EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

Le 22 août 2023

Avis 39/2023

sur la proposition de règlement concernant les services de paiement dans le marché intérieur et la proposition de directive concernant les services de paiement et les services de monnaie électronique dans le marché intérieur

edps.europa.eu

Le Contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'UE, chargée, en vertu de l'article 52, paragraphe 2, du règlement (UE) 2018/1725, «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment le droit à la protection des données, soient respectés par les institutions et organes de l'Union» et, en vertu de l'article 52, paragraphe 3, du même règlement, «de conseiller les institutions et organes de l'Union et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel».

Wojciech Rafał Wiewiorówski a été nommé Contrôleur le 5 décembre 2019 pour un mandat de cinq ans.

*Conformément à l'**article 42, paragraphe 1**, du règlement (UE) 2018/1725, «[à] la suite de l'adoption de propositions d'acte législatif, de recommandations ou de propositions au Conseil en vertu de l'article 218 du traité sur le fonctionnement de l'Union européenne ou lors de l'élaboration d'actes délégués ou d'actes d'exécution, la Commission consulte le [CEPD] en cas d'incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel».*

Le présent avis porte sur la proposition de règlement concernant les services de paiement dans le marché intérieur[1] et sur la proposition de directive concernant les services de paiement et les services de monnaie électronique dans le marché intérieur[2]. Le présent avis n'exclut pas que le CEPD formule ultérieurement des observations ou des recommandations complémentaires, en particulier si d'autres difficultés se posent ou si de nouvelles informations apparaissent. En outre, le présent avis est fourni sans préjudice de toute mesure future qui pourrait être prise par le CEPD dans l'exercice des pouvoirs qui lui sont attribués par le règlement (UE) 2018/1725. Le présent avis se limite aux dispositions de la proposition pertinentes sous l'angle de la protection des données.

[1] COM(2023) 367 final.
[2] COM(2023) 366 final.

Résumé

Le 28 juin 2023, la Commission européenne a publié une proposition de règlement du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur et modifiant le règlement (UE) nº 1093/2010 (ci-après la «proposition de RSP») et une proposition de directive du Parlement européen et du Conseil concernant les services de paiement et les services de monnaie électronique dans le marché intérieur, modifiant la directive 98/26/CE et abrogeant les directives 2015/2366/UE et 2009/110/CE (ci-après la «proposition de DSP3»), ci-après dénommées ensemble «les propositions».

Les services de paiement impliquent souvent le traitement de données à caractère personnel qui peuvent révéler des informations sensibles sur une personne concernée. Le CEPD se félicite dès lors des efforts déployés pour assurer la cohérence avec le règlement général sur la protection des données (ci-après le «RGPD»). Il souligne également la nécessité de distinguer clairement les «permissions» prévues par la proposition de la base juridique du traitement des données à caractère personnel au titre du RGPD.

L'un des objectifs de la proposition est de permettre aux fournisseurs de systèmes de paiement et de services de paiement de traiter des catégories particulières de données à caractère personnel dans l'intérêt général du bon fonctionnement du marché intérieur des services de paiement. Étant donné que le traitement de telles données est susceptible de constituer une ingérence grave dans les droits au respect de la vie privée et à la protection des données à caractère personnel, il importe que la législation démontre avec suffisamment de précision le lien objectif entre chaque catégorie de données dans un contexte de paiement spécifique et l'objectif d'intérêt général à atteindre.

Le CEPD se félicite que la proposition exige des prestataires de services de paiement gestionnaires du compte (ci-après les «PSPGC») qu'ils fournissent à l'utilisateur un tableau de bord lui permettant de suivre et de gérer la permission qu'il a accordée. Afin de réduire davantage le risque de partage illicite de données à caractère personnel par les PSPGC, le CEPD recommande de:

◦ veiller à ce que le tableau de bord fasse référence au(x) service(s) de paiement spécifique(s) préalablement indiqué(s) pour le(s)quel(s) l'utilisateur a accordé sa permission ;

◦ veiller à ce que les demandes d'accès restent limitées à ce qui est nécessaire pour fournir le service demandé;

◦ garantir la clarté de la base juridique des demandes d'accès;

◦ permettre aux PSPGC de vérifier la permission accordée par l'utilisateur du service de paiement ou d'introduire d'autres garanties appropriées dans la proposition de RSP.

Enfin, le CEPD recommande d'assurer une coopération étroite entre les autorités compétentes en vertu de la proposition et les autorités de contrôle de la protection des données afin de garantir la cohérence entre l'application et la mise en œuvre de la proposition et la législation de l'UE en matière de protection des données. Le CEPD préconise donc de faire expressément référence aux autorités de contrôle chargées du suivi et de l'application de la législation sur la protection des données à l'article 93, paragraphe 3, de la proposition de RSP.

Table des matières

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne,

vu le 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 (ci-après le «RPDUE»)[3], et notamment son article 42, paragraphe 1,

A ADOPTÉ LE PRÉSENT AVIS:

1. Introduction

1. Le 28 juin 2023, la Commission européenne a publié une proposition de règlement du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur et modifiant le règlement (UE) nº 1093/2010 (ci-après la «proposition de règlement relatif aux services de paiement» ou la «proposition de RSP»)[4] et une proposition de directive du Parlement européen et du Conseil concernant les services de paiement et les services de monnaie électronique dans le marché intérieur, modifiant la directive 98/26/CE et abrogeant les directives (UE) 2015/2366 et 2009/110/CE (ci-après la «proposition de troisième directive relative aux services de paiement» ou la «proposition de DSP3»)[5], ci-après dénommées ensemble les «propositions».

2. La proposition de RSP et la proposition de DSP3 sont accompagnées chacune de trois annexes (six annexes au total), décrivant les types de services de paiement (annexe I) ainsi que le type de services de monnaie électronique (annexe II) relevant du champ d'application des projets de propositions. Enfin, l'annexe III présente un tableau de correspondance entre les dispositions des directives 2015/2366/UE et 2009/110/CE et les dispositions des propositions.

3. Le CEPD note que les types de services couverts par les propositions semblent être essentiellement les mêmes que ceux couverts par la 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 (la «DSP2»)[6].

4. Les objectifs spécifiques de la proposition de RSP[7] sont les suivants:

    a. renforcer la protection des utilisateurs et leur confiance dans les paiements, notamment en améliorant l'application de l'authentification forte du client (SCA), en créant une base juridique pour l'échange d'informations sur la fraude, en

[3] JO L 295 du 21.11.2018, p. 39.
[4] COM(2023) 367 final.
[5] COM(2023) 366 final.
[6] 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.
[7] COM(2023) 367 final, pages 5-6.

étendant la vérification du numéro de compte bancaire international (IBAN) à tous les virements et en améliorant les droits et l'information des utilisateurs;

b. améliorer la compétitivité des services bancaires ouverts en: i) exigeant des prestataires de services de paiement gestionnaires de comptes (les «PSPGC») qu'ils mettent en place une interface d'accès aux données dédiée et des «tableaux de bord des permissions» afin de permettre aux utilisateurs de gérer les permissions d'accès de banque ouverte qu'ils ont accordées; et ii) définissant des spécifications plus détaillées quant aux exigences minimales pour les interfaces de données bancaires ouvertes;

c. améliorer l'application et la mise en œuvre du cadre juridique applicable aux services de paiement dans les États membres, notamment en remplaçant la DSP2 par un règlement directement applicable (la «proposition de RSP») qui précise certains aspects peu clairs de la DSP2, et en renforçant la coopération entre les autorités compétentes et les autres autorités; et

d. améliorer l'accès (direct ou indirect) aux systèmes de paiement et aux comptes bancaires pour les prestataires de services de paiement non bancaires, y compris les prestataires de services d'initiation de paiement (PSIP) et les prestataires de services d'initiation de compte (PSIC).

5. Les propositions sont présentées conjointement avec la proposition de règlement relatif à l'accès aux données financières[8], qui couvre, entre autres, l'accès aux données financières autres que les données relatives aux comptes de paiement, lequel relève du champ d'application des propositions qui font l'objet du présent avis[9].

6. En substance, la proposition de RSP:

   a. établirait des exigences en matière de transparence des conditions et des exigences en matière d'information pour les services de paiement[10];

   b. établirait des droits et des obligations en ce qui concerne la fourniture et l'utilisation de services de paiement, y compris des règles sur les interfaces d'accès aux données pour les services d'information sur les comptes et les services d'initiation de paiement[11] et sur la gestion de l'accès aux données par les utilisateurs de services de paiement[12]; sur la protection des données[13]; sur les mécanismes de signalement des fraudes et de suivi des transactions et le partage de données relatives à la fraude[14]; sur la SCA[15]; sur les procédures d'exécution, les autorités compétentes et les sanctions[16], et sur les pouvoirs d'intervention de l'Autorité bancaire européenne (ABE)[17].

7. La proposition de DSP3 repose en grande partie sur le titre II de la DSP2 actuelle, en ce qui concerne les «prestataires de services de paiement», qui ne s'applique qu'aux

[8] COM(2023) 360 final.
[9] COM(2023) final, page 4.
[10] Articles 4 à 26 de la proposition de RSP.
[11] Articles 35 à 38 de la proposition de RSP.
[12] Article 43 de la proposition de RSP.
[13] Article 80 de la proposition de RSP.
[14] Articles 82 à 84 de la proposition de RSP.
[15] Articles 85 à 86 de la proposition de RSP.
[16] Chapitre 8 de la proposition de RSP.
[17] Chapitre 9 de la proposition de RSP.

établissements de paiement. Elle actualise et clarifie les dispositions relatives aux établissements de paiement et intègre les établissements de monnaie électronique en tant que sous-catégorie d'établissements de paiement. Elle comprend également des dispositions concernant les services de retrait d'espèces fournis par des détaillants ou des fournisseurs de DAB indépendants[18].

8. Le présent avis du CEPD est émis en réponse à une demande de consultation présentée par la Commission européenne le 29 juin 2023, conformément à l'article 42, paragraphe 1, du RPDUE. Le CEPD se félicite de la référence faite à cette consultation au considérant 147 de la proposition de RSP et au considérant 77 de la proposition de DSP3. À cet égard, le CEPD note également avec satisfaction qu'il a déjà été préalablement consulté de manière informelle en ce qui concerne les propositions, conformément au considérant 60 du RPDUE.

2. Observations générales

9. Le CEPD reconnaît l'importance de renforcer la protection des utilisateurs et la confiance dans les paiements. Il soutient également l'objectif d'améliorer l'application et la mise en œuvre du cadre réglementaire applicable aux services de paiement dans les États membres, ainsi que l'objectif d'améliorer la compétitivité des services bancaires ouverts.

10. L'exposé des motifs de la proposition de RSP note que le droit fondamental à la protection des données est particulièrement concerné par cette proposition[19]. Il souligne également que le traitement des données à caractère personnel doit être conforme au règlement général sur la protection des données (le «RGPD»)[20], qui s'applique directement à tous les services de paiement concernés par la proposition de RSP[21].

11. Le CEPD se félicite du considérant 97 de la proposition de RSP, qui énonce notamment que, lorsque des données à caractère personnel sont traitées, le traitement doit être conforme au RGPD, y compris aux principes de limitation de la finalité, de minimisation des données et de limitation de la conservation. Il se réjouit aussi de la confirmation explicite que les autorités de contrôle en vertu du RGPD et du RPDUE doivent être responsables du contrôle du traitement des données à caractère personnel effectué dans le cadre de la proposition de RSP. Le CEPD salut également le considérant 99 de la proposition de RSP, qui précise que la fourniture d'informations aux personnes sur le traitement des données à caractère personnel doit être effectuée conformément au RGPD et au RPDUE.

12. Le CEPD note que la proposition de RSP vise à assurer la cohérence avec la proposition de règlement relatif à l'accès aux données financières. À cet égard, il renvoie aux recommandations formulées dans son avis sur la proposition sur l'accès aux données financières, en particulier en ce qui concerne le terme «permission», qui est mentionné à la

[18] COM(2023) 367 final, page 7.
[19] COM(2023) 367 final, page 8.
[20] 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.
[21] COM(2023) 367 final, page 8.

fois dans la proposition de RSP et dans la proposition de règlement relatif à l'accès aux données financières

3. Le rôle des «permissions»

13. Le CEPD se félicite que la proposition de RSP vise à traiter certaines des interactions entre la DSP2 et le cadre de l'UE en matière de protection des données. L'une de ces interactions, également mentionnée dans les lignes directrices publiées par le comité européen de la protection des données sur la question[22], concerne la distinction entre le «consentement explicite» au titre de la DSP2, d'une part, et le «consentement» et le «consentement explicite» au titre du RGPD, d'autre part.

14. Le CEPD remarque que le considérant 69 de la proposition de RSP précise que «*(...) la permission ne devrait pas être interprétée exclusivement comme un "consentement" ou un "consentement explicite" au sens du règlement (UE) 2016/679*». Le CEPD considère que le terme «exclusivement» introduit un certain degré d'incertitude et ne permet pas de distinguer clairement entre, d'une part, la «permission» (qui fait référence à l'acceptation du service commercial par le consommateur) et, d'autre part, le «consentement» [au titre de l'article 6, paragraphe 1, point a), du RGPD] ou le «consentement explicite» [au titre de l'article 9, paragraphe 2, point a), du RGPD]. Il convient dès lors de modifier le considérant 69 afin de préciser que «*la permission ne devrait pas être interprétée comme un "consentement", un "consentement explicite" ou une "nécessité d'exécuter un contrat" au sens du règlement (UE) 2016/679*»[23].

15. Le CEPD recommande également de préciser — à l'instar du considérant 10 de la proposition de règlement relatif à l'accès aux données financières — la nécessité pour les prestataires de services d'initiation de paiement (PSIP) et les prestataires de services d'information sur les comptes (PSIC) de disposer d'un fondement juridique en vertu du RGPD pour traiter les données à caractère personnel[24]. De même, le CEPD recommande de préciser que l'octroi de la permission par un utilisateur de services de paiement est sans préjudice, en particulier, des obligations incombant aux utilisateurs de données en vertu des articles 6 et 9 du RGPD[25].

---

[22] Lignes directrices de l'EDPB de 2020 relatives à l'interaction entre la deuxième directive sur les services de paiement et le RGPD, adoptées le 15 décembre 2020, point 44.

[23] Dans le même ordre d'idées, le CEPD et le comité européen de la protection des données ont recommandé d'éviter toute ambiguïté entre l'expression «permission» au sens de l'acte sur la gouvernance des données (DGA) et la base juridique en vertu de l'article 6 du RGPD. Voir Avis conjoint 03/2021 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données), version 1.1, adopté le 9 juin 2021, points 41, 45, 47, 48, 49, 50, 102; voir en particulier le point 50: «*L'EDPB et le CEPD font aussi remarquer qu'en cas de traitement de données à caractère personnel, la "permission" visée dans la proposition ne saurait remplacer la nécessité d'un fondement juridique approprié au titre de l'article 6, paragraphe 1, du RGPD pour le traitement licite des données à caractère personnel. En d'autres termes, d'après le RGPD, le traitement de données à caractère personnel n'est licite que si, et dans la mesure où, au moins une des bases juridiques citées à l'article 6, paragraphe 1, du RGPD s'applique. La proposition devrait clairement préciser cet aspect afin d'éviter toute ambiguïté.*»

[24] Le considérant 10 de la proposition de règlement relatif à l'accès aux données financières indique qu'«*en cas de traitement de données à caractère personnel, un utilisateur de données devrait disposer d'une base légale valable pour procéder au traitement des données conformément au règlement (UE) 2016/679*».

[25] Voir également, dans le même ordre d'idées, le considérant 48 de la proposition de règlement relatif à l'accès aux données financières: « *L'octroi de la permission d'un client est sans préjudice des obligations incombant aux utilisateurs de données en vertu de l'article 6 du règlement (UE) 2016/679. Les données à caractère personnel mises à la disposition d'un utilisateur de données et partagées avec lui devraient être traitées aux seules fins des services fournis par celui-ci lorsqu'il existe une base juridique valable en vertu de l'article 6, paragraphe 1, du règlement (UE) 2016/679 et, le cas échéant, lorsque les exigences de l'article 9 dudit règlement concernant le traitement de catégories particulières de données sont remplies.*»

4. Vérification de la permission par le PSPGC

16. Le CEPD note que l'article 43, paragraphe 4, point b), de la proposition de RSP exigerait que les prestataires de services d'initiation de paiement (PSIP) et les prestataires de services d'information sur les comptes (PSIC) informent en temps réel les prestataires de services de paiement gestionnaires du compte (PSPGC) d'une nouvelle permission accordée par un utilisateur de services de paiement.

17. Le CEPD est toutefois préoccupé par le fait que l'article 44, paragraphe 1, point c), et l'article 49, paragraphe 4, de la proposition de RSP empêcheraient les PSPGC de vérifier la permission donnée par l'utilisateur de services de paiement aux PSIP et aux PSIC d'accéder aux informations relatives à son compte de paiement. Bien que le terme «permission» ne doive pas être interprété comme un «consentement» ou un «consentement explicite» au sens du RGPD, une interdiction de vérifier la permission donnée par l'utilisateur peut amener les PSPGC à partager des données à caractère personnel avec des tiers qui n'ont *pas* obtenu de base juridique appropriée en vertu du RGPD (ou à partager davantage de données à caractère personnel que ne l'avait envisagé l'utilisateur).

18. Chaque responsable du traitement a le devoir de veiller à ce que les données à caractère personnel ne soient pas traitées ultérieurement d'une manière incompatible avec les finalités pour lesquelles elles ont été initialement collectées. Toute divulgation par un responsable du traitement requiert une base juridique et une évaluation de la compatibilité, indépendamment du fait que le destinataire soit un responsable du traitement distinct ou un responsable conjoint du traitement[26]. Par conséquent, le CEPD invite le colégislateur à réexaminer l'interdiction applicable aux PSPGC de vérifier la permission prévue à l'article 44, paragraphe 1, point c), et à l'article 49, paragraphe 4, de la proposition de RSP. En particulier, le CEPD recommande soit i) de supprimer l'interdiction applicable aux PSPGC de vérifier la permission d'accès aux données en vertu de l'article 44, paragraphe 1, point c), et de l'article 49, paragraphe 4, de la proposition de RSP, soit ii) d'introduire des garanties appropriées pour protéger les utilisateurs de services de paiement contre le risque de potentiel partage illicite de données à caractère personnel par les PSPGC que cette interdiction pourrait entraîner.

5. Procédures d'authentification forte du client et utilisation des données de sécurité personnalisées

19. En 2014, la Banque centrale européenne (ci-après la «BCE») a émis la recommandation suivante: «*Il ne devrait pas y avoir de partage de données entre les prestataires de services de paiement tiers et le prestataire de services de paiement gestionnaire du compte; le prestataire de services de paiement tiers devrait soit rediriger le payeur de manière sécurisée vers son prestataire de services de paiement gestionnaire du compte, soit émettre ses propres données. Ces deux options devraient faire partie d'une interface européenne normalisée pour l'accès aux*

[26] Lignes directrices 07/2020 de l'EDPB concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, 7 juillet 2021, p. 45 (point 167 et note de bas de page 76).

comptes de paiement qui doit être développée[27].» En 2016, le groupe des parties intéressées au secteur bancaire de l'ABE a également déclaré: «*Afin de protéger les consommateurs, de réduire les risques et d'éviter la fraude, nous recommandons que les données de sécurité personnalisées ne soient pas accessibles directement par les prestataires tiers*»[28].

20. Le CEPD note que l'article 86, paragraphe 2, de la proposition de RSP permettrait aux PSIP et aux PSIC de «s'appuyer» sur les procédures d'authentification fournies par les PSPGC à l'utilisateur de services de paiement. Dans le même temps, les PSIP ne seraient pas autorisés à «conserver» [article 46, paragraphe 2, point a)] et les PSIC ne seraient pas autorisés à «demander» [article 47, paragraphe 2, point a)], des «données de paiement sensibles», ce qui inclut les «données de sécurité personnalisées»[29].

21. Le CEPD estime que tout partage éventuel avec les PSIP et les PSIC des données que l'utilisateur de services de paiement utilise pour s'authentifier avec le PSPGC créerait des risques inutiles[30] et devrait donc être exclu. Pour éviter toute ambiguïté, le CEPD recommande de modifier l'article 46, paragraphe 2, point a), et l'article 47, paragraphe 2, point a), de la proposition de RSP afin d'indiquer que les PSIP et les PSIC ne doivent pas accéder aux données de sécurité personnalisées fournies par le PSPGC (et pas seulement «ne pas [les] conserver» ou «ne pas [les] demander»).

22. L'article 89, paragraphe 1, imposerait à l'ABE d'élaborer des projets de normes techniques de réglementation pour préciser les exigences en matière d'authentification forte du client. L'ABE serait également tenue de préciser les exigences auxquelles les mesures de sécurité doivent se conformer pour protéger la confidentialité et l'intégrité des données de sécurité personnalisées des utilisateurs de services de paiement[31]. La Commission se verrait déléguer le pouvoir d'adopter les normes élaborées par l'ABE conformément aux articles 10 à 14 du règlement (UE) nº 1093/2010. À cet égard, le CEPD rappelle à la Commission l'obligation qui lui incombe de le consulter lors de l'élaboration d'actes délégués ou d'actes d'exécution qui auraient une incidence sur la protection des droits et libertés des personnes physiques en ce qui concerne le traitement des données à caractère personnel, conformément à l'article 42, paragraphe 1, du RPDUE.

23. Enfin, le CEPD recommande également de clarifier la définition de «données de paiement sensibles» visée à l'article 3, paragraphe 38, de la proposition de RSP (désignées, de manière générale, comme des «*données susceptibles d'être utilisées pour commettre une fraude, y*

---

[27] Recommandations finales de la BCE pour la sécurité des services d'accès aux comptes de paiement à la suite d'une consultation publique, mai 2014, p. 5.

[28] Projet de réponse du groupe des parties intéressées au secteur bancaire au document de réflexion EBA/DP/2015/03 relatif aux futurs projets de normes techniques de réglementation sur l'authentification forte du consommateur et à la sécurité des communications au titre de la directive révisée sur les services de paiement (PSD2), page 2.

[29] Au titre de l'article 3, paragraphe 38, de la proposition de RSP, on entend par «*"données de paiement sensibles" les données susceptibles d'être utilisées pour commettre une fraude, y compris les données de sécurité personnalisées.*»

[30] La conservation des données des utilisateurs de services de paiement à plusieurs endroits augmenterait la surface d'attaque et, par conséquent, le risque d'accès non autorisé (par exemple en raison d'une violation de données). En outre, l'accès aux données des utilisateurs de services de paiement augmenterait le risque de traitement non autorisé des données, car les données pourraient être utilisés par des PSIC ou des PSIP pour contourner l'utilisation autorisée de l'interface d'accès aux données dédiée (par exemple, un PSIC se connectant à l'interface web du PSPGC). En outre, le fait de permettre aux utilisateurs de services de paiement de partager avec des tiers les données qu'ils utilisent pour s'authentifier avec le PSPGC serait contraire aux meilleures pratiques et normes en matière de sécurité. Par exemple, la norme ISO 27002:2022 énumère parmi les responsabilités de l'utilisateur l'obligation de préserver la confidentialité des «*informations d'authentification secrètes telles que les mots de passe*», tout en indiquant que «*Les informations personnelles secrètes relatives à l'authentification ne doivent pas être partagées avec quiconque*».

[31] Article 89, paragraphe 1, points a) et c), de la proposition de RSP; l'article 89, paragraphe 2, point b), de la proposition de RSP dispose que, lors de l'élaboration des normes techniques de réglementation, l'ABE devra tenir compte de «la nécessité d'assurer la sécurité des fonds et des données à caractère personnel des utilisateurs de services de paiement».

compris les données de sécurité personnalisées») en précisant davantage les catégories de données à caractère personnel qui relèvent de cette définition.

6. Catégories particulières de données à caractère personnel

24. Les transactions financières peuvent révéler des informations sensibles sur une personne concernée, y compris celles relatives à des catégories particulières de données à caractère personnel[32]. L'article 80 de la proposition de RSP, lu à la lumière du considérant 98 de ladite proposition, dispose que les systèmes de paiement et les prestataires de services de paiement doivent être autorisés à traiter des catégories particulières de données à caractère personnel visées à l'article 9, paragraphe 1, du RGPD et à l'article 10, paragraphe 1, du RPDUE dans la mesure nécessaire à la fourniture de services de paiement et au respect des obligations prévues par ce règlement dans l'intérêt public du bon fonctionnement du marché intérieur des services de paiement, sous réserve de garanties appropriées pour les libertés et droits fondamentaux des personnes physiques. L'article 80 donne également une liste (non exhaustive) de ces garanties.

25. L'article 9, paragraphe 2, point g), du RGPD, qui prévoit une exception à l'interdiction de traiter des catégories particulières de données à caractère personnel en vertu de l'article 9, paragraphe 1, du RGPD pour des raisons d'intérêt public important, est assorti d'un certain nombre de conditions et doit être interprété de manière restrictive[33]. Ces conditions sont les suivantes: (i) le traitement des données à caractère personnel doit être nécessaire à la finalité déclarée; (ii) il doit être fondé sur une loi de l'Union ou d'un État membre; et (iii) la loi de l'Union ou de l'État membre elle-même doit être proportionnée à l'objectif spécifique poursuivi, respecter l'essence des droits fondamentaux à la vie privée et à la protection des données à caractère personnel; et prévoir des mesures appropriées et spécifiques pour sauvegarder les droits fondamentaux et les intérêts des personnes concernées[34].

26. Le CEPD estime que l'article 80 de la proposition de RSP ne satisfait pas aux exigences de nécessité et de proportionnalité. Conformément au principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union européenne ou au besoin de protection des droits et libertés d'autrui. Elles doivent s'opérer dans les limites du strict nécessaire et la réglementation comportant l'ingérence doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause[35]. Le strict respect des principes de nécessité et de proportionnalité est particulièrement important en ce qui concerne le traitement de catégories particulières de données à caractère personnel, le traitement de ces données étant susceptible de constituer une atteinte grave aux droits à la vie privée et à la protection des données à caractère personnel. Compte tenu de la gravité

---

[32] Voir les lignes directrices de l'EDPB relatives à l'interaction entre la deuxième directive sur les services de paiement et le RGPD, adoptées le 15 décembre 2020, point 52. Voir également l'arrêt de la Cour de justice du 1er août 2022, OT/Vyriausioji tarnybinės etikos komisija, C-184/20, ECLI:EU:C:2022:601, points 117 à 128, et l'arrêt de la Cour de justice du 4 juillet 2023, Meta Platforms e.a. (Conditions générales d'utilisation d'un réseau social), C-252/21, ECLI:EU:C:2023:537, points 69 à 73.

[33] Voir l'arrêt de la Cour de justice du 4 juillet 2023, Meta Platforms e.a. (Conditions générales d'utilisation d'un réseau social), C-252/21, ECLI:EU:C:2023:537, point 93 «[...] *les justifications prévues à cette dernière disposition, en ce qu'elles permettent de rendre licite un traitement de données à caractère personnel effectué en l'absence du consentement de la personne concernée, doivent faire l'objet d'une interprétation restrictive [voir, en ce sens, arrêt du 24 février 2022, Valsts ieņēmumu dienests (Traitement des données personnelles à des fins fiscales), C-175/20, EU:C:2022:124, point 73 et jurisprudence citée].*» et points 133-134.

[34] Voir également l'avis 33/2023 du CEPD sur la proposition de règlement en matière de protection des adultes, publié le 18 juillet 2023, points 14 à 15.

[35] Arrêt de la Cour de justice du 22 juin 2021, Latvijas Republikas Saeima (Points de pénalité), C-439/19, EU:C:2021:504, point 105.

de l'ingérence qu'implique le traitement de catégories particulières de données, il est important que la législation soit suffisamment précise pour montrer le lien objectif entre chaque catégorie de données dans un contexte de paiement spécifique et l'objectif d'intérêt public à atteindre.

27. Afin de satisfaire aux exigences de nécessité et de proportionnalité, la proposition de RSP devrait:

    a. délimiter davantage les finalités spécifiques du traitement, en précisant le(s) type(s) de service(s) de paiement[36] pour lesquels les systèmes de paiement et les prestataires de services de paiement seraient habilités à traiter les catégories particulières de données à caractère personnel[37]. La proposition de RSP devrait également justifier (dans un considérant) les raisons pour lesquelles le traitement des catégories particulières de données à caractère personnel pour le service désigné en cause est strictement nécessaire et ne peut être évité (c'est-à-dire qu'il ne serait pas possible d'éviter le traitement de ces données); et

    b. indiquer clairement quelles catégories particulières de données à caractère personnel seraient nécessaires pour atteindre la finalité spécifique et à qui (quel type d'opérateurs commerciaux précisément) cette base juridique s'appliquerait.

28. Le CEPD considère que dans certains cas, par exemple en ce qui concerne l'authentification multifactorielle de l'utilisateur de services de paiement, lorsqu'il est possible d'utiliser des moyens d'authentification non biométriques, le consentement (explicite) de la personne concernée peut être un fondement plus approprié pour le traitement des données sensibles conformément aux articles 6 et 9 du RGPD.

29. En ce qui concerne les garanties requises au titre de l'article 9, paragraphe 2, point g), du RGPD, le CEPD se félicite de la liste non exhaustive de garanties prévue à l'article 80 de la proposition de RSP. Toutefois, le CEPD recommande également d'inclure une référence aux exigences d'enregistrement lors de l'ouverture de session (afin de vérifier si un accès non autorisé a eu lieu).

[36] Bien que les types de services couverts par la proposition de RSP semblent être substantiellement les mêmes que ceux prévus par la DSP2, le considérant 26 souligne également que le nouveau modèle économique fondé sur la banque ouverte requiert une modification de la définition des services d'information sur les comptes afin de préciser que les informations agrégées par le prestataire autorisé de services d'information sur les comptes peuvent être transmises à un tiers afin de permettre à ce tiers de fournir un autre service à l'utilisateur final, avec la permission de l'utilisateur final.

[37] Voir également les lignes directrices de l'EDPB relatives à l'interaction entre la deuxième directive sur les services de paiement et le RGPD, adoptées le 15 décembre 2020, point 56 [soulignement ajouté]: «*Les services de paiement peuvent nécessiter le traitement de catégories particulières de données à caractère personnel pour des motifs d'intérêt public important, mais uniquement lorsque toutes les conditions prévues à l'article 9, paragraphe 2, point g), du RGPD sont remplies. Cela signifie que le traitement des catégories particulières de données à caractère personnel doit faire l'objet d'une dérogation spécifique à l'article 9, paragraphe 1, du RGPD dans le droit de l'Union ou des États membres. Cette disposition devra aborder la proportionnalité au regard de l'objectif poursuivi par le traitement et contenir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée. En outre, cette disposition en vertu du droit de l'Union ou des États membres devra respecter l'essence du droit à la protection des données. Enfin, il y a aussi lieu de démontrer que le traitement des catégories particulières de données est nécessaire pour le motif d'intérêt public important, y compris des intérêts d'importance systémique. Ce n'est que lorsque toutes ces conditions sont remplies que cette dérogation peut être rendue applicable à certains types de services de paiement.*»

7. Mise à disposition d'interfaces d'accès dédiées

30. Le CEPD note que l'article 35, paragraphe 6, de la proposition de RSP, sur la mise en place d'un dispositif de test par les PSPGC pour leur interface spécialisée interdit le partage de «données de paiement sensibles ou de toute autre donnée à caractère personnel» par l'intermédiaire du dispositif. Le CEPD se félicite de cette précision, étant donné qu'en règle générale, les données à caractère personnel ne devraient pas non plus être traitées lors de l'essai d'une fonctionnalité, conformément aux principes de minimisation des données et de protection des données dès la conception et par défaut[38].

8. Gestion de l'accès aux données

31. Le CEPD se félicite de l'article 43, qui impose aux PSPGC de fournir à l'utilisateur de services de paiement un tableau de bord pour contrôler et gérer la permission qu'il a accordée aux PSIC ou aux PSIP pour des paiements multiples et récurrents. En ce qui concerne les informations que les PSPGC doivent transmettre aux utilisateurs de services de paiement via le tableau de bord[39], le CEPD se réjouit en particulier de la référence faite aux «catégories de données partagées»[40]. Cet ajout contribue à assurer une vue d'ensemble et un contrôle efficaces des flux de données à caractère personnel par l'utilisateur de services de paiement, qui est une personne concernée au sens du RGPD. Toutefois, le CEPD recommande d'ajouter à l'article 43, paragraphe 2, point a), une référence au(x) service(s) désigné(s) pour le(s)quel(s) la permission est accordée[41].

32. En ce qui concerne les obligations spécifiques des PSIP et des PSIC, le CEPD se félicite en particulier de la limitation selon laquelle les PSIP et les PSIC ne peuvent traiter les données à caractère personnel qu'aux fins de la fourniture du service de paiement ou d'information sur les comptes pour lequel l'utilisateur du service de paiement a donné sa permission[42]. Le CEPD note toutefois que l'exigence prévue à l'article 46, paragraphe 2, point b), selon laquelle les PSIP ne peuvent demander à l'utilisateur de services de paiement que les données nécessaires pour fournir le service d'initiation de paiement, n'est pas incluse mutatis mutandis dans l'article 47, paragraphe 2, concernant les obligations des PSIC. Il recommande donc d'insérer une disposition équivalente à l'article 47, paragraphe 2, de la proposition de RSP.

33. Le CEPD prend également note avec satisfaction de l'obligation faite aux PSPGC de fournir aux utilisateurs de services de paiement, par l'intermédiaire du tableau de bord, une vue d'ensemble de chaque permission en cours donnée pour le(s) service(s) d'information sur

---

[38] Article 5, paragraphe 1, point c), et article 25, paragraphe 1, du RGPD.

[39] Conformément à l'article 43, paragraphe 2, de la proposition de RSP, le tableau de bord doit fournir à l'utilisateur de services de paiement des informations sur:
(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) la finalité de la permission;
(iv) la durée de validité de la permission;
(v) les catégories de données partagées.
Voir également considérant 65 de la proposition de RSP.

[40] Article 43, paragraphe 2, point v), de la proposition de RSP.

[41] Conformément à l'article 8, paragraphe 2, point a), ii), de la proposition de règlement relatif à l'accès aux données financières.

[42] Voir l'article 46, paragraphe 2, point c), et l'article 47, paragraphe 2, point b), de la proposition de RSP.

les comptes ou le(s) service(s) d'initiation de paiement, y compris: le nom du PSIP ou PSIC auquel l'accès a été accordé; le compte client auquel l'accès a été accordé; la finalité de la permission; une description des catégories de données partagées; et la durée de validité de la permission[43]. Afin de veiller à ce que les PSPGC soient en mesure de communiquer aux utilisateurs de services de paiement tous les éléments d'information visés à l'article 43, paragraphe 2, de la proposition de RSP, le CEPD recommande que les PSIP et les PSIC soient tenus, en vertu de l'article 43, paragraphe 4, point b), d'informer également les PSPGC du compte client auquel l'accès est demandé.

34. En outre, le CEPD recommande que l'article 43, paragraphe 4, point b), de la proposition de RSP exige des PSIP et PSIC qu'ils informent les PSPGC de la base juridique prévue à l'article 6, paragraphe 1, du RGPD et (le cas échéant) de l'exception prévue à l'article 9, paragraphe 2, du RGPD, sur laquelle ils s'appuieraient pour accéder aux (catégories particulières de) données à caractère personnel de l'utilisateur de services de paiement. Cela contribuerait à empêcher les PSPGC d'accorder l'accès à des données à caractère personnel en l'absence d'une base juridique appropriée tirée du RGPD[44].

35. Le CEPD se félicite de l'exigence prévue à l'article 43, paragraphe 3, de la proposition de RSP, selon laquelle le tableau de bord doit être «*facile à trouver dans son interface utilisateur et les informations affichées sur le tableau de bord doivent être claires, exactes et facilement compréhensibles par l'utilisateur de services de paiement*». Le considérant 65 de la proposition de RSP ajoute que le tableau de bord «*devrait permettre aux clients de gérer leurs permissions de manière éclairée et impartiale, ainsi que d'exercer un contrôle important sur la manière dont leurs données à caractère personnel et non personnel sont utilisées.*»

36. En effet, dans un domaine sensible tel que les services de paiement, les consommateurs peuvent être particulièrement inconscients des conséquences du partage de leurs données à caractère personnel avec les prestataires de services de paiement[45]. Le CEPD recommande donc que la proposition de RSP, et notamment son article 43, point b), précise que le tableau de bord ne doit pas être conçu de manière à inciter indûment les utilisateurs de services de paiement à accorder ou à retirer des permissions.

9. Mécanismes de suivi des transactions et partage des données relatives à la fraude

37. L'article 83 de la proposition de RSP établirait l'obligation pour les prestataires de services de paiement de mettre en place des mécanismes de suivi des transactions qui, entre autres, permettent aux prestataires de services de paiement de prévenir et de détecter les

[43] Article 43, paragraphe 2, point a), de la proposition de RSP.
[44] Voir les points 17 et 18 du présent avis.
[45] The Finance Innovation Lab, «Open Finance and Vulnerability - A Policy Discussion Paper», juillet 2021, page 9: «*Les conditions générales relatives au partage des données sont difficiles à comprendre et prennent du temps à lire. Des chercheurs de la LSE ont constaté que cela rendait très difficile la détermination du «consentement éclairé» dans le domaine des services financiers. Les contrats impliquent souvent des chaînes de données complexes, qui cèdent le contrôle des données à beaucoup plus d'entreprises qu'il n'y paraît à première vue. Il peut en résulter un partage de données ayant une incidence sur l'accès à de multiples services. Il existe donc un réel danger que les personnes ne comprennent pas toutes les implications de l'octroi de l'accès à des données de finance ouverte.*», voir également page 10: «*Il existe un risque que le partage de données devienne une condition préalable à l'accès à des services financiers essentiels.*»

opérations de paiement potentiellement frauduleuses, y compris celles impliquant des PSIP[46].

38. L'article 83, paragraphe 2, de la proposition de RSP prévoit que les mécanismes de surveillance des transactions seront «*basés sur l'analyse des opérations de paiement antérieures et l'accès aux comptes de paiement en ligne*» et précise les données requises à cette fin, à savoir: a) des informations sur l'utilisateur de services de paiement, y compris les caractéristiques environnementales et comportementales qui sont typiques de l'utilisateur de services de paiement dans les circonstances d'une utilisation normale des données de sécurité personnalisées; b) des informations sur le compte de paiement, y compris l'historique des opérations de paiement; c) des informations sur les transactions, y compris le montant de l'opération et l'identifiant unique du bénéficiaire; d) les données de session, y compris la plage d'adresses IP de l'appareil à partir duquel le compte de paiement a été consulté.

39. L'article 83, paragraphe 3, précise également que les mécanismes de suivi des transactions doivent prendre en compte, au minimum, les facteurs de risque suivants: a) les listes des éléments d'authentification compromis ou volés; b) le montant de chaque opération de paiement; c) les scénarios de fraude connus dans la prestation de services de paiement; d) les signes d'infection par des logiciels malveillants dans toutes les sessions de la procédure d'authentification; e) l'utilisation anormale du dispositif d'accès ou du logiciel (dans le cas où le dispositif d'accès ou le logiciel est fourni par le prestataire de services de paiement).

40. Le CEPD se félicite que la proposition vise à définir, de manière exhaustive, les catégories de données qui peuvent être utilisées à des fins de mécanismes de suivi des transactions. Il note toutefois que certaines catégories de données à caractère personnel restent très larges, compte tenu du fait que l'exposé des motifs mentionne comme «*caractéristiques environnementales et comportementales*» «*la localisation de l'utilisateur de services de paiement, le moment de la transaction, l'appareil utilisé, les habitudes de consommation, la boutique en ligne où l'achat est effectué*»[47].

41. Le CEPD note également que les prestataires de services de paiement effectuent déjà des activités de traitement de données à des fins de contrôle de la fraude sur la base de l'article 6, paragraphe 1, point f), du RGPD (intérêts légitimes)[48]. Cette base juridique impose aux responsables du traitement, tels que les prestataires de services de paiement, de procéder à une mise en balance minutieuse. Pour invoquer l'article 6, paragraphe 1, point f), du RGPD, trois conditions cumulatives doivent être remplies, à savoir: i) la poursuite d'un intérêt légitime par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, ii) la nécessité de traiter les données à caractère personnel aux fins des intérêts légitimes poursuivis, et iii) la condition que ne prévalent pas les libertés et droits fondamentaux de la personne concernée dont les données doivent être protégées[49]. Les nouvelles dispositions de l'article 83 de la proposition de RSP créeraient toutefois une obligation légale pour les prestataires de services de paiement de mener de telles activités de traitement au sens de l'article 6, paragraphe 1, point c), du RGPD. Si le traitement doit toujours être «limité» aux catégories de données énumérées, la proposition

[46] Article 83, paragraphe 1, point c), de la proposition de RSP.
[47] COM(2023) 367 final, page 13.
[48] Voir la référence à la prévention de la fraude au considérant 47 du RGPD comme l'un des intérêts légitimes possibles protégés par l'article 6, paragraphe 1, point f), du RGPD.
[49] Voir l'arrêt de la Cour de justice du 29 juillet 2019, Fashion ID, C-40/17, ECLI:EU:C:2019:629, point 95.

n'impose pas aux prestataires de services de paiement de procéder à un exercice de mise en balance avant de traiter les données à caractère personnel des utilisateurs de services de paiement à des fins de contrôle de la fraude conformément à la proposition de RSP.

42. Étant donné que la proposition de RSP prévoirait une obligation légale de traiter des données à caractère personnel, elle devrait définir clairement les limites de ce traitement. Il faut pour cela déterminer clairement les catégories de données à caractère personnel que les prestataires de services de paiement seraient autorisés à traiter dans le cadre des mécanismes de contrôle des transactions. À cet égard, le CEPD recommande de fournir une définition claire et complète des «informations sur l'utilisateur de services de paiement» visées à l'article 83, paragraphe 2, point a), de la proposition. En outre, le CEPD recommande d'indiquer explicitement que le traitement des catégories de données énumérées au paragraphe 2 ne peut être effectué que «dans la mesure où cela est nécessaire» pour atteindre les objectifs visés à l'article 83, paragraphe 1, de la proposition de RSP. Enfin, il préconise de définir des durées maximales de conservation des données appropriées pour les données à caractère personnel collectées au titre de l'article 83[50].

43. Le CEPD se félicite que les accords de partage d'informations entre prestataires de services de paiement doivent être précédés d'une analyse d'impact relative à la protection des données (AIPD) au sens de l'article 35 du RGPD, qui doit être menée conjointement par les prestataires de services de paiement participant à l'accord[51], ainsi que d'une consultation préalable, le cas échéant, au titre de l'article 36 du RGPD. Dans le même temps, le CEPD note que le terme «accord de partage d'informations» n'est pas défini dans la proposition de RSP et recommande d'en inclure une définition à l'article 3 de la proposition de RSP.

44. Le CEPD se félicite que le traitement des données à caractère personnel conformément à l'accord de partage d'informations ne puisse pas entraîner la cessation de la relation du client avec le prestataire de services de paiement ou avoir des conséquences sur son intégration future par un autre prestataire de services de paiement[52]. Il s'agit d'une garantie importante en ce qui concerne l'incidence éventuelle sur la personne concernée du traitement de données à caractère personnel dans le contexte des mécanismes de contrôle des transactions. Toutefois, le CEPD recommande de prévoir expressément dans la proposition de RSP — de manière plus générale — que *tout* traitement de données à caractère personnel dans le but de respecter les obligations légales en matière de prévention de la fraude au titre de l'article 83 (et pas seulement au titre de l'article 83, paragraphe 4) ne peut avoir lieu que dans le but spécifique de prévention de la fraude et ne peut entraîner la cessation de la relation du client avec le prestataire de services de paiement ou avoir des conséquences sur l'intégration de l'utilisateur de services de paiement par un autre prestataire de services de paiement.

45. Le CEPD note que les exigences techniques relatives aux mécanismes de surveillance des transactions seraient précisées dans des projets de normes techniques de réglementation élaborés par l'ABE et adoptés par la Commission par le biais d'un acte d'exécution([53]). À cet égard, le CEPD rappelle à la Commission l'obligation qui lui incombe de le consulter lors de l'élaboration d'actes d'exécution qui auraient une incidence sur la protection des droits

[50] Voir également le considérant 102 de la proposition de RSP.
[51] Article 83, paragraphe 4, de la proposition de RSP.
[52] Article 83, paragraphe 6, de la proposition de RSP.
[53] Article 89, paragraphe 1, point g), et paragraphe 2, de la proposition de RSP.

et libertés des personnes physiques en ce qui concerne le traitement des données à caractère personnel, conformément à l'article 42, paragraphe 1, du RPDUE.

10. Autorités compétentes

46. Conformément à l'article 91, paragraphe 2, de la proposition de RSP, les États membres doivent désigner des autorités compétentes chargées de garantir et de contrôler le respect effectif de la proposition. Ces autorités seraient soit a) des autorités publiques, soit b) 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. L'article 93, paragraphe 3, prévoit que dans l'exercice de leurs pouvoirs d'enquête et de sanction, y compris dans les affaires transfrontalières, les autorités compétentes doivent coopérer entre elles et garantir une assistance mutuelle aux autres autorités concernées.

47. Le considérant 130 de la proposition de RSP souligne à juste titre que l'efficacité du cadre juridique applicable aux services de paiement dépend de la coopération entre les autorités compétentes, y compris les autorités nationales chargées de la protection des données[54]. Le CEPD estime qu'une telle coopération contribuerait à assurer la cohérence entre l'application et la mise en œuvre de la proposition de RSP et la législation de l'UE en matière de protection des données.

48. Afin de garantir une base juridique claire pour l'échange d'informations pertinentes, le CEPD recommande que les autorités de contrôle chargées du suivi et de l'application de la législation sur la protection des données soient explicitement mentionnées à l'article 93, paragraphe 3, de la proposition de RSP.

11. Publication des sanctions et mesures administratives

49. L'article 101, paragraphe 1, de la proposition de RSP prévoit que, dans le cadre de la publication sur leur site web des décisions imposant une sanction administrative ou une mesure administrative à des personnes physiques et morales pour infraction au présent règlement et, le cas échéant, à tous les accords de règlement conclus, l'identité des personnes physiques visées par une décision imposant une sanction administrative ou une mesure administrative n'est pas publiée. Uniquement par dérogation à l'article 101, paragraphe 1, si l'autorité nationale compétente juge nécessaire de publier l'identité ou d'autres données à caractère personnel de personnes physiques, elle peut aussi publier l'identité de la personne concernée[55].

50. Le CEPD estime que la publication de données à caractère personnel avec les décisions des autorités compétentes devrait effectivement constituer l'exception, qui doit être décidée à la suite d'une évaluation au cas par cas. Cette démarche laisserait aux autorités compétentes la possibilité, à la suite d'une telle évaluation, de publier lesdites données à caractère personnel en cas d'infractions graves et lorsque des effets dissuasifs importants

[54] Voir également le considérant 76 de la proposition de DSP3: «*Tout traitement de données à caractère personnel dans le cadre de la présente directive doit être conforme au règlement (UE) 2016/679 et au règlement (UE) 2018/1725. Par conséquent, les autorités de contrôle en vertu du règlement (UE) 2016/679 et du règlement (UE) 2018/1725 sont responsables du contrôle du traitement des données à caractère personnel effectué dans le cadre de la présente directive.*»

[55] Article 101, paragraphe 2, de la proposition de RSP. Voir également le considérant 136 de la proposition de RSP.

sont nécessaires. Le CEPD relève que la publication des données à caractère personnel des personnes sanctionnées pour infraction au règlement ne devrait avoir lieu que dans des cas exceptionnels dûment justifiés, étant donné que la publication de ces types de données à caractère personnel pourrait être considérée comme une atteinte grave à leurs droits fondamentaux consacrés aux articles 7 et 8 de la charte.

51. Enfin, le CEPD se félicite que l'article 101, paragraphe 4, de la proposition de RSP dispose, conformément au principe de limitation de la conservation[56], que les données à caractère personnel contenues dans la publication ne doivent être conservées sur le site web officiel de l'autorité compétente que si un réexamen annuel montre qu'il reste nécessaire de publier ces données pour protéger la stabilité des marchés financiers ou pour garantir l'application effective de la proposition de RSP, et en tout état de cause pas plus de cinq ans.

12. Conclusions

52. Eu égard aux considérations qui précèdent, le CEPD formule les recommandations suivantes:

(1) établir une distinction claire entre le terme «permission» et la base juridique du traitement au titre du RGPD, en précisant, au considérant 62 de la proposition de RSP, que «la permission ne devrait pas être interprétée comme un "consentement", un "consentement explicite" ou une "nécessité d'exécuter d'un contrat" au sens du règlement (UE) 2016/679»;

(2) préciser, au moyen d'un considérant, que l'octroi d'une permission par l'utilisateur de services de paiement est sans préjudice, en particulier, des obligations incombant aux prestataires de services d'initiation de paiement et aux prestataires de services d'information sur les comptes en vertu de l'article 6 et de l'article 9 du règlement (UE) 2016/679;

(3) réexaminer l'interdiction applicable aux PSPGC de vérifier la permission prévue à l'article 49, paragraphe 4, de la proposition de RSP ou introduire d'autres garanties appropriées dans le dispositif de la proposition de RSP visant à protéger les utilisateurs de services de paiement contre le risque de potentiel partage illicite de données à caractère personnel par les PSPGC que cette interdiction pourrait entraîner;

(4) modifier l'article 46, paragraphe 2, point a), et l'article 47, paragraphe 2, point a), de la proposition de RSP afin d'indiquer que les prestataires de services d'initiation de paiement et les prestataires de services d'information sur les comptes n'ont pas accès aux données de sécurité personnalisées;

(5) clarifier la définition de «données de paiement sensibles» au sens de l'article 3, paragraphe 38, de la proposition de RSP, en précisant notamment les types de données à caractère personnel couverts par cette définition;

(6) préciser pour quel(s) type(s) spécifique(s) de service(s) de paiement désigné(s) les systèmes de paiement et le prestataire de services de paiement seraient habilités à traiter quelles catégories

[56] Article 5, paragraphe 1, point c), du RGPD.

de catégories particulières de données à caractère personnel visées à l'article 80 de la proposition de RSP;

(7) justifier (dans un considérant) les raisons pour lesquelles le traitement des catégories particulières de données à caractère personnel pour le(s) service(s) de paiement désigné(s) à l'article 80 de la proposition de RSP est nécessaire et proportionné et ne peut être évité par le recours à d'autres moyens techniques;

(8) inclure une référence à l'enregistrement lors de l'ouverture de session (pour vérifier si un accès non autorisé a eu lieu) parmi les garanties de protection des données visées à l'article 80 de la proposition de RSP;

(9) ajouter à l'article 43, paragraphe 2, point a), une référence au(x) service(s) de paiement désigné(s) pour le(s)quel(s) la permission est accordée par l'utilisateur de services de paiement;

(10) ajouter à l'article 47, paragraphe 2, concernant les obligations des prestataires de services d'information sur les comptes, l'exigence prévue à l'article 46, paragraphe 2, point b), selon laquelle les prestataires de services de paiement ne peuvent demander à l'utilisateur de services de paiement que les données nécessaires pour fournir le service demandé;

(11) exiger des prestataires de services de paiement et des prestataires de services d'information sur les comptes, en vertu de l'article 43, paragraphe 4, point b), qu'ils informent les prestataires de services de paiement gestionnaires de comptes du compte client auquel l'accès est demandé et de la base juridique prévue à l'article 6, paragraphe 1, du RGPD et (le cas échéant) de l'exception prévue à l'article 9, paragraphe 2, du RGPD sur laquelle ils s'appuieraient pour accéder aux données à caractère personnel de l'utilisateur de services de paiement;

(12) préciser à l'article 43, point b), que le tableau de bord ne doit pas être conçu de manière à encourager ou à inciter indûment les utilisateurs de services de paiement à accorder ou à retirer des permissions;

(13) déterminer clairement les catégories de données à caractère personnel que les prestataires de services de paiement seraient autorisés à traiter dans le cadre des mécanismes de suivi des transactions [notamment en fournissant une définition des «informations sur l'utilisateur de services de paiement» visées à l'article 83, paragraphe 2, point a)];

(14) définir des durées de conservation appropriées pour les données à caractère personnel collectées en vertu de l'article 83;

(15) inclure une définition de «l'accord d'échange d'informations» à l'article 3 de la proposition de RSP;

(16) prévoir dans la proposition de RSP que tout traitement de données à caractère personnel aux fins du respect des obligations légales en matière de prévention de la fraude au titre de l'article 83 ne peut avoir lieu qu'à cette fin spécifique et ne peut conduire à la cessation de la relation du client avec le prestataire de services de paiement ni porter atteinte à l'intégration de l'utilisateur de services de paiement par un autre prestataire de services de paiement;

(17) mentionner explicitement les autorités de contrôle chargées du suivi et de l'application de la législation sur la protection des données à l'article 93, paragraphe 3, de la proposition de RSP.

Wojciech Rafał WIEWIÓROWSKI

p.o. Leonardo CERVERA NAVAS
Secrétaire-général