestataire de services de paiement concerné. Le consentement à l'exécution d'une opération de paiement peut aussi être donné par l'intermédiaire du bénéficiaire ou du prestataire de services d'initiation de paiement.

   La procédure de consentement fait l'objet d'un accord entre l'utilisateur de services de paiement et le prestataire de services de paiement concerné.

7. Le payeur peut retirer à tout moment son consentement à l'exécution d'une opération de paiement ou à l'accès à un compte de paiement aux fins de services d'initiation de paiement, mais au plus tard au moment de l'irrévocabilité conformément à l'article 69. L'utilisateur de services de paiement peut retirer à tout moment son consentement à l'accès à un compte de paiement aux fins de services d'information sur les comptes. Le payeur peut également retirer son consentement à l'exécution d'une série d'opérations de paiement, auquel cas toute opération de paiement postérieure est réputée non autorisée.

Article 51

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

Dans le cas de virements, les prestataires de services de paiement se conforment à l'article 5 *quater*, paragraphes 1 à 7, et à l'article 5 *ter*, paragraphe 2, du règlement (UE) nº 260/2012, et ces articles s'appliquent mutatis mutandis à tous les virements, y compris ceux qui relèvent du champ d'application du règlement (UE) nº 260/2012.

Aux fins du premier alinéa du présent paragraphe, lorsque le compte de paiement du bénéficiaire n'est pas identifié par l'identifiant de compte de paiement précisé au point 1), a) de l'annexe du règlement (UE) nº 260/2012, les références à l'identifiant de compte de paiement figurant à l'article 5 *quater* dudit règlement s'entendent comme faites à l'identifiant unique utilisé pour permettre l'identification certaine du compte de paiement du bénéficiaire.

Article 52

Limitation et blocage de l'utilisation des instruments de paiement

1. Le prestataire de services de paiement offre à l'utilisateur de services de paiement, dans le contrat-cadre, la possibilité de fixer une limite établissant le montant maximal pouvant être transféré, qui peut différer en fonction du moyen de paiement, y compris les virements, et de l'instrument de paiement. Une limite peut être fixée pour chaque opération ou dans un délai déterminé, à la seule discrétion de l'utilisateur de services de paiement.

   Les prestataires de services de paiement ne modifient pas unilatéralement les limites de dépenses fixées dans le contrat-cadre conclu avec leurs utilisateurs de services de paiement.

Il est possible pour l'utilisateur de services de paiement de modifier les limites de dépenses fixées dans le contrat-cadre. Les prestataires de services de paiement veillent à ce que le payeur soit en mesure de modifier les limites de dépenses fixées avant la passation d'un ordre de paiement.

2. Si l'utilisateur de services de paiement augmente les limites de dépenses à distance, les prestataires de services de paiement fixent un délai de quatre heures pour que cette augmentation prenne effet. Les utilisateurs de services de paiement ont le droit d’ajuster ce délai ou de renoncer à son application. Lorsqu'un délai est en place, il s'applique avant l'entrée en vigueur de toute adaptation ou renonciation ultérieure.

   Les prestataires de services de paiement informent immédiatement les utilisateurs de services de paiement, selon des modalités convenues, lorsqu'une modification d'une limite de dépenses est demandée, lorsque le délai visé au premier alinéa a expiré ou lorsque l'adaptation ou la renonciation visée au premier alinéa est exercée.

3. Lorsque l'ordre de paiement d'un utilisateur de services de paiement dépasse le montant maximal ou donne lieu au dépassement dudit montant, le prestataire de services de paiement du payeur n'exécute pas l'ordre de paiement, informe l'utilisateur de services de paiement des motifs de cette non-exécution et lui indique comment modifier le montant maximal.

4. Le prestataire de services de paiement peut bloquer l'instrument de paiement, pour des raisons objectivement justifiées ayant trait à la sécurité de l'instrument de paiement, à des suspicions 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.

5. Lorsqu'un instrument de paiement est bloqué en application du paragraphe 4, le prestataire de services de paiement informe le payeur, selon des modalités convenues, du blocage de l'instrument de paiement et des raisons spécifiques 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 soit interdit en vertu d'une autre disposition du droit de l'Union ou de droit national pertinente. Le prestataire de services de paiement du payeur évalue, sans retard injustifié et dans un délai maximal de deux jours ouvrables, si les raisons justifiant le blocage de l'instrument de paiement sont toujours motivées.

6. 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.

7. Lorsque le prestataire de services de paiement offre à l'utilisateur de services de paiement la possibilité d'initier des opérations de paiement ou de consentir à celles-ci au moyen d'une application mobile, il exige une authentification forte du client et l'utilisation de différents canaux de communication pour activer cette application mobile.

8. Si l'utilisateur de services de paiement active l'application mobile à distance, le prestataire de services de paiement fixe un délai de quatre heures pour que cette activation prenne effet. L'utilisateur de services de paiement a le droit d’ajuster ce délai ou de renoncer à son application. Lorsqu'un délai est en place, il s'applique avant l'entrée en vigueur de tout ajustement ultérieur ou de toute renonciation ultérieure.

9. Le prestataire de services de paiement notifie immédiatement à l'utilisateur de services de paiement, selon des modalités convenues, et par différents canaux de communication, l'activation d'une application mobile. La notification comprend des instructions dans le cas où l'utilisateur de services de paiement n'a pas installé lui-même l'application mobile.

La procédure relative à la notification visée dans le présent paragraphe fait l'objet d'un accord entre l'utilisateur de services de paiement et le prestataire de services de paiement.

10. Lorsque l'utilisateur de services de paiement informe le prestataire de services de paiement qu'il n'a pas activé l'application mobile liée à son compte de paiement conformément à la procédure visée au paragraphe 9, le prestataire de services de paiement veille, sans retard injustifié, à ce que l'application mobile ne permette pas d'accéder au compte de paiement de l'utilisateur de services de paiement, ni d'initier des opérations de paiement ou de donner son consentement à celles-ci.

11. Les paragraphes 7, 8 et 9 ne s'appliquent pas à l'établissement initial de la relation client entre le prestataire de services de paiement et l'utilisateur de services de paiement au moyen de l'utilisation d'une application mobile, ni à l'activation, par le prestataire de services de paiement dans ses locaux physiques, d'une application mobile sur un appareil de l'utilisateur de services de paiement.

12. Le présent article s'applique à tous les virements, y compris les virements en euros, nonobstant le règlement (UE) nº 260/2012.

Article 53

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 ou des données de sécurité personnalisées concernées, le notifie sans retard injustifié au prestataire de services de paiement ou à l'entité désignée par celui-ci.

Aux fins du premier alinéa, 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 54

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) veille à ce que les données de sécurité personnalisées ne soient 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 53;

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 et à titre gratuit, de moyens appropriés permettant à l'utilisateur de services de paiement de procéder à la notification prévue à l'article 53, premier alinéa, point b), ou de demander le déblocage de l'instrument de paiement conformément à l'article 52, paragraphe 6, et à la disponibilité, à tout le moins pendant les heures d'ouverture et à titre gratuit, d'une assistance humaine à ces fins dans une langue officielle de l'État membre dans lequel le service de paiement est fourni;

d) fournit à l'utilisateur de services de paiement la possibilité de procéder à la notification prévue à l'article 53, premier alinéa, 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 53, premier alinéa, point b);

f) veille à ce que les données de paiement sensibles soient transmises à l'utilisateur de services de paiement par des canaux sûrs.

Aux fins du premier alinéa, point c), le prestataire de services de paiement fournit à l'utilisateur de services de paiement, à sa demande, pendant dix-huit mois après la notification, les moyens de prouver que l'utilisateur de services de paiement a effectué 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 55

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 à l'article 57, 60 ou 87 sans retard injustifié 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 79, et, en tout état de cause, au plus tard dix-huit mois après 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 57, paragraphe 4, et de l'article 79, paragraphe 1.

Article 56

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 sur le prestataire de services de paiement que pèse 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, le fait que l'opération de paiement a été authentifiée, y compris, le cas échéant, au moyen d'une authentification forte du client, dûment enregistrée et comptabilisée et n'ayant pas été affectée par une déficience technique ou autre du service fourni par le prestataire de services de paiement ne suffit pas nécessairement en tant que tel 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, de manière intentionnelle ou à la suite d'une négligence grave, à une ou à plusieurs des obligations qui lui incombent au titre de l'article 53. 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.

3. Aux fins des paragraphes 1 et 2 du présent article, et avant de conclure qu'un utilisateur de services de paiement a autorisé l'opération, a agi frauduleusement ou n'a pas satisfait, de manière intentionnelle ou à la suite d'une négligence grave, à une ou à plusieurs des obligations qui lui incombent au titre de l'article 53, le prestataire de services de paiement invite l'utilisateur de services de paiement à fournir des informations sur les événements qui ont conduit à l'opération de paiement et inclut ces informations dans son évaluation. Lorsque l'utilisateur de services de paiement ne fournit pas ces informations, cela ne conduit pas en soi le prestataire de services de paiement à conclure que l'utilisateur de services de paiement a autorisé l'opération, a agi frauduleusement ou n'a pas satisfait, de manière intentionnelle ou à la suite d'une négligence grave, à une ou à plusieurs des obligations qui lui incombent au titre de l'article 53. L'utilisateur de services de paiement n'est pas tenu de fournir d'autres informations que celles qu'il est raisonnablement susceptible d'avoir.

Article 57

Responsabilité du prestataire de services de paiement en cas d'opérations de paiement non autorisées

1. Sans préjudice de l'article 55, 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 constaté ou été informé de l'opération non autorisée, 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 raisons objectivement justifiées de soupçonner que le payeur a manqué, de manière intentionnelle ou à la suite d'une négligence grave, à une ou à plusieurs des obligations qui lui incombent au titre de l'article 53, et s'il communique ces motifs par écrit au payeur, ou s'il a des raisons objectivement justifiées de soupçonner que le payeur a agi frauduleusement.

2. Lorsqu'il a des raisons objectivement justifiées de soupçonner que le payeur a agi frauduleusement ou qu'il a manqué, de manière intentionnelle ou à la suite d'une négligence grave, à une ou à plusieurs des obligations qui lui incombent au titre de l'article 53, le prestataire de services de paiement du payeur, dans un délai de quinze jours ouvrables après avoir constaté ou été informé de l'opération:

a) soit rembourse au payeur le montant de l'opération de paiement non autorisée s'il a conclu, après enquête complémentaire, que le payeur n'a pas agi frauduleusement ni manqué, de manière intentionnelle ou à la suite d'une négligence grave, à une ou à plusieurs des obligations qui lui incombent au titre de l'article 53;

b) soit justifie auprès du payeur son refus de remboursement, en indiquant les organismes que le payeur peut saisir conformément aux articles 100, 101, 103, 104 et 105 si le payeur n'accepte pas les raisons données et, lorsque le prestataire de services de paiement conclut que le payeur a agi frauduleusement, il communique les raisons ayant conduit à cette conclusion à l'autorité nationale compétente.

Aux fins du premier alinéa, point b), les États membres publient le nom de l'autorité nationale compétente à laquelle la justification doit être fournie.

3. Le cas échéant, le prestataire de services de paiement du payeur rétablit le compte de paiement débité dans l'état dans lequel 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 le montant 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 dans lequel 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 56, 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. Tout autre préjudice financier causé au payeur peut être indemnisé conformément au droit applicable au contrat conclu entre le payeur et le prestataire de services de paiement concerné.

Article 58

Responsabilité du prestataire de services de paiement en cas d'application incorrecte du service de vérification de la concordance

Lorsqu'un prestataire de services de paiement ne respecte pas l'article 51, et que ce non-respect entraîne la mauvaise exécution d’une opération de paiement, le prestataire de services de paiement du payeur restitue sans tarder au payeur le montant viré et, le cas échéant, rétablit le compte de paiement débité dans l'état dans lequel il se serait trouvé si l'opération n'avait pas eu lieu.

Lorsque ce non-respect survient parce que le prestataire de services de paiement du bénéficiaire ou le prestataire de services d'initiation de paiement n'a pas respecté l'article 51, le prestataire de services de paiement du bénéficiaire ou, le cas échéant, le prestataire de services d'initiation de paiement indemnise le prestataire de services de paiement du payeur pour le préjudice financier subi du fait de ce non-respect.

Tout autre préjudice financier causé au payeur peut être indemnisé conformément au droit applicable au contrat conclu entre le payeur et le prestataire de services de paiement concerné.

Article 59

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 n'ont pas fourni, dans le cadre de leur relation contractuelle, les services nécessaires pour permettre l'application d'une authentification forte du client, de façon proportionnée à ce manquement et pour un montant n'excédant pas le montant de l'opération en question.

Article 60

Responsabilité du prestataire de services de paiement en cas d'usurpation d'identité

1. Les prestataires de services de paiement mettent en place des mesures de prévention adéquates et des garanties techniques solides pour empêcher la reproduction et l'utilisation abusive par des fraudeurs de leurs canaux de communication visant à amener les utilisateurs de services de paiement à effectuer des opérations frauduleuses.

2. Lorsqu'un utilisateur de services de paiement qui est un consommateur a été manipulé par un tiers prétendant être le prestataire de services de paiement du consommateur en utilisant les canaux de communication attribués au prestataire de services de paiement du consommateur et que cette manipulation a entraîné 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 retard injustifié après avoir eu connaissance de la fraude, informé son prestataire de services de paiement et signalé la fraude aux forces de l'ordre.

3. Dans un délai de quinze jours ouvrables après avoir été informé conformément au paragraphe 2 et avoir reçu le rapport de police remis par le consommateur ou le dépôt de plainte effectué par le consommateur auprès des forces de l'ordre, le prestataire de services de paiement:

   a) soit rembourse au consommateur le montant de l'opération de paiement autorisée frauduleusement;

   b) soit, s'il a des raisons objectivement justifiées de soupçonner que le consommateur a commis une fraude ou une négligence grave, justifie auprès du consommateur son refus de remboursement et indique les organismes que le consommateur peut saisir conformément aux articles 100, 101, 103, 104 et 105 s'il n'accepte pas les raisons données et, s'il conclut que le consommateur a agi frauduleusement, communique les raisons ayant conduit à cette conclusion à l'autorité nationale visée à l'article 57, paragraphe 2, premier alinéa, point b).

4. Le paragraphe 2 ne s'applique pas en cas d'agissement frauduleux ou de négligence grave du consommateur.

5. La charge de la preuve que le consommateur a agi frauduleusement ou a commis une négligence grave pèse sur le prestataire de services de paiement.

Avant de conclure que le consommateur a agi frauduleusement ou a commis une négligence grave, le prestataire de services de paiement invite le consommateur à fournir des informations sur les événements qui ont conduit à l'opération de paiement et tient compte de ces informations dans son évaluation. Lorsque le consommateur ne fournit pas ces informations, cela ne conduit pas en soi le prestataire de services de paiement à conclure que le consommateur a agi frauduleusement ou a commis une négligence grave. Le consommateur n'est pas tenu de fournir d'autres informations que celles qu'il est raisonnablement susceptible d'avoir.

Article 61

Coopération intersectorielle aux fins de la prévention et de la détection de la fraude

1. Lorsque la fraude en matière de paiements provient de la publication de contenus frauduleux en ligne, les prestataires de services de paiement informent, sans retard injustifié, les fournisseurs de services d'hébergement en suivant la procédure prévue à l'article 16 ou, le cas échéant, à l'article 22 du règlement (UE) 2022/2065.

2. Dans la mesure nécessaire aux fins de la prévention et de la détection d'opérations de paiement potentiellement frauduleuses, y compris les opérations impliquant des services d'initiation de paiement, lorsqu'il existe des raisons objectivement justifiées de soupçonner un comportement frauduleux de la part d'un utilisateur de leurs services, des données peuvent être échangées:

a) entre les prestataires de services de paiement et les fournisseurs de services d'hébergement;

b) entre les prestataires de services de paiement et les fournisseurs de services de communications interpersonnelles.

3. Aux fins du paragraphe 2, et sans préjudice de la directive (UE) 2022/2555, de la directive 2002/58/CE ou de l'article 101 du présent règlement, les fournisseurs de services de communications interpersonnelles ainsi que les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne établissent des canaux de communication spécifiques ou participent à un système de communication efficace ou à un mécanisme de partage d'informations, afin de permettre des échanges plus rapides et plus efficaces conformément au règlement (UE) 2016/679 et à la directive 2002/58/CE.

4. Les fournisseurs de services de communications interpersonnelles ainsi que les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne mettent en place toutes les mesures éducatives nécessaires, y compris des dispositifs d'alerte de leurs clients par tous les moyens et médias appropriés lorsque de nouvelles formes d'escroqueries en ligne apparaissent, en tenant compte des besoins des groupes de destinataires de leurs services les plus vulnérables.

Aux fins du premier alinéa du présent paragraphe, les fournisseurs de services de communications interpersonnelles donnent aux destinataires de leurs services des indications claires en ce qui concerne:

a) la manière d'identifier les tentatives de fraude;

b) les mesures et les précautions à prendre pour éviter d'être victimes d'une activité frauduleuse pouvant les viser; et

c) la procédure à suivre pour signaler toute activité frauduleuse.

Aux fins du premier alinéa du présent paragraphe, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne donnent aux destinataires de leurs services des indications claires en ce qui concerne:

a) la manière d'identifier les tentatives de fraude;

b) les mesures et les précautions à prendre pour éviter d'être victimes d'une activité frauduleuse pouvant les viser; et

c) la procédure à suivre pour signaler toute activité frauduleuse, aux fins du respect de l'article 16 du règlement (UE) 2022/2065.

5. La Commission et le comité européen des services numériques encouragent et facilitent l'élaboration d'un code de conduite volontaire au niveau de l'Union visant à favoriser la prévention, à renforcer la sécurité et à lutter contre la fraude aux paiements et les escroqueries financières, dans les conditions visées à l'article 45 du règlement (UE) 2022/2065.

6. Sans préjudice de la directive (UE) 2022/2555, les fournisseurs de services de communications interpersonnelles prennent les mesures organisationnelles et techniques appropriées pour détecter et prévenir l'utilisation de leurs services à des fins de fraude par usurpation d'identité, y compris par la manipulation de l'identification de la ligne appelante ou des adresses de courrier électronique, lorsque cette utilisation vise à inciter les utilisateurs de services de paiement à effectuer un paiement ou à prendre une mesure susceptible de compromettre la sécurité du compte de paiement. Ces mesures sont conformes au droit de l'Union applicable en matière de protection des données, en particulier le règlement (UE) 2016/679 et la directive 2002/58/CE.

Article 62

Publicité de services financiers réglementés sur les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne

1. Aux fins du présent article, on entend par "service financier réglementé" tout service ayant trait à la banque, au crédit, à l'assurance, aux pensions individuelles, aux paiements ou aux investissements, y compris les crypto-actifs et le financement participatif, pour lequel l'agrément ou l'enregistrement auprès d'une autorité compétente est requis par le droit de l'Union.

2. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne demandent à chaque annonceur d'un service financier réglementé de fournir un numéro d'agrément, un numéro d'enregistrement ou toute autre information attestant que l'annonceur est un prestataire de services financiers réglementés agréé ou enregistré pour fournir le service financier réglementé faisant l'objet de la publicité dans un État membre ou au niveau de l'Union ou qu'il agit pour le compte d'un tel prestataire.

3. Lorsqu'ils reçoivent les informations visées au paragraphe 2 du présent article, et avant d'autoriser l'annonceur concerné à utiliser leur service aux fins de la publicité de ces services financiers réglementés, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne mettent tout en œuvre, y compris en utilisant les registres des prestataires agréés ou enregistrés de services financiers réglementés mis à disposition conformément à la directive (UE) 2026/...[+] ou à d'autres dispositions pertinentes du droit de l'Union, pour évaluer si ces informations, dont l'exactitude relève de la responsabilité exclusive des annonceurs aux fins du présent règlement, sont fiables et complètes, à condition que cette évaluation puisse être effectuée de manière proportionnée à l'aide d'outils automatisés.

4. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne qui n'ont pas obtenu les informations visées au paragraphe 2 refusent d'autoriser l'annonceur de services financiers réglementés à utiliser leurs services aux fins de la publicité de ces services financiers réglementés.

5. Aux fins du respect de l'article 39, paragraphe 2, points a), b) et c), du règlement (UE) 2022/2065, lorsque l'objet d'une publicité est un service financier réglementé, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne incluent dans leurs registres de publicités des informations indiquant que l'objet de la publicité est un service financier réglementé et si l'annonceur agit pour le compte d'un prestataire de services financiers réglementés.

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

Article 63

Responsabilité du payeur en cas d'opérations de paiement non autorisées

1. Par dérogation à l'article 57, le payeur peut être tenu de supporter, jusqu'à concurrence de 50 EUR, les pertes liées à la perte, au vol ou au détournement d'un instrument de paiement ou de données de sécurité personnalisées.

Le premier alinéa ne s'applique pas:

a) si la perte, le vol ou le détournement d'un instrument de paiement ou de données de sécurité personnalisées 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.

Lorsque le payeur n'a pas agi de manière frauduleuse ni n'a manqué de manière intentionnelle aux obligations qui lui incombent au titre de l'article 53, les autorités compétentes nationales, les organismes de règlement des litiges 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. 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, de manière intentionnelle ou à la suite d'une négligence grave, à une ou à plusieurs des obligations qui lui incombent au titre de l'article 53. Dans ces cas, le montant maximal visé au paragraphe 1 du présent article ne s'applique pas.

3. 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 91, le payeur ne supporte aucune perte financière éventuelle à moins qu'il ait agi frauduleusement. Le payeur ne supporte pas non plus de perte financière lorsque le prestataire de services de paiement du payeur ou celui du bénéficiaire applique une exemption à l'utilisation de l'authentification forte du client. Lorsque le bénéficiaire ou son prestataire de services de paiement ne met pas au point ou ne modifie pas 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 la perte financière causée au prestataire de services de paiement du payeur.

4. 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.

5. 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 53, premier alinéa, 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 54, paragraphe 1, premier alinéa, 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.

6. La Commission est habilitée à adopter un acte délégué conformément à l'article 115 afin de modifier le présent règlement en mettant à jour le montant visé au paragraphe 1 du présent article.

Article 64

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, en particulier dans le cadre d'une opération de paiement liée à une carte ou d'un virement, 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 son consentement concernant le montant exact des fonds à bloquer.

2. Le montant des fonds bloqués par le prestataire de services de paiement du payeur en application du paragraphe 1 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 en application du paragraphe 1 immédiatement après réception des informations sur le montant exact de l'opération de paiement.

Article 65

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 un bénéficiaire ou par son intermédiaire 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 de prélèvements, le payeur jouit d'un droit au remboursement inconditionnel dans les délais fixés à l'article 66.

2. Aux fins du paragraphe 1, premier alinéa, point b), du présent article, 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, premier alinéa, point e), et à l'article 20, paragraphe 3, premier alinéa, point c), 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 selon des modalités convenues, 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 66

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 65, 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 quinze 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 100, 101, 103, 104 et 105 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 en cas de prélèvements.

Chapitre 5
Exécution des opérations de paiement

SECTION 1
ORDRES DE PAIEMENT ET MONTANTS TRANSFERES

Article 67

Réception des ordres de paiement

1. Le moment de réception d'un ordre de paiement est le moment où celui-ci 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 73 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 champ d'application du règlement (UE) nº 260/2012.

Article 68

Refus du prestataire de services de paiement du payeur d'exécuter une opération de paiement

1. Sous réserve du paragraphe 2, et sauf disposition contraire du droit de l'Union ou du droit national applicable, lorsque toutes les conditions énoncées dans le contrat-cadre du payeur sont remplies, le prestataire de services de paiement 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 l'intermédiaire d'un prestataire de services d'initiation de paiement, ou par un bénéficiaire ou par son intermédiaire.

2. Sans préjudice du règlement (UE) 2024/1624, le prestataire de services de paiement du bénéficiaire refuse d'exécuter une opération de paiement dans les circonstances décrites au présent paragraphe.

Nonobstant l'article 5 *quater*, paragraphe 5, du règlement (UE) nº 260/2012, et l'article 51 et l'article 73, paragraphe 1, du présent règlement, lorsque, sur la base de la surveillance des opérations visé à l'article 87 du présent règlement ou de toute autre information pertinente dont dispose le prestataire de services de paiement, mais pas uniquement sur la base du résultat du service assurant la vérification du bénéficiaire, le prestataire de services de paiement d'un payeur a des raisons objectivement justifiées de soupçonner qu'une opération de paiement est frauduleuse, le prestataire de services de paiement du payeur suspend l'exécution de l'opération de paiement.

Lorsque le prestataire de services de paiement du payeur a des raisons objectivement justifiées de soupçonner qu'une opération de paiement est frauduleuse et ne suspend pas l'exécution de l'opération de paiement conformément au présent article, le payeur ne supporte aucune perte financière, sauf s'il a agi de manière frauduleuse.

Il incombe au prestataire de services de paiement de prouver qu'il n'y a pas eu violation du présent article.

Sans retard injustifié après la suspension de l'exécution de l'opération de paiement, 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 notifie au payeur, selon des modalités convenues, toute information ou mesure requise de la part du payeur pour permettre au prestataire de services de paiement d'évaluer si les raisons de cette suspension sont toujours justifiées. La notification fournit au payeur des informations suffisantes pour lui permettre de comprendre les risques que le prestataire de services de paiement a recensés. Dans les délais prévus à l'article 73, paragraphe 1, le prestataire de services de paiement déploie tous les efforts raisonnables pour contacter le payeur, et veille à ce que des moyens appropriés soient disponibles à tout moment pour permettre au payeur de contacter le prestataire de services de paiement lorsque celui-ci demande des informations supplémentaires pour évaluer s'il existe des raisons objectivement justifiées de soupçonner une fraude.

Si, sur la base de l'évaluation visée au cinquième alinéa, il existe encore des raisons objectivement justifiées de soupçonner une fraude, le prestataire de services de paiement du payeur refuse d'exécuter l'opération de paiement et, le cas échéant, rétablit le compte de paiement débité dans l'état dans lequel il se serait trouvé si l'ordre de paiement n'avait pas été passé.

L'obligation de notifier le payeur en vertu du cinquième alinéa ne s'applique pas dans le cas des virements instantanés. En pareils cas, ou lorsqu'il n'a pas été possible pour le prestataire de services de paiement du payeur de recevoir des informations de la part du payeur dans les délais prévus à l'article 73, paragraphe 1, le prestataire de services de paiement évalue, sur la base de la surveillance des opérations visé à l'article 87 et de toute autre information pertinente dont il dispose, mais pas uniquement sur la base du résultat du service assurant la vérification du bénéficiaire, s'il y a des raisons objectivement justifiées de soupçonner une fraude, auquel cas il refuse d'exécuter l'opération de paiement.

3. Lorsque, sur la base de l'évaluation prévue au paragraphe 2, le prestataire de services de paiement refuse d'exécuter une opération de paiement, il le notifie au payeur et au prestataire de services de paiement du bénéficiaire et, le cas échéant, il met à la disposition du prestataire de services d'initiation de paiement le refus, les motifs spécifiques de ce refus et, le cas échéant, la procédure à suivre pour corriger la décision visant à refuser d'exécuter l'opération, à moins qu'une telle notification ne soit interdite au titre des dispositions pertinentes du droit de l'Union ou du droit national.

Le prestataire de services de paiement du payeur procède à la notification selon des modalités convenues et, le cas échéant, la met à la disposition du prestataire de services d'initiation de paiement sans retard injustifié et en tout état de cause dans les délais prévus à l'article 73. Dans le cas des virements instantanés, le prestataire de services de paiement du payeur procède à la notification et, le cas échéant, met les informations à la disposition du prestataire de services d'initiation de paiement, dans un délai de dix secondes à compter de la réception de l'ordre de paiement par le prestataire de services de paiement du payeur.

Le contrat-cadre peut prévoir la possibilité pour le prestataire de services de paiement d'imputer des frais raisonnables pour un refus d'exécuter une opération de paiement si un tel refus est objectivement justifié, mais pas en cas de refus dû à une opération frauduleuse présumée.

4. Aux fins du présent article, le fait qu'un ordre de paiement soit inhabituel ne constitue pas en soi une raison objectivement justifiée de soupçonner une fraude.

5. Aux fins des articles 73 et 79, un ordre de paiement pour une opération de paiement dont l'exécution a été refusée est réputé non reçu.

Article 69

Irrévocabilité des ordres de paiement

1. Un 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 ou le bénéficiaire ou par son intermédiaire, le payeur ne révoque pas l'ordre de paiement après avoir donné son consentement à ce que le prestataire de services d'initiation de paiement initie l'opération de paiement ou après avoir donné son consentement 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 les circonstances visées à l'article 67, 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 70

Montants transférés et montants reçus

1. Le prestataire de services de paiement du payeur, le prestataire 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. Lorsque 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.

Article 71

Opérations de paiement effectuées au moyen de jetons de monnaie électronique

1. Par dérogation à l'article 13, paragraphe 1, premier alinéa, points b) et d), à l'article 20, paragraphe 2, point e), à l'article 20, paragraphe 3, premier alinéa, point a), et à l'article 24, lorsque des prestataires de service de paiement ne sont pas en mesure, en raison de circonstances qui ne leur sont pas imputables, de se conformer aux obligations énoncées dans ces articles en ce qui concerne les opérations de paiement effectuées au moyen de jetons de monnaie électronique réglées dans le registre distribué, les prestataires de service de paiement fournissent les informations visées auxdits articles au moyen d'une estimation motivée, dans les meilleurs délais et, en tout état de cause, avant que le payeur n'autorise l'opération de paiement.

2. Les exigences prévues aux articles 41 et 42 pour les prestataires de services de paiement gestionnaires de comptes en ce qui concerne les services d'initiation de paiement et les services d'information sur les comptes ne s'appliquent pas aux opérations de paiement effectuées au moyen de jetons de monnaie électronique.

3. Les articles 51 et 58 ne s'appliquent pas aux prestataires de services de paiement en ce qui concerne les opérations de paiement effectuées au moyen de jetons de monnaie électronique.

4. La Commission est habilitée à adopter des actes délégués conformément à l'article 115 pour modifier le présent règlement en adaptant les dérogations et les exigences énoncées aux paragraphes 1, 2 et 3 du présent article en ce qui concerne les opérations de paiement effectuées au moyen de jetons de monnaie électronique afin de tenir compte des évolutions survenues après l'adoption du présent règlement et les spécificités de l'utilisation de la technologie des registres distribués ou d'une technologie similaire pour ces opérations.

SECTION 2

DELAI D'EXECUTION ET DATE DE VALEUR

Article 72

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 les devises des États membres dont la monnaie n'est pas l'euro;

c) aux opérations de paiement entraînant une seule conversion entre l'euro et la devise d'un État membre dont la monnaie n'est pas l'euro, à condition que la conversion requise soit effectuée dans l'État membre concerné dont la monnaie n'est pas l'euro et que, en cas d'opérations de paiement transfrontalières, le transfert transfrontalier s'effectue en euros.

2. La présente section s'applique aux opérations de paiement non mentionnées au paragraphe 1 du présent article, à moins que l'utilisateur de services de paiement et le prestataire de services de paiement n'en soient convenus autrement, à l'exception de l'article 77, 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 73 pour des opérations de paiement à l'intérieur de l'Union, ce délai plus long ne peut pas dépasser cinq jours ouvrables à compter de la réception mentionnée à l'article 67.

Article 73

Opérations de paiement effectuées vers un compte de paiement

1. Sans préjudice des dispositions pertinentes du droit de l'Union ou du droit national en matière de lutte contre le blanchiment de capitaux et de lutte contre le financement du terrorisme, le prestataire de services de paiement du payeur veille à ce que, après la réception mentionnée à l'article 67, 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. Sans préjudice des dispositions pertinentes du droit de l'Union ou du droit national en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, le prestataire de services de paiement du bénéficiaire attribue une date de valeur à l'opération de paiement et en met le montant à disposition sur le compte de paiement du bénéficiaire après que le prestataire de services de paiement a reçu les fonds conformément à l'article 77.

3. Par dérogation au paragraphe 2 du présent article, si, sur la base de la surveillance des opérations effectuée conformément à l'article 87 ou de toute information pertinente dont dispose le prestataire de services de paiement du bénéficiaire, mais pas uniquement sur la base du résultat du service assurant la vérification du bénéficiaire, le prestataire de services de paiement du bénéficiaire a des raisons objectivement justifiées de soupçonner qu'une opération de paiement créditée ou à créditer sur son compte est frauduleuse, ce prestataire de services de paiement peut, conformément à son obligation de s'abstenir d'exécuter des transactions suspectes prévue à l'article 71 du règlement (UE) 2024/1624, décider de ne pas mettre les fonds à disposition sur le compte de paiement du bénéficiaire et de les restituer au prestataire de services de paiement du payeur, à condition que cette décision ait lieu dans le délai fixé à l'article 77 du présent règlement.

Lorsque les raisons de soupçonner qu'une opération de paiement créditée ou à créditer sur le compte du bénéficiaire est frauduleuse sont claires et incontestables, le prestataire de services de paiement du bénéficiaire ne met pas les fonds à disposition sur le compte de paiement du bénéficiaire et les restitue au prestataire de services de paiement du payeur.

Lorsque le prestataire de services de paiement du bénéficiaire ne respecte pas l'obligation énoncée au deuxième alinéa, le payeur ne supporte aucune perte financière à moins qu'il ait agi frauduleusement.

Les premier et deuxième alinéas du présent paragraphe sont sans préjudice de l'obligation qui incombe au prestataire de services de paiement du bénéficiaire de déclarer les transactions suspectes prévue à l'article 69 du règlement (UE) 2024/1624.

Aux fins du présent article, le fait qu'une opération de paiement soit inhabituelle ne constitue pas en soi une raison objectivement justifiée de soupçonner une fraude.

Il incombe au prestataire de services de paiement du bénéficiaire de prouver qu'il n'y a pas eu violation du deuxième alinéa.

4. Lorsque le prestataire de services de paiement du bénéficiaire restitue les fonds au prestataire de services de paiement du payeur conformément au paragraphe 3, premier ou deuxième alinéa, le prestataire de services de paiement du bénéficiaire:

a) notifie immédiatement au prestataire de services de paiement du payeur la restitution des fonds, ainsi que les motifs du refus de mettre les fonds à disposition sur le compte de paiement du bénéficiaire, conformément aux règles relatives à l'interdiction de divulgation énoncées à l'article 73, paragraphe 5, du règlement (UE) 2024/1624; et

b) veille à ce que le montant de l'opération de paiement soit crédité au prestataire de services de paiement du payeur dans le délai fixé au paragraphe 1 du présent article.

5. Dès réception de la notification prévue au paragraphe 4, point a), du présent article, le prestataire de services de paiement du payeur informe immédiatement le payeur, sans frais, que les fonds n'ont pas été mis à disposition sur le compte de paiement du bénéficiaire en raison de mesures visant à prévenir la fraude, sans préjudice de l'article 73 du règlement (UE) 2024/1624, et, le cas échéant, met cette information à la disposition du prestataire de services d'initiation de paiement. Le prestataire de services de paiement du payeur informe également le payeur de la restitution des fonds et du délai dans lequel le montant de l'opération de paiement sera mis à disposition sur le compte de paiement du payeur. Le prestataire de services de paiement du payeur attribue une date de valeur et met à disposition le montant de l'opération de paiement crédité sur son compte conformément au paragraphe 4, point b), du présent article sur le compte de paiement du payeur conformément à l'article 77 du présent règlement.

6. Dans le cas d'un virement instantané, lorsque le prestataire de services de paiement du bénéficiaire restitue les fonds au prestataire de services de paiement du payeur conformément au paragraphe 3, premier ou deuxième alinéa, le prestataire de services de paiement du bénéficiaire:

   a) dans un délai de dix secondes à compter de la réception de l'ordre de paiement pour un virement instantané par le prestataire de services de paiement du payeur, notifie au prestataire de services de paiement du payeur la restitution des fonds, ainsi que les motifs du refus de mettre les fonds à disposition sur le compte de paiement du bénéficiaire, conformément aux règles relatives à l'interdiction de divulgation énoncées à l'article 73, paragraphe 5, du règlement (UE) 2024/1624; et

   b) lorsque le montant de l'opération a été crédité sur son compte, veille à ce que ces fonds soient crédités immédiatement au prestataire de services de paiement du payeur.

7. Dès réception de la notification visée au paragraphe 6, point a), le prestataire de services de paiement du payeur:

a) rétablit le compte de paiement du payeur dans l'état dans lequel il se serait trouvé si l'opération n'avait pas eu lieu; et

b) informe le payeur, sans frais, de la restitution des fonds et, sans préjudice de l'article 73 du règlement (UE) 2024/1624, du fait que les fonds n'ont pas été mis à disposition sur le compte de paiement du bénéficiaire en raison de mesures visant à prévenir la fraude et, le cas échéant, met ces informations à la disposition du prestataire de services d'initiation de paiement.

8. 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. Le paragraphe 3 s'applique en conséquence.

Article 74

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 73, paragraphe 1.

Dans le cas d'opérations de paiement effectuées en jetons de monnaie électronique depuis un portefeuille de conservation vers une adresse auto-hébergée, le prestataire de services de paiement du payeur transfère les fonds à l'adresse auto-hébergée du bénéficiaire dans le délai fixé à l'article 73, paragraphe 1.

Article 75

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 76

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.

Au plus tard le … [21 mois à compter de la date d'entrée en vigueur du présent règlement], les États membres notifient à la Commission les dispositions législatives qu'ils adoptent en vertu du premier alinéa. Ils notifient sans retard injustifié à la Commission toute modification ultérieure qui y est apportée et toute disposition législative qu'ils adoptent en vertu du premier alinéa à une date ultérieure.

Article 77

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, l'une des conditions suivantes s'applique:

   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 78

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 79 de l'inexécution ou de la mauvaise exécution de l'opération de paiement.

   Toutefois, 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 deuxième 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.

3. 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. Ces frais sont raisonnables et proportionnés aux dépenses engagées.

4. 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, paragraphe 2, point b), 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.

5. 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 80.

Article 79

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 55, de l'article 78, paragraphe 2, et de l'article 83, 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 73, 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 dans lequel 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 77.

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 55, de l'article 78, paragraphe 2, et de l'article 83, 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 73, paragraphe 8. 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 55, de l'article 78, paragraphe 2, et de l'article 83, 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 77. 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 sans retard injustifié, le montant de l'opération de paiement non exécutée ou mal exécutée et rétablit le compte de paiement débité dans l'état dans lequel 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 80

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 55 et de l'article 78, paragraphe 2, 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 dans lequel 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 67 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 81

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 82

Droit de recours

1. Lorsque la responsabilité d'un prestataire de services de paiement au titre des articles 57, 58 et 60, de l'article 68, paragraphe 2, de l'article 73, paragraphe 3, et des articles 79, 80 et 87 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 57, 58 et 60, de l'article 68, paragraphe 2, de l'article 73, paragraphe 3, et des articles 79, 80 et 87. Cette indemnisation s'applique au cas où l'un des prestataires de services de paiement n'applique pas l'authentification forte du client.

2. Lorsqu'un fournisseur de services d'hébergement ne remplit pas les conditions énoncées à l'article 6, paragraphe 1, points a) et b), du règlement (UE) 2022/2065 en ce qui concerne le stockage de contenus illicites au sens de l'article 3, point h), dudit règlement et que ces contenus donnent lieu à une ou plusieurs opérations de paiement non autorisées visées à l'article 57 du présent règlement, ou à une ou plusieurs opérations de paiement autorisées de façon frauduleuse visées à l'article 60 du présent règlement, ce fournisseur indemnise le prestataire de services de paiement pour toute perte subie ou toute somme payée au titre des articles 57 et 60 du présent règlement.

3. Des indemnisations financières complémentaires peuvent être fixées conformément aux conventions qui existent entre les prestataires de services de paiement ou les intermédiaires et conformément à la loi applicable à la convention qu'ils ont conclue.

Article 83

Circonstances anormales et imprévisibles

Aucune responsabilité au titre du chapitre 4 ou du présent chapitre 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 84

Protection des données

Les systèmes de paiement, les schémas de paiement, les entités de traitement 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 d'un marché intérieur performant des services de paiement, sous réserve de garanties appropriées pour les libertés et droits fondamentaux des personnes physiques, y compris:

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, y compris 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 85

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:

   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 35, paragraphe 1, de la directive (UE) 2026/…[+]; et

   c) aux établissements de paiement exemptés en vertu de l'article 33, paragraphe 1, de la directive (UE) 2026/…[+].

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

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'ENISA (l'Agence de l'Union européenne pour la cybersécurité).

Article 86

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.

   Les données statistiques relatives à la fraude comprennent le nombre et la valeur des opérations de paiement frauduleuses remboursées et des opérations de paiement pour lesquelles un remboursement a été refusé conformément au présent règlement, ainsi que le motif de ce refus, telle que l'indication que le consommateur a agi frauduleusement ou a commis une négligence grave.

2. Les autorités compétentes peuvent autoriser les prestataires de services de paiement à satisfaire à l'obligation prévue au paragraphe 1 en déclarant les données relatives à la fraude au titre d'une autre obligation de déclaration de données, si ladite obligation n'est pas moins étendue que l'obligation de déclaration prévue par le présent article et si des dispositions ont été prises en vertu desquelles l'ABE et la BCE recevront les données dues au titre du présent article.

3. L'ABE et la BCE publient dans un rapport annuel conjoint les données statistiques sous forme agrégée et une analyse des tendances observées sur la base de ces données.

4. L'ABE élabore, en étroite coopération avec la BCE, des projets de normes techniques de réglementation précisant les données statistiques relatives à la fraude à fournir conformément au paragraphe 1.

L'ABE soumet les projets de normes techniques de réglementation visés au premier alinéa à la Commission au plus tard le … [12 mois à compter de la date d'entrée en vigueur du présent règlement].

La Commission est habilitée à adopter ces normes techniques de réglementation conformément aux articles 10 à 14 du règlement (UE) nº 1093/2010.

5. 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. Ces normes techniques d'exécution ne sont pas applicables si l'autorité compétente fait usage de la possibilité visée au paragraphe 2.

L'ABE soumet les normes techniques d'exécution visées au premier alinéa à la Commission au plus tard le … [12 mois à compter de la date d'entrée en vigueur du présent règlement].

La Commission est habilitée à adopter ces normes techniques d'exécution conformément à l'article 15 du règlement (UE) n° 1093/2010.

Article 87

Mécanismes de surveillance des opérations

1. Les prestataires de services de paiement mettent en place des mécanismes de surveillance des opérations afin de:

   a) prendre en charge l'application de la procédure d'authentification forte du client conformément à l'article 91;

   b) déroger à l'application de l'authentification forte du client sur la base des critères énoncés à l'article 91, paragraphe 9, 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) prévenir et détecter les opérations de paiement potentiellement frauduleuses, y compris les opérations impliquant des services d'initiation de paiement.

   Les mécanismes de surveillance des opérations sont fondés sur l'analyse des opérations de paiement antérieures et de l'accès aux comptes de paiement en ligne.

2. Les prestataires de services de paiement veillent à ce que leurs mécanismes de surveillance 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. Le prestataire de services de paiement du payeur procède à la surveillance des opérations prévue au paragraphe 1 avant l'exécution d'une opération de paiement.

Le prestataire de services de paiement du bénéficiaire procède à la surveillance des opérations visée au paragraphe 1 du présent article avant que les fonds ne soient mis à la disposition du bénéficiaire conformément à l'article 73, paragraphe 2.

Lorsqu'un prestataire de services de paiement ne procède pas à la surveillance des opérations conformément au présent article à l'égard d'une opération et que le payeur subit un préjudice financier, ce prestataire de services de paiement en assume la responsabilité à l'égard du payeur.

Lorsque le prestataire de services de paiement du payeur ne fournit pas au payeur la preuve que la surveillance des opérations a été effectuée par les deux prestataires, il rembourse au payeur le montant de l'opération.

Le payeur ne supporte aucune conséquence financière résultant de cette opération, sauf agissement frauduleux de sa part.

Il incombe au prestataire de services de paiement concerné de prouver qu'il n'y a pas eu violation du présent paragraphe.

4. Le traitement par le prestataire de services de paiement du payeur est limité aux données suivantes, dans la mesure où cela est nécessaire aux fins mentionnées au paragraphe 1:

a) les informations sur le payeur, y compris 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, y compris l'historique des opérations de paiement;

c) les informations relatives à l'opération, y compris le montant de l'opération, l'instrument de paiement, la devise, la date et l'heure de l'exécution, ainsi que l'identifiant unique du bénéficiaire;

d) les données de la session, y compris la plage d'adresse IP de l'appareil à partir duquel le compte de paiement a été consulté et à partir duquel l'opération a été initiée;

e) les données de l'appareil, y compris les identifiants de l'appareil à partir duquel l'opération a été initiée;

f) les informations sur le bénéficiaire, y compris son identifiant unique;

g) les informations reçues dans le cadre des dispositifs de partage d'informations.

5. Le traitement par le prestataire de services de paiement du bénéficiaire est limité aux données suivantes, dans la mesure où cela est nécessaire aux fins mentionnées au paragraphe 1:

a) les informations sur le bénéficiaire;

b) les informations reçues dans le cadre des dispositifs de partage d'informations;

c) les informations sur le compte de paiement du bénéficiaire, y compris l'historique des opérations de paiement;

d) les informations relatives à l'opération, y compris le montant de l'opération, l'instrument de paiement, la devise, la date et l'heure de l'exécution, ainsi que le nom du payeur.

6. Les prestataires de services de paiement ne conservent pas les données mentionnées aux paragraphes 4 et 5 plus longtemps que nécessaire aux fins énoncées au paragraphe 1, et, en tout état de cause, pas plus de cinq ans après la cessation de la relation avec le client.

Article 88

Partage d'informations relatives à la fraude

1. Les prestataires de services de paiement participent aux dispositifs de partage d'informations avec les autres prestataires de services de paiement comme prévu au paragraphe 4 et échangent des données dans la mesure nécessaire pour se conformer aux obligations qui leur incombent en vertu de l'article 87, paragraphe 1, premier alinéa, point c), du présent règlement lorsque le prestataire de services de paiement a des raisons objectivement justifiées de soupçonner un comportement frauduleux de la part d'un utilisateur de services de paiement. Les catégories de données à partager sont limitées aux données énumérées à l'article 87, paragraphe 4, points a) à f), et paragraphe 5, points a), c) et d), du présent règlement, aux raisons objectivement justifiées qui ont amené le prestataire de services de paiement à soupçonner un comportement frauduleux sur la base de ces données, et aux notifications effectuées par le prestataire de services de paiement à un fournisseur de services d'hébergement conformément à l'article 16 du règlement (UE) 2022/2065. Les informations sur les caractéristiques de l'environnement et du comportement du payeur qui sont typiques d'une utilisation normale des données de sécurité personnalisées sont exclues du partage d'informations au titre du présent article.

2. Les prestataires de services de paiement mettent en œuvre des mesures techniques et organisationnelles appropriées, y compris des mesures permettant la pseudonymisation, afin de garantir un niveau de sécurité et de confidentialité proportionné à la nature et à l'étendue des informations échangées.

3. Les prestataires de services de paiement ne conservent pas les données obtenues à la suite de l'échange d'informations mentionné au paragraphe 1 du présent article plus longtemps qu'il n'est nécessaire aux fins prévues à l'article 87, paragraphe 1, premier alinéa, point c), et en tout état de cause pas plus de cinq ans après que l'opération frauduleuse présumée a eu lieu.

4. Les dispositifs de partage d'informations précisent les modalités de participation et les détails des éléments opérationnels, y compris de l'utilisation de plateformes 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 conformément à l'article 35 du règlement (UE) 2016/679 et, le cas échéant, consultent au préalable l'autorité de contrôle conformément à l'article 36 dudit règlement.

5. Les prestataires de services de paiement ne tirent pas de conclusions ni ne prennent de décisions ayant une incidence sur une relation d'affaires avec l'utilisateur de services de paiement, telles que la résiliation de la relation contractuelle avec l'utilisateur ou la perturbation de leur future entrée en relation, en se fondant uniquement sur les informations reçues d'autres prestataires de services de paiement adhérant à un dispositif de partage d'informations sans avoir évalué ces informations.

Article 89

Plateforme de lutte contre la fraude

1. La Commission met en place une plateforme de lutte contre la fraude dans le domaine des services de paiement dans l'Union. La plateforme de lutte contre la fraude est composée d'un éventail large et équilibré de représentants et d'experts, issus tant du secteur public que du secteur privé, ayant des connaissances et une expérience avérées dans le domaine de la fraude aux services de paiement.

2. La plateforme de lutte contre la fraude:

   a) conseille la Commission sur l'élaboration et le suivi de la mise en œuvre d'actes juridiques visant à lutter contre la fraude dans le domaine des services de paiement;

   b) adresse des recommandations à la Commission et au comité européen des services numériques aux fins de l'élaboration du code de conduite volontaire visé à l'article 61, paragraphe 5;

   c) partage des informations et analyse les tendances en matière de fraude dans le domaine des services de paiement;

   d) partage des informations sur les mesures de lutte contre la fraude dans le domaine des services de paiement, y compris les mesures d'atténuation;

   e) partage des informations sur la manière d'améliorer la coopération transfrontalière et intersectorielle relative aux moyens de lutter contre la fraude dans le domaine des services de paiement.

3. La plateforme de lutte contre la fraude est présidée par un représentant de la Commission et constituée dans le respect des règles horizontales applicables à la création et au fonctionnement des groupes d'experts de la Commission.

4. La plateforme de lutte contre la fraude rend compte chaque année de ses activités au Parlement européen et au Conseil.

Article 90

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 orientations claires sur la manière d'identifier les tentatives de fraude et les conseillent quant aux mesures nécessaires et aux précautions à prendre pour éviter d'être victimes d'une activité frauduleuse pouvant les viser. Les prestataires de services de paiement indiquent à leurs clients où ils peuvent signaler une activité frauduleuse et obtenir rapidement des informations relatives à la fraude.

2. Les États membres mettent en place des mesures adéquates, dotées d'un financement approprié, pour sensibiliser le public aux tendances et aux nouvelles formes de fraude en matière de paiements, aux procédures à suivre pour identifier les tentatives de fraude et aux droits et obligations conférés par le présent règlement en matière de fraude. Les mesures de communication sont suffisantes et bien ciblées, en particulier pour atteindre les groupes de consommateurs les plus vulnérables, y compris les jeunes et les personnes âgées ainsi que les personnes ayant des compétences numériques limitées. Les États membres informent la Commission des mesures adoptées.

3. Les prestataires de services de paiement, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne et les fournisseurs de services de communications interpersonnelles coopèrent gratuitement avec les États membres dans le cadre des mesures visées au paragraphe 2.

4. 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 qui participent activement à la conception, à la maintenance ou à la fourniture de services de paiement, 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 en matière de paiements.

Article 91

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) passe un ordre de paiement pour une opération de paiement électronique;

   c) exécute, grâce à un moyen de communication à distance, toute autre action susceptible de comporter un risque de fraude en matière de paiements ou de toute autre utilisation frauduleuse, y compris le fait de demander la création ou le remplacement d'un instrument de paiement tokenisé par l'intermédiaire d'un moyen de communication à distance, d'augmenter ses limites de dépenses conformément à l'article 52, de modifier son mot de passe en ligne ou de modifier ses coordonnées en ligne.

2. Les opérations de paiement qui sont initiées 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. Les remboursements initiés par le bénéficiaire initial en faveur du payeur initial dans le cadre de telles opérations ne sont pas soumis à une authentification forte du client.

3. Lorsque le mandat du payeur au bénéficiaire pour passer des ordres de paiement concernant des opérations initiées par des commerçants 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.

4. En ce qui concerne les prélèvements, lorsque le mandat du payeur au bénéficiaire pour initier un ou plusieurs prélèvements est donné grâce à un moyen de communication à distance avec la participation directe du prestataire de services de paiement du payeur, la mise en place d'un tel mandat est soumise à une authentification forte du client.

5. Les opérations fondées sur des ordres de paiement passés par courrier ou par téléphone ne sont pas soumises à une authentification forte du client, à condition que le prestataire de services de paiement du payeur mette en œuvre des exigences de sécurité et des vérifications permettant une forme d'authentification de l'opération de paiement.

6. Pour la passation à distance d'un ordre de paiement mentionnée au paragraphe 1, point b), 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.

7. Pour la passation d'un ordre de paiement mentionnée au paragraphe 1, point b), 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.

8. 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.

9. Toute exemption à l'application de l'authentification forte du client prévue par l'ABE en vertu de l'article 97 repose sur un ou plusieurs des critères suivants:

   a) le niveau de risque de fraude lié au service fourni, en particulier sur la base des mécanismes de surveillance des opérations prévus à l'article 87;

   b) le montant, le caractère récurrent de l'opération ou les deux;

   c) le moyen utilisé pour exécuter l'opération;

   d) le fait que le payeur soit ou non un consommateur.

Les exemptions à l'application de l'authentification forte du client ne sont pas obligatoires. Un prestataire de services de paiement qui met en œuvre une exemption conserve toujours le droit de décider que, en fonction des circonstances et sur la base d'une évaluation des risques, une authentification forte du client est nécessaire.

10. Les deux éléments ou plus mentionnés à l'article 3, point 60), sur lesquels repose l'authentification forte du client appartiennent à des catégories différentes.

Par dérogation au premier alinéa du présent paragraphe, un prestataire de services de paiement peut mettre en œuvre une authentification forte du client utilisant deux éléments appartenant uniquement à la catégorie "inhérence" s'il démontre à l'autorité nationale compétente que l'indépendance des deux éléments est à tout moment totalement préservée et que la procédure d'authentification garantit à tout moment un niveau élevé de sécurité.

L'ABE élabore, au plus tard le … [18 mois à compter de la date d'entrée en vigueur du présent règlement], conformément à l'article 16 du règlement (UE) n° 1093/2010, des orientations sur la manière d'évaluer si l'indépendance des deux éléments relevant de la catégorie "inhérence" est totalement préservée.

Article 92

Authentification forte du client en ce qui concerne certains virements

1. Par dérogation à l'article 91, paragraphe 1, point b), dans le contexte d'un ou de plusieurs virements récurrents initiés par le prestataire de services de paiement du payeur conformément au présent article, l'obligation d'appliquer l'authentification forte du client ne s'applique pas lorsque toutes les conditions suivantes sont remplies:

   a) les virements sont initiés par le prestataire de services de paiement du payeur à la demande du bénéficiaire;

   b) la demande du bénéficiaire est fondée sur un accord entre le payeur et le bénéficiaire fixant les conditions de paiement en ce qui concerne la fréquence et les montants à payer, y compris la question de savoir si les montants peuvent varier et les circonstances dans lesquelles les montants peuvent varier;

   c) le payeur accepte que son prestataire de services de paiement exécute les virements respectifs conformément à l'accord visé au point b) du présent paragraphe et la mise en place d'un tel accord est soumise à une authentification forte du client;

   d) aucune mesure supplémentaire n'est requise de la part du payeur pour initier les virements respectifs.

2. Lorsque le paragraphe 1 s'applique, les articles 64, 65 et 66 s'appliquent mutatis mutandis, à l'exception de l'article 65, paragraphe 1, quatrième alinéa, et de l’article 66, paragraphe 2, second alinéa.

Article 93

Authentification forte du client en ce qui concerne les services d'initiation de paiement et d'information sur les comptes

1. L'article 91, paragraphes 6, 7 et 10, s'applique lorsque les opérations de paiement sont initiées par l'intermédiaire d'un prestataire de services d'initiation de paiement. L'article 91, paragraphe 8, 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 91, paragraphes 1 et 8, et, lorsque le prestataire de services d'initiation de paiement intervient, conformément à l'article 91, paragraphes 1, 6, 7, 8 et 10.

3. Sans préjudice du paragraphe 2, lorsque les données 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, mais pas pour les accès ultérieurs de ce prestataire de services d'information sur les comptes à ce compte de paiement, sauf si le prestataire de services de paiement gestionnaire du compte a des motifs raisonnables de soupçonner une fraude.

4. Les prestataires de services d'information sur les comptes appliquent l'authentification forte du client lorsque l'utilisateur de services de paiement accède aux données sur les comptes de paiement en recourant à ce prestataire de services d'information sur les comptes au moins 180 jours après la dernière application de l'authentification forte du client. Les prestataires de services d'information sur les comptes peuvent appliquer leur propre authentification forte du client ou celle du prestataire de services de paiement gestionnaire du compte.

Article 94

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 le prestataire de services techniques dans les cas où ce dernier fournit et vérifie les éléments de l'authentification forte du client.

Article 95

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 leurs clients, y compris les personnes handicapées, les personnes âgées, les personnes ayant des compétences numériques limitées 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, sans frais, à une authentification forte du client. Dans les cas où l'utilisateur de services de paiement demande de l'aide ou a besoin d'une assistance, le prestataire de services de paiement veille à ce qu'un soutien soit fourni. Cette exigence ne s'étend pas à la fourniture de dispositifs à l'utilisateur de services de paiement. Les prestataires de services de paiement veillent à ce que les utilisateurs de services de paiement soient correctement informés des différents moyens à leur disposition pour 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 subordonnent pas l'exécution de l'authentification forte du client, explicitement ou implicitement, à la possession d'un téléphone intelligent (smartphone) ou d'un autre dispositif intelligent, à moins que l'utilisateur de services de paiement n'ait consenti à la prestation de services exclusivement au moyen d'applications mobiles sur un tel dispositif. Les prestataires de services de paiement mettent au point plus d'un moyen d'application de l'authentification forte du client afin de tenir compte de la situation spécifique de leurs clients, y compris ceux visés au paragraphe 1.

Article 96

Accès équitable, raisonnable et non discriminatoire aux appareils mobiles

1. Sans préjudice de l'article 6, paragraphe 7, du règlement (UE) 2022/1925, les fabricants d'équipements d'origine d'appareils mobiles et les fournisseurs de services de communications électroniques permettent aux prestataires de services de paiement et aux prestataires de services techniques agissant en leur nom d'interopérer efficacement avec les caractéristiques techniques, telles que les caractéristiques matérielles et logicielles, qui sont nécessaires au traitement et à l'exécution sécurisés des opérations de paiement, ainsi que d'accéder à ces caractéristiques aux fins de l'interopérabilité, dans des conditions équitables, raisonnables et non discriminatoires.

2. Rien n'empêche les fabricants d'équipements d'origine d'appareils mobiles et les fournisseurs de services de communications électroniques de prendre des mesures strictement nécessaires et proportionnées visant à éviter que l'interopérabilité ne compromette l'intégrité des caractéristiques matérielles et logicielles concernées par l'obligation d'interopérabilité, à condition que ces mesures soient dûment justifiées.

3. Aux fins de l'application de conditions équitables, raisonnables et non discriminatoires d'interopérabilité efficace et d'accès conformément au paragraphe 1, les fabricants d'équipements d'origine d'appareils mobiles et les fournisseurs de services de communications électroniques publient les conditions générales applicables à cette interopérabilité efficace et à cet accès.

Article 97

Normes techniques de réglementation concernant l'authentification, la communication et les mécanismes de surveillance 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 91;

   b) les dérogations à l'application de l'article 91, paragraphes 1, 6 et 7, sur la base des critères énoncés à l'article 91, paragraphe 9;

   c) les exigences auxquelles doivent satisfaire les mesures de sécurité, conformément à l'article 91, paragraphe 8, 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 94, 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 dédiées;

g) les exigences techniques applicables aux mécanismes de surveillance des opérations mentionnés à l'article 87.

Aux fins du premier alinéa, 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:

a) les conditions qui doivent être remplies pour qu'une opération de paiement électronique à distance soit considérée comme présentant un faible niveau de risque;

b) les méthodes et modèles de mise en œuvre de l'analyse des risques liés à l'opération;

c) 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 d'instruments de paiement et des services d'acquisition d'opérations de paiement, ou au sein des prestataires de services de paiement fournissant des services d'émission d'instruments de paiement et des services d'acquisition d'opérations de paiement par l'intermédiaire d'une entité juridique unique;

d) 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;

f) la nécessité de trouver un équilibre entre le risque de fraude dans le service ou l'activité économique concerné et l'expérience du consommateur, en particulier en ce qui concerne les opérations de faible valeur;

g) le fait que les payeurs intervenant dans une opération soient ou non des consommateurs.

L'ABE soumet les projets de normes techniques de réglementation visés au paragraphe 1 à la Commission au plus tard le … [12 mois à compter de la date d'entrée en vigueur du présent règlement].

La Commission est habilitée à adopter ces normes techniques de réglementation 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 les normes techniques de réglementation et, le cas échéant, élabore à intervalles réguliers des projets de normes techniques de réglementation actualisées, 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 sanctions

SECTION 1

EXECUTION EN CE QUI CONCERNE LES TRES GRANDES PLATEFORMES EN LIGNE ET LES TRES GRANDS MOTEURS DE RECHERCHE EN LIGNE

Article 98

Exécution des dispositions en ce qui concerne les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne

La Commission dispose de pouvoirs exclusifs pour surveiller et contrôler le respect de l'article 61, paragraphe 4, troisième alinéa, point c), et de l'article 62, lorsque les obligations prévues par ces dispositions s'appliquent aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne.

Le chapitre IV du règlement (UE) 2022/2065 s'applique aux fins de cette surveillance et de ce contrôle. Toute référence au respect des dispositions pertinentes du règlement (UE) 2022/2065 qui y figure est réputée inclure l'article 61, paragraphe 4, troisième alinéa, point c), et l'article 62 du présent règlement, lorsque les obligations prévues par ces dispositions s'appliquent aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne.

Dans la mesure où des pouvoirs sont conférés à la Commission en vertu du chapitre IV du règlement (UE) 2022/2065, ces pouvoirs couvrent également l'application de l'article 61, paragraphe 4, troisième alinéa, point c), et de l'article 62 du présent règlement, lorsque ces obligations s'appliquent aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne.

SECTION 2

INTERDICTION DE FOURNIR DES SERVICES DE PAIEMENT

Article 99

Interdiction faite aux personnes autres que les prestataires de services de paiement de fournir des services de paiement

Les personnes physiques ou morales qui ne sont ni des prestataires de services de paiement, ni exclues du champ d'application du présent règlement en application de l'article 2, paragraphe 3, ne peuvent pas fournir des services de paiement.

SECTION 3

PROCEDURES DE RECLAMATION ET POUVOIRS D'ENQUETE

Article 100

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 visées à l'article 101 en cas de violation alléguée 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 du présent article informe l'auteur de la réclamation de l'existence des procédures de règlement extrajudiciaire des litiges instituées conformément à l'article 105.

3. Au plus tard le … [21 mois à compter de 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 visées au paragraphe 1, notamment concernant les canaux de dépôt des réclamations, les informations demandées aux auteurs des réclamations et la publication de l'analyse agrégée des réclamations.

Article 101

Autorités compétentes et pouvoirs de surveillance et d'enquête

1. Les États membres désignent les autorités compétentes chargées d'exercer les fonctions et missions prévues par le présent règlement. Ils notifient la liste de ces autorités compétentes à l'ABE et à la Commission.

   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, y compris les banques centrales nationales.

   Les autorités compétentes sont indépendantes des instances économiques et ne présentent aucun conflit d'intérêts. Sans préjudice du deuxième alinéa, point b), les établissements de paiement, les établissements de crédit et les offices de chèques postaux ne peuvent être désignés comme autorités compétentes.

2. Si les États membres désignent plusieurs autorités compétentes en vertu du paragraphe 1, ils définissent les missions de chacune et désignent une autorité compétente comme point de contact unique aux fins de la coopération administrative transfrontalière entre les autorités compétentes ainsi qu'avec l'ABE. Les États membres peuvent désigner un point de contact unique différent pour chaque type de coopération administrative.

3. Les autorités compétentes exercent leurs pouvoirs d'enquête sur les infractions potentielles au présent règlement et imposent des sanctions administratives, des astreintes et d'autres 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 leurs pouvoirs à d'autres autorités ou organes conformément au premier alinéa, point c), cette délégation de pouvoir précise les tâches déléguées et les conditions dans lesquelles elles doivent être exécutées et 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 leurs pouvoirs sont délégués.

4. Les autorités compétentes prennent toutes les mesures appropriées pour garantir et contrôler le respect effectif du présent règlement.

5. Les autorités compétentes disposent de tous les pouvoirs de surveillance et d'enquête et des ressources nécessaires à l'exercice de leurs fonctions.

Ces pouvoirs comprennent au moins:

a) dans le cadre des procédures d'enquête sur les infractions potentielles au présent règlement, le pouvoir d'exiger toutes les informations nécessaires à l'accomplissement des missions des autorités compétentes de la part, entre autres, des personnes physiques ou morales suivantes:

i) les prestataires de services de paiement;

ii) les prestataires de services techniques, les opérateurs de schémas de paiement et les opérateurs de systèmes de paiement qui ne sont pas couverts par le règlement (UE) 2025/1355, sans préjudice de la surveillance des opérations de ces systèmes de paiement par l'Eurosystème ou les banques centrales des États membres dont la monnaie n'est pas l'euro;

iii) les fournisseurs de distributeurs automatiques de billets;

iv) les fournisseurs de services de communications interpersonnelles;

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 les succursales des entités mentionnées aux points i), ii) et iii) qui sont établis dans l'État membre de l'autorité compétente;

viii) dans la mesure où le droit national le permet, toute autre personne, en particulier celles participant à l'initiation, au traitement ou à l'exécution de services de paiement;

b) le pouvoir de mener toutes les enquêtes nécessaires auprès de toute personne mentionnée au point a), qui est établie ou située sur le territoire de l'État membre de l'autorité compétente ou qui y fournit 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 aux points 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 aux points 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 des personnes morales et sur des sites autres que la résidence privée des personnes physiques mentionnées au point a), sous réserve de notification préalable par les autorités compétentes concernées;

d) le pouvoir de pénétrer, dans le respect du droit national, dans les locaux de personnes physiques et morales afin de saisir des articles, des documents et des données, sous quelque forme que ce soit, lorsqu'il existe une suspicion raisonnable que des articles, des documents ou des données liés à l'objet de l'inspection ou de l'enquête pourraient se révéler nécessaires et pertinents pour apporter la preuve d'une d'infraction au présent règlement;

e) le pouvoir de se faire remettre, dans la mesure où le droit national l'autorise, les enregistrements existants d'échanges de données détenus par un opérateur de télécommunications, lorsqu'il existe une suspicion raisonnable d'infraction et que de tels enregistrements peuvent se révéler nécessaires pour une enquête relative à une infraction au présent règlement;

f) le pouvoir de demander le gel ou la mise sous séquestre d'actifs, ou les deux;

g) le pouvoir de renvoyer une affaire à des fins d'enquête pénale;

h) en l'absence d'autres moyens disponibles pour faire cesser ou prévenir toute infraction au présent règlement et afin de prévenir le risque de préjudice grave pour les intérêts des consommateurs, dans la mesure où le droit national l'autorise et conformément, le cas échéant, à l'article 9 du règlement (UE) 2022/2065, le pouvoir de prendre l'une des mesures suivantes, y compris en demandant à un tiers ou à une autre autorité publique de les mettre en œuvre:

   i) émettre une injonction pour retirer un contenu d'une interface en ligne, restreindre l'accès à celle-ci ou afficher explicitement une mise en garde à l'intention des consommateurs lorsqu'ils accèdent à une interface en ligne;

   ii) ordonner à un fournisseur de services d'hébergement qu'il supprime ou désactive l'accès à une interface en ligne;

   iii) ordonner aux opérateurs de registre de noms de domaine ou aux bureaux d'enregistrement de noms de domaine de supprimer un nom de domaine complet et permettre à l'autorité compétente concernée de l'enregistrer;

i) le pouvoir d'interdire une offre de services de paiement lorsque les autorités compétentes constatent qu'il y a eu infraction au présent règlement ou lorsqu'il existe des motifs raisonnables de soupçonner qu'il y aura infraction au présent règlement;

j) le pouvoir de suspendre ou interdire les communications commerciales lorsqu'il existe des motifs raisonnables de soupçonner qu'il y a eu infraction au présent règlement;

k) le pouvoir d'interdire la prestation de services de paiement lorsque les autorités compétentes constatent qu'il y a eu infraction au présent règlement;

l) lorsqu'il y a lieu de supposer qu'une personne fournit des services de paiement sans l'agrément ou l'enregistrement requis, le pouvoir d'ordonner la cessation immédiate de l'activité sans préavis ni délai;

m) le pouvoir d'émettre des avis au public.

Aux fins du premier alinéa, point m), si les informations publiées par l'autorité compétente se révèlent fausses ou si les circonstances sous-jacentes se révèlent inexactes, l'autorité compétente informe le public de cette circonstance de la même manière qu'elle a précédemment publié les informations en question.

6. L'ABE publie, sur son site internet, la liste des autorités compétentes désignées au titre des paragraphes 1 et 2.

7. Lorsque le droit d'un État membre prévoit des sanctions pénales applicables aux infractions au présent règlement conformément à l'article 106, paragraphes 1 et 2, cet État membre met en place les 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.

8. 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. 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.

Article 102

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 103 sont soumises au secret professionnel tant au sein de l'autorité communiquant les informations qu'au sein de l'autorité destinataire.

3. Les articles 53 à 61 de la directive 2013/36/UE s'appliquent mutatis mutandis.

4. Le présent article ne fait pas obstacle à l'échange d'informations entre les autorités compétentes et les autorités fiscales du même État membre, conformément au droit national. Lorsque les informations proviennent d'un autre État membre, elles ne sont échangées qu'avec l'accord exprès des autorités compétentes qui les ont divulguées.

Article 103

Compétence et coopération entre les autorités compétentes

1. En cas d'infraction ou d'infraction présumée aux 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 d'infractions ou d'infractions présumées aux titres II et III de la part de prestataires de services techniques, d'opérateurs de schémas de paiement, d'opérateurs de systèmes de paiement, d'entités de traitement, de fournisseurs de distributeurs automatiques de billets, de fournisseurs 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 transfrontalières, les autorités compétentes coopèrent entre elles conformément au droit de l'Union et au droit national, en échangeant des informations entre elles et en assurant une assistance mutuelle avec les autres autorités compétentes dont l'assistance est nécessaire à l'application effective des sanctions administratives et mesures administratives.

4. Les autorités des autres secteurs concernés coopèrent avec les autorités compétentes en vue de l'application effective des sanctions administratives et mesures administratives.

SECTION 4

PROCEDURES DE REGLEMENT DES LITIGES ET SANCTIONS

Article 104

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 qui concernent les droits et obligations énoncés aux titres II et III. 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 répondent, 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 quinze jours ouvrables suivant la réception de la réclamation. Dans des situations exceptionnelles, si une réponse ne peut être donnée dans les quinze 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 trente-cinq jours ouvrables.

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 des litiges compétente pour connaître des litiges concernant les droits et obligations énoncés aux titres II et III.

4. Les informations mentionnées au paragraphe 3 sont présentées de manière claire, complète et aisément accessible sur le site internet du prestataire de services de paiement et sur l'application mobile correspondante, quand ils existent, 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’entité de règlement extrajudiciaire des litiges concernée et sur les conditions d'un tel recours peuvent être obtenues.

Article 105

Procédures de règlement extrajudiciaire des litiges

1. Les États membres mettent en place des procédures de règlement extrajudiciaire des litiges adéquates, indépendantes, impartiales, transparentes et efficaces pour le règlement des litiges entre les utilisateurs de services de paiement et les prestataires de services de paiement qui portent sur les droits et obligations énoncés aux titres II et III. Ces procédures sont établies conformément au droit de l'Union et au droit national applicables et aux exigences de qualité définies dans la directive 2013/11/UE, en recourant, le cas échéant, aux organismes existants. Les procédures de règlement extrajudiciaire des litiges sont applicables aux prestataires de services de paiement.

2. Les prestataires de services de paiement ont l'obligation de prendre part aux procédures de règlement extrajudiciaire des litiges destinées aux consommateurs, à moins que l'État membre ne démontre à la Commission que d'autres mécanismes sont tout aussi efficaces.

3. Les paragraphes 1 et 2 sont sans préjudice du droit des utilisateurs de services de paiement d'engager une procédure pour contester l'opération de paiement litigieuse réalisée par les prestataires de services de paiement devant une juridiction conformément au droit national applicable.

4. Les organismes mentionnés au paragraphe 1 coopèrent efficacement à la résolution des litiges transfrontaliers concernant les droits et obligations énoncés aux titres II et III.

5. Les États membres désignent une autorité compétente conformément à l'article 18 de la directive 2013/11/UE, laquelle assume les fonctions prévues aux articles 19 et 20 de ladite directive en ce qui concerne les entités de règlement extrajudiciaire des litiges établies sur leur territoire qui sont chargées du règlement des litiges portant sur les droits et obligations énoncés aux titres II et III du présent règlement.

6. Les autorités compétentes visées au paragraphe 5 notifient à la Commission l'entité ou les entités de règlement extrajudiciaire des litiges compétentes sur leur territoire pour régler les litiges portant sur les droits et obligations énoncés aux titres II et III du présent règlement, conformément à l'article 20 de la directive 2013/11/UE.

7. La Commission publie une liste des entités de règlement extrajudiciaire des litiges qui lui ont été notifiées conformément au paragraphe 6 et met à jour cette liste chaque fois que des changements lui sont communiqués.

Les États membres mettent à la disposition du public un hyperlien vers le site internet de la Commission contenant les informations visées au premier alinéa.

Article 106

Sanctions administratives et mesures administratives

1. Sans préjudice des pouvoirs de surveillance des autorités compétentes désignées en vertu de la directive (UE) 2026/...[+], 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 administratives et mesures administratives applicables aux infractions au présent règlement et veillent à ce qu'il soit mis en œuvre. Ces sanctions administratives et mesures administratives sont effectives, proportionnées et dissuasives.

2. Les États membres peuvent décider de ne pas fixer de régime de sanctions administratives et mesures administratives applicable aux infractions au présent règlement qui sont passibles de sanctions pénales en vertu du droit pénal national. Dans ce cas, les États membres notifient à la Commission les dispositions pertinentes de droit pénal applicable et leurs modifications ultérieures conformément à l'article 113.

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

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 administratives 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 pour manquement allégué au présent règlement à la suite d'un accord de règlement ou d'une procédure d'exécution accélérée.

Le pouvoir que les autorités compétentes ont de transiger ou d'ouvrir des procédures d'exécution accélérées est sans incidence sur les obligations qui incombent aux États membres au titre du paragraphe 1.

Les paragraphes 1, 3 et 4 du présent article s'appliquent aux sanctions administratives et mesures administratives visées à l'article 107.

Article 107

Sanctions administratives et mesures administratives pour des infractions spécifiques

1. Sans préjudice de l'article 106, paragraphe 2, les dispositions législatives, réglementaires et administratives nationales fixent les sanctions administratives et mesures administratives mentionnées au paragraphe 2 du présent article applicables en cas d'infraction aux dispositions suivantes:

a) les règles d'accès aux comptes détenus auprès d'un établissement de crédit prévues à l'article 33;

b) les règles relatives aux services d'information sur les comptes et aux services d'initiation de paiement énoncées au titre III, chapitre 3;

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 91, 93 et 94;

d) l'obligation de respecter les exigences de transparence en matière de frais pesant sur les opérateurs de distributeurs automatiques de billets ou autres distributeurs d'espèces, conformément à l'article 20, paragraphe 3, premier alinéa, point b);

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 57, paragraphe 2, à l'article 58, premier alinéa, à l'article 60, paragraphe 3, et à l'article 66, paragraphe 2.

2. Dans le cas des infractions mentionnées au paragraphe 1, les sanctions administratives et mesures administratives applicables consistent notamment en:

a) des amendes administratives;

i) dans le cas d'une personne morale, d'un maximum d'au moins 10 % de son chiffre d'affaires annuel total tel qu'il est défini au paragraphe 3;

ii) dans le cas d'une personne physique, d'un maximum d'au moins 3 000 000 EUR ou, dans les États membres dont la monnaie n'est pas l'euro, la valeur correspondante dans la monnaie nationale le ... [date d'entrée en vigueur du présent règlement];

iii) d'un maximum d'au moins deux fois le montant de l'avantage retiré de l'infraction ou des pertes qu'elle a permis d'éviter, lorsque cet avantage ou ces pertes peuvent être déterminés, même si cette amende dépasse les montants maximaux fixés au point i), en ce qui concerne les personnes morales, ou au point ii), en ce qui concerne les personnes physiques;

b) une déclaration publique indiquant le nom 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 morale ou toute autre personne physique tenue pour responsable de l'infraction, 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 108, paragraphe 1, du présent règlement est égal au chiffre d'affaires net tel qu'il est 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 de l'entreprise mère ultime.

4. Les États membres peuvent habiliter les autorités compétentes, conformément à leur droit national, à imposer d'autres types de sanctions administratives et mesures administratives et d'autres types de pouvoirs de sanction en plus de ceux visés au paragraphe 2.

Article 108

Astreintes

1. Les autorités compétentes sont habilitées à infliger des astreintes aux personnes physiques ou morales pour des infractions en cours au présent règlement ou des violations de toute décision rendue par une autorité compétente conformément au présent règlement.

Ces astreintes sont effectives et proportionnées et consistent en un montant journalier à payer jusqu'au rétablissement de la conformité. Elles 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 107, paragraphe 3, divisé par 365. Lorsqu'une astreinte est infligée à un établissement de crédit, le chiffre d'affaires journalier moyen est le chiffre d'affaires annuel total visé à l'article 66, paragraphe 3, et à l'article 67, paragraphe 3, de la directive 2013/36/UE, divisé par 365.

2. Les États membres peuvent prévoir des montants d'astreintes plus élevés que ceux prévus au paragraphe 1.

Article 109

Éléments à prendre en considération pour déterminer les sanctions administratives et les mesures administratives

1. Les autorités compétentes tiennent compte de tous les éléments et circonstances pertinents afin de s'assurer que le type et le niveau des sanctions administratives ou des mesures administratives qu'elles appliquent en cas d'infraction au présent règlement sont proportionnés, notamment:

a) la gravité et la durée de l'infraction;

b) le degré de responsabilité de la personne physique ou morale responsable de l'infraction;

c) 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) 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) les pertes subies par des tiers du fait de l'infraction, dans la mesure où ils peuvent être déterminés;

f) les sanctions pénales antérieurement infligées pour la même infraction à la personne physique ou morale responsable de cette infraction;

g) l'incidence de l'infraction sur les intérêts des consommateurs et des autres utilisateurs de services de paiement;

h) les conséquences systémiques négatives réelles ou potentielles de l'infraction;

i) la complicité ou la participation de plus d'une personne physique ou morale à l'infraction;

j) les infractions antérieurement commises par la personne physique ou morale responsable de l'infraction;

k) le degré de coopération avec les autorités compétentes dont a fait preuve la personne physique ou morale responsable de l'infraction;

l) toute action ou 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 106, paragraphe 4, adaptent les sanctions administratives et mesures administratives pertinentes prévues aux articles 106 et 107, et les astreintes prévues à l'article 108 au cas concerné afin de garantir leur proportionnalité.

Article 110

Droit de recours

1. Les décisions d'imposer des sanctions administratives ou des mesures administratives prises par les autorités compétentes en vertu du présent règlement sont susceptibles de recours.

2. Lorsque le présent règlement fixe un délai d'action à l'autorité compétente, l'absence d'action dans ce délai peut faire l'objet d'un recours.

Article 111

Publication des sanctions administratives et des mesures administratives

1. Les autorités compétentes publient sur leurs sites internet toutes les décisions imposant une sanction administrative ou une mesure administrative à des personnes physiques et morales pour infraction au présent règlement et, le cas échéant, tous les accords de règlement. Cette publication comprend une brève description de l'infraction, de la sanction administrative ou mesure administrative imposée ou, le cas échéant, une déclaration relative à l'accord de règlement. Lorsqu'une personne physique fait l'objet d'une décision imposant une sanction administrative ou une mesure administrative ou est partie à un accord de règlement, l'identité de cette personne physique n'est pas publiée.

Les autorités compétentes publient une décision ou un accord de règlement visés au premier alinéa sans retard injustifié après que la personne morale ou physique faisant l'objet de la décision ou étant partie à l'accord de règlement a été informée de cette décision ou que l'accord de règlement a été signé.

2. Par dérogation au paragraphe 1 du présent article, 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 107, paragraphe 2, point b), ou des interdictions temporaires visées à l'article 107, paragraphe 2, point d), l'autorité compétente nationale peut publier l'identité des personnes ou d'autres 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 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 ne s'applique pas, 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 reste sur leurs sites internet officiels pendant au moins cinq ans. Les données à caractère personnel contenues dans le document publié ne sont conservées sur le site internet officiel d'une autorité compétente que pendant la durée nécessaire conformément aux règles applicables en matière de protection des données à caractère personnel.

Article 112

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 administratives ou de mesures administratives pour des infractions au présent règlement;

   b) les astreintes infligées conformément à l'article 108 pour des infractions au présent règlement en cours;

   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 106, paragraphe 4;

   d) les procédures pénales donnant lieu à une condamnation et les sanctions correspondantes signalées par les autorités judiciaires conformément à l'article 101, paragraphe 7, point a);

e) tout recours contre les décisions d'imposer des sanctions pénales ou administratives ou des mesures administratives pour des infractions au présent règlement et l'issue de ce recours.

2. Lorsque l'autorité compétente rend publique une sanction ou mesure administrative conformément à l'article 111, elle la notifie simultanément à l'ABE.

3. Au plus tard le … [45 mois à compter de la date d'entrée en vigueur 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 113

Notification des mesures de mise en œuvre

Au plus tard le … [21 mois à compter de la date d'entrée en vigueur du présent règlement], les États membres notifient à la Commission les dispositions législatives, réglementaires et administratives adoptées en vertu du présent chapitre, y compris toute disposition pertinente de droit pénal. Ils notifient sans retard injustifié à la Commission toute modification ultérieure qui y est apportée et toute disposition législative, réglementaire et administrative qu'ils adoptent conformément au présent chapitre à une date ultérieure.

Chapitre 9
Pouvoirs d'intervention de l'ABE en matière de produits

Article 114

Pouvoirs d'intervention temporaires 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. Une telle interdiction ou 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 vise à faire face à une menace pour le bon fonctionnement ou l'intégrité des marchés des paiements ou des marchés de monnaie électronique, 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 concerné ne répondent 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 au premier alinéa du présent paragraphe 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 n'ait été fourni ou distribué aux utilisateurs de services de paiement.

3. Lorsqu'elle intervient au titre du présent article, l'ABE veille à ce que:

a) 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, qui serait disproportionnée par rapport aux bénéfices apportés par la mesure;

b) la mesure ne suscite pas de risque d'arbitrage réglementaire; et que

c) la mesure a été prise après consultation de l'autorité compétente nationale concernée.

4. Avant de décider de prendre une mesure en vertu du présent article, l'ABE notifie aux autorités compétentes concernées la mesure qu'elle propose.

5. L'ABE publie sur son site internet une notification de toute décision de prendre une mesure 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 tous les trois mois, elle expire.

7. Les mesures adoptées par l'ABE en vertu du présent article prévalent sur toute mesure antérieure prise par une autorité compétente.

8. La Commission est habilitée à adopter, conformément à l'article 115, des actes délégués pour compléter le présent règlement en précisant les critères et les facteurs que doit prendre en compte l'ABE pour déterminer quand il existe un nombre important d'utilisateurs de services de paiement ou une menace pour le bon fonctionnement ou l'intégrité des marchés des paiements ou des marchés de monnaie électronique, ou pour la stabilité de tout ou partie de ces marchés, dans l'Union.

Les critères et facteurs précisés dans les actes délégués adoptés par la Commission comprennent:

a) le degré de complexité d'un service ou instrument de paiement, et en quoi ils ont un lien avec le type d'utilisateurs, y compris les consommateurs, auxquels ils sont proposés;

b) le degré de risque, pour les consommateurs, que présente un service ou instrument de paiement;

c) l'utilisation éventuelle du service ou instrument de paiement par des fraudeurs;

d) la taille ou le niveau d'utilisation du service ou instrument de paiement;

e) le degré d'innovation que présente un service ou instrument de paiement.

TITRE IV
ACTES DÉLÉGUÉS

Article 115

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 aux articles 32, 63, 71 et 114 est conféré à la Commission pour une durée indéterminée à compter du ... [date d'entrée en vigueur du présent règlement].

3. La délégation de pouvoir visée aux articles 32, 63, 71 et 114 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 celui de 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 l'adoption d'un acte délégué, la Commission consulte les experts désignés par les États membres, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 "Mieux légiférer".

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 des articles 32, 63, 71 et 114 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 116

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 58 et 60, et prévoir des mesures de prévention de la fraude plus strictes que celles prévues à l'article 87, paragraphe 1, et à l'article 90.

2. Au plus tard le … [21 mois à compter de la date d'entrée en vigueur du présent règlement], les États membres notifient à la Commission les dispositions législatives qu'ils adoptent en vertu du paragraphe 1. Ils notifient sans retard injustifié à la Commission toute modification ultérieure qui y est apportée et toute disposition législative qu'ils adoptent en vertu du paragraphe 1 à une date ultérieure.

Article 117

Clause de réexamen

1. La Commission soumet, au plus tard le ... [18 mois à compter de 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 les pratiques des schémas de cartes de paiement, les entités de traitement, les prestataires de services de paiement qui fournissent des services d'acquisition d'opérations de paiement et en particulier sur:

   a) l'évolution de leurs frais dans l'Espace économique européen (EEE); en ce compris:

      i) les frais facturés par les schémas de cartes de paiement et les entités de traitement aux prestataires de services de paiement qui fournissent des services d'acquisition d'opérations de paiement, par catégorie d'opérations clés, par État membre;

      ii) les frais facturés par les prestataires de services de paiement qui fournissent des services d'acquisition d'opérations de paiement aux utilisateurs de services de paiement agissant à des fins professionnelles;

b) les conditions liées à l'application des nouvelles règles et des frais associés, tels que les délais de notification de ces règles et frais par les schémas de cartes de paiement et les entités de traitement;

c) la communication par les schémas de cartes de paiement aux prestataires de services de paiement qui fournissent des services d'acquisition d'opérations de paiement et aux entités de traitement quant aux règles et aux frais et à leur calendrier de mise en œuvre;

d) la capacité des émetteurs et des acquéreurs à négocier les règles et les frais proposés par les schémas de cartes de paiement;

e) le comportement concurrentiel des schémas de cartes de paiement sur les marchés de l'acquisition et de l'émission.

Le cas échéant, la Commission accompagne son rapport d'une proposition législative.

Une version non confidentielle du rapport est mise à la disposition du public, y compris des informations agrégées sur l'évolution des frais.

2. La Commission soumet, au plus tard le … [trois ans à compter de 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 évaluant:

a) 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;

b) si, à la lumière des risques et des défis posés par les IBAN virtuels, y compris du point de vue de la répression en matière de lutte contre le blanchiment de capitaux ou de financement du terrorisme, et de leurs avantages, il est nécessaire d'introduire de nouvelles mesures réglementant les IBAN virtuels au niveau de l'Union;

c) l'adéquation et l'incidence des règles énoncées aux titres II et III du présent règlement en ce qui concerne les opérations de paiement effectuées en jetons de monnaie électronique;

d) si, compte tenu de l'évolution de la situation, il est souhaitable d'appliquer les exigences du présent règlement relatives à la vérification du bénéficiaire et à la banque ouverte («open banking») aux opérations de paiement effectuées en jetons de monnaie électronique.

Le cas échéant, la Commission accompagne son rapport d'une proposition législative.

3. La Commission soumet, au plus tard le … [cinq ans à compter de 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 examinant:

a) l'incidence des dispositions relatives à la surfacturation figurant à l'article 28, y compris les effets sur les consommateurs, les commerçants et la concurrence, et évaluant la nécessité d'une harmonisation plus poussée; et

b) l'incidence des mécanismes de remboursement gérés par des opérateurs de schémas de paiement ou des prestataires de services de paiement qui sont applicables aux opérations de paiement initiées par un bénéficiaire, à l'exclusion des prélèvements, ainsi que les effets de ces mécanismes de remboursement sur les consommateurs, les commerçants et la concurrence;

c) l'incidence des dispositions de l'article 61 en ce qui concerne les obligations imposées aux fournisseurs de services de communications interpersonnelles, en particulier la question de savoir si ces obligations améliorent l'efficacité de la coopération entre les fournisseurs de services de communications interpersonnelles et les prestataires de services de paiement au titre de l'article 61;

d) l'incidence des dispositions de l'article 61 en ce qui concerne les obligations imposées aux fournisseurs de services d'hébergement et aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne, en particulier la question de savoir si ces obligations améliorent l'efficacité de la coopération entre les fournisseurs de services d'hébergement et les fournisseurs de services de paiement au titre des articles 61 et 62, et le droit de recours des prestataires de services de paiement au titre de l'article 82.

Sur la base des évaluations visées au premier alinéa, points c) et d), la Commission détermine s'il est nécessaire d'introduire d'autres mesures réglementant la participation des fournisseurs de services de communications électroniques, des fournisseurs de services d'hébergement, des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne et des prestataires de services de paiement à la sécurité des opérations de paiement au niveau de l'Union.

Le cas échéant, la Commission accompagne son rapport d'une proposition législative.

4. La Commission soumet, au plus tard le … [sept ans à compter de 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 l'application et l'incidence du présent règlement, et en particulier sur:

a) l'adéquation et l'incidence sur la concurrence et l'utilisation du système de banque ouverte («open banking») 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 dédiées et de leurs dérogations respectivement prévues aux articles 39 et 40;

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 35;

c) l'adéquation et l'impact des règles en matière de prévention et de réparation de la fraude sur les opérations de paiement non autorisées et autorisées, compte tenu des types et de l'évolution des comportements frauduleux;

d) l'adéquation et l'impact des règles sur l'étendue des situations dans lesquelles un consommateur dispose d'un droit au remboursement pour des opérations de paiement autorisées conformément à l'article 60.

Le cas échéant, la Commission accompagne son rapport d'une proposition législative.

Article 118

Dispositions transitoires

Par dérogation à la directive (UE) 2015/2366, jusqu'au ... [21 mois à compter de la date d'entrée en vigueur du présent règlement]:

a) les opérations de paiement qui suivent sont exclues de l’application de la directive (UE) 2015/2366:

i) les opérations de paiement effectuées exclusivement en jetons de monnaie électronique et allant directement du payeur au bénéficiaire, sans l'intervention du moindre intermédiaire;

ii) les opérations de paiement effectuées par un prestataire de services sur crypto-actifs qui sert d'intermédiaire entre un acheteur et un vendeur lorsque des jetons de monnaie électronique sont échangés contre d'autres jetons de monnaie électronique ou contre des crypto-actifs, ainsi qu'à l'échange de jetons de monnaie électronique contre des fonds, y compris des jetons de monnaie électronique, ou des crypto-actifs, effectuées par un prestataire de services sur crypto-actifs agissant en son nom propre en tant qu'acheteur ou vendeur de ces jetons de monnaie électronique;

iii) les opérations de paiement effectuées entre des prestataires de services sur crypto-actifs ou leurs succursales pour leur propre compte;

b) en ce qui concerne les opérations de paiement avec des jetons de monnaie électronique réglées dans le registre distribué, lorsque des prestataires de services de paiement ne sont pas en mesure, en raison de circonstances qui ne leur sont pas imputables, de se conformer aux obligations énoncées à l'article 45, paragraphe 1, points b) et c), à l'article 52, paragraphe 2, point e), à l'article 52, paragraphe 3, point a), et à l'article 56 de la directive (UE) 2015/2366, les prestataires de services de paiement fournissent les informations qui y sont requises au moyen d'une estimation motivée dès que possible et, en tout état de cause, avant que le payeur n'autorise l'opération;

c) les prestataires de services de paiement ne sont pas tenus d'appliquer l'article 66, paragraphe 4, et l'article 67, paragraphe 3, de la directive (UE) 2015/2366 en ce qui concerne les opérations de paiement effectuées au moyen de jetons de monnaie électronique.

Article 119

Modifications du règlement (UE) n° 1093/2010

Le règlement (UE) nº 1093/2010 est modifié comme suit:

1) À l'article 1er, le paragraphe 2 est remplacé par le texte suivant:

"2. 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 2009/110/CE, du règlement (UE) n° 575/2013*, de la directive 2013/36/UE**, de la directive 2014/49/UE***, de la directive 2014/92/UE****, du règlement (UE) 2023/1114*****, de la directive (UE) 2023/2225******, de la directive (UE) 2026/...******, du règlement (UE) 2026/…******* 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. L'Autorité agit aussi conformément au règlement (UE) n° 1024/2013 du Conseil********.

---

* Règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et modifiant le règlement (UE) n° 648/2012 (JO L 176 du 27.6.2013, p. 1, ELI: http://data.europa.eu/eli/reg/2013/575/oj).

** 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, 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, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

*** Directive 2014/49/UE du Parlement européen et du Conseil du 16 avril 2014 relative aux systèmes de garantie des dépôts (JO L 173 du 12.6.2014, p. 149, ELI: http://data.europa.eu/eli/dir/2014/49/oj).

**** Directive 2014/92/UE du Parlement européen et du Conseil du 23 juillet 2014 sur la comparabilité des frais liés aux comptes de paiement, le changement de compte de paiement et l'accès à un compte de paiement assorti de prestations de base (JO L 257 du 28.8.2014, p. 214, ELI: http://data.europa.eu/eli/dir/2014/92/oj).

***** Règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs, et modifiant les règlements (UE) nº 1093/2010 et (UE) nº 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937 (JO L 150 du 9.6.2023, p. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

****** Directive (UE) 2023/2225 du Parlement européen et du Conseil du 18 octobre 2023 relative aux contrats de crédit aux consommateurs et abrogeant la directive 2008/48/CE (JO L, 2023/2225, 30.10.2023, ELI: http://data.europa.eu/eli/dir/2023/2225/oj).

******* Directive (UE) 2026/… du Parlement européen et du Conseil du … concernant les services de paiement dans le marché intérieur, modifiant la directive 98/26/CE et le règlement (UE) 2023/1114 et abrogeant les directives (UE) 2009/110/CE et 2015/2366 (JO L, …, ELI: …)[+].

******** Règlement (UE) 2026/… du Parlement européen et du Conseil du … concernant les services de paiement dans le marché intérieur et modifiant les règlements (UE) nº 1093/2010, (UE) nº 260/2012, (UE) 2017/2394 et (UE) 2021/1230 (JO L, …, ELI: …)[++].

********* Règlement (UE) n° 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit (JO L 287 du 29.10.2013, p. 63, ELI: http://data.europa.eu/eli/reg/2013/1024/oj);

+ JO: veuillez insérer les informations détaillées concernant la directive figurant dans le document ST 8535/26 (2023/0209(COD)).

++ JO: veuillez insérer les informations détaillées concernant le présent règlement.

2) À l'article 4, le point 2 est modifié comme suit:

a) le point i) est remplacé par le texte suivant:

"i) 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 vi), vii) et viii) sont supprimés.

Article 120

Modifications du règlement (UE) n° 260/2012

Le règlement (UE) nº 260/2012 est modifié comme suit:

1) À l'article 2, le point suivant est inséré:

"15 *bis*) "IBAN virtuel", un identifiant qui contient les éléments spécifiés par l'ISO visés au point 15) et qui a pour effet de rediriger les paiements vers un compte de paiement identifié par un IBAN différent de cet identifiant;".

2) L'article suivant est inséré:

"*Article 2* bis
Identifiant du compte de paiement

Aux fins du présent règlement, un IBAN virtuel est considéré comme un identifiant de compte de paiement valide lorsque l'utilisation d'un IBAN est requise.".

3) À l'article 5 *quater*, les paragraphes 5 et 6 sont remplacés par le texte suivant:

"5. Sans préjudice du paragraphe 6, troisième alinéa, les prestataires de services de paiement veillent à ce que l'exécution du service assurant la vérification et du service décrit au paragraphe 2 n'empêche pas les payeurs d'autoriser le virement concerné.

6. Les prestataires de services de paiement fournissent aux utilisateurs de services de paiement qui ne sont pas des consommateurs les moyens de renoncer à bénéficier du service garantissant la vérification lorsqu'ils transmettent des ordres de paiement via des canaux d'initiation de paiement reposant sur des processus ou protocoles automatisés dédiés et qui sont uniquement mis à la disposition des utilisateurs de services de paiement qui ne sont pas des consommateurs.

Les prestataires de services de paiement veillent à ce que les utilisateurs de services de paiement qui ne sont pas des consommateurs et qui ont choisi de renoncer à recevoir le service assurant la vérification aient le droit de choisir à tout moment de recevoir ce service à nouveau.

Dans le cas d'ordres de paiement soumis via des canaux d'initiation de paiement visés au premier alinéa, y compris lorsqu'il s'agit de plusieurs ordres de paiement soumis sous une forme groupée, les prestataires de services de paiement offrent aux utilisateurs de services de paiement qui ne sont pas des consommateurs la possibilité de convenir dans le contrat-cadre que:

a) le service assurant la vérification est fourni après l'autorisation de ces ordres de paiement; et que

b) le prestataire de services de paiement du payeur n'exécute ces ordres de paiement sans autre contribution de l'utilisateur de services de paiement que dans au moins un des cas suivants:

   i) les informations reçues par le prestataire de services de paiement du payeur de la part du prestataire de services de paiement du bénéficiaire montrent que le nom du bénéficiaire tel que fourni par le payeur correspond à l'identifiant de compte de paiement visé au point 1) a) de l'annexe;

   ii) les informations reçues par le prestataire de services de paiement du payeur de la part du prestataire de services de paiement du bénéficiaire montrent que le nom du bénéficiaire tel que fourni par le payeur correspond presque à l'identifiant de compte de paiement visé au point 1) a) de l'annexe;

   iii) le service assurant la vérification ne peut être fourni pour des raisons techniques.

La possibilité pour l'utilisateur de services de paiement qui n'est pas un consommateur de convenir contractuellement que le prestataire de services de paiement du payeur exécute les ordres de paiement conformément au troisième alinéa est sans préjudice de l'obligation prévue au paragraphe 1, point a), pour le prestataire de services de paiement du payeur d'indiquer au payeur, dans les cas où le nom du bénéficiaire fourni par le payeur correspond presque à l'identifiant de compte de paiement précisé au point 1) a) de l'annexe fourni par le payeur, le nom du bénéficiaire associé à cet identifiant de compte de paiement.

Aux fins du paragraphe 8, lorsque le prestataire de services de paiement du payeur procède à l'exécution des ordres de paiement conformément au contrat-cadre visé au troisième alinéa, ce prestataire de services de paiement n'est pas tenu responsable du non-respect de l'obligation de proposer le service assurant la vérification du bénéficiaire.".

Article 121

Modification du règlement (UE) 2017/2394

Dans l'annexe du règlement (UE) 2017/2394, le point suivant est ajouté:

"31. Règlement (UE) 2026/… du Parlement européen et du Conseil du … concernant les services de paiement dans le marché intérieur et modifiant les règlements (UE) nº 1093/2010, (UE) nº 260/2012, (UE) 2017/2394 et (UE) 2021/1230 (JO L, …, ELI: …)[+].".

[+] JO: veuillez insérer les informations détaillées concernant le présent règlement.

Article 122

Modifications du règlement (UE) 2021/1230

Le règlement (UE) 2021/1230 est modifié comme suit:

1) À l'article 4, le paragraphe 1 est remplacé par le texte suivant:

"1. En ce qui concerne les exigences en matière d'informations concernant les frais de conversion monétaire et le taux de change applicable, visées à l'article 5, paragraphe 2, à l'article 13, paragraphe 1, et à l'article 20, paragraphe 3, du règlement (UE) 2026/... du Parlement européen et du Conseil[*+], les prestataires de services de paiement et les parties fournissant des services de conversion monétaire à un distributeur automatique de billets ou au point de vente visés à l'article 5, paragraphe 2, dudit règlement, expriment le total des frais de conversion monétaire en montant monétaire dans la monnaie du compte du payeur et en marge de pourcentage sur un taux de change moyen du marché agrégé, tel que visé à l'article 5, paragraphe 3, dudit règlement. Cette marge et tous les autres frais applicables sont communiqués au payeur avant l'initiation de l'opération de paiement.

---

[*] Règlement (UE) 2026/… du Parlement européen et du Conseil du … concernant les services de paiement dans le marché intérieur et modifiant les règlements (UE) nº 1093/2010, (UE) nº 260/2012, (UE) 2017/2394 et (UE) 2021/1230 (JO L, …, ELI: …)[++].";

[+] JO: prière d'insérer le numéro du présent règlement.

[++] JO: veuillez insérer les informations détaillées concernant le présent règlement.

2) À l'article 5, le paragraphe 1 est remplacé par le texte suivant:

"1. Lorsqu'un service de conversion monétaire est proposé par le prestataire de services de paiement du payeur en relation avec un virement, tel que défini à l'article 3, point 53), du règlement (UE) 2026/...[+], initié directement en ligne au moyen du site internet ou de l'application mobile de banque à distance du prestataire de services de paiement, le prestataire de services de paiement, s'agissant de l'article 13, paragraphe 1, et de l'article 20, paragraphe 3, dudit règlement, informe le payeur, avant d'initier l'opération de paiement, de manière claire, neutre et compréhensible, des frais estimés de conversion monétaire et de tous les autres frais applicables au virement. Les frais estimés de conversion monétaire liés aux virements sont exprimés en montant monétaire dans la monnaie du compte du payeur et en marge de pourcentage sur un taux de change moyen du marché agrégé, tel que visé à l'article 5, paragraphe 3, dudit règlement.".

Article 123

Tableau de correspondance

Les références faites aux directives 2009/110/CE et (UE) 2015/2366/CE s'entendent comme faites à la directive (UE) 2026/...[++] ou au présent règlement et sont à lire selon le tableau de correspondance figurant à l'annexe du présent règlement.

[+] JO: prière d'insérer le numéro du présent règlement.

[++] JO: veuillez insérer le numéro de la directive figurant dans le document PE .../... (2023/0209(COD)).

Article 124

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 … [21 mois à compter de la date d'entrée en vigueur du présent règlement].

Toutefois, les articles 51 et 58 sont applicables à partir du ... [27 mois à compter de la date d'entrée en vigueur du présent règlement].

Les articles 92 et 118 sont applicables à partir du … [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 …, le …

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président/La présidente*

ANNEXE

Tableau de correspondance

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 1er, paragraphe 1	Article 1er, paragraphe 1	–	Article 2, paragraphe 1
Article 1er, paragraphe 1, point a)	Article 1er, paragraphe 1, point a)	–	Article 2, paragraphe 1, point a)
Article 1er, paragraphe 1, point b)	Article 1er, paragraphe 1, point b)	–	–
Article 1er, paragraphe 1, point c)	Article 1er, paragraphe 1, point c)	–	Article 2, paragraphe 1, point b)
Article 1er, paragraphe 1, point d)		–	Article 2, paragraphe 1, point c)
Article 1er, paragraphe 1, point e)	Article 1er, paragraphe 1, point d)	–	Article 2, paragraphe 1, point d)
Article 1er, paragraphe 1, point f)	Article 1er, paragraphe 1, point e)	–	Article 2, paragraphe 1, point e)
–	Article 1er, paragraphe 2	Article 1er, paragraphe 1	–
–	Article 1er, paragraphe 3	Article 1er, paragraphe 2	–
Article 1er, paragraphe 2	–	–	Article 1er, paragrahe 1
Article 2, paragraphe 1	–	–	Article 2, paragraphe 1
Article 2, paragraphe 2	–	–	Article 2, paragraphe 4
Article 2, paragraphe 3	–	–	Article 2, paragraphe 5
Article 2, paragraphe 4	–	–	Article 2, paragraphe 6
Article 2, paragraphe 5	–	–	Article 2, paragraphe 7
Article 3, point a)	–	–	Article 2, paragraphe 3, point a)
Article 3, point b)	–	–	Article 2, paragraphe 3, point c)
Article 3, point c)	–	–	Article 2, paragraphe 3, point p)
Article 3, point d)	–	–	Article 2 paragraphe 3, point d)
Article 3, point e)	–	–	Article 2, paragraphe 3, point e)
Article 3, point f)	–	–	Article 2, paragraphe 3, point q)
Article 3, point g)	–	–	Article 2, paragraphe 3, point g)

[+] JO: veuillez insérer le numéro de la directive figurant dans le document ST 8535/26 (2023/0209) (COD)).

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 3, point h)	–	–	Article 2, paragraphe 3, point h)
Article 3, point i)	–	–	Article 2, paragraphe 3, point i)
Article 3, point j)	–	–	-
Article 3, point k)	Article 1er, paragraphe 4	–	Article 2, paragraphe 3, point k)
Article 3, point l)	Article 1er, paragraphe 5	–	Article 2, paragraphe 3, point l)
Article 3, point m)	–	–	Article 2, paragraphe 3, point m)
Article 3, point n)	–	–	Article 2, paragraphe 3, point o)
Article 3, point o)	–	–	-
Article 4, points 1) et 2)	–	–	Article 3, points 15) et 16)
Article 4, point 3)	–	–	Article 3, point 1)
Article 4, point 4)	–	–	Article 3, point 13)
Article 4, point 5)	–	–	Article 3, point 8)
Article 4, point 6)	–	–	Article 3, point 12)
Article 4, point 7)	–	–	Article 3, point 20)
Article 4, points 8) et 9)	–	–	Article 3, points 5) et 6)
Article 4, point 10)	–	–	Article 3, point 3)
Article 4, point 11)	–	–	Article 3, point 2)
Article 4, point 12)	–	–	Article 3, point 35)
Article 4, point 13)	–	–	Article 3, point 11)
Article 4, points 14), 15) et 16)	–	–	Article 3, points 42), 43) et 44)
Article 4, point 17)	–	–	Article 3, point 37)
Article 4, points 18) et 19)	–	–	Article 3, points 45) et 46)
Article 4, point 20)	–	–	Article 3, point 4)

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 4, point 21)	–	–	Article 3, point 33)
Article 4, point 22)	–	–	Article 3, point 41)
Article 4, points 23) et 24)	–	–	Article 3, points 52) et 53)
Article 4, point 25)	–	–	Article 3, point 7)
Article 4, points 26), 27) et 28)	–	–	Article 3, points 55), 56) et 57)
Article 4, points 29) à 33)	–	–	Article 3, points 59) à 63)
Article 4, point 34)	–	–	Article 3, point 34)
Article 4, point 35)	–	–	Article 3, point 39)
Article 4, point 36)	–	–	Article 3, point 32)
Article 4, point 37)	–	–	Article 3, point 64)
Article 4, points 38), 39) et 40)	–	–	Article 3, points 17), 18) et 19)
Article 4, points 41) et 42)	–	–	–
Article 4, point 43)	–	–	Article 3, point 31)
Article 4, points 44) et 45)	–	–	Article 3, points 50) et 51)
Article 4, point 46)	–	Article 2, point 2)	–
Article 4, point 47)	–	–	–
Article 4, point 48)	–	–	–
–	Article 2, point 1)	–	–
–	Article 2, point 2)	–	Article 3, point 30)
–	Article 2, point 3)	–	–
–	Article 2, point 4)	Article 2, point 3)	–

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 5, paragraphe 1	Article 3, paragraphe 1	Article 3, paragraphe 3	–
–	Article 3, paragraphe 2	Article 9, paragraphe 7	–
Article 5, paragraphe 2	–	Article 3, paragraphe 5	–
Article 5, paragraphe 3	–	Article 35, paragraphe 4	–
Article 5, paragraphes 4 et 5	–	–	–
Article 5, paragraphe 6	–	Article 3, paragraphes 6 et 7	–
Article 5, paragraphe 7	–	–	–
Article 6, paragraphe 1	Article 3, paragraphe 3	Article 4, paragraphe 1	–
	Article 3, paragraphe 4	Article 19	–
Article 6, paragraphe 2	–	Article 4, paragraphe 2	–
Article 6, paragraphe 3	–	Article 4, paragraphe 3	–
Article 6, paragraphe 4	–	Article 4, paragraphe 4	–
Article 7	Article 4	Article 5	–
Article 8, paragraphe 1	Article 5, paragraphe 1	Article 6, paragraphe 1	–
Article 8, paragraphe 2	Article 5, paragraphe 6	Article 6, paragraphe 2	–
Article 8, paragraphe 3	Article 5, paragraphe 7	Article 6, paragraphe 3	–
Article 9, paragraphe 1	–	Article 7, paragraphes 1 et 2	–
Article 9, paragraphe 2	–	Article 7, paragraphe 3	–
Article 9, paragraphe 3	–	Article 7, paragraphe 5	–
	Article 5, paragraphe 2	Article 8, paragraphes 2 et 3	–
	Article 5, paragraphe 3	Article 8, paragraphe 2	–
	Article 5, paragraphe 4	Article 8, paragraphe 4	–
	Article 5, paragraphes 5, 6 et 7	-	–
Article 10, paragraphe 1	–	Article 9, paragraphes 1 et 2	–

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 10, paragraphe 2	–	Article 9, paragraphe 4	–
–	Article 7, paragraphe 1	Article 9, paragraphe 4	–
–	Article 7, paragraphes 2, 3 et 4	–	–
Article 11, paragraphe 1	–	Article 13, paragraphe 1	–
Article 11, paragraphe 2	–	Article 13, paragraphe 2	–
Article 11, paragraphe 3	–	Article 13, paragraphe 4	–
Article 11, paragraphe 4	–	Article 13, paragraphe 5	–
Article 11, paragraphe 5	–	Article 13, paragraphe 5	–
Article 11, paragraphe 6	–	Article 13, paragraphe 6	–
Article 11, paragraphe 7	–	Article 13, paragraphe 6, point b)	–
Article 11, paragraphe 8	–	Article 13, paragraphe 6, point c)	–
Article 11, paragraphe 9	–	Article 13, paragraphe 7	–
Article 12	–	Article 14	–
Article 13, paragraphe 1	–	Article 16, paragraphe 1	–
Article 13, paragraphe 2	–	Article 16, paragraphe 2	–
Article 13, paragraphe 3	–	Article 16, paragraphe 3	–
Article 14, paragraphe 1	–	Article 17, paragraphe 1	–
Article 14, paragraphe 2	–	Article 17, paragraphes 2 et 3	–
Article 14, paragraphe 3	–	Article 17, paragraphe 4	–
Article 14, paragraphe 4	–	Article 17, paragraphe 5	–
Article 15, paragraphe 1	–	Article 18, paragraphes 1 et 2	–
Article 15, paragraphe 2	–	Article 18, paragraphe 3	–
Article 15, paragraphe 3	–	Article 18, paragraphe 4	–
Article 15, paragraphe 4	–	Article 18, paragraphe 5	–

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 15, paragraphe 5	–	Article 18, paragraphe 6	–
Article 16	–	Article 15	–
Article 17, paragraphe 1	–	Article 11, paragraphe 1	–
Article 17, paragraphe 2	–	Article 11, paragraphe 2	–
Article 17, paragraphe 3	–	Article 11, paragraphe 3	–
Article 17, paragraphe 4	–	Article 11, paragraphe 4	–
Article 18, paragraphe 1	Article 6, paragraphe 1, point a)	Article 10, paragraphe 1	–
Article 18, paragraphe 1, point a)	Article 6, paragraphe 1, point c)	Article 10, paragraphe 1, point a)	–
Article 18, paragraphe 1, point b)	Article 6, paragraphe 1, point d)	Article 10, paragraphe 1, point b)	–
Article 18, paragraphe 1, point c)	Article 6, paragraphe 1, point e)	Article 10, paragraphe 1, point (c)	–
Article 18, paragraphe 2	Article 6, paragraphe 4	Article 10, paragraphe 2	–
Article 18, paragraphe 3	Article 6, paragraphe 4	Article 10, paragraphe 3	–
Article 18, paragraphe 4	Article 6, paragraphe 1, point b)	Article 10, paragraphe 4	–
Article 18, paragraphe 5	Article 6, paragraphes 2 et 4	Article 10, paragraphe 5	–
–	Article 6, paragraphe 3	Article 10, paragraphe 6	–
Article 18, paragraphe 6	–	Article 10, paragraphe 7	–
Article 19, paragraphe 1	–	Article 19, paragraphe 1	–
Article 19, paragraphe 2	–	Article 19, paragraphe 2	–
Article 19, paragraphe 3	–	Article 19, paragraphe 3	–
Article 19, paragraphe 4	–	Article 19, paragraphe 4	–
Article 19, paragraphe 5	–	Article 19, paragraphe 5	–
Article 19, paragraphe 6	–	Article 21, paragraphe 1	–
Article 19, paragraphe 7	–	Article 19, paragraphe 6, et article 20, paragraphe 2	–

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 19, paragraphe 8	–	Article 19, paragraphe 7, et article 21, paragraphe 2	–
Article 20, paragraphe 1	–	Article 22, paragraphe 1	–
Article 20, paragraphe 2	–	Article 22, paragraphe 2	–
Article 21	–	Article 12	–
Article 22, paragraphe 1	–	Article 23, paragraphe 1	–
Article 22, paragraphe 2	–	Article 23, paragraphe 2	–
Article 22, paragraphe 3	–	Article 23, paragraphe 3	–
Article 22, paragraphe 4	–	Article 23, paragraphe 4	–
Article 22, paragraphe 5	–	Article 23, paragraphe 5	–
Article 23, paragraphe 1	–	Article 24, paragraphe 1	–
Article 23, paragraphe 1, point a)	–	Article 24, paragraphe 1, point a)	–
Article 23, paragraphe 1, point b)	–	Article 24, paragraphe 1, point b)	–
Article 23, paragraphe 1, point c)	–	Article 24, paragraphe 1, point c)	–
Article 23, paragraphe 1, point d)	–	Article 24, paragraphe 1, point d)	–
Article 23, paragraphe 2	–	Article 24, paragraphe 2	–
Article 23, paragraphe 3	–	Article 23, paragraphe 3	–
Article 24, paragraphe 1	–	Article 25, paragraphe 1	Article 102, paragraphe 1
Article 24, paragraphe 2	–	Article 25, paragraphe 2	Article 102, paragraphe 2
Article 24, paragraphe 3	–	Article 25, paragraphe 3	Article 102, paragraphe 3
Article 25, paragraphe 1	–	Article 26, paragraphe 1	–
Article 25, paragraphe 2	–	Article 26, paragraphe 2	–
Article 26, paragraphe 1	–	Article 27, paragraphe 1	–

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 26, paragraphe 2	–	Article 27, paragraphe 2	–
Article 27, paragraphe 1	–	Article 28, paragraphe 1	–
Article 27, paragraphe 2	–	Article 28, paragraphe 2	–
Article 28, paragraphe 1	–	Article 29, paragraphe 1	–
Article 28, paragraphe 2	–	Article 29, paragraphe 2	–
Article 28, paragraphe 3	–	Article 29, paragraphe 3	–
Article 28, paragraphe 4	–	Article 29, paragraphe 4	–
Article 28, paragraphe 5	–	Article 29, paragraphe 5	–
Article 29, paragraphe 1	–	Article 30, paragraphe 1	–
Article 29, paragraphe 2	–	Article 30, paragraphe 2	–
Article 29, paragraphe 3	–	Article 30, paragraphe 3	–
Article 29, paragraphe 4	–	Article 30, paragraphe 4	–
Article 29, paragraphe 5	–	Article 30, paragraphe 5	–
Article 29, paragraphe 6	–	-	–
Article 30, paragraphe 1	–	Article 31, paragraphe 1	–
Article 30, paragraphe 2	–	Article 31, paragraphe 2	–
Article 30, paragraphe 3	–	Article 31, paragraphe 3	–
Article 30, paragraphe 4	–	Article 31, paragraphe 4	–
Article 31, paragraphe 1	–	Article 32, paragraphe 1	–
Article 31, paragraphe 2	–	Article 32, paragraphe 2	–
–	Article 8, paragraphes 1, 2 et 3	-	–
Article 32, paragraphe 1, point a)	–	Article 33, paragraphe 1, point a)	–
–	Article 9, paragraphe 1, point a)	Article 33, paragraphe 1, point b)	–

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 32, paragraphe 1, point b)	Article 9, paragraphe 1, point b)	Article 33, paragraphe 1, point c)	–
Article 32, paragraphe 2	Article 9, paragraphe 2	Article 33, paragraphe 3	–
Article 32, paragraphe 3	Article 9, paragraphe 3	Article 33, paragraphe 4	–
Article 32, paragraphe 4	Article 9, paragraphe 4	Article 33, paragraphe 5	–
Article 32, paragraphe 5	Article 9, paragraphes 5, 6 et 7	Article 33, paragraphes 6 et 7	–
Article 32, paragraphe 6	Article 9, paragraphe 8	Article 33, paragraphe 8	–
Article 33, paragraphe 1	–	Article 35, paragraphes 1 à 5	–
Article 33, paragraphe 2	–	Article 3, paragraphe 2	Article 47, paragraphe 2
Article 34	Article 9, paragraphe 9	Article 34	–
–	Article 10	Article 45, paragraphes 2 et 4	–
–	Article 11, paragraphe 1	–	Article 30, paragraphe 1
–	Article 11, paragraphe 2	–	Article 30, paragraphe 2
–	Article 11, paragraphe 3	–	Article 30, paragraphe 3
–	Article 11, paragraphe 4	–	Article 30, paragraphe 4
–	Article 11, paragraphe 5	–	Article 30, paragraphe 5
–	Article 11, paragraphe 6	–	Article 30, paragraphe 6
–	Article 11, paragraphe 7	–	Article 30, paragraphe 7
–	Article 12	–	Article 30, paragraphe 8
Article 35, paragraphe 1	–	–	Article 31, paragraphes 1, 2 et 4
Article 35, paragraphe 2	–	–	Article 31, paragraphes 3, 5 et 6
Article 36	–	–	Article 33

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 37, paragraphe 1	–	–	Article 99
Article 37, paragraphe 2	–	Article 38, paragraphe 1	–
Article 37, paragraphe 3	–	Article 38, paragraphe 2	–
Article 37, paragraphe 4	–	Article 38, paragraphe 3	–
Article 37, paragraphe 5	–	Article 38, paragraphe 4	–
Article 38, paragraphe 1	–	–	Article 4, paragraphe 1
Article 38, paragraphe 2	–	–	Article 4, paragraphe 2
Article 38, paragraphe 3	–	–	–
Article 39	–	–	–
Article 40, paragraphe 1	–	–	Article 8, paragraphe 1
Article 40, paragraphe 2	–	–	Article 8, paragraphe 2
Article 40, paragraphe 3	–	–	Article 8, paragraphe 3
Article 41	–	–	Article 9
Article 42, paragraphe 1	–	–	Article 10
Article 42, paragraphe 2	–	–	–
Article 43, paragraphe 1	–	–	Article 11, paragraphe 1
Article 43, paragraphe 2	–	–	Article 11, paragraphe 2
Article 44, paragraphe 1	–	–	Article 12, paragraphe 1
Article 44, paragraphe 2	–	–	Article 12, paragraphe 2
Article 44, paragraphe 3	–	–	Article 12, paragraphe 3
Article 45, paragraphe 1, point a)	–	–	Article 13, paragraphe 1, point a)
Article 45, paragraphe 1, point b)	–	–	Article 13, paragraphe 1, point b)
Article 45, paragraphe 1, point c)	–	–	Article 13, paragraphe 1, point d)
Article 45, paragraphe 1, point d)	–	–	Article 13, paragraphe 1, point e)

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 45, paragraphe 2, point a)	–	–	Article 13, paragraphe 2, point a)
Article 45, paragraphe 2, point b)	–	–	Article 13, paragraphe 2, point b)
Article 45, paragraphe 3	–	–	Article 13, paragraphe 3
Article 46	–	–	Article 14
Article 47	–	–	Article 15
Article 48	–	–	Article 16
Article 49	–	–	Article 17
Article 50	–	–	Article 18
Article 51, paragraphe 1	–	–	Article 19, paragraphe 1
Article 51, paragraphe 2	–	–	Article 19, paragraphe 2
Article 51, paragraphe 3	–	–	Article 19, paragraphe 3
Article 52, paragraphe 1, point a)	–	–	Article 20, paragraphe 1, point a)
Article 52, paragraphe 1, point b)	–	–	Article 20, paragraphe 1, point b)
Article 52, paragraphe 2, point a)	–	–	Article 20, paragraphe 2, point a)
Article 52, paragraphe 2, point b)	–	–	Article 20, paragraphe 2, point b)
Article 52, paragraphe 2, point c)	–	–	Article 20, paragraphe 2, point c)
Article 52, paragraphe 2, point d)	–	–	Article 20, paragraphe 2, point d)
Article 52, paragraphe 2, point e)	–	–	Article 20, paragraphe 2, point e)
Article 52, paragraphe 2, point f)	–	–	Article 20, paragraphe 2, point g)
Article 52, paragraphe 2, point g)	–	–	Article 20, paragraphe 2, point h)
Article 52, paragraphe 3, point a)	–	–	Article 20, paragraphe 3, point a)

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 52, paragraphe 3, point b)	–	–	Article 20, paragraphe 3, point c)
Article 52, paragraphe 3, point c)	–	–	Article 20, paragraphe 3, point d)
Article 52, paragraphe 4, point a)	–	–	Article 20, paragraphe 4, point a)
Article 52, paragraphe 4, point b)	–	–	Article 20, paragraphe 4, point b)
Article 52, paragraphe 4, point c)	–	–	Article 20, paragraphe 4, point c)
Article 52, paragraphe 4, point d)	–	–	Article 20, paragraphe 4, point d)
Article 52, paragraphe 5, point a)	–	–	Article 20, paragraphe 5, point a)
Article 52, paragraphe 5, point b)	–	–	Article 20, paragraphe 5, point b)
Article 52, paragraphe 5, point c)	–	–	Article 20, paragraphe 5, point c)
Article 52, paragraphe 5, point d)	–	–	Article 20, paragraphe 5, point d)
Article 52, paragraphe 5, point e)	–	–	Article 20, paragraphe 5, point e)
Article 52, paragraphe 5, point f)	–	–	Article 20, paragraphe 5, point g)
Article 52, paragraphe 5, point g)	–	–	Article 20, paragraphe 5, point h)
Article 52, paragraphe 6, point a)	–	–	Article 20, paragraphe 6, point a)
Article 52, paragraphe 6, point b)	–	–	Article 20, paragraphe 6, point b)
Article 52, paragraphe 6, point c)	–	–	Article 20, paragraphe 6, point c)
Article 52, paragraphe 7, point a)	–	–	Article 20, paragraphe 7, point a)
Article 52, paragraphe 7, point b)	–	–	Article 20, paragraphe 7, point b)
Article 53	–	–	Article 21

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 54, paragraphe 1	–	–	Article 22, paragraphe 1
Article 54, paragraphe 2	–	–	Article 22, paragraphe 3
Article 54, paragraphe 3	–	–	Article 22, paragraphe 4
Article 55, paragraphe 1	–	–	Article 23, paragraphe 1
Article 55, paragraphe 2	–	–	Article 23, paragraphe 2
Article 55, paragraphe 3	–	–	Article 23, paragraphe 3
Article 55, paragraphe 4	–	–	Article 23, paragraphe 4
Article 55, paragraphe 5	–	–	Article 23, paragraphe 5
Article 55, paragraphe 6	–	–	Article 23, paragraphe 6
Article 56	–	–	Article 24
Article 57, paragraphe 1	–	–	Article 25, paragraphe 1
Article 57, paragraphe 2	–	–	Article 25, paragraphe 2
Article 57, paragraphe 3	–	–	Article 25, paragraphe 3
Article 58, paragraphe 1	–	–	Article 26, paragraphe 1
Article 58, paragraphe 2	–	–	Article 26, paragraphe 2
Article 58, paragraphe 3	–	–	Article 26, paragraphe 3
Article 59, paragraphe 1	–	–	Article 5, paragraphe 1
Article 59, paragraphe 2	–	–	Article 5, paragraphe 2
Article 60, paragraphe 1	–	–	Article 6, paragraphe 1
Article 60, paragraphe 2	–	–	Article 6, paragraphe 2
Article 60, paragraphe 3	–	–	Article 6, paragraphe 3
Article 61, paragraphe 1	–	–	Article 27, paragraphe 1
Article 61, paragraphe 2	–	–	Article 27, paragraphe 2
Article 61, paragraphe 3	–	–	Article 27, paragraphe 3
Article 61, paragraphe 4	–	–	–

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 62, paragraphe 1	–	–	Article 28, paragraphe 1
Article 62, paragraphe 2	–	–	Article 28, paragraphe 2
Article 62, paragraphe 3	–	–	Article 28, paragraphe 5
Article 62, paragraphe 4	–	–	Article 28, paragraphe 3
Article 62, paragraphe 5	–	–	Article 28, paragraphe 4
Article 63, paragraphe 1	–	–	Article 29, paragraphes 1 et 2
Article 63, paragraphe 2	–	–	–
Article 63, paragraphe 3	–	–	Article 29, paragraphe 3
Article 64, paragraphe 1	–	–	Article 50, paragraphe 1
Article 64, paragraphe 2, premier alinéa	–	–	Article 50, paragraphe 6, premier alinéa
Article 64, paragraphe 2, deuxième alinéa	–	–	Article 50, paragraphe 4
Article 64, paragraphe 3	–	–	Article 50, paragraphe 7
Article 64, paragraphe 4	–	–	Article 50, paragraphe 6, deuxième alinéa
Article 65, paragraphe 1	–	–	–
Article 65, paragraphe 2	–	–	–
Article 65, paragraphe 3	–	–	–
Article 65, paragraphe 4	–	–	–
Article 65, paragraphe 5	–	–	–
Article 65, paragraphe 6	–	–	–
Article 66, paragraphe 1	–	–	Article 34, paragraphe 1
Article 66, paragraphe 2	–	–	Article 41; article 50
Article 66, paragraphe 3	–	–	Article 47
Article 66, paragraphe 4	–	–	Article 41
Article 66, paragraphe 5	–	–	Article 35

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 67, paragraphe 1	–	–	Article 34, paragraphe 2
Article 67, paragraphe 2	–	–	Article 48, paragraphes 1 et 2
Article 67, paragraphe 3	–	–	Article 42, paragraphe 1
Article 67, paragraphe 4	–	–	Article 35
Article 68, paragraphe 1	–	–	Article 52, paragraphe 1
Article 68, paragraphe 2	–	–	Article 52, paragraphe 4
Article 68, paragraphe 3	–	–	Article 52, paragraphe 5
Article 68, paragraphe 4	–	–	Article 52, paragraphe 5
Article 68, paragraphe 5	–	–	Article 43, paragraphe 1
Article 68, paragraphe 6	–	–	Article 43, paragraphe 2
Article 69, paragraphe 1, point a)	–	–	Article 53, premier alinéa, point a)
Article 69, paragraphe 1, point b)	–	–	Article 53, premier alinéa, point b)
Article 69, paragraphe 2	–	–	Article 53, deuxième alinéa,
Article 70, paragraphe 1, point a)	–	–	Article 54, paragraphe 1, point a)
Article 70, paragraphe 1, point b)	–	–	Article 54, paragraphe 1, point b)
Article 70, paragraphe 1, point c)	–	–	Article 54, paragraphe 1, premier alinéa, point c), et deuxième alinéa
Article 70, paragraphe 1, point d)	–	–	Article 54, paragraphe 1, premier alinéa, point d)
Article 70, paragraphe 1, point e)	–	–	Article 54, paragraphe 1, premier alinéa, point e)

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 70, paragraphe 2	–	–	Article 54, paragraphe 2
Article 71, paragraphe 1	–	–	Article 55, paragraphe 1
Article 71, paragraphe 2	–	–	Article 55, paragraphe 2
Article 72, paragraphe 1	–	–	Article 56, paragraphe 1
Article 72, paragraphe 2	–	–	Article 56, paragraphe 2
Article 73, paragraphe 1	–	–	Article 57, paragraphe 1, paragraphe 2, point b), et paragraphe 3
Article 73, paragraphe 2	–	–	Article 57, paragraphe 4
Article 73, paragraphe 2, deuxième alinéa	–	–	Article 57, paragraphe 5
Article 73, paragraphe 3	–	–	Article 57, paragraphe 6
Article 74, paragraphe 1	–	–	Article 63, paragraphe 1
Article 74, paragraphe 1, deuxième alinéa, point a)	–	–	Article 63, paragraphe 1, deuxième alinéa, point a)
Article 74, paragraphe 1, deuxième alinéa, point b)	–	–	Article 63, paragraphe 1, deuxième alinéa, point b)
Article 74, paragraphe 1, troisième alinéa	–	–	Article 63, paragraphe 2
Article 74, paragraphe 1, quatrième alinéa	–	–	Article 63, paragraphe 1, troisième alinéa
Article 74, paragraphe 2	–	–	Article 63, paragraphe 3
Article 74, paragraphe 3	–	–	Article 63, paragraphe 5
Article 75, paragraphe 1	–	–	Article 64, paragraphe 1
Article 75, paragraphe 2	–	–	Article 64, paragraphe 4
Article 76, paragraphe 1, premier alinéa, point a)	–	–	Article 65, paragraphe 1, premier alinéa, point a)

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 76, paragraphe 1, premier alinéa, point b)	–	–	Article 65, paragraphe 1, premier alinéa, point b)
Article 76, paragraphe 1, deuxième alinéa	–	–	Article 65, paragraphe 1, deuxième alinéa
Article 76, paragraphe 1, troisième alinéa	–	–	Article 65, paragraphe 1, troisième alinéa
Article 76, paragraphe 1, quatrième alinéa	–	–	Article 65, paragraphe 1, quatrième alinéa
Article 76, paragraphe 2	–	–	Article 65, paragraphe 2
Article 76, paragraphe 3, point a)	–	–	Article 65, paragraphe 3, point a)
Article 76, paragraphe 3, point b)	–	–	Article 65, paragraphe 3, point b)
Article 76, paragraphe 4	–	–	Article 65, paragraphe 4
Article 77, paragraphe 1	–	–	Article 66, paragraphe 1
Article 77, paragraphe 2	–	–	Article 66, paragraphe 2
Article 78, paragraphe 1	–	–	Article 67, paragraphe 1
Article 78, paragraphe 2	–	–	Article 67, paragraphe 2
Article 79, paragraphe 1	–	–	Article 68, paragraphe 3
Article 79, paragraphe 2	–	–	Article 68, paragraphe 1
Article 79, paragraphe 3	–	–	Article 68, paragraphe 5
Article 80, paragraphe 1	–	–	Article 69, paragraphe 1
Article 80, paragraphe 2	–	–	Article 69, paragraphe 2
Article 80, paragraphe 3	–	–	Article 69, paragraphe 3
Article 80, paragraphe 4	–	–	Article 69, paragraphe 4
Article 80, paragraphe 5	–	–	Article 69, paragraphe 5
Article 81, paragraphe 1	–	–	Article 70, paragraphe 1
Article 81, paragraphe 2	–	–	Article 70, paragraphe 2

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 81, paragraphe 3	–	–	Article 70, paragraphe 3
Article 82, paragraphe 1	–	–	Article 72, paragraphe 1
Article 82, paragraphe 2	–	–	Article 72, paragraphe 2
Article 83, paragraphe 1	–	–	Article 73, paragraphe 1
Article 83, paragraphe 2	–	–	Article 73, paragraphe 2
Article 83, paragraphe 3	–	–	Article 73, paragraphe 8
Article 84	–	–	Article 74, premier alinéa
Article 85	–	–	Article 75
Article 86	–	–	Article 76, premier alinéa
Article 87, paragraphe 1	–	–	Article 77, paragraphe 1
Article 87, paragraphe 2	–	–	Article 77, paragraphe 2
Article 87, paragraphe 3	–	–	Article 77, paragraphe 3
Article 88, paragraphe 1	–	–	Article 78, paragraphe 1
Article 88, paragraphe 2	–	–	Article 78, paragraphe 2, premier alinéa
Article 88, paragraphe 3, premier alinéa	–	–	Article 78, paragraphe 2, deuxième alinéa
Article 88, paragraphe 3, deuxième alinéa	–	–	Article 78, paragraphe 2, troisième alinéa
Article 88, paragraphe 4	–	–	Article 78, paragraphe 3
Article 88, paragraphe 5	–	–	Article 78, paragraphe 4
Article 89, paragraphe 1	–	–	Article 79, paragraphe 1
Article 89, paragraphe 2	–	–	Article 79, paragraphe 2
Article 89, paragraphe 3	–	–	Article 79, paragraphe 3
Article 90, paragraphe 1	–	–	Article 80, paragraphe 1
Article 90, paragraphe 2	–	–	Article 80, paragraphe 2

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…+	Le présent règlement
Article 91	–	–	Article 81
Article 92, paragraphe 1	–	–	Article 82, paragraphe 1
Article 92, paragraphe 2	–	–	Article 82, paragraphe 3
Article 93	–	–	Article 83
Article 94, paragraphes 1 et 2	–	–	Article 84
Article 95, paragraphe 1	–	–	Article 85, paragraphe 1
Article 95, paragraphe 1, deuxième alinéa, point a)	–	–	Article 85, paragraphe 1, deuxième alinéa, point a)
Article 95, paragraphe 1, deuxième alinéa, point b)	–	–	Article 85, paragraphe 1, deuxième alinéa, point b)
Article 95, paragraphe 1, deuxième alinéa, point c)	–	–	Article 85, paragraphe 1, deuxième alinéa, point c)
Article 95, paragraphe 1, deuxième alinéa, point d)	–	–	Article 85, paragraphe 1, deuxième alinéa, point c)
Article 95, paragraphe 2	–	–	-
Article 95, paragraphe 3	–	–	-
Article 95, paragraphe 4	–	–	-
Article 95, paragraphe 5	–	–	Article 85, paragraphe 2
Article 96, paragraphe 1	–	–	-
Article 96, paragraphe 2	–	–	-
Article 96, paragraphe 3	–	–	-
Article 96, paragraphe 4	–	–	-
Article 96, paragraphe 5	–	–	-
Article 96, paragraphe 6	–	–	Article 86
Article 96, paragraphe 7	–	–	-

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 97, paragraphe 1	–	–	Article 91, paragraphe 1
Article 97, paragraphe 1, point a)	–	–	Article 91, paragraphe 1, point a)
Article 97, paragraphe 1, point b)	–	–	Article 91, paragraphe 1, point b)
Article 97, paragraphe 1, point c)	–	–	Article 91, paragraphe 1, point c)
Article 97, paragraphe 2	–	–	Article 91, paragraphes 6 et 7
Article 97, paragraphe 3	–	–	Article 91, paragraphe 8
Article 97, paragraphe 4	–	–	Article 93, paragraphe 1
Article 97, paragraphe 5	–	–	Article 93, paragraphe 2
Article 98, paragraphe 1	–	–	Article 97, paragraphe 1
Article 98, paragraphe 1, point a)	–	–	Article 97, paragraphe 1, premier alinéa, point a)
Article 98, paragraphe 1, point b)	–	–	Article 97, paragraphe 1, premier alinéa, point b)
Article 98, paragraphe 1, point c)	–	–	Article 97, paragraphe 1, premier alinéa, point c)
Article 98, paragraphe 1, point d)	–	–	Article 97, paragraphe 1, premier alinéa, point e)
Article 98, paragraphe 2	–	–	Article 97, paragraphe 2
Article 98, paragraphe 2, point a)	–	–	Article 97, paragraphe 2, premier alinéa, point a)
Article 98, paragraphe 2, point b)	–	–	Article 97, paragraphe 2, premier alinéa, point b)

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 98, paragraphe 2, point c)	–	–	Article 97, paragraphe 2, premier alinéa, point c)
Article 98, paragraphe 2, point d)	–	–	Article 97, paragraphe 2, premier alinéa, point d)
Article 98, paragraphe 2, point e)	–	–	Article 97, paragraphe 2, premier alinéa, point e)
Article 98, paragraphe 3	–	–	Article 91, paragraphe 9
Article 98, paragraphe 3, point a)	–	–	Article 91, paragraphe 9, premier alinéa, point a)
Article 98, paragraphe 3, point b)	–	–	Article 91, paragraphe 9, premier alinéa, point b)
Article 98, paragraphe 3, point c)	–	–	Article 91, paragraphe 9, premier alinéa, point c)
Article 98, paragraphe 4	–	–	Article 97, paragraphe 2, deuxième et troisième alinéas
Article 98, paragraphe 5	–	–	Article 97, paragraphe 3
Article 99, paragraphe 1	–	–	Article 100, paragraphe 1
Article 99, paragraphe 2	–	–	Article 100, paragraphe 2
Article 100, paragraphe 1	–	–	Article 101, paragraphe 1
Article 100, paragraphe 2	–	–	Article 101, paragraphes 2 et 5
Article 100, paragraphe 3	–	–	Article 101, paragraphe 3, points a) et b)

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 100, paragraphes 4 et 5	–	–	Article 103, paragraphe 1
Article 100, paragraphe 5	–	–	Article 101, paragraphe 1, premier alinéa
Article 100, paragraphe 6	–	–	Article 100, paragraphe 3
Article 101, paragraphe 1	–	–	Article 104, paragraphe 1
Article 101, paragraphe 2	–	–	Article 104, paragraphe 2
Article 101, paragraphe 3	–	–	Article 104, paragraphe 3
Article 101, paragraphe 4	–	–	Article 104, paragraphe 4
Article 102, paragraphe 1	–	–	Article 105, paragraphe 1
Article 102, paragraphe 2	–	–	Article 105, paragraphe 4
Article 103, paragraphe 1	–	–	Article 106, paragraphe 1
Article 103, paragraphe 2	–	–	Article 111
Article 104, point b)	–	Article 39	Article 63, paragraphe 6
Article 105, paragraphe 1	–	Article 40, paragraphe 1	Article 115, paragraphe 1
Article 105, paragraphe 2	–	Article 40, paragraphe 2	Article 115, paragraphe 2
Article 105, paragraphe 3	–	Article 40, paragraphe 3	Article 115, paragraphe 3
Article 105, paragraphe 4	–	Article 40, paragraphe 5	Article 115, paragraphe 5
Article 105, paragraphe 5	–	Article 46, paragraphe 6	Article 115, paragraphe 6
Article 106	–	–	–
–	Article 13	–	Article 100; article 106, paragraphe 1; article 103, paragraphe 1; article 105, paragraphes 1 et 4
–	Article 14, paragraphes 1 et 2	Article 39	–
–	Article 15, paragraphes 1 et 2	Article 40	–
Article 107, paragraphe 1	Article 16, paragraphe 1	Article 41, paragraphe 1	–

Directive (UE) 2015/2366	Directive 2009/110/CE	Directive (UE) 2026/…[+]	Le présent règlement
Article 107, paragraphe 2	–	Article 41, paragraphe 2	–
Article 107, paragraphe 3	Article 16, paragraphe 2	Article 41, paragraphe 3	–
Article 108	Article 17	Article 42	Article 117
Article 109, paragraphe 1	–	–	–
Article 109, paragraphe 2	–	–	–
Article 109, paragraphe 3	–	–	–
Article 109, paragraphe 4	–	–	–
Article 109, paragraphe 5	–	–	–
–	Article 18, paragraphe 1	–	–
–	Article 18, paragraphe 2	–	–
–	Article 18, paragraphe 3	–	–
–	Article 18, paragraphe 4	–	–
Article 114	Article 21	Article 48	–
Article 115, paragraphe 1	Article 22, paragraphe 1	Article 49, paragraphe 1	–
Article 115, paragraphe 2	–	Article 49, paragraphe 1, deuxième et troisième alinéas	–
Article 115, paragraphe 3	Article 22, paragraphe 2	Article 49, paragraphe 2	–
Article 115, paragraphe 4	–	–	–
Article 115, paragraphe 5	–	–	–
Article 115, paragraphe 6	–	–	–
Article 116	Article 23	Article 50	Article 124
Article 117	Article 24	Article 51	–
Annexe I	–	Annexe I	–
Annexe II	–	Annexe II	Annexe