EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

22 août 2023

Avis 38/2023

sur la proposition de règlement relatif à un cadre pour l'accès aux données financières

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».*

Cet avis concerne la proposition de règlement du Parlement européen et du Conseil relatif à un cadre pour l'accès aux données financières et modifiant les règlements (UE) nº 1093/2010, (UE) nº 1094/2010, (UE) nº 1095/2010 et (UE) 2022/2554[1]. 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) 360 final.

Résumé

Le 28 juin 2023, la Commission européenne a publié une proposition de règlement du Parlement européen et du Conseil relatif à un cadre pour l'accès aux données financières et modifiant les règlements (UE) nº 1093/2010, (UE) nº 1094/2010, (UE) nº 1095/2010 et (UE) 2022/2554[2] (ci-après la «proposition»). L'objectif de la proposition est de promouvoir le développement de services et de produits financiers fondés sur les données en permettant aux consommateurs et aux entreprises de mieux contrôler l'accès à leurs données financières.

Le CEPD se réjouit que la proposition entende donner aux clients, y compris aux personnes concernées, le pouvoir de décider de la manière dont leurs données sont utilisées, et par qui. Il note toutefois que la définition des «données clients» est particulièrement large et inclut potentiellement des données à caractère personnel de nature très sensible. Les catégories de données à caractère personnel qui seront mises à disposition dans le cadre de la proposition doivent être clairement délimitées, en tenant compte des risques encourus par les personnes dont les données à caractère personnel seraient consultées et utilisées. Le CEPD recommande également d'exclure explicitement de la définition des «données clients» les données créées à la suite d'un profilage.

Le CEPD se félicite du fait que la proposition imposerait aux détenteurs et aux utilisateurs de données plusieurs obligations qui pourraient avoir un effet positif sur le niveau de protection des données à caractère personnel. Pour favoriser cet objectif, les utilisateurs de données devraient avoir l'obligation d'indiquer clairement, pour chaque demande, les types de données clients spécifiques auxquels ils souhaitent avoir accès. La proposition devrait également interdire le refus des services financiers aux clients qui n'installent pas et n'utilisent pas le tableau de bord des permissions ou ne permettent pas d'une autre manière le partage de données par les détenteurs de données avec les utilisateurs de données au titre de la proposition.

Le CEPD estime qu'un périmètre d'utilisation des données clairement défini et strictement appliqué est nécessaire pour délimiter les utilisations appropriées des données à caractère personnel et pour protéger les consommateurs vulnérables. À cet égard, le CEPD se félicite du fait que la proposition prévoie l'élaboration d'orientations par l'Autorité bancaire européenne et l'Autorité européenne des assurances et des pensions professionnelles, en coopération avec le comité européen de la protection des données (EDPB). Afin de veiller à ce que les orientations soient pleinement conformes à la législation en matière de protection des données, le CEPD considère qu'une consultation formelle de l'EDPB est nécessaire. Le CEPD recommande également d'étendre le champ d'application des futures orientations à d'autres produits et services financiers pertinents, tels que les contrats de crédit hypothécaire, les services de paiement, d'autres produits d'assurance, les produits d'investissement et les produits d'épargne-retraite. Les orientations devraient également préciser, le cas échéant, les limites de la combinaison de «données clients» avec d'autres types de données à caractère personnel, telles que les données à caractère personnel obtenues auprès de sources tierces (par exemple, les réseaux de médias sociaux ou les courtiers de données).

[2] COM(2023) 360 final.

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 l'exécution de la proposition, d'une part, et la législation de l'UE en matière de protection des données, d'autre part. Une telle coopération étroite pourrait être favorisée en clarifiant les circonstances dans lesquelles les autorités compétentes peuvent consulter les autorités chargées de la protection des données et échanger des informations avec elles.

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 relatif à un cadre pour l'accès aux données financières et modifiant les règlements (UE) nº 1093/2010, (UE) nº 1094/2010, (UE) nº 1095/2010 et (UE) 2022/2554[4] (ci-après la «proposition»).

2. L'objectif de la proposition est de promouvoir le développement de services et de produits financiers fondés sur les données en permettant aux consommateurs et aux entreprises de mieux contrôler l'accès à leurs données financières[5]. Ce faisant, la proposition permettrait aux consommateurs et aux entreprises de bénéficier de produits et services financiers autres que les paiements qui sont adaptés à leurs besoins sur la base de données pertinentes. En parallèle, la proposition vise à traiter les risques inhérents à l'augmentation du partage des données financières et à l'accès à celles-ci[6].

3. La proposition est un élément sectoriel constitutif de la stratégie européenne pour les données, qui permet le partage de données dans le secteur financier ainsi qu'avec d'autres secteurs[7]. Elle est directement liée à l'une des priorités de la stratégie de la Commission en matière de finance numérique pour l'UE, à savoir la création d'un espace européen des données financières pour promouvoir l'innovation fondée sur les données, en s'appuyant sur la stratégie européenne en matière de données[8], y compris un meilleur accès aux données et un meilleur partage des données au sein du secteur financier[9].

4. En substance, la proposition:

[3] JO L 295 du 21.11.2018, p. 39.
[4] COM(2023) 360 final.
[5] COM(2023) 360 final, p. 1.
[6] COM(2023) 360 final, p. 1-2.
[7] COM(2023) 360 final, p. 3.
[8] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions — «Une stratégie européenne pour les données», COM(2020) 66 final du 19.2.2020.
[9] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions — «Une stratégie en matière de finance numérique pour l'UE», COM(2020) 591 final du 24.09.2020, p. 4-5.

a. établirait les règles selon lesquelles des catégories spécifiques de «données clients» dans le domaine financier[10] (y compris des données à caractère personnel) peuvent être consultées, partagées et utilisées par les établissements financiers et les prestataires de services d'information financière (les «entités éligibles»[11]), agissant soit en tant que détenteurs[12], soit en tant qu'utilisateurs[13] de données;

b. donnerait au client, qui peut être une personne physique ou morale[14], le droit de demander au détenteur de données de partager ces données avec un utilisateur de données aux fins et dans les conditions convenues entre l'utilisateur de données et le client[15];

c. imposerait certaines obligations aux utilisateurs de données qui reçoivent des données à la demande des clients et fixerait certaines limites quant à la manière dont les données des clients peuvent être utilisées[16];

d. mandaterait l'Autorité bancaire européenne (ci-après l'«ABE») et l'Autorité européenne des assurances et des pensions professionnelles (ci-après l'«AEAPP»), en coopération avec le comité européen de la protection des données (ci-après l'«EDPB»), pour élaborer des orientations ciblées portant sur les domaines dans lesquels le partage des données et l'accès envisagé dans la proposition pourraient entraîner des risques d'exclusion plus élevés pour les clients[17], établissant ainsi un «périmètre d'utilisation des données»[18];

e. permettrait aux clients de surveiller et de gérer les permissions d'accès aux données qu'ils ont accordées aux utilisateurs de données au moyen de tableaux de bord des permissions d'accès aux données financières. (qui doivent être obligatoirement mis en place par les détenteurs de données)[19]; et

f. introduirait des exigences pour la création et la gouvernance des systèmes de partage de données financières — dont les détenteurs de données, les utilisateurs de données et les organisations de consommateurs seraient parties — afin d'élaborer (entre autres) des normes en matière de données et d'interfaces et un cadre contractuel et normalisé commun régissant l'accès à des ensembles de données spécifiques[20].

5. 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 54 de la proposition. À cet égard, le CEPD note également avec satisfaction qu'il a déjà été

[10] Énumérées à l'article 2, paragraphe 1, de la proposition.
[11] Énumérées à l'article 2, paragraphe 2, de la proposition.
[12] Article 3, paragraphe 5, de la proposition: «"détenteur de données", un établissement financier, autre qu'un prestataire de services d'information sur les comptes, qui collecte, conserve et traite d'une autre manière les données visées à l'article 2, paragraphe 1».
[13] Article 3, paragraphe 6, de la proposition: «"utilisateur de données", une entité visée à l'article 2, paragraphe 2, qui, après avoir reçu la permission d'un client, dispose d'un accès licite aux données client de ce dernier, telles que visées à l'article 2, paragraphe 1».
[14] Article 3, paragraphe 2, de la proposition.
[15] Article 5 de la proposition.
[16] Article 6 de la proposition.
[17] Notamment les produits et services liés à l'évaluation du risque de crédit associé à des consommateurs, ainsi qu'à l'évaluation du risque associé à un consommateur et à la fixation d'un prix pour celui-ci dans le cadre de produits d'assurance vie, santé et maladie. Voir également le considérant 18 de la proposition.
[18] Article 7 de la proposition.
[19] Article 8 de la proposition.
[20] Titres IV et V de la proposition.

préalablement consulté de manière informelle, conformément au considérant 60 du RPDUE.

2. Remarques d'ordre général

6. Le CEPD reconnaît qu'il est important de veiller à ce que les clients des établissements financiers aient la possibilité de bénéficier d'une innovation ouverte, équitable et sûre dans le secteur financier. Il relève également avec satisfaction que la proposition vise à permettre aux clients — y compris les personnes concernées au sens de la législation européenne sur la protection des données — «*[de] décider de la manière dont leurs données financières sont utilisées, et par qui, et [de] pouvoir choisir de donner à des entreprises accès à leurs données en échange, s'ils le souhaitent, de services financiers et de services d'information.*»[21].

7. Le partage des données clients entre les entités éligibles au titre de la proposition serait contrôlé, étant donné que ce partage est soumis à la demande du client[22]. Dans le même temps, le CEPD note qu'en l'absence de garanties appropriées, notamment un périmètre d'utilisation des données clairement défini et strictement appliqué[23], un partage et une utilisation plus étendus des données pourraient, dans des cas spécifiques, entraîner pour des clients présentant un profil de risque défavorable un risque d'augmentation des prix pour des services financiers importants ou d'exclusion. À cet égard, il convient d'accorder une attention particulière aux services qui, intrinsèquement, nécessitent une mutualisation des risques, tels que l'assurance[24], ou aux services qui peuvent être nécessaires dans la vie quotidienne des citoyens, tels que le crédit à la consommation. Les consommateurs de services financiers sont souvent la partie la plus faible, exposée à des risques d'abus, de fraude et d'exploitation[25], et ils sont souvent soumis à des asymétries d'information et de pouvoir vis-à-vis des prestataires de services financiers.

8. Le CEPD note que la collecte et l'utilisation de données à caractère personnel pour évaluer la solvabilité seront également réglementées par la directive révisée relative aux crédits aux consommateurs[26], qui prévoit des limitations claires sur la collecte et l'utilisation des données à caractère personnel (notamment sur les catégories particulières de données à caractère personnel et les données provenant des réseaux sociaux). Le CEPD, comme il l'a

[21] Considérant 2 de la proposition.
[22] Article 4 et article 5, paragraphe 1, de la proposition. Voir également SWD(2023) 224 final, p. 65.
[23] Voir l'article 7 de la proposition.
[24] Dans son analyse d'impact, la Commission note que «l'utilisation inappropriée d'informations financières pourrait entraîner un biais injuste ou un préjudice pour le consommateur. En conséquence, certains consommateurs pourraient être exclus d'un marché, tandis que ceux qui choisiraient de ne pas participer au partage de données pourraient finir par payer un prix plus élevé pour les services. Les associations de consommateurs participant au groupe d'experts de la Commission ont mis en évidence plusieurs types de risques d'exclusion financière liés à un partage accru des données en l'absence de garanties appropriées. Y figurent, entre autres, les risques qu'une sélection plus granulaire des risques peut poser pour les consommateurs vulnérables présentant un profil de risque plus élevé. En outre, les consommateurs qui ne décident pas de partager leurs données risquent de ne pas avoir accès à tous les services et produits proposés. La mutualisation des risques inhérente à certains secteurs, tels que la fourniture d'assurances, pourrait également être en jeu, ce qui pourrait entraîner une hausse des prix pour de nombreuses personnes.», SWD(2023) 224 final, p. 17.
[25] Fiche analytique du Groupe consultatif d'assistance aux plus pauvres (CGAP) «Combining Open Finance and Data Protection for Low-Income Consumers» («Combiner finance ouverte et protection des données pour les consommateurs à faibles revenus»), février 2023, p. 5.
[26] Voir article 18, paragraphe 2, de la proposition de directive du Parlement européen et du Conseil relative aux crédits aux consommateurs [COM(2021)0347 – C9-0244/2021 – 2021/0171(COD)], accord provisoire résultant de négociations interinstitutionnelles.

souligné dans son avis sur cette proposition[27], rappelle l'importance de ces limitations pour contribuer à garantir, entre autres, la proportionnalité du traitement des données à caractère personnel dans le cadre de l'octroi de crédits aux consommateurs. La proportionnalité du traitement est également très pertinente en ce qui concerne l'accès à d'autres services financiers, tels que les crédits hypothécaires ou les assurances, en tant que services «de base» nécessaires à l'inclusion financière et sociale.

9. Le CEPD se félicite que le considérant 48 de la proposition souligne que le règlement (UE) 2016/679 (ci-après le «RGPD»)[28] s'applique en cas de traitement de données à caractère personnel dans le cadre de la proposition. Toutefois, il existerait des situations dans lesquelles des entités éligibles ou des organes de l'UE tels que l'ABE seraient soumis à des actes juridiques de l'UE concernant le respect de la vie privée et la protection des données autres que le RGPD, notamment le RPDUE et la directive vie privée et communications électroniques[29]. Le CEPD recommande donc de reformuler légèrement la phrase initiale du considérant 48 de la proposition comme suit: «*Le traitement des données à caractère personnel dans le cadre du présent règlement devrait être effectué conformément au règlement (UE) 2016/679 et au règlement (UE) 2018/1725, ainsi que, le cas échéant, à la directive vie privée et communications électroniques.*»

10. Le CEPD note que la proposition s'appuie sur la directive sur les services de paiement (DSP2)[30], qui permet le partage des données relatives aux comptes de paiement pour les services de paiement et les services d'information sur les comptes, et qui est actuellement en cours de révision. Il note également que la proposition vise à assurer la cohérence avec la proposition de règlement concernant les services de paiement[31] (ci-après la «proposition de RSP»)[32]. À cet égard, le CEPD renvoie aux recommandations formulées dans son avis sur la proposition de RSP, en particulier en ce qui concerne le terme «permission», qui est mentionné à la fois dans la proposition et dans la proposition de RSP.

3. Accès aux données et utilisation des données

3.1. Catégories de données clients

11. L'article 2, paragraphe 1, de la proposition définit les catégories de données clients qui entrent dans le champ d'application de la proposition. Les catégories suivantes de données clients seraient partagées, consultées et utilisées:

---

[27] Voir l'avis 11/2021 du CEPD sur la proposition de directive relative aux crédits aux consommateurs, 26 août 2021, point 17.
[28] 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.
[29] 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. 37–47.
[30] 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 (texte présentant de l'intérêt pour l'EEE), JO L 337 du 23.12.2015, p. 35.
[31] 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, COM/2023/367 final.
[32] Considérant 49 de la proposition.

a. les contrats de crédit hypothécaire, prêts et comptes, à l'exception des comptes de paiement au sens de la DSP2[33], y compris les données sur les conditions, les soldes et les transactions. Conformément au considérant 13 de la proposition, ces données clients devraient également comprendre des informations relatives aux besoins et aux préférences en matière de durabilité.

b. les données relatives à l'épargne et aux investissements dans des instruments financiers, des produits d'investissement fondés sur l'assurance, des crypto-actifs, des biens immobiliers et d'autres actifs financiers liés, ainsi qu'aux avantages économiques tirés de ces actifs, y compris les données collectées aux fins de la réalisation d'une évaluation de l'adéquation et du caractère approprié conformément à l'article 25 de la directive 2014/65/UE[34] (directive concernant les marchés d'instruments financiers — MiFID II). Conformément au considérant 13 de la proposition, ces données clients devraient également comprendre des informations relatives aux besoins et aux préférences en matière de durabilité.

c. les données relatives aux droits à pension dans le cadre de régimes de retraite professionnelle, conformément à la directive 2009/138/CE[35] («Solvabilité II») et à la directive (UE) 2016/2341[36] (directive concernant les fonds de pension — IRP II»), ou dans le cadre de la fourniture de produits paneuropéens d'épargne-retraite individuelle (PEPP), conformément au règlement (UE) 2019/1238[37]. Selon le considérant 15 de la proposition, cela inclurait des «*données relatives aux droits à pension [qui] concernent notamment les droits à la retraite accumulés, les niveaux de prestation de retraite projetés, ainsi que les risques et les garanties des membres et des bénéficiaires de régimes de retraite professionnelle*».

d. la fourniture de données relatives aux produits d'assurance non-vie (par exemple, l'assurance couvrant les habitations, les véhicules et d'autres biens) conformément à la directive Solvabilité II, à l'exception des produits d'assurance maladie et santé[38]. Le considérant 14 de la proposition précise que ces données doivent comprendre à la fois des informations sur les produits d'assurance — telles que des renseignements détaillés sur une couverture d'assurance — et des données spécifiques aux actifs assurés des consommateurs. Seraient incluses les données collectées aux fins d'une évaluation des exigences et des besoins, ainsi que les données collectées aux fins

[33] En revanche, le considérant 12 de la proposition prévoit que « Les comptes de crédit couverts par une ligne de crédit qui ne peuvent pas être utilisés aux fins de l'exécution d'opérations de paiement à des tiers devraient entrer dans le champ d'application du présent règlement».

[34] Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE (refonte), texte présentant de l'intérêt pour l'EEE, JO L 173 du 12.6.2014, p. 349–496. Plus particulièrement, l'article 25, paragraphes 2 et 3, de la directive MiFID II impose aux entreprises d'investissement de se procurer «les informations nécessaires concernant les connaissances et l'expérience du client ou du client potentiel en matière d'investissement en rapport avec le type spécifique de produit ou de service, sa situation financière, y compris sa capacité à subir des pertes, et ses objectifs d'investissement, y compris sa tolérance au risque».

[35] Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (solvabilité II) (refonte) (Texte présentant de l'intérêt pour l'EEE), JO L 335 du 17.12.2009, p. 1–155.

[36] Directive (UE) 2016/2341 du Parlement européen et du Conseil du 14 décembre 2016 concernant les activités et la surveillance des institutions de retraite professionnelle (IRP) (refonte) (Texte présentant de l'intérêt pour l'EEE) JO L 354 du 23.12.2016, p. 37–85.

[37] Règlement (UE) 2019/1238 du Parlement européen et du Conseil du 20 juin 2019 relatif à un produit paneuropéen d'épargne-retraite individuelle (PEPP) (Texte présentant de l'intérêt pour l'EEE) PE/24/2019/REV/1 JO L 198 du 25.7.2019, p. 1–63.

[38] Voir également SWD(2023) 224 final, p. 104 (qui souligne qu'«une attention particulière doit être accordée aux services qui font intrinsèquement l'objet d'une mutualisation des risques d'assurance, et à la manière dont la personnalisation des produits peut affecter ce modèle. Compte tenu de la nature des données à caractère personnel sensibles, les risques globaux liés aux données relatives à la santé, par exemple, seraient plus importants.»)

d'une évaluation de l'adéquation et du caractère approprié conformément (respectivement) aux articles 20 et 30 de la directive (UE) 2016/97[39] (DDA).

e. les données relevant d'une évaluation de la solvabilité d'une entreprise qui sont collectées dans le cadre d'une procédure de demande de prêt ou d'une demande de notation de crédit. Selon le considérant 16 de la proposition, cela peut inclure «*des états financiers et des projections financières, des informations sur les passifs financiers et les arriérés de paiement, des justificatifs de la propriété de la sûreté, des justificatifs de l'assurance de la sûreté et des informations sur les garanties*».

12. Les données financières à caractère personnel traitées par les prestataires de services de paiement, les entreprises d'assurance, les fournisseurs de produits d'épargne-retraite et d'autres établissements financiers sont intrinsèquement sensibles[40]. Par conséquent, le CEPD se félicite que certaines catégories de données aient été exclues du champ d'application de la proposition en vertu de l'article 2, paragraphe 1, points a), e) et f), en particulier les données clients concernant: les comptes de paiement[41]; la fourniture de produits d'assurance vie, maladie et santé; et les données qui font partie de l'évaluation de la solvabilité des personnes physiques.

13. Nonobstant l'exclusion de certaines catégories de données, les données clients relevant du champ d'application de l'article 2, paragraphe 1, peuvent toujours être de nature très sensible. Selon l'analyse d'impact de la Commission, certaines données clients peuvent même inclure des catégories particulières de données à caractère personnel relatives au client, telles que les données relatives à la santé[42]. À titre d'exemple, selon la directive IRP II, les droits à pension peuvent inclure des prestations de retraite [43]«*sous la forme de versements en cas de décès, d'invalidité ou de cessation d'activité, ou sous la forme d'aides ou de services en cas de maladie, d'indigence ou de décès*». Dans le même ordre d'idées, les contrats concernant les produits paneuropéens d'épargne-retraite individuelle peuvent couvrir des «risques biométriques», c'est-à-dire des risques liés au décès, à l'invalidité et/ou à la longévité, et peuvent donc impliquer la collecte de catégories particulières de données sur les clients[44]. Un autre exemple concerne les crédits hypothécaires. À cet égard, l'analyse

[39] Directive (UE) 2016/97 du Parlement européen et du Conseil du 20 janvier 2016 sur la distribution d'assurances (refonte) (Texte présentant de l'intérêt pour l'EEE), JO L 26 du 2.2.2016, p. 19–59.

[40] Voir Groupe de travail «Article 29» sur la protection des données, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP 248 rev.01, telles que modifiées et adoptées en dernier lieu le 4 octobre 2017, p. 11: «Ces données à caractère personnel sont considérées comme sensibles (au sens commun du terme) [...] dans la mesure où leur violation aurait clairement des incidences graves dans la vie quotidienne de la personne concernée (données financières susceptibles d'être utilisées pour des paiements frauduleux, par exemple).»

[41] Comité européen de la protection des données (EDPB), Lignes directrices 6/2020 relatives à l'interaction entre la deuxième directive sur les services de paiement et le RGPD, Version 2.0, adoptées le 15 décembre 2020, point 52: «les opérations financières peuvent révéler des informations sensibles au sujet d'une personne concernée, notamment celles liées à des catégories particulières de données à caractère personnel. Par exemple, selon les détails de l'opération, les opinions politiques et les croyances religieuses peuvent être révélées par des dons faits à des partis politiques ou à des organisations, à des églises ou à des paroisses. [...] Des données à caractère personnel concernant la santé peuvent être obtenues en analysant les factures médicales payées par une personne concernée à un professionnel de la santé (par exemple, un psychiatre).»

[42] SWD(2023) 224 final, p. 107 [qui indique que «les données relatives aux pensions peuvent contenir des données à caractère personnel sensibles des consommateurs» et que les établissements financiers peuvent avoir besoin de se fonder sur le consentement explicite de la personne concernée, conformément à l'article 9, paragraphe 2, point a), du RGPD, pour traiter ces données à caractère personnel].

[43] Article 6, paragraphe 4, de la directive IRP II.

[44] Article 2, paragraphe 29, et article 49 du règlement (UE) 2019/1238 du Parlement européen et du Conseil du 20 juin 2019 relatif à un produit paneuropéen d'épargne-retraite individuelle (PEPP) (Texte présentant de l'intérêt pour l'EEE), PE/24/2019/REV/1, JO L 198 du 25.7.2019, p. 1–63.

d'impact de la Commission note que les crédits hypothécaires standard d'un consommateur peuvent contenir des données à caractère personnel sensibles[45]. Par conséquent, la combinaison du crédit hypothécaire avec d'autres services financiers (tels que les produits d'assurance et les comptes de paiement) pourrait conduire à une discrimination injuste[46].

14. Le CEPD note que permettre aux établissements financiers d'accéder à des données à caractère personnel hautement sensibles par le biais des dispositions de la proposition relatives au partage, à la consultation et à l'utilisation des données constitue non seulement une ingérence dans les droits fondamentaux de ces personnes au respect de la vie privée et à la protection des données à caractère personnel, mais pourrait également entraîner des risques importants pour les droits et libertés des personnes, tels que des risques d'exclusion financière du fait d'une discrimination par les prix ou du refus de fournir des produits financiers. Ce résultat irait à l'encontre de l'un des objectifs déclarés de la proposition au considérant 18, à savoir veiller à ce que les catégories de données à caractère personnel relevant du champ d'application de la proposition «*permettent le développement de produits innovants au bénéfice des consommateurs, tout en étant les moins intrusives pour les personnes concernées en ce qui concerne la limitation des droits fondamentaux, notamment le droit au respect de la vie privée et la protection des données à caractère personnel*»[47].

15. Le CEPD invite les colégislateurs à clarifier et à délimiter clairement les catégories de données à caractère personnel énumérées à l'article 2, paragraphe 1. À cet égard, le CEPD attire l'attention sur le fait que la définition actuelle des «données clients» est particulièrement large. L'article 3, paragraphe 3, de la proposition définit les «données clients» comme «*les données à caractère personnel et non personnel qui sont collectées, conservées et traitées d'une autre manière par un établissement financier dans le cadre de ses relations commerciales normales avec ses clients et qui recouvrent à la fois les données fournies par les clients et les données générées à la suite d'une interaction entre un client et l'établissement financier*». Conformément au principe de minimisation des données[48], les catégories de données à caractère personnel à mettre à disposition au titre de la proposition devraient être clairement circonscrites, compte tenu de la nature des services et produits financiers proposés par les entités éligibles énumérées à l'article 2, paragraphe 2, de la proposition et des risques pour les personnes dont les données à caractère personnel seraient consultées et utilisées.

16. Tel qu'il est actuellement rédigé, l'article 3, paragraphe 3, de la proposition pourrait être interprété comme incluant les données collectées par les détenteurs de données à la fois au stade de la prévente, de l'intégration et de l'exécution contractuelle de leur relation avec les clients, y compris les données collectées du fait d'obligations légales[49]. Toutefois, certaines

[45] SWD(2023) 224, p. 101.
[46] SWD(2023) 224, p. 101.
[47] SWD(2023) 224 final, p. 98.
[48] Article 5, paragraphe 1, point c), du RGPD.
[49] Telles que la vigilance renforcées à l'égard de la clientèle au titre de l'article 18 *bis* de la directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE (Texte présentant de l'intérêt pour l'EEE), PE/72/2017/REV/1, JO L 156 du 19.6.2018, p. 43–74.

parties de l'analyse d'impact de la proposition suggèrent[50] que les données que le détenteur des données *déduit* ou *dérive*[51] des données fournies par un client à la suite d'un profilage[52] ne sont pas censées entrer dans le champ d'application de la proposition. Par conséquent, le CEPD demande également l'exclusion explicite des données créées à la suite du profilage de la définition des «données clients», afin de réduire au minimum les risques pour les droits et libertés des personnes[53].

3.2. Le rôle des «permissions»

17. Selon la proposition, les entités éligibles agissant en tant qu'utilisateurs de données ne peuvent obtenir un accès légal aux données clients détenues par d'autres entités éligibles agissant en tant que détenteurs de données qu'après «permission» du client. Le CEPD note que le terme «permission» n'est pas défini à l'article 3 de la proposition, ce qui pourrait engendrer une insécurité juridique tant pour les détenteurs de données que pour les utilisateurs et les clients. En outre, l'utilisation du terme «permission» à l'article 6, paragraphe 3, et aux considérants 10 et 22 de la proposition pourrait être interprétée comme faisant référence au consentement tel que défini à l'article 4, paragraphe 11, du RGPD ou comme une base juridique contractuelle au titre de l'article 6, paragraphe 1, point b), du RGPD[54].

18. À cet égard, le CEPD note avec satisfaction que la proposition souligne la nécessité pour les utilisateurs de données de garantir une base juridique au titre du RGPD pour le traitement des données à caractère personnel[55], et que «[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 RGPD[56]. Toutefois, le CEPD est d'avis qu'une ambiguïté subsiste dans la proposition entre le terme «permission» et la base juridique du traitement au titre du RGPD, à savoir le «consentement», le «consentement explicite» ou la «nécessité d'exécuter un contrat». Le CEPD recommande donc de préciser en outre, au considérant 48, que «la permission ne doit pas être interprétée comme un "consentement", un "consentement explicite" ou une "nécessité d'exécuter un contrat" au sens du règlement (UE) 2016/679».

[50] Dans son analyse d'impact, la Commission indique que les évaluations des risques liées aux retraites et d'autres données enrichies en ce qui concerne les retraites personnelles liées aux consommateurs devraient rester hors du champ d'application de la proposition, étant donné que ces données peuvent comporter des risques d'exclusion financière [SWD (2023) 224 final, p. 108].
[51] Concernant la définition des «données déduites et dérivées», voir Groupe de travail «Article 29» sur la protection des données, Lignes directrices relatives au droit à la portabilité des données, WP 242 rev.01, version révisée et adoptée le 5 avril 2017, p. 10 et 11.
[52] Article 4, paragraphe 4, du RGPD et Groupe de travail «Article 29» sur la protection des données, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, WP 251 rev.01, version révisée et adoptée le 6 février 2018, page 7.
[53] Groupe de travail «Article 29» sur la protection des données, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, WP 251 rev.01, version révisée et adoptée le 6 février 2018, page 8.
[54] Eu égard à l'article 6, paragraphe 1, point b), du RGPD, nous rappelons les lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées, version 2.0, adoptées le 8 octobre 2019, paragraphes 23 et 30. Sur les conditions et les limites d'un éventuel recours à l'article 6, paragraphe 1, point b), du RGPD, voir également l'arrêt de la Cour de justice du 4 juillet 2023, Meta Platforms et autres (Conditions générales d'utilisation d'un réseau social) (C-252/21) ECLI:EU:C:2023:537, points 98 à 100.
[55] Considérant 10 de la proposition.
[56] Considérant 48 de la proposition.

3.3. Obligations des détenteurs de données et des utilisateurs de données

19. Les articles 5 et 6 de la proposition énoncent les obligations qui s'appliqueraient aux entités éligibles agissant en tant que détenteurs de données ou utilisateurs de données en ce qui concerne les données clients qu'elles sont tenues de partager ou auxquelles elles ont le droit d'accéder en vertu de la proposition. Le CEPD se félicite que plusieurs de ces obligations puissent avoir un effet positif sur le niveau de protection des données à caractère personnel que les détenteurs et les utilisateurs de données traiteraient dans le cadre de la proposition. Par exemple, l'obligation faite aux détenteurs de données, en vertu de l'article 5, paragraphe 3, point d), de la proposition, de fournir au client un tableau de bord des permissions pour le suivi et la gestion de ses permissions pourrait accroître la transparence et le contrôle pour les personnes physiques[57]. Un autre exemple est l'obligation pour les utilisateurs de données, en vertu de l'article 6, paragraphe 4, point f), de la proposition, de ne pas partager les données clients avec d'autres entités du groupe d'entreprises dont ils pourraient faire partie.

20. Néanmoins, le CEPD estime que d'autres garanties et limitations devraient être incluses en ce qui concerne le traitement des données des clients par les utilisateurs de données au titre de l'article 6, afin de protéger les personnes contre les risques qui pèsent sur leurs droits fondamentaux en matière de respect de la vie privée et de protection des données découlant du partage accru de données financières sensibles dans le cadre de la proposition.

21. Le CEPD se félicite de l'objectif annoncé de la proposition, qui est de prévenir les risques d'exclusion financière des clients en ce qui concerne à la fois l'éligibilité et la tarification des produits et services financiers[58]. Il attire également l'attention sur les incidences prévisibles sur les droits fondamentaux au respect de la vie privée et à la protection des données qu'auront le partage des «données clients» et l'accès à celles-ci, tels qu'ils sont actuellement prévus par la proposition.

22. Afin de garantir la réalisation de cet objectif, le CEPD recommande d'insérer dans le dispositif de la proposition une disposition qui interdirait le refus des services financiers énumérés à l'article 2, paragraphe 2, de la proposition aux clients qui n'installent pas et n'utilisent pas le tableau de bord des permissions prévu à l'article 8 de la proposition ou ne permettent pas d'une autre manière le partage de données par les détenteurs de données avec les utilisateurs de données au titre de la proposition[59].

23. En outre, le CEPD recommande d'inclure l'obligation pour les utilisateurs de données d'indiquer clairement, dans leurs demandes d'accès aux clients, les types spécifiques de données clients auxquels ils souhaitent avoir accès. Cela garantirait que les clients puissent autoriser de manière sélective l'accès à certains types de données clients relevant de l'article 2, paragraphe 1, mais pas à tous. Par exemple, un client peut souhaiter partager des informations sur son compte d'épargne avec un utilisateur de données particulier, mais pas

[57] Voir également l'article 8 de la proposition.
[58] Considérant 18 de la proposition.
[59] Groupe d'experts sur l'espace européen des données financières, Report on Open Finance («Rapport sur la finance ouverte»), 24 octobre 2022, p. 22: «du point de vue de l'inclusion financière, il est important que les données que les consommateurs sont tenus de fournir pour accéder à des services jugés essentiels à la vie quotidienne (par exemple, les comptes de paiement, les comptes d'épargne, certains produits d'assurance et de retraite) fassent partie d'ensembles de données que tous les consommateurs sont pleinement en mesure de fournir.»

des données relatives aux pensions ou aux investissements[60]. Cette exigence, qui s'ajoute aux exigences de transparence prévues par le RGPD, contribuerait à éviter le risque de demandes d'accès aux données à caractère personnel formulées en termes généraux et génériques, indépendamment des entités éligibles qui les détiennent ou du caractère sensible d'ensembles de données spécifiques.

24. Le CEPD recommande également de modifier le libellé de l'article 6, paragraphe 2, de la proposition comme suit [modifications soulignées]: «*Un utilisateur de données ne peut demander des données clients et y accéder en vertu de l'article 5, paragraphe 1 que lorsqu'elles sont adéquates, pertinentes et nécessaires aux fins et aux conditions pour lesquelles le client lui a donné sa permission. Il efface ces données client lorsqu'il n'en a plus besoin aux fins pour lesquelles le client lui a donné sa permission.*»

25. En outre, le CEPD se félicite de l'exclusion du traitement des données clients à des fins publicitaires à l'article 6, paragraphe 4, point e), de la proposition. Néanmoins, l'exception prévue pour la « *prospection conformément au droit de l'Union et au droit national*» créerait une insécurité juridique, notamment en ce qui concerne les types d'activités de prospection qui seraient autorisés. Afin d'accroître la sécurité juridique et de réduire les risques de publicité ciblée qui n'est pas attendue par la personne concernée, le CEPD recommande de remplacer la référence au droit de l'Union et au droit national en précisant qu'un utilisateur de données ne peut contacter des clients à des fins de prospection que sous réserve de leur consentement préalable ou en leur proposant des offres de produits ou de services similaires à ceux pour lesquels il a accédé à des données clients et dans les conditions prévues à l'article 13, paragraphe 2, de la directive vie privée et communications électroniques.

3.4. Périmètre d'utilisation des données

26. L'article 7 de la proposition fait référence à un «périmètre d'utilisation des données» pour les données clients et rappelle explicitement que le traitement des données à caractère personnel visé à l'article 2, paragraphe 1 doit être limité à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées[61].

27. L'accès aux services, notamment aux services nécessaires à la vie quotidienne, tels que le crédit aux consommateurs ou les services d'assurance ou de retraite, ne devrait pas être subordonné à un traitement excessif des données. C'est particulièrement important dans le secteur financier, où les asymétries d'information et de pouvoir pourraient également affaiblir la liberté des personnes concernées de refuser d'accorder aux établissements financiers un accès disproportionné à leurs données à caractère personnel. En outre, les risques d'exclusion financière augmentent lorsque le recours à un profilage approfondi pour des produits ou services financiers devient la «solution par défaut», ou lorsque la solution non fondée sur un tel profilage cesse d'être abordable pour le consommateur.

[60] La fiche analytique du CGAP «Combining Open Finance and Data Protection for Low-Income Consumers» («Combiner finance ouverte et protection des données pour les consommateurs à faibles revenus»), février 2023, fournit un autre exemple à la page 22: «Si une technologie financière offre un service d'initiation de paiement, il n'est alors probablement pas nécessaire de collecter dix ans d'historique de remboursement de prêts auprès de la banque actuelle du consommateur.»
[61] Article 5, paragraphe 1, point c), du RGPD.

28. Le CEPD note que l'article 7, paragraphes 2 et 3, de la proposition, tel que motivé par le considérant 19[62], prévoit que l'ABE et l'AEAPP, en étroite coopération avec l'EDPB, élaboreront des orientations sur le traitement des données clients conformément à l'article 7, paragraphe 1, dans le contexte des produits et services liés à la note de crédit du consommateur et à l'évaluation du risque associé à un consommateur et à la fixation d'un prix pour celui-ci dans le cadre de produits d'assurance vie, santé et maladie[63].

29. Le CEPD souligne l'importance de garantir le respect des principes d'équité, de proportionnalité et de minimisation des données[64]. À cet égard, le CEPD comprend qu'il peut être impossible d'indiquer de manière exhaustive, dans la proposition, les catégories de données à caractère personnel qui pourraient raisonnablement être utilisées pour chaque produit ou service financier possible. Toutefois, il convient de rappeler l'existence d'une législation et de lignes directrices sectorielles applicables aux entités éligibles énumérées à l'article 2, paragraphe 2, en particulier la législation qui s'applique aux crédits aux consommateurs et aux prêts hypothécaires[65]. Le CEPD recommande de modifier l'article 7 de la proposition afin de faire explicitement référence au respect, par les utilisateurs de données, des règles et lignes directrices existantes de l'UE concernant l'accès aux données à caractère personnel et leur utilisation aux fins de la fourniture des services et produits financiers entrant dans le champ d'application de la proposition. Cela inclurait, par exemple, les règles applicables à la réalisation d'évaluations de la solvabilité des consommateurs, telles qu'énoncées dans le texte convenu de la directive relative aux crédits aux consommateurs[66] et de la directive relative au crédit hypothécaire[67], ou l'obligation pour les entreprises d'investissement d'agir au mieux des intérêts du client lorsqu'elles procèdent à des évaluations de l'adéquation[68].

30. Le CEPD se félicite que la proposition prévoie l'élaboration d'orientations par l'ABE et l'AEAPP, en coopération avec l'EDPB, sur la mise en œuvre du principe clé de la

---

[62] Le considérant 19 précise que ces orientations «[fournissent] un cadre proportionné régissant la manière dont il convient d'utiliser les données à caractère personnel d'un consommateur relevant du champ d'application du présent règlement» et qu'elles «devraient être élaborées d'une manière qui soit adaptée aux besoins du consommateur et proportionnée à la fourniture de ces produits et services». À cet égard, l'analyse d'impact note que «les orientations ont été efficaces pour préciser les exigences en matière de données à utiliser dans les produits et services financiers, tandis que leur nature non contraignante fournirait au marché un cadre souple permettant d'utiliser et de combiner des ensembles de données d'une manière innovante et d'offrir ces services aux clients. Une approche fondée sur des orientations suivrait également les pratiques réglementaires existantes» (SWD(2023) 224 final, p. 49).
[63] Comme indiqué au considérant 20 et à l'article 7, paragraphe 4, de la proposition.
[64] Article 5, paragraphe 1, points a) et c), du RGPD. Voir également CEPD, Avis 11/2021 sur la proposition de directive relative aux crédits aux consommateurs, publié le 26 août 2021, point 15: «les données pour l'évaluation de la solvabilité devraient avoir un lien clair avec la capacité de l'emprunteur à rembourser le prêt et ne pas avoir une incidence disproportionnée ou inattendue sur les droits fondamentaux à la vie privée et à la protection des données à caractère personnel de la personne concernée.» (soulignement ajouté).
[65] Rapport final de l'ABE: Orientations sur l'octroi et le suivi des prêts (EBA/GL/2020/06), du 29 mai 2020.
[66] Proposition de directive du Parlement européen et du Conseil relative aux crédits aux consommateurs [COM(2021)0347 – C9-0244/2021 – 2021/0171(COD)], accord provisoire résultant de négociations interinstitutionnelles.
[67] Directive 2014/17/UE du Parlement européen et du Conseil du 4 février 2014 sur les contrats de crédit aux consommateurs relatifs aux biens immobiliers à usage résidentiel et modifiant les directives 2008/48/CE et 2013/36/UE et le règlement (UE) nº 1093/2010 (la «directive relative au crédit hypothécaire») (Texte présentant de l'intérêt pour l'EEE), JO L 60 du 28.2.2014, p. 34, articles 18 («Obligation d'évaluer la solvabilité du consommateur») et 20 («Divulgation et vérification des informations concernant le consommateur»). Les sections 5.1, 5.2 et l'annexe 2 du rapport final de l'ABE Orientations sur l'octroi et le suivi des prêts (EBA/GL/2020/06), du 29 mai 2020, exposent en détail les types d'informations que les établissements de crédit devraient collecter auprès des consommateurs dans le cadre de ces évaluations de la solvabilité.
[68] Article 24 de la directive MiFID II et article 24 du Règlement délégué (UE) 2017/565 de la Commission du 25 avril 2016 complétant la directive 2014/65/UE du Parlement européen et du Conseil en ce qui concerne les exigences organisationnelles et les conditions d'exercice applicables aux entreprises d'investissement et la définition de certains termes aux fins de ladite directive (Texte présentant de l'intérêt pour l'EEE), C/2016/2398, JO L 87 du 31.3.2017, p. 1–83.

minimisation des données pour des produits et services financiers spécifiques. Le CEPD note que les orientations, malgré leur caractère non contraignant, gagneraient probablement une valeur d'autorité s'agissant de définir le «périmètre» des données jugées nécessaires pour fournir des produits et services financiers spécifiques. Compte tenu de ce qui précède, afin de veiller à ce que ces orientations au titre de l'article 7, paragraphes 2 et 3, de la proposition soient pleinement alignées sur la législation en matière de protection des données, le CEPD recommande vivement de prévoir une consultation formelle de l'EDPB par l'ABE et par l'AEAPP lors de l'élaboration des orientations. Plus précisément, le CEPD recommande d'ajouter à l'article 7, paragraphe 4, après «*coopèrent étroitement*», le libellé «*et sous réserve d'une consultation formelle de*». En outre, il devrait être précisé dans la proposition que la consultation formelle de l'EDPB, l'émission de l'avis de l'EDPB et l'adoption des orientations devraient avoir lieu le plus tôt possible, compte tenu de la date d'applicabilité de la proposition, afin de permettre aux utilisateurs de données de mettre en œuvre les orientations en temps utile.

31. Le CEPD se félicite de la référence spécifique faite par l'article 7, paragraphes 2 et 3, de la proposition à certains produits et services susceptibles de présenter des risques de collecte excessive de données et/ou d'exclusion financière, tels que les produits et services liés à la note de crédit du consommateur et les produits et services liés à l'évaluation du risque associé à un consommateur et à la fixation d'un prix pour celui-ci dans le cadre de produits d'assurance vie, santé et maladie. Le CEPD recommande d'étendre le champ d'application de l'article 7, paragraphes 2 et 3, de la proposition à d'autres produits et services financiers importants qui relèveraient du champ d'application de la proposition, tels que les contrats de crédit hypothécaire[69], la prestation de services de paiement, les produits d'investissement, les produits d'assurance autres que ceux énumérés à l'article 7, paragraphe 3, et les produits d'épargne-retraite.

32. Enfin, le CEPD estime que les orientations visées à l'article 7, paragraphes 2 et 3, de la proposition ne devraient pas être strictement limitées à l'utilisation des données visées à l'article 2, paragraphe 1, de la proposition. Comme le reconnaît le considérant 18 de la proposition, les utilisateurs de données peuvent en pratique choisir de combiner des sources traditionnelles avec des sources «nouvelles» de données, ce qui peut conduire à une analyse plus fine ou plus complète de certaines catégories vulnérables de consommateurs, telles que les personnes à faible revenu, ou peut accroître le risque de conditions déloyales ou de pratiques de tarification différenciée telles que la facturation de primes différenciées.

33. À cet égard, le CEPD souligne que ces combinaisons de données à caractère personnel sont déjà soumises aux exigences du RGPD, notamment en ce qui concerne les principes de légalité, d'équité, de limitation de la finalité, de minimisation des données et d'adéquation[70]. Il note également que certaines combinaisons de données peuvent déjà être expressément interdites en vertu du droit de l'UE ou du droit national applicables, ce qui est le cas du traitement de catégories particulières de données et de données à caractère personnel

[69] Le rapport SWD(2023) 224 final précise en outre, à la page 101, que «des garanties claires, telles que des périmètres d'utilisation des données à caractère personnel qui précisent quand des données liées à des prêts hypothécaires devraient être utilisées pour les différents types de cas d'utilisation, permettraient de délimiter l'utilisation appropriée des données».
[70] Article 5, paragraphe 1, points a), b), c) et d), du RGPD.

obtenues sur les réseaux sociaux dans le cadre des évaluations de la solvabilité des consommateurs[71].

34. Le CEPD estime que le législateur devrait prévoir que les orientations soient élaborées par l'ABE et l'AEAPP, en consultation avec l'EDPB, afin de préciser, s'il y a lieu, les limites de la combinaison des «données clients» obtenues en vertu de la proposition avec d'autres types de données à caractère personnel. Ces orientations peuvent être particulièrement pertinentes pour les combinaisons de données qui peuvent être illégales et/ou présenter des risques accrus pour les personnes, telles que les données à caractère personnel obtenues à partir de sources tierces (par exemple, les réseaux de médias sociaux ou les courtiers en données), les données obtenues par le biais de cookies et d'autres technologies de suivi[72], ainsi que les données à caractère personnel obtenues par les utilisateurs de données en vertu de la loi sur les données[73], étant donné qu'elles sont susceptibles de contenir des données à caractère personnel très sensibles concernant les clients[74].

3.5. Tableaux de bord des permissions d'accès aux données financières

35. Aux termes de l'article 8 de la proposition, les détenteurs de données seraient tenus de fournir au client un tableau de bord des permissions d'accès aux données financières pour surveiller et gérer les permissions qu'ils ont accordées aux utilisateurs de données. 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*»[75]. L'article 8, paragraphe 3, de la proposition dispose que «*le tableau de bord des permissions [devrait être] facile à trouver dans son interface utilisateur et [...] les informations qui y sont affichées [devraient être] claires, exactes et facilement compréhensibles par le client*».

36. Le CEPD prend note avec satisfaction des exigences énoncées à l'article 8, paragraphe 2, de la proposition visant à ce que les détenteurs de données fournissent aux clients un tableau

[71] Voir le texte final approuvé de la directive relative aux crédits aux consommateurs, article 19, paragraphe 3 *bis*, qui dispose que «les créanciers et les intermédiaires de crédit ne traitent pas les catégories particulières de données visées à l'article 9, paragraphe 1, du règlement (UE) 2016/679 ni les données à caractère personnel traitées à partir de réseaux sociaux qui peuvent être contenues dans les bases de données visées au paragraphe 1».

[72] Voir également CEPD, avis 11/2021 sur la proposition de directive relative aux crédits aux consommateurs, publié le 26 août 2021, point 17.

[73] Comme l'indique l'analyse d'impact: «La proposition de loi sur les données introduit une obligation pour les détenteurs de données de mettre à la disposition de l'utilisateur, ou de tiers à la demande de l'utilisateur, les données de l'internet des objets générées par l'utilisation de produits ou de services connexes (articles 3, 4 et 5 de la proposition de loi sur les données). Bien que ces données soient généralement en dehors du champ d'application du cadre de la finance ouverte, les établissements financiers peuvent être des bénéficiaires potentiels de ce droit d'accès, notamment les établissements financiers qui sont actives dans les services d'après-vente axés sur les données liées aux produits de l'internet des objets.» (SWD(2023)224 final, p. 110).

[74] Voir également l'avis conjoint 2/2022 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), adopté le 4 mai 2022, au point 13 et aux points 54 et 55 («En conséquence, l'EDPB et le CEPD conseillent d'inclure dans la proposition des limitations ou des restrictions claires concernant l'utilisation des données à caractère personnel générées par l'utilisation d'un produit ou d'un service par toute autre entité que la personne concernée (qu'il s'agisse de l'"utilisateur", du "détenteur de données" ou d'un "tiers"), notamment lorsque, à partir des données en question, il serait possible de tirer des conclusions précises concernant leur vie privée ou lorsque leur utilisation impliquerait autrement d'importants risques pour les droits et libertés des personnes concernées. Plus particulièrement, l'EDPB et le CEPD préconisent d'introduire des limitations claires concernant l'utilisation des données à caractère personnel générées par l'utilisation d'un produit ou de services connexes à des fins de marketing direct ou de publicité, de suivi des employés, d'évaluation du risque de crédit ou encore pour déterminer l'admissibilité à l'assurance maladie, ou pour calculer ou modifier les primes d'assurance.») (soulignement ajouté).

[75] Considérant 21 de la proposition.

de bord des permissions avec une vue d'ensemble des différentes permissions en cours de validité données à des utilisateurs de données, y compris: les noms des utilisateurs de données auxquels l'accès a été accordé; le compte client, le produit financier ou le service financier 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[76]. Afin de garantir que les détenteurs de données soient en mesure de communiquer aux clients tous les éléments d'information visés à l'article 8, paragraphe 2, le CEPD recommande que les utilisateurs de données soient tenus, au titre de l'article 8, paragraphe 4, point b), d'informer également les détenteurs de données du compte client, du produit financier ou du service financier auquel l'accès est demandé.

37. En outre, le CEPD recommande que l'article 8, paragraphe 4, point b), exige des utilisateurs de données qu'ils informent les détenteurs de données de la base juridique en vertu de 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 contenues dans l'ensemble de données du client. Cela permettrait d'éviter que les détenteurs de données n'accordent l'accès aux données à caractère personnel en l'absence d'une base juridique appropriée au titre du RGPD[77]. Comme l'a clarifié par l'EDPB, chaque responsable du traitement a le devoir de s'assurer que les données à caractère personnel ne sont pas traitées ultérieurement d'une manière incompatible avec les finalités pour lesquelles elles ont été initialement collectées. Chaque communication de données par un responsable du traitement requiert une base légale et une évaluation de la compatibilité, que le destinataire soit un responsable distinct ou conjoint du traitement[78].

38. Le CEPD se félicite également de la référence, au considérant 21, au fait que le tableau de bord des permissions «*[devrait] permettre aux clients de gérer leurs permissions de manière éclairée et impartiale*» et qu'il «*ne [devrait] pas être [conçu] de manière à encourager les clients à accorder ou retirer des permissions, ni de manière à les influencer indûment dans un sens ou dans l'autre*». En effet, dans un domaine aussi sensible que celui des finances personnelles, les consommateurs peuvent être particulièrement peu conscients des conséquences qu'entraîne le fait d'accepter de partager de grandes quantités de leurs données personnelles avec des établissements financiers[79]. Le CEPD recommande donc de refléter le considérant 21 dans le dispositif de la proposition, notamment à l'article 8.

39. Le CEPD note également que l'article 8, paragraphe 4, de la proposition établirait une obligation pour les détenteurs et utilisateurs de données de coopérer pour mettre les informations à la disposition du client via le tableau de bord en temps réel. À cet égard, le

[76] Article 8, paragraphe 2, point a), de la proposition.
[77] Considérant 48 de la proposition: «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»
[78] Comité européen de la protection des données, Lignes directrices 07/2020 sur les notions de responsable du traitement et de sous-traitant dans le RGPD, du 7 juillet 2021, p. 45 (point 167 et note de bas de page 76).
[79] The Finance Innovation Lab, «Open Finance and Vulnerability - A Policy Discussion Paper» («Finance ouverte et vulnérabilité: document de discussion sur les politiques»), juillet 2021, p. 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 risque réel que les citoyens ne comprennent pas pleinement les implications de l'accès aux données relatives à la finance ouverte.»

CEPD se félicite de l'échange de ces informations entre les détenteurs et les utilisateurs de données concernant les permissions données, retirées ou modifiées par les clients dans le cadre de la proposition. Néanmoins, le CEPD recommande d'obliger les utilisateurs de données à démontrer de manière appropriée aux détenteurs de données qu'ils ont obtenu la permission du client d'accéder aux données clients détenues par le détenteur de données. S'il est vrai que la proposition obligerait les détenteurs de données à «*[demander] à l'utilisateur de données de démontrer qu'il a obtenu du client la permission d'accéder aux données client de ce dernier que lui-même détient*»[80], la proposition ne prévoit actuellement aucune obligation correspondante pour les utilisateurs de données de faire une telle démonstration avant d'obtenir le droit d'accéder aux données clients.

40. Dans la même veine, le considérant 10 prévoit qu'une demande de partage de données du client «*peut être présentée par un utilisateur de données agissant pour le compte du client*». Même si cette partie du considérant 10 n'est pas reflétée dans le dispositif de la proposition, cette possibilité pourrait ouvrir la voie à des abus si le détenteur de données ne peut pas vérifier les pouvoirs de représentation prétendument conférés à l'utilisateur de données par le client. Par conséquent, le CEPD recommande soit de supprimer la partie pertinente du considérant 10, soit, si le considérant 10 est conservé, de modifier l'article 5 afin de préciser que le détenteur de données doit demander la preuve des pouvoirs de représentation obtenus auprès du client. L'article 6 devrait, quant à lui, prévoir l'obligation pour l'utilisateur de données de fournir la preuve de ses pouvoirs de représentation.

4. Prestataires de services d'information financière

41. La proposition cite les prestataires de services d'information financière comme étant des entités qui peuvent agir soit en tant que détenteurs de données, soit en tant qu'utilisateurs de données[81]. Les prestataires de services d'information financière doivent obtenir un agrément préalable délivré par une autorité compétente avant de pouvoir accéder aux données clients[82]. Si les autorités compétentes l'autorisent en vertu de l'article 14 de la proposition, les prestataires de services d'information financière seraient autorisés à tirer parti des mécanismes d'accès aux données des clients de la proposition «aux fins de la fourniture de services d'information financière»[83]. L'autorité compétente serait en mesure de retirer l'agrément si le prestataire de services d'information financière représentait un risque pour la protection des consommateurs et la sécurité des données[84].

42. Le CEPD recommande l'inclusion, dans l'article 14, paragraphe 7, de la proposition, de la possibilité pour les autorités compétentes de retirer l'agrément dans les cas où les autorités de contrôle en vertu du RGPD établissent qu'un prestataire de services d'information financière a manqué aux obligations qui lui incombent en vertu du droit de l'Union en

[80] Passage selon lequel le détenteur de données «demande à l'utilisateur de données de démontrer qu'il a obtenu du client la permission d'accéder aux données client de ce dernier que lui-même détient». Cette obligation est également conforme aux recommandations formulées par le groupe d'experts sur l'espace européen des données financières dans son rapport «Report on Open Finance» sur la finance ouverte, aux pages 17 et 18: «le détenteur de données devrait être en mesure de vérifier la validité du consentement donné par la personne concernée».
[81] Article 2, paragraphe 2, point o), de la proposition.
[82] Article 12, paragraphe 1, de la proposition.
[83] Article 3, paragraphe 7, de la proposition.
[84] Article 14, paragraphe 7, point d), de la proposition.

matière de protection des données. Cela pourrait être particulièrement important en ce qui concerne l'incapacité potentielle des prestataires de services d'information financière à mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir que les données à caractère personnel des clients sont adéquatement protégées dans le contexte des mécanismes d'accès et de partage des données créés par la proposition[85]. Le retrait d'un agrément pour la raison recommandée par le CEPD pourrait être facilité par l'échange d'informations entre les autorités de contrôle au titre du RGPD et les autorités compétentes dans le cadre de la proposition, que le CEPD recommande de faciliter dans la section 6 du présent avis.

43. Le CEPD note que la proposition ne définit pas plus avant ce qui constitue des «services d'information financière». Pour faire en sorte que le rôle des fournisseurs de services financiers soit clair tant pour les détenteurs de données que pour les clients, le CEPD recommande de fournir une définition des «services d'information financière» dans la proposition[86].

5. Systèmes de partage de données financières

44. L'article 9 de la proposition imposerait aux détenteurs de données et aux utilisateurs de données de s'affilier à un ou plusieurs systèmes de partage de données financières dans un délai de 18 mois à compter de l'entrée en vigueur de la proposition, et de mettre les données clients à la disposition des utilisateurs de données au titre de la proposition uniquement conformément aux règles et modalités du système de partage de données financières.

45. Le CEPD note avec satisfaction que l'article 10, point g), de la proposition exigerait que les systèmes de partage de données financières établissent des normes communes pour les données des clients et les interfaces techniques nécessaires pour permettre aux clients de demander le partage de données conformément à l'article 5, paragraphe 1, de la proposition. Le CEPD recommande d'exiger des systèmes de partage de données financières qu'ils définissent également les mesures techniques et organisationnelles minimales que leurs membres devraient mettre en œuvre pour garantir un niveau de sécurité approprié pour les données à caractère personnel échangées.

46. En outre, le CEPD observe que l'article 11 de la proposition habiliterait la Commission à adopter un acte délégué précisant les «*modalités [...], selon lesquelles un détenteur de données doit mettre à disposition [...] les données client*», en l'absence d'un système de partage des données financières. Ces modalités comprendraient également des «*normes communes pour les données et, le cas échéant, les interfaces techniques à utiliser pour permettre aux clients de demander le partage de données au titre de l'article 5, paragraphe 1*». À cet égard, le CEPD rappelle à la Commission l'obligation qui lui incombe en vertu de l'article 42, paragraphe 1, du RPDUE de le consulter lors de l'élaboration d'actes d'exécution qui auraient une

[85] Article 32, paragraphe 1, du RGPD.
[86] À titre de comparaison, le CEPD fait remarquer que les «services d'information sur les comptes» sont définis à l'article 4, paragraphe 16, de la directive concernant les services de paiement comme «un service en ligne consistant à fournir des informations consolidées concernant un ou plusieurs comptes de paiement détenus par l'utilisateur de services de paiement soit auprès d'un autre prestataire de services de paiement, soit auprès de plus d'un prestataire de services de paiement».

incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel.

47. Le CEPD se félicite du fait que le considérant 25 de la proposition indique que les systèmes de partage de données financières doivent respecter les règles de l'Union dans les domaines de la concurrence, de la protection des consommateurs et de la protection des données et du respect de la vie privée, et qu'ils soient encouragés à élaborer des codes de conduite semblables à ceux établis par les responsables du traitement et les sous-traitants en vertu de l'article 40 du RGPD afin de clarifier les obligations des responsables du traitement et des sous-traitants impliqués dans les systèmes de partage de données financières. Toutefois, par souci de clarté et de cohérence, le CEPD recommande de remplacer le mot «semblables» après «élaborer des codes de conduite» par «*conformes à l'article 40 du RGPD*».

6. Autorités compétentes et coopération

48. La coopération entre les régulateurs financiers et les autorités de contrôle de la protection des données a été explicitement reconnue comme un objectif dans le droit de l'Union. Par exemple, l'ABE est actuellement chargée de coopérer étroitement avec le comité européen de la protection des données «*en vue d'éviter les doubles emplois, les incohérences et l'insécurité juridique dans le domaine de la protection des données*». L'ABE peut également inviter les autorités nationales de surveillance de la protection des données à participer en tant qu'observateurs à son comité de la protection des consommateurs et de l'innovation financière[87]. Étant donné que l'échange de données à caractère personnel dans le secteur financier est susceptible d'augmenter de manière significative dans le cadre de la proposition, le CEPD estime qu'il existe un besoin proportionné de coopération accrue entre les autorités compétentes en matière financière et les autorités chargées de la protection des données, tant au niveau national qu'au niveau de l'UE.

49. Le CEPD note que, conformément à l'article 14, paragraphe 1, de la proposition, lorsqu'elles évaluent si un demandeur d'agrément de prestataire de services d'information financière satisfait aux exigences énoncées à l'article 12, paragraphe 1, et avant d'octroyer ledit agrément, les autorités compétentes peuvent consulter «d'autres autorités publiques concernées». La même possibilité existerait en ce qui concerne les «autres autorités compétentes» en ce que les autorités compétentes seraient appelées à évaluer si les caractéristiques et modalités de gouvernance d'un système de partage de données financières notifié sont conformes aux exigences de l'article 10, paragraphe 1, de la proposition[88]. Compte tenu des implications prévisibles en matière de protection des données des services des prestataires de services d'information financière et des règles et

[87] Article 3, paragraphe 6, point c), du Règlement (UE) 2019/2175 du Parlement européen et du Conseil du 18 décembre 2019 modifiant le règlement (UE) nº 1093/2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), le règlement (UE) nº 1094/2010 instituant une Autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles), le règlement (UE) nº 1095/2010 instituant une Autorité européenne de surveillance (Autorité européenne des marchés financiers), le règlement (UE) nº 600/2014 concernant les marchés d'instruments financiers, le règlement (UE) 2016/1011 concernant les indices utilisés comme indices de référence dans le cadre d'instruments et de contrats financiers ou pour mesurer la performance de fonds d'investissement et le règlement (UE) 2015/847 sur les informations accompagnant les transferts de fonds (Texte présentant de l'intérêt pour l'EEE), PE/75/2019/REV/1, JO L 334 du 27.12.2019, p. 1–145.
[88] Article 10, paragraphe 6, de la proposition.

modalités des systèmes de partage de données financières, le CEPD recommande de préciser expressément que les autorités de contrôle au titre du RGPD font partie des «autres autorités publiques concernées» ou des «autres autorités compétentes» qui peuvent être consultées en vertu de ces dispositions.

50. Le CEPD note en outre que l'article 18, paragraphe 3, et l'article 26, paragraphe 2, de la proposition prévoient l'échange d'informations entre les autorités compétentes de différents États membres dans le cadre de l'exercice de leurs pouvoirs d'enquête et de sanction. L'article 26, paragraphe 5, prévoit que les autorités compétentes doivent également coopérer avec les autorités de contrôle au titre du RGPD lorsque les obligations prévues par la proposition concernent le traitement de données à caractère personnel[89]. Afin d'assurer une base juridique claire pour l'échange d'informations pertinentes, le CEPD recommande de faire explicitement référence aux autorités de contrôle au titre du RGPD à l'article 18, paragraphe 3, de la proposition (qui fait actuellement référence aux «autorités de tout secteur concerné»).

7. Publication des décisions administratives

51. L'article 25, paragraphe 1, de la proposition prévoit qu'en règle générale, l'identité des personnes physiques visées par une décision d'une autorité compétente imposant une sanction administrative ou une mesure administrative n'est pas publiée. Cette règle fait l'objet d'une dérogation en vertu de l'article 25, paragraphe 2, «*si l'autorité nationale compétente juge nécessaire de publier l'identité ou d'autres données à caractère personnel de la personne physique pour protéger la stabilité des marchés financiers ou pour assurer l'application effective du présent règlement*», pour autant que la publication soit limitée à ce qui est strictement nécessaire pour garantir ces objectifs et dûment justifiée[90].

52. Le CEPD estime que la publication de données à caractère personnel dans le contexte de la publication des décisions des autorités compétentes devrait en effet constituer l'exception, à la suite de l'évaluation au cas par cas prévue à l'article 25, paragraphe 2, de la proposition. Le CEPD relève que la publication des données à caractère personnel relatives à des personnes qui ont été sanctionnées pour une violation au titre de la proposition 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.

53. Le CEPD se félicite du fait que l'article 25, paragraphe 4, de la proposition dispose que «*les données à caractère personnel contenues dans cette publication ne sont 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 garantir l'application effective du présent règlement, et en tout état de cause pas plus de cinq ans*», car

[89] Voir également le considérant 36 de la proposition.
[90] En outre, le considérant 43 de la proposition prévoit que «la publication devrait dès lors être anonymisée, à moins que l'autorité compétente ne juge nécessaire de publier des décisions contenant des données à caractère personnel aux fins de l'application effective du présent règlement, y compris dans le cas de déclarations publiques ou d'interdictions temporaires. Dans ce cas, l'autorité compétente motive sa décision».

cette règle est conforme au principe de limitation de la conservation énoncé à l'article 5, paragraphe 1, point e), du RGPD.

8. Conclusions

54. À la lumière des considérations qui précèdent, le CEPD émet les recommandations suivantes:

(1) préciser dans le considérant 48 que le traitement des données à caractère personnel dans le cadre de la proposition de règlement doit être effectué conformément au RGPD, au RPDUE et à la directive vie privée et communications électroniques;

(2) délimiter clairement les catégories de données à caractère personnel visées à l'article 2, paragraphe 1, de la proposition, en tenant compte de la nature des services et produits financiers proposés par les entités éligibles énumérées à l'article 2, paragraphe 2, de la proposition et des risques encourus par les personnes dont les données à caractère personnel seraient consultées et utilisées par les utilisateurs de données;

(3) exclure explicitement les données créées à la suite d'un profilage de la définition des «données clients» figurant à l'article 3, paragraphe 3, de la proposition;

(4) éviter toute ambiguïté entre le terme «permission» au sens de la proposition et la base juridique du traitement en vertu du RGPD, en précisant en outre dans le considérant 48 que la permission ne doit pas être interprétée comme un «consentement», un «consentement explicite» ou une «nécessité d'exécuter un contrat» tels que définis dans le RGPD;

(5) insérer dans le dispositif de la proposition une disposition qui interdirait le refus des services financiers énumérés à l'article 2, paragraphe 2, de la proposition aux clients qui n'installent pas et n'utilisent pas le tableau de bord des permissions en vertu de l'article 8 de la proposition ou ne permettent pas d'une autre manière le partage de données par les détenteurs de données avec les utilisateurs de données en vertu de la proposition;

(6) inclure à l'article 6 de la proposition l'obligation pour les utilisateurs de données d'indiquer clairement dans leurs demandes d'accès aux clients les types particuliers de données clients auxquels ils souhaitent avoir accès;

(7) modifier le libellé de l'article 6, paragraphe 2, de la proposition comme suit: «Un utilisateur de données ne peut demander des données clients et y accéder en vertu de l'article 5, paragraphe 1 que lorsqu'elles sont adéquates, pertinentes et nécessaires aux fins et aux conditions pour lesquelles le client lui a donné sa permission»;

(8) préciser qu'un utilisateur de données ne peut contacter des clients à des fins de prospection que sous réserve de leur consentement préalable ou en leur proposant des offres de produits ou de services similaires à ceux pour lesquels il a accédé à des données clients et dans les conditions prévues à l'article 13, paragraphe 2, de la directive vie privée et communications électroniques;

(9) inclure, à l'article 7 de la proposition, une référence explicite à la nécessité de se conformer aux règles et lignes directrices sectorielles existantes de l'UE concernant l'accès aux données

à caractère personnel et leur utilisation aux fins de la fourniture des services et produits financiers entrant dans le champ d'application de la proposition;

(10) prévoir une consultation formelle de l'EDPB, tant par l'ABE que par l'AEAPP, lors de l'élaboration des orientations proposées relatives au périmètre d'utilisation des données, en ajoutant à l'article 7, paragraphe 4, après «coopèrent étroitement», le libellé «et sous réserve d'une consultation formelle de»;

(11) prévoir l'adoption d'orientations au titre de l'article 7, sous réserve de la consultation formelle de l'EDPB, le plus tôt possible compte tenu de la date d'applicabilité de la proposition;

(12) étendre le champ d'application des orientations visées à l'article 7 à d'autres produits et services financiers importants entrant dans le champ d'application de la proposition;

(13) préciser que les orientations visées à l'article 7 devraient également porter, le cas échéant, sur les limites de la combinaison de «données clients» obtenues en vertu de la proposition avec d'autres types de données à caractère personnel;

(14) exiger des utilisateurs de données au titre de l'article 8, paragraphe 4, point b), qu'ils informent également les détenteurs de données du compte client, du produit financier ou du service financier auquel l'accès est demandé;

(15) exiger des utilisateurs de données en vertu de l'article 8, paragraphe 4, point b), qu'ils informent les détenteurs de données de la base juridique en vertu de l'article 6, paragraphe 1, du RGPD et (le cas échéant) de l'exception en vertu de l'article 9, paragraphe 2, du RGPD sur laquelle ils s'appuieraient pour accéder aux données à caractère personnel contenues dans l'ensemble de données clients;

(16) préciser à l'article 8 de la proposition que le tableau de bord des permissions ne devrait pas être conçu de manière à encourager les clients à accorder ou retirer des permissions, ni de manière à les influencer indûment dans un sens ou dans l'autre;

(17) exiger des utilisateurs de données qu'ils démontrent de manière appropriée aux détenteurs de données qu'ils ont obtenu la permission du client d'accéder aux données clients détenues par le détenteur de données;

(18) si les utilisateurs de données peuvent demander l'accès aux données clients pour le compte d'un client, exiger des détenteurs de données qu'ils demandent la preuve des pouvoirs de représentation obtenus auprès du client (et des utilisateurs de données qu'ils fournissent cette preuve);

(19) modifier l'article 14, paragraphe 7, de la proposition afin de préciser que les autorités compétentes peuvent retirer l'agrément qu'elles ont accordé à un prestataire de services d'information financière dans les cas où les autorités de contrôle au titre du RGPD établissent que le prestataire de services d'information financière a enfreint ses obligations au titre de la législation de l'UE en matière de protection des données;

(20) prévoir une définition des «services d'information financière» à l'article 3 de la proposition;

(21) exiger des systèmes de partage de données financières qu'ils définissent les mesures techniques et organisationnelles minimales que leurs membres devraient mettre en œuvre

pour garantir un niveau de sécurité approprié pour les données à caractère personnel échangées;

(22) *dans le considérant 25 de la proposition, remplacer le mot «semblables» après «élaborer des codes de conduite» par «conformes à l'article 40 du RGPD»;*

(23) *préciser que les autorités de contrôle au titre du RGPD font partie des «autres autorités publiques concernées» ou des «autres autorités compétentes» que les autorités compétentes doivent consulter conformément à l'article 14, paragraphe 1, et à l'article 10, paragraphe 6, de la proposition; et*

(24) *faire explicitement référence aux autorités de contrôle au titre du RGPD à l'article 18, paragraphe 3, de la proposition.*

Bruxelles, le 22 août 2023

Wojciech Rafał WIEWIÓROWSKI

p.o. Leonardo CERVERA NAVAS
Secrétaire-général