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

Historique des versions

Version 2.0	15.12.2020.	Adoption des lignes directrices après consultation publique
Version 1.0	17.7.2020.	Adoption des lignes directrices pour consultation publique

Table des matières

Le comité européen de la protection des données,

vu l'article 70, paragraphe 1, point e), du 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 (ci-après le «RGPD»),

vu l'accord sur l'Espace économique européen, et notamment son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[1],

vu l'article 12 et l'article 22 de son règlement intérieur,

considérant ce qui suit:

(1) Le règlement général sur la protection des données prévoit un ensemble cohérent de règles applicables au traitement des données à caractère personnel dans toute l'Union européenne (UE).

(2) La deuxième directive sur les services de paiement (la directive 2015/2366/CE du Parlement européen et du Conseil du 23 décembre 2015, ci-après la «DSP2») abroge la directive 2007/64/CE et prévoit de nouvelles règles en vue de garantir la sécurité juridique pour les consommateurs, les commerçants et les entreprises dans la chaîne de paiement, ainsi que la modernisation du cadre juridique relatif au marché des services de paiement[2]. Les États membres étaient tenus de transposer la directive dans leur droit national avant le 13 janvier 2018.

(3) Une caractéristique importante de la DSP2 est l'introduction d'un cadre juridique pour les nouveaux services d'initiation de paiement et services d'information sur les comptes. La DSP2 permet à ces nouveaux prestataires de services de paiement d'avoir accès aux comptes de paiements des personnes concernées aux fins de la fourniture desdits services.

(4) En ce qui concerne la protection des données, conformément à l'article 94, paragraphe 1, de la DSP2, tout traitement de données à caractère personnel, y compris la communication d'informations sur le traitement, aux fins de la DSP2, est effectué conformément au RGPD[3] et au règlement (UE) 2018/1725.

(5) Selon le considérant 89 de la DSP2, lorsque des données à caractère personnel font l'objet d'un traitement aux fins de la directive, la finalité du traitement devrait être précisée, la base juridique applicable devrait être nommée, les exigences de sécurité applicables du RGPD mises en œuvre, et les principes de nécessité, de proportionnalité, de limitation de la finalité et de la durée proportionnée de conservation devraient être respectés. De même, la protection des données dès la conception et la protection des données par défaut devraient être intégrées dans tous les systèmes de traitement des données développés et utilisés dans le cadre de la DSP2[4].

(6) Selon le considérant 93 de la DSP2, les services d'initiation de paiement (ci-après, les «PSIP») et les prestataires de services d'information sur les comptes (ci-après, les «PSIC»), d'une part, et le prestataire de services de paiement gestionnaire du compte (ci-après, les PSPGC»), d'autre part,

[1] Dans le présent document, on entend par «États membres» les États membres de l'EEE.
[2] Considérant 6 de la DSP2.
[3] La DSP2 étant antérieure au RGPD, elle fait encore référence à la directive 95/46/CE. L'article 94 du RGPD dispose que les références faites à la directive 95/46/CE abrogée s'entendent comme faites au RGPD.
[4] Considérant 89 de la DSP2.

doivent respecter les nécessaires exigences de protection des données et de sécurité prescrites ou visées dans la directive ou incluses dans les normes techniques de réglementation,

A ADOPTÉ LES LIGNES DIRECTRICES SUIVANTES:

1. INTRODUCTION

1. La DSP2 a introduit plusieurs nouveautés dans le domaine des services de paiement. Si elle crée de nouvelles possibilités pour les consommateurs et améliore la transparence dans ce domaine, l'application de la DSP2 soulève certaines questions et certaines inquiétudes quant à la nécessité que les personnes concernées conservent le contrôle total de leurs données à caractère personnel. Le RGPD s'applique au traitement des données à caractère personnel, y compris les activités de traitement effectuées dans le contexte des services de paiement tels que définis par la DSP2[5]. Les responsables du traitement actifs dans le domaine couvert par la DSP2 doivent donc toujours garantir le respect des exigences du RGPD, y compris les principes de protection des données définis à l'article 5 du RGPD, ainsi que les dispositions pertinentes de la directive «Vie privée et communications électroniques»[6]. Si la DSP2[7] et les normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication (ci-après, les «NTR»[8]) contiennent certaines dispositions relatives à la protection et à la sécurité des données, des incertitudes demeurent quant à l'interprétation de ces dispositions et quant à l'interaction entre le cadre général de protection des données et la DSP2.

2. Le 5 juillet 2018, le Comité européen de la protection des données (ci-après l'«EDPBD») a publié une lettre concernant la DSP2 dans laquelle il donnait des éclaircissements sur des questions concernant la protection des données à caractère personnel en relation avec la DSP2, en particulier sur le traitement des données à caractère personnel des parties non contractantes (les «données des parties silencieuses») par des PSIC et des PSIP, les procédures d'octroi et de retrait du consentement, les NTR et la coopération entre les PSPGC concernant les mesures de sécurité. Considérant que le travail préparatoire des présentes lignes directrices a nécessité la collecte de contributions des parties concernées, par écrit et lors d'un événement leur étant destiné, afin de déterminer les problèmes les plus urgents.

3. Les présentes lignes directrices visent à fournir des orientations complémentaires sur les aspects liés à la protection des données dans le contexte de la DSP2, en particulier sur la relation entre les dispositions pertinentes du RGPD et la DSP2. Les présentes lignes directrices sont essentiellement axées sur le traitement des données à caractères personnel par les PSIC et les PSIP. Le présent document aborde donc les conditions d'octroi de l'accès aux informations sur les comptes de

[5] Article 1er, paragraphe 1, du RGPD.
[6] 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.
[7] Article 94 de la DSP2, etc.
[8] Règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication (Texte présentant de l'intérêt pour l'EEE); C/2017/7782; JO L 69 du 13.3.2018, p. 23; disponible à l'adresse https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018R0389&from=FR

paiement par les PSPGC et de traitement des données à caractère personnel par les PSIP et les PSIC, y compris les exigences et les garanties en relation avec le traitement des données à caractère personnel par les PSIP et les PSIC à des fins autres que celles pour lesquelles les données ont initialement été collectées, en particulier lorsqu'elles ont été collectées dans le contexte de la fourniture de services d'information sur les comptes[9]. Le présent document aborde aussi différentes notions du consentement explicite au titre de la DSP2 et du RGPD, le traitement des «données des parties silencieuses», le traitement des catégories particulières de données à caractère personnel par les PSIP et les PSIC, l'application des principaux principes de protection des données énoncés dans le RGPD, dont la minimisation des données, la transparence, la responsabilité et les mesures de sécurité. La DSP2 fait intervenir des responsabilités transversales dans les domaines, entre autres, de la protection des consommateurs et du droit de la concurrence. Les présentes lignes directrices ne couvrent pas les aspects liés à ces domaines.

4. Pour faciliter la lecture des présentes lignes directrices, les principales définitions utilisées dans ce document sont fournies ci-après.

1.1 Définitions

Aux fins des présentes lignes directrices, on entend par:

«*prestataire de services d'information sur les comptes*» («*PSIC*»), un prestataire de services en ligne qui fournit 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;

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

«*minimisation des données*», principe de protection des données selon lequel les données à caractère personnel sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées;

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

«*bénéficiaire*», une personne physique ou morale qui est le destinataire prévu de fonds ayant fait l'objet d'une opération de paiement;

«*compte de paiement*», un compte détenu au nom d'un ou de plusieurs utilisateurs de services de paiement et utilisé aux fins de l'exécution d'opérations de paiement;

«*prestataire de services d'initiation de paiement*» («*PSIP*»), un prestataire de services qui initie un ordre de paiement à la demande de l'utilisateur de services de paiement concernant un compte de paiement détenu auprès d'un autre prestataire de services de paiement;

[9] Un service d'information sur les comptes est 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.

«*prestataire de services de paiement*», une entité visée à l'article 1er, paragraphe 1, de la DSP2[10] ou une personne physique ou morale bénéficiant d'une dérogation au titre des articles 32 ou 33 de la DSP2;

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

«donnée à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); «personne physique identifiable», une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

«*protection des données dès la conception*», ensemble de mesures techniques et organisationnelles intégrées dans un produit ou un service, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du RGPD et de protéger les droits de la personne concernée;

«*protection des données par défaut*», ensemble de mesures techniques et organisationnelles appropriées mises en œuvre dans un produit ou un service pour garantir que, par défaut, seules les données à caractère personnel nécessaires au regard de chaque finalité spécifique du traitement sont traitées;

«*NTR*», les normes objet du règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication;

«*prestataires tiers*» («*PT*»), les PSIP et les PSIC confondus.

1.2 Services au titre de la DSP2

5. La DSP2 introduit deux nouveaux types de (prestataires de) services: les PSIP et les PSIC. L'annexe 1 de la DSP2 contient les huit services de paiement qui sont couverts par la directive.

[10] L'article 1er, paragraphe 1, de la DSP2 fixe les règles selon lesquelles les États membres distinguent les six catégories suivantes de *prestataires de services de paiement*:
a) les établissements de crédit au sens de l'article 4, paragraphe 1, point 1), du règlement (UE) nº 575/2013 du Parlement européen et du Conseil, y compris leurs succursales au sens du point 17) dudit article 4, paragraphe 1, lorsque ces succursales sont situées dans l'Union, qu'il s'agisse de succursales d'établissements de crédit ayant leur siège dans l'Union ou, conformément à l'article 47 de la directive 2013/36/UE et au droit national, hors de l'Union;
b) les établissements de monnaie électronique au sens de l'article 2, point 1), de la directive 2009/110/CE, y compris, conformément à l'article 8 de ladite directive et au droit national, une succursale d'un tel établissement, lorsque celle-ci est située dans l'Union et son siège hors de l'Union, dans la mesure où les services de paiement fournis par ladite succursale sont liés à l'émission de monnaie électronique;
c) les offices de chèques postaux qui sont habilités en droit national à fournir des services de paiement;
d) les établissements de paiement;
e) la BCE et les banques centrales nationales lorsqu'elles n'agissent pas en qualité d'autorités monétaires ou d'autres autorités publiques;
f) les États membres ou leurs autorités régionales ou locales lorsqu'ils n'agissent pas en qualité d'autorités publiques.

6. Les PSIP fournissent des services consistant à initier un ordre de paiement à la demande de l'utilisateur de services de paiement concernant un compte de paiement détenu auprès d'un autre prestataire de services de paiement[11]. Un PSIP peut demander à un PSPGC (généralement, une banque) d'initier une opération pour le compte de l'utilisateur de services de paiement. L'utilisateur (de services de paiement) peut être une personne physique (personne concernée) ou une personne morale.

7. Les PSIC fournissent des services 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[12]. Conformément au considérant 28 de la DSP2, l'utilisateur de services de paiement est en mesure d'avoir immédiatement une vue d'ensemble de sa situation financière à un moment donné.

8. En ce qui concerne les services d'informations sur les comptes, plusieurs types de services différents peuvent être proposés, qui mettent chacun l'accent sur différentes prestations et finalités. Par exemple, certains prestataires peuvent proposer aux utilisateurs des services tels que la planification de leur budget et le suivi de leurs dépenses. Le traitement des données à caractère personnel dans le contexte de ces services est couvert par la DSP2. Les services qui requièrent des évaluations de la solvabilité de l'utilisateur de services de paiement ou les services d'audit fournis sur la base de la collecte d'informations par l'intermédiaire d'un service d'information sur les comptes ne relèvent pas de la DSP2 et sont par conséquent soumis au RGPD. En outre, les comptes autres que les comptes de paiement (par exemple, les comptes d'épargne ou d'investissement) ne sont pas non plus couverts par la DSP2. En tout état de cause, le RGPD est le cadre juridique applicable pour le traitement des données à caractère personnel.

Exemple 1:

HappyPayments est une société proposant un service en ligne qui consiste à fournir des informations sur un ou plusieurs comptes de paiement par l'intermédiaire d'une application mobile à des fins de contrôle financier (un service d'information sur les comptes). Grâce à ce service, l'utilisateur peut voir en un instant les soldes et les opérations récentes sur deux comptes de paiement ou plus auprès de différentes banques. Elle propose aussi, lorsqu'un utilisateur de services de paiement le décide, de catégoriser les dépenses et les revenus selon différentes typologies (salaire, loisirs, énergie, crédit hypothécaire, etc.), aidant ainsi l'utilisateur de services de paiement à planifier ses finances. Avec cette application, HappyPayments propose aussi un service qui consiste à initier des paiements directement à partir du ou des comptes de paiement désigné(s) de l'utilisateur (un service d'initiation de paiement).

9. Pour fournir ces services, la DSP2 régit les conditions juridiques en vertu desquelles les PSIP et les PSIC peuvent accéder aux comptes de paiement pour fournir un service à l'utilisateur de services de paiement.

10. L'article 66, paragraphe 1, et l'article 67, paragraphe 1, de la DSP2 déterminent que l'accès aux services de paiement et d'information sur les comptes et leur utilisation sont des droits de l'utilisateur de services de paiement. Cela signifie que l'utilisateur de services de paiement devrait

[11] Article 4, point 15, de la DSP2.
[12] Article 4, point 16, de la DSP2.

demeurer entièrement libre au regard de l'exercice de ce droit et ne peut être contraint d'y recourir.

11. L'accès aux comptes de paiement et l'utilisation des informations sur les comptes de paiement sont en partie régis par les articles 66 et 67 de la DSP2, qui contiennent des garanties concernant la protection des données (à caractère personnel). L'article 66, paragraphe 3, point f), de la DSP2 dispose que le PSIP ne demande pas à l'utilisateur de services de paiement des données autres que celles nécessaires pour fournir le service d'initiation de paiement, et l'article 66, paragraphe 3, point g), de la DSP2 dispose que le PSIP n'utilise, ne consulte ou ne stocke des données à des fins autres que la fourniture du service d'initiation de paiement expressément demandée par l'utilisateur de services de paiement. En outre, l'article 67, paragraphe 2, point d), de la DSP2 limite l'accès du PSIC aux informations provenant des comptes de paiement désignés et des opérations de paiement associées, tandis que l'article 67, paragraphe 2, point f), de la DSP2 dispose que le PSIC n'utilise, ne consulte ou ne stocke des données à des fins autres que la fourniture du service d'information sur les comptes expressément demandée par l'utilisateur de services de paiement, conformément aux règles relatives à la protection des données. Ces dernières soulignent que, dans le contexte des services d'information sur les comptes, les données à caractère personnel peuvent uniquement être collectées pour des finalités déterminées, explicites et légitimes. Un PSIC devrait donc indiquer explicitement dans le contrat les finalités déterminées pour lesquelles des données à caractère personnel vont être traitées dans le contexte du service d'information sur les comptes qu'il fournit. Le contrat devrait être licite, loyal et transparent au titre de l'article 5 du RGPD et respecter les autres dispositions législatives relatives à la protection des consommateurs.

12. Selon les circonstances, le prestataire de services de paiement peut être un responsable du traitement ou un sous-traitant au titre du RGPD. Dans les présentes lignes directrices, par «responsable du traitement», il faut entendre les prestataires de services de paiement qui, seuls ou conjointement avec d'autres, déterminent les finalités et les moyens du traitement de données à caractère personnel. De plus amples informations à ce sujet figurent dans les lignes directrices 7/2020 de l'EDPB sur les notions de responsable du traitement et de sous-traitant dans le RGPD.

2 MOTIFS LÉGITIMES ET TRAITEMENT ULTÉRIEUR AU TITRE DE LA DSP2

2.1 Motifs légitimes de traitement

13. En vertu du RGPD, les responsables du traitement doivent disposer d'une base juridique afin de traiter des données à caractère personnel. L'article 6, paragraphe 1, du RGPD constitue une liste exhaustive et restrictive de six bases juridiques du traitement des données à caractère personnel au titre du RGPD[13]. Il incombe au responsable du traitement de définir la base juridique adéquate et de veiller à ce que toutes les conditions de cette base juridique soient remplies. Pour déterminer quelle base est valable et la plus appropriée dans une situation donnée, il faut tenir compte des circonstances dans lesquelles le traitement a lieu, notamment de la finalité du traitement et de la relation entre le responsable du traitement et la personne concernée.

2.2 Article 6, paragraphe 1, point b), du RGPD (le traitement est nécessaire à l'exécution d'un contrat)

14. Les services de paiement sont fournis sur la base d'un contrat entre l'utilisateur de services de paiement et le prestataire de services de paiement. Tel qu'indiqué au considérant 87 de la DSP2, «*[l]a présente directive ne devrait concerner que les obligations contractuelles et les responsabilités respectives de l'utilisateur de services de paiement et du prestataire de services de paiement.*» En ce qui concerne le RGPD, la principale base juridique pour le traitement des données à caractère personnel pour la fourniture de services de paiement est l'article 6, paragraphe 1, point b), du règlement, autrement dit, le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci.

15. Les services de paiement au titre de la DSP2 sont définis à l'annexe 1 de la directive. La fourniture de ces services telle que définie par la DSP2 est une exigence en vue de l'établissement d'un contrat dans le cadre duquel les parties ont accès aux données sur les comptes de paiement de l'utilisateur des services de paiement. Ces prestataires de services de paiement doivent aussi être

[13] Conformément à l'article 6, le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:

(a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;

(b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

(c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;

(d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;

(e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;

(f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

des opérateurs agréés. En ce qui concerne les services d'initiation de paiement et les services d'information sur les comptes au titre de la DSP2, les contrats peuvent contenir des clauses qui imposent aussi des conditions relatives à des services supplémentaires qui ne sont pas régis par la DSP2. Les *lignes directrices 2/2019 de l'EDPB 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* indiquent clairement que les responsables du traitement doivent évaluer quel traitement des données à caractère personnel est objectivement nécessaire pour exécuter le contrat. Ces lignes directrices soulignent que la justification de la nécessité dépend de la nature du service, des perspectives et attentes mutuelles des parties au contrat, de la justification du contrat et des éléments essentiels du contrat.

16. Les lignes directrices 2/2019 de l'EDPB indiquent aussi clairement qu'à la lumière de l'article 7, paragraphe 4, du RGPD, une distinction est établie entre les activités de traitement nécessaires à l'exécution d'un contrat, d'un côté, et les clauses subordonnant le service à certaines activités de traitement qui ne sont en fait pas nécessaires à l'exécution du contrat, de l'autre. «Nécessaire à l'exécution» suppose quelque chose de plus qu'une simple clause contractuelle[14]. Le responsable des données devrait être en mesure de démontrer comment l'objet principal du contrat spécifique avec la personne concernée ne peut, en fait, être exécuté si le traitement spécifique des données à caractère personnel en question n'a pas lieu. Il ne suffit pas de simplement faire référence au traitement des données ou de le mentionner dans un contrat pour que le traitement en question relève de l'article 6, paragraphe 1, point b), du RGPD.

17. L'article 5, paragraphe 1, point b), du RGPD prévoit le principe de limitation de la finalité, selon lequel les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Pour déterminer si l'article 6, paragraphe 1, point b), constitue une base juridique appropriée pour un service (de paiement) en ligne, il convient de tenir compte du but, de la finalité ou de l'objectif particulier du service[15]. Les finalités du traitement doivent être indiquées clairement et communiquées à la personne concernée, conformément aux obligations de limitation de la finalité et de transparence du responsable du traitement. L'évaluation de ce qui est «nécessaire» implique une évaluation factuelle globale du traitement «aux fins de l'objectif poursuivi et de déterminer si ce traitement est moins intrusif par rapport aux autres moyens de réaliser le même objectif». L'article 6, paragraphe 1, point b), ne couvrira pas les traitements qui sont utiles mais non objectivement nécessaires à l'exécution du service contractuel ou à la mise en œuvre des mesures précontractuelles pertinentes à la demande de la personne concernée, même s'ils sont nécessaires pour les autres finalités commerciales du responsable du traitement[16].

18. Les lignes directrices 2/2019 de l'EDPB indiquent clairement qu'un contrat ne peut élargir artificiellement les catégories de données à caractère personnel ou les types de traitements que le responsable du traitement doit effectuer pour garantir l'exécution du contrat au sens de l'article 6, paragraphe 1, point b)[17]. Ces lignes directrices traitent aussi des cas dans lesquels des situations de type «à prendre ou à laisser» pourraient être créées pour les personnes concernées, qui pourraient n'être intéressées que par un seul de ces services. Cela peut se produire lorsqu'un

[14] 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, EDPB, p. 8.
[15] Idem.
[16] Idem, p. 7.
[17] Idem, p. 10.

responsable du traitement souhaite regrouper, au sein d'un même contrat, plusieurs services ou éléments distincts d'un même service, avec des finalités, des caractéristiques et des motifs fondamentaux différents. Lorsque le contrat consiste en plusieurs services ou éléments distincts d'un même service, qui peuvent en fait être raisonnablement exécutés indépendamment les uns des autres, l'applicabilité de l'article 6, paragraphe 1, point b), devrait être évaluée dans le contexte de chacun de ces services séparément, en examinant ce qui est objectivement nécessaire pour exécuter chacun des services que la personne concernée a activement demandés ou souscrits[18].

19. Selon les lignes directrices susmentionnées, les responsables du traitement doivent évaluer ce qui est objectivement nécessaire à l'exécution du contrat. Lorsque les responsables du traitement ne peuvent démontrer que le traitement des données à caractère personnel sur les comptes de paiement est objectivement nécessaire pour fournir chacun de ces services séparément, l'article 6, paragraphe 1, point b), du RGPD n'est pas un motif légitime de traitement valable. Dans ces cas, le responsable du traitement devrait envisager une autre base juridique pour le traitement.

2.3 Prévention de la fraude

20. L'article 94, paragraphe 1, de la DSP2 dispose que les États membres autorisent le traitement des données à caractère personnel par les systèmes de paiement et les prestataires de services de paiement lorsque cela est nécessaire pour garantir la prévention, la recherche et la détection des fraudes en matière de paiements. Le traitement de données à caractère personnel strictement nécessaire à des fins de prévention de la fraude peut constituer un intérêt légitime du prestataire de services de paiement concerné, pour autant que les intérêts ou les libertés et droits fondamentaux de la personne concernée ne prévalent pas sur ces intérêts[19]. Les activités de traitement à des fins de prévention de la fraude devraient reposer sur une évaluation approfondie au cas par cas par le responsable du traitement, conformément au principe de responsabilité. En outre, pour prévenir la fraude, les responsables du traitement peuvent aussi être soumis à des obligations juridiques particulières qui nécessitent le traitement de données à caractère personnel.

2.4 Traitement ultérieur (PSIC et PSIP)

21. L'article 6, paragraphe 4, du RGPD définit les conditions du traitement des données à caractère personnel à une fin autre que celle pour laquelle les données à caractère personnel ont été collectées. Plus précisément, ce traitement ultérieur peut avoir lieu lorsqu'il est fondé sur le droit d'un État membre de l'UE, qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, paragraphe 1, lorsque la personne concernée a donné son consentement ou lorsque le traitement à une fin autre que celle pour laquelle les données à caractère personnel ont été collectées est compatible avec la finalité initiale.

22. L'article 66, paragraphe 3, point g), et l'article 67, paragraphe 2, point f), de la DSP2 doivent être soigneusement pris en considération. Comme mentionné ci-dessus, l'article 66, paragraphe 3, point g), de la DSP2 dispose que le PSIP n'utilise, ne consulte ou ne stocke des données à des fins autres que la fourniture du service d'initiation de paiement expressément demandée par le payeur. L'article 67, paragraphe 2, point f), de la DSP2 dispose que le PSIC n'utilise, ne consulte ou ne stocke des données à des fins autres que la fourniture du service d'information sur les comptes

[18] Idem, p. 11.
[19] Considérant 47 du RGPD.

expressément demandée par l'utilisateur de services de paiement, conformément aux règles relatives à la protection des données.

23. En conséquence, l'article 66, paragraphe 3, point g), et l'article 67, paragraphe 2, point f), de la DSP2 limitent considérablement les possibilités de traitement à d'autres fins, ce qui signifie que le traitement pour une autre finalité n'est pas autorisé, sauf si la personne concernée a donné son consentement en application de l'article 6, paragraphe 1, point a), du RGPD ou si le traitement est prévu par le droit de l'Union ou celui de l'État membre auquel le responsable du traitement est soumis, en application de l'article 6, paragraphe 4, du RGPD. Lorsque le traitement pour une finalité autre que celle pour laquelle les données ont été collectées n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre, les limitations prévues à l'article 66, paragraphe 3, point g), et à l'article 67, paragraphe 2, point f), de la DSP2 indiquent clairement que toute autre finalité n'est pas compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées. Le test de compatibilité de l'article 6, paragraphe 4, du RGPD ne peut donner lieu à une base juridique pour le traitement.

24. L'article 6, paragraphe 4, du RGPD permet le traitement ultérieur sur la base du droit de l'Union ou d'un État membre. Par exemple, tous les PSIP et les PSIC sont des entités assujetties en vertu de l'article 3, paragraphe 2, point a), de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme. Ces entités assujetties sont donc tenues d'appliquer les mesures de vigilance à l'égard de la clientèle tel que spécifié dans la directive. Les données à caractère personnel traitées en relation avec un service au titre de la DSP2 sont donc traitées ultérieurement sur la base d'au moins une obligation juridique incombant au prestataire de services[20].

25. Comme mentionné au point 20, l'article 6, paragraphe 4, du RGPD indique que le traitement pour une autre finalité que celle pour laquelle les données à caractère personnel ont été collectées pourrait être fondé sur le consentement de la personne concernée, si toutes les conditions du consentement au titre du RGPD sont réunies. Comme indiqué ci-dessus, le responsable du traitement doit démontrer qu'il est possible de refuser ou de retirer son consentement sans subir de préjudice (considérant 42 du RGPD).

2.5 Motif légitime d'octroyer l'accès au compte (PSPGC)

26. Comme mentionné au point 10, les utilisateurs de services de paiement peuvent exercer leur droit de recourir à des services d'initiation de paiement et d'information sur les comptes. Les obligations imposées aux États membres à l'article 66, paragraphe 1, et à l'article 67, paragraphe 1, de la DSP2 devraient être mises en œuvre dans le droit national afin de garantir l'application effective du droit de l'utilisateur de services de paiement de bénéficier des services de paiement susvisés. L'application effective de ces droits ne serait pas possible sans l'existence d'une obligation correspondante de la part du PSPGC, généralement une banque, d'octroyer au prestataire de services de paiement l'accès au compte à la condition qu'il ait satisfait à toutes les exigences d'accès au compte de l'utilisateur de services de paiement. En outre, l'article 66, paragraphe 5, et l'article 67, paragraphe 4, de la DSP2 indiquent clairement que la fourniture de services d'initiation de paiement et d'information sur les comptes n'est pas subordonnée à l'existence de relations contractuelles entre le PSIP/PSIC et le PSPGC.

[20] Il est à noter qu'un examen approfondi de la question de savoir si la directive anti-blanchiment répond aux exigences de l'article 6, paragraphe 4, du RGPD ne fait pas l'objet du présent document.

27. Le traitement des données à caractère personnel par le PSPGC qui consiste à octroyer l'accès aux données à caractère personnel requises par le PSIP et le PSIC afin de fournir leur service de paiement à l'utilisateur de services de paiement est fondé sur une obligation juridique. Pour atteindre les objectifs de la DSP2, les PSPGC doivent fournir les données à caractère personnel pour les services des PSIP et des PSIC, ce qui est une condition nécessaire pour permettre à ces derniers de fournir leurs services et qui garantit donc les droits prévus à l'article 66, paragraphe 1, et à l'article 67, paragraphe 1, de la DSP2. Par conséquent, la base juridique applicable dans ce cas est l'article 6, paragraphe 1, point c), du RGPD.

28. Dès lors que le RGPD précise que le traitement fondé sur une obligation juridique doit être clairement défini par le droit de l'Union ou d'un État membre (voir article 6, paragraphe 3, du RGPD), l'obligation pour les PSPGC d'octroyer l'accès devrait découler de la disposition du droit national transposant la DSP2.

3 CONSENTEMENT EXPLICITE

3.1 Consentement au titre du RGPD

29. En vertu du RGPD, le consentement constitue l'une des six bases juridiques de la licéité du traitement de données à caractère personnel. L'article 4, paragraphe 11, du RGPD défini le consentement comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement». Ces quatre conditions (libre, spécifique, éclairée et univoque) sont essentielles pour que le consentement soit valable. Selon les lignes directrices 5/2020 de l'EDPB sur le consentement au sens du règlement (UE) 2016/679, le consentement ne constitue une base juridique appropriée que si la personne concernée dispose d'un contrôle et d'un choix réel concernant l'acceptation ou le refus des conditions proposées ou de la possibilité de les refuser sans subir de préjudice. Lorsqu'il sollicite un consentement, le responsable du traitement a l'obligation d'évaluer si celui-ci satisfera à toutes les conditions d'obtention d'un consentement valable. S'il a été obtenu dans le plein respect du RGPD, le consentement est un outil qui confère aux personnes concernées un contrôle sur le traitement éventuel de leurs données à caractère personnel. Dans le cas contraire, le contrôle de la personne concernée devient illusoire et le consentement ne constituera pas une base juridique valable pour le traitement des données, rendant de ce fait l'activité de traitement illicite[21].

30. Le RGPD contient aussi d'autres garanties en son article 7, qui dispose que le responsable du traitement doit être en mesure de démontrer qu'il y a eu un consentement valable au moment du traitement. De plus, la demande de consentement doit être présentée sous une forme qui la distingue clairement des autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. La personne concernée doit par ailleurs être informée du droit de retirer son consentement à tout moment, aussi simplement qu'elle l'avait octroyé.

31. Conformément à l'article 9 du RGPD, le consentement constitue l'une des exceptions à l'interdiction générale de traitement de catégories particulières de données à caractère personnel. Dans ce cas, le consentement de la personne concernée doit toutefois être «explicite»[22].

32. Selon les lignes directrices 5/2020 de l'EDPB sur le consentement au sens du règlement (UE) 2016/679, le consentement explicite au titre du RGPD se rapporte à la façon dont le consentement est exprimé par la personne concernée. Il implique que la personne concernée doit formuler une déclaration de consentement exprès. Une manière évidente de s'assurer que le consentement est explicite serait de confirmer expressément le consentement dans une déclaration écrite. Le cas échéant, le responsable du traitement pourrait s'assurer que la déclaration écrite est signée par la personne concernée afin de prévenir tout doute potentiel et toute absence potentielle de preuve à l'avenir.

33. Le consentement ne peut en aucun cas être déduit de déclarations ou d'actions potentiellement équivoques. Un responsable du traitement doit également être conscient que le consentement ne

[21] Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, CEPD, point 3.
[22] Voir également avis 15/2011 sur la définition du consentement (CP 187), p. 6-9 et/ou avis 6/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE (WP 217), p. 9, 10, 13 et 14.

peut être obtenu moyennant la même action que lorsqu'une personne concernée accepte un contrat ou les conditions générales d'un service.

3.2 Consentement au titre de la DSP2

34. L'EDPB note que le cadre juridique relatif au consentement explicite est complexe, étant donné que tant la DSP2 que le RGPD incluent la notion de « consentement explicite ». Il y a donc lieu de se demander si le « consentement explicite » tel que visé à l'article 94, paragraphe 2, de la DSP2 doit être interprété de la même façon que le consentement explicite au titre du RGPD.

3.2.1 Consentement explicite au sens de l'article 94, paragraphe 2, de la DSP2

35. La DSP2 inclut une série de règles particulières concernant le traitement des données à caractère personnel, en particulier en son article 94, paragraphe 1, qui dispose que le traitement des données à caractère personnel aux fins de la DSP2 doit respecter le droit de l'UE en matière de protection des données. Par ailleurs, l'article 94, paragraphe 2, de la DSP2 dispose que les prestataires de services de paiement n'ont accès à des données à caractère personnel nécessaires à l'exécution de leurs services de paiement, ne les traitent et ne les conservent qu'avec le consentement explicite de l'utilisateur de services de paiement. En application de l'article 33, paragraphe 2, de la DSP2, cette exigence de consentement explicite de l'utilisateur de services de paiement ne s'applique pas aux PSIC. Cependant, l'article 67, paragraphe 2, point a), de la DSP2 prévoit que les PSIC fournissent des services sur la base du consentement explicite.

36. Ainsi que nous l'avons indiqué ci-dessus, la liste des bases juridiques du traitement au titre du RGPD est exhaustive. Comme signalé au point 14, la principale base juridique du traitement des données à caractère personnel pour la fourniture de services de paiement est, en principe, l'article 6, paragraphe 1, point b), du règlement, autrement dit, le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci. Il s'ensuit que l'article 94, paragraphe 2, de la DSP2 ne peut être considéré comme une base juridique supplémentaire du traitement des données à caractère personnel. L'EDPB estime qu'eu égard à ce qui précède, ce point devrait être interprété, d'une part, de façon cohérente avec le cadre juridique applicable en matière de protection des données et, d'autre part, de manière à préserver son effet utile. Le consentement explicite au sens de l'article 94, paragraphe 2, de la DSP2 devrait donc être considéré comme une exigence supplémentaire de nature contractuelle[23] en relation avec l'accès à des données à caractère personnel et avec leur traitement ultérieur et leur conservation, aux fins de fournir des services de paiement, et n'est donc pas identique au consentement (explicite) au sens du RGPD.

37. Le « consentement explicite » visé à l'article 94, paragraphe 2, de la DSP2 est un consentement contractuel. Cela signifie que l'article 94, paragraphe 2, de la DSP2 devrait être interprété comme signifiant que lorsqu'elles concluent un contrat avec un prestataire de services de paiement au titre de la DSP2, les personnes concernées doivent être pleinement informées des catégories particulières de données à caractère personnel qui seront traitées. Elles doivent en outre être informées de la finalité précise (service de paiement) pour laquelle leurs données à caractère personnel seront traitées et doivent marquer leur accord explicite avec ces clauses. Ces clauses devraient pouvoir être distinguées clairement des autres questions abordées dans le contrat et devraient être explicitement acceptées par la personne concernée.

[23] Lettre de l'EDPB concernant la DSP2, 5 juillet 2018, p. 4.

38. L'obtention de l'accès aux données à caractère personnel pour traiter ultérieurement et conserver ces données aux fins de la fourniture de services de paiement est centrale pour la notion de « consentement explicite » au sens de l'article 94, paragraphe 2, de la DSP2. Cela signifie que le prestataire services de paiement[24] ne traite pas encore les données à caractère personnel, mais a besoin d'accéder à des données à caractère personnel qui ont été traitées sous la responsabilité d'un autre responsable du traitement. Si un utilisateur de services de paiement conclut un contrat avec, par exemple, un prestataire de services d'initiation de paiement, ce prestataire doit obtenir l'accès aux données à caractère personnel de l'utilisateur de services de paiement qui sont traitées sous la responsabilité du prestataire de services de paiement gestionnaire du compte. L'objet du consentement explicite au sens de l'article 94, paragraphe 2, de la DSP2 est la permission d'obtenir l'accès à ces données à caractère personnel afin de pouvoir traiter et conserver les données à caractère personnel qui sont nécessaires aux fins de la fourniture du service de paiement. Si la personne concernée donne son consentement, le prestataire de services de paiement gestionnaire du compte est tenu d'octroyer l'accès aux données à caractère personnel indiquées.

39. Bien que le consentement au sens de l'article 94, paragraphe 2, de la DSP2, ne constitue pas une base juridique pour le traitement des données à caractère personnel, ce consentement est expressément lié aux données à caractère personnel et à la protection des données, et garantit à l'utilisateur de services de paiement la transparence et un certain contrôle[25]. Si la DSP2 ne précise pas les conditions de fond du consentement au titre de l'article 94, paragraphe 2, de la DSP2, il devrait, tel qu'indiqué ci-dessus, être interprété de manière cohérente avec le cadre juridique applicable en matière de protection des données et de manière à préserver son effet utile.

40. Concernant les informations que les responsables du traitement doivent fournir et l'exigence de transparence, les lignes directrices sur la transparence du groupe de travail «Article 29» indiquent qu'un «*aspect primordial du principe de transparence mis en lumière dans ces dispositions est que la personne concernée devrait être en mesure de déterminer à l'avance ce que la portée et les conséquences du traitement englobent afin de ne pas être prise au dépourvu à un stade ultérieur quant à la façon dont ses données à caractère personnel ont été utilisées*»[26].

41. En outre, tel que requis par le principe de limitation de la finalité, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes [article 5, paragraphe 1, point b), du RGPD]. Lorsque des données à caractère personnel sont collectées pour plusieurs finalités, «*les responsables du traitement devraient éviter de ne définir qu'une seule finalité générale pour justifier plusieurs activités de traitement ultérieur qui ne sont en fait que vaguement liées à la finalité initiale réelle*»[27]. L'EDPB a mis en évidence, dernièrement dans le contexte de contrats relatifs à des services en ligne, le risque d'inclusion de clauses générale de traitement dans les contrats et a déclaré que la finalité de la collecte devait être indiquée d'une manière claire et spécifique: elle doit être suffisamment détaillée pour déterminer quel type de traitement est ou n'est pas inclus dans la finalité spécifiée, mais aussi pour permettre l'évaluation du respect de la loi et l'application de garanties de protection des données[28].

[24] Cela s'applique aux services 1 à 7 de l'annexe 1 de la DSP2.
[25] L'article 94, paragraphe 2, de la DSP2 relève du chapitre 4 «Protection des données».
[26] Groupe de travail «Article 29», Lignes directrices sur la transparence au sens du règlement (UE) 2016/679, point 10 (adoptées le 11 avril 2018) – approuvées par l'EDPB.
[27] Avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité (WP203), p. 16.
[28] 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,

42. Dans le contexte de l'exigence supplémentaire de consentement explicite en application de l'article 94, paragraphe 2, de la DSP2, cela signifie que les responsables du traitement doivent fournir aux personnes concernées des informations précises et explicites concernant les finalités particulières définies par le responsable du traitement et pour lesquelles leurs données à caractère personnel sont consultées, traitées et conservées. Conformément à l'article 94, paragraphe 2, de la DSP2, les personnes concernées doivent accepter explicitement ces finalités particulières.

43. En outre, comme indiqué ci-dessus au point 10, l'EDPB souligne que l'utilisateur de services de paiement doit pouvoir choisir de recourir ou non au service et ne peut y être contraint. Le consentement au sens de l'article 94, paragraphe 2, de la DSP2, doit donc lui aussi être un consentement libre.

3.3 Conclusion

44. Le consentement explicite au sens de la DSP2 est différent du consentement (explicite) au sens du RGPD. Le consentement explicite au sens de l'article 94, paragraphe 2, de la DSP2 est une exigence supplémentaire de nature contractuelle. Lorsqu'un prestataire de services de paiement doit accéder à des données à caractère personnel pour fournir un service de paiement, le consentement explicite au sens de l'article 94, paragraphe 2, de la DSP2 de l'utilisateur de services de paiement est requis.

point 16 (version pour consultation publique) et avis 3/2013 du groupe de travail « Article 29» sur la limitation de la finalité (WP203), p. 15-16.

4 TRAITEMENT DES DONNÉES DES PARTIES SILENCIEUSES

4.1 Données des parties silencieuses

45. Une des questions relatives à la protection des données qui requiert une attention toute particulière est celle du traitement de ce que l'on appelle les «données des parties silencieuses». Dans le contexte du présent document, les données des parties silencieuses sont des données à caractère personnel relatives à une personne concernée qui n'est pas l'utilisateur d'un service de paiement donné, mais dont les données à caractère personnel sont traitées par le prestataire du service aux fins de l'exécution d'un contrat entre lui-même et l'utilisateur de services de paiement. Tel est, par exemple, le cas lorsqu'un utilisateur de services de paiement, la personne concernée A, a recours aux services d'un PSIC et la personne concernée B a effectué une série d'opérations de paiement sur le compte de paiement de la personne concernée A. Dans ce cas, la personne concernée B est considérée comme la «partie silencieuse» et les données à caractère personnel (telles que le numéro de compte de la personne concernée B et le montant de ces opérations) relatives à la personne concernée B sont considérées comme des «données des parties silencieuses».

4.2 Intérêt légitime du responsable du traitement

46. L'article 5, paragraphe 1, point b), du RGPD, exige que les données à caractère personnel soient uniquement collectées pour des finalités déterminées, explicites et légitimes, et ne soient pas traitées ultérieurement de manière incompatible avec ces finalités. En outre, le RGPD impose que tout traitement de données à caractère personnel soit nécessaire, proportionné et conforme aux principes de protection des données tels que ceux de la limitation des finalités et de la minimisation des données.

47. Le RGPD peut autoriser le traitement de données des parties silencieuses lorsque ce traitement est nécessaire aux fins des intérêts légitimes poursuivis par un responsable du traitement ou par un tiers [article 6, paragraphe 1, point f), du RGPD]. Ce traitement ne peut cependant seulement avoir lieu que lorsque «les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel» ne prévalent pas sur l'intérêt légitime du responsable du traitement.

48. Une base légale pour le traitement des données des parties silencieuses par les PSIP et les PSIC – dans le contexte de la fourniture de services de paiement au titre de la DSP2 – pourrait donc être l'intérêt légitime d'un responsable du traitement ou d'un tiers à exécuter le contrat avec l'utilisateur de services de paiement. La nécessité de traiter les données à caractère personnel des parties silencieuses est limitée et déterminée par les attentes raisonnables de ces personnes concernées. Dans le contexte de la fourniture des services de paiement couverts par la DSP2, des mesures effectives et appropriées doivent être prises pour garantir que les intérêts ou les droits et libertés fondamentaux des parties silencieuses prévalent et pour veiller à ce que les attentes raisonnables de ces personnes concernées à l'égard du traitement de leurs données à caractère personnel soient respectées. À cet égard, le responsable du traitement (PSIC ou PSIP) doit mettre en place les garanties nécessaires pour le traitement afin de protéger les droits des personnes concernées. Cela inclut des mesures techniques en vue de garantir que les données des parties silencieuses ne sont pas traitées à une fin autre que celle pour laquelle les données à caractère personnel ont initialement été collectées par les PSIP et les PSIC. Si possible, le chiffrement et d'autres techniques devraient aussi être appliqués afin d'atteindre un niveau suffisant de sécurité et de minimisation des données.

4.3 Traitement ultérieur des données à caractère personnel des parties silencieuses

49. Comme indiqué au point 29, les données à caractère personnel traitées en relation avec un service de paiement régi par la DSP2 peuvent être traitées ultérieurement sur la base d'obligations juridiques imposées au prestataire de services. Ces obligations juridiques peuvent concerner les données à caractère personnel de la partie silencieuse.

50. Concernant le traitement ultérieur des données des parties silencieuses sur la base d'un intérêt légitime, l'EDPB est d'avis que ces données ne peuvent être utilisées à une fin autre que celle pour laquelle les données à caractère personnel ont été collectées, sur la base du droit de l'Union ou du droit d'un État membre. Le consentement de la partie silencieuse ne peut juridiquement pas être obtenu, car il faudrait pour ce faire collecter ou traiter les données à caractère personnel de la partie silencieuse, et l'article 6 du RGPD ne prévoit aucune base juridique à cet effet. Le test de compatibilité de l'article 6, paragraphe 4, du RGPD ne peut pas non plus servir de base au traitement à d'autres fins (par exemple, des activités de prospection). Les droits et libertés de ces parties silencieuses concernées ne seront pas respectés si le nouveau responsable du traitement utilise les données à caractère personnel à d'autres fins, compte tenu du contexte dans lequel les données à caractère personnel ont été collectées, en particulier l'absence de relation avec les personnes concernées qui sont des parties silencieuses[29]; l'absence de relation entre toute autre fin et la fin pour laquelle les données à caractère personnel ont initialement été collectées (c.-à-d. le fait que les prestataires de services de paiement ont uniquement besoin des données des parties silencieuses afin d'exécuter un contrat avec l'autre partie contractante); la nature des données à caractère personnel en cause[30]; le fait que les personnes concernées ne sont pas en position de raisonnablement s'attendre à un traitement ultérieur voire de savoir quel responsable du traitement est susceptible de traiter leurs données à caractère personnel et étant donné les limitations juridiques du traitement prévues à l'article 66, paragraphe 3, point g), et à l'article 67, paragraphe 2, point f), de la DSP2.

[29] Selon le considérant 87 de la DSP2, la directive ne devrait concerner que « les obligations contractuelles et les responsabilités respectives de l'utilisateur de services de paiement et du prestataire de services de paiement ». Les données des parties silencieuses ne relèvent donc pas de la DSP2.

[30] Il y a lieu d'être particulièrement attentif lors du traitement des données à caractère personnel financières car le traitement est réputé accroître le risque pour les droits et libertés des personnes selon les lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD).

5 TRAITEMENT DE CATÉGORIES PARTICULIÈRES DE DONNÉES À CARACTÈRE PERSONNEL AU TITRE DE LA DSP2

5.1 Catégories particulières de données à caractère personnel

51. L'article 9, paragraphe 1, du RGPD interdit le traitement de « données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique».

52. Il est à souligner que dans certains États membres, les paiements électroniques sont déjà omniprésents et sont préférés aux paiements en espèces par de nombreuses personnes dans leurs opérations quotidiennes. Dans le même temps, 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. L'appartenance à un syndicat peut être révélée par le prélèvement d'une cotisation annuelle sur le compte bancaire d'une personne. 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). Enfin, des informations sur certains achats peuvent révéler des informations sur la vie sexuelle ou l'orientation sexuelle d'une personne. Comme le montrent ces exemples, même des opérations uniques peuvent contenir des catégories particulières de données à caractère personnel. En outre, les services d'information sur les comptes peuvent recourir au profilage tel que défini à l'article 4, paragraphe 4, du RGPD. Comme indiqué dans les lignes directrices du groupe de travail «Article 29» relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, approuvées par l'EDPB, «le profilage peut engendrer des données d'une catégorie particulière par inférence à partir de données qui n'appartiennent pas à une catégorie particulière en soi, mais qui le deviennent lorsqu'elles sont combinées avec d'autres données»[31]. Cela signifie qu'en faisant la somme des opérations financières, différents types d'habitudes de comportement peuvent être révélés, qui peuvent inclure des catégories particulières de données à caractère personnel. Par conséquent, les chances qu'un prestataire de services qui traite des informations sur les opérations financières d'une personne concernée traite aussi des catégories particulières de données à caractère personnel sont considérables.

53. En ce qui concerne le terme « données de paiement sensibles», l'EDPB note ceci: la définition des données de paiement sensibles dans la DSP2 diffère considérablement de la manière dont le terme «données à caractère personnel sensibles» est communément utilisé dans le contexte du RGPD et (du droit) de la protection des données. Là où la DSP2 définit les «données de paiement sensibles» comme «des données, y compris les données de sécurité personnalisées, qui sont susceptibles d'être utilisées pour commettre une fraude», le RGPD insiste sur la nécessité d'une protection spécifique des données à caractère personnel qui, en vertu de l'article 9 du RGPD, sont, par nature,

[31] Lignes directrices du groupe de travail «Article 29» relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, WP251rev.01, p. 15.

particulièrement sensibles du point de vue des libertés et des droits fondamentaux, telles que les catégories particulières de données à caractère personnel[32]. À cet égard, il est recommandé d'au moins recenser et catégoriser précisément le type de données à caractère personnel qui sera traité. Il est très probable qu'une analyse d'impact relative à la protection des données (AIPD) sera requise conformément à l'article 35 du RGPD, ce qui facilitera l'exercice de recensement. Des orientations complémentaires concernant les DPIA figurent dans les lignes directrices du groupe de travail «Article 29» 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, telles qu'approuvées par l'EDPB.

5.2 Possibilités de dérogations

54. L'interdiction prévue à l'article 9 du RGPD n'est pas absolue. En particulier, alors que les dérogations des points b) à f) et h) à j) de l'article 9, paragraphe 2, du RGPD ne sont manifestement pas applicables au traitement des données à caractère personnel dans le contexte de la DSP2, les deux dérogations suivantes de l'article 9, paragraphe 2, du RGPD pourraient quant à elles être envisagées.

a) L'interdiction ne s'applique pas si la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques [article 9, paragraphe 2, point a), du RGPD].

b) L'interdiction ne s'applique pas si le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée [article 9, paragraphe 2, point g), du RGPD].

55. Il est à noter que la liste des dérogations de l'article 9, paragraphe 2, du RGPD est exhaustive. La possibilité que des catégories particulières de données à caractère personnel figurent parmi les données à caractère personnel traitées aux fins de la fourniture d'un des services relevant de la DSP2 doit être reconnue par le prestataire de services. Comme l'interdiction prévue à l'article 9, paragraphe 1, du RGPD est applicable à ces prestataires de services, ils doivent garantir qu'une des exceptions prévues à l'article 9, paragraphe 2, de la DSP2 leur est applicable. Il y a lieu de souligner que lorsque le prestataire de services n'est pas en mesure de démontrer qu'il peut déroger aux interdictions, l'interdiction prévue à l'article 9, paragraphe 1, s'applique.

5.3 Intérêt public important

56. 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

[32] Par exemple, au considérant 10 du RGPD, les catégories particulières de données à caractère personnel sont qualifiées de «données sensibles».

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.

5.4 Consentement explicite

57. Dans les cas où la dérogation prévue à l'article 9, paragraphe 2, point g), du RGPD ne s'applique pas, l'obtention du consentement explicite conformément aux conditions de validité du consentement du RGPD semble être la seule dérogation licite possible en vue du traitement des catégories particulières de données à caractère personnel par des PT. Selon les lignes directrices 5/2020 de l'EDPB sur le consentement au sens du règlement (UE) 2016/679[33], «[l]'article 9, paragraphe 2, ne reconnaît pas le caractère «nécessaire à l'exécution d'un contrat» comme une exception à l'interdiction générale de traiter des catégories particulières de données. Les responsables du traitement et les États membres se trouvant dans cette situation devraient se pencher sur les exceptions spécifiques des points b) à j) de l'article 9, paragraphe 2. Lorsque les prestataires de services se fondent sur l'article 9, paragraphe 2, point a), du RGPD, ils doivent veiller à obtenir le consentement explicite avant d'entamer le traitement». Le consentement explicite tel que défini à l'article 9, paragraphe 2, point a), du RGPD doit satisfaire à toutes les exigences du RGPD.

5.5 Absence de dérogation valable

58. Tel qu'indiqué ci-dessus, lorsque le prestataire de services n'est pas en mesure de montrer qu'une des dérogations est valable, l'interdiction prévue à l'article 9, paragraphe 1, s'applique. Dans ce cas, des mesures techniques peuvent être mises en place pour prévenir le traitement de catégories particulières de données à caractère personnel, par exemple en empêchant le traitement de certains points de données. À cet égard, les prestataires de services de paiement peuvent étudier les possibilités techniques permettant à la fois d'exclure les catégories particulières de données à caractère personnel tout en permettant un accès sélectif empêchant le traitement des catégories particulières de données à caractère personnel relatives aux parties silencieuses par des PT.

[33] Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, CEPD, point 99.

6 MINIMISATION DES DONNÉES, SÉCURITÉ, TRANSPARENCE, RESPONSABILITÉ ET PROFILAGE

6.1 Minimisation des données et protection des données dès la conception et par défaut

59. Le principe de minimisation des données est inscrit à l'article 5, paragraphe 1, point c), du RGPD: «[l]es données à caractère personnel doivent être […] adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées». En substance, en vertu du principe de minimisation des données, les responsables du traitement ne devraient pas traiter plus de données à caractère personnel qu'il n'en faut pour parvenir à la finalité spécifique en question. Comme indiqué au chapitre 2, la quantité et le type de données à caractère personnel nécessaires pour fournir le service de paiement sont déterminés par une finalité contractuelle qui doit pouvoir être comprise par une personne concernée moyenne[34]. La minimisation des données est applicable à chaque traitement (par exemple, chaque collecte de ou accès à, et demande de données à caractère personnel). Selon les lignes directrices 4/2019 de l'EDPB relatives à l'article 25 du RGPD – Protection des données dès la conception et protection des données par défaut, «les sous-traitants et les fournisseurs de technologies sont aussi reconnus comme des catalyseurs essentiels pour la protection des données dès la conception et par défaut; ils devraient aussi savoir que les responsables du traitement sont tenus de traiter les données à caractère personnel uniquement avec des systèmes et des technologies dotés d'une protection des données intégrée»[35].

60. L'article 25 du RGPD prévoit les obligations d'appliquer la protection des données dès la conception et par défaut. Ces obligations revêtent une importance particulière pour le principe de minimisation des données. Cet article dispose que les responsables du traitement mettent en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées qui sont destinées à mettre en œuvre les principes relatifs à la protection des données de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du RGPD et de protéger les droits de la personne concernée. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. Ces mesures peuvent inclure le chiffrement, la pseudonymisation et d'autres mesures techniques.

61. Lorsque l'obligation prévue à l'article 25 du RGPD est appliquée, l'état des connaissances, les coûts de mise en œuvre et la nature, la portée, le contexte et les finalités du traitement ainsi que les risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques sont les éléments qui doivent être pris en compte. Des précisions concernant cette obligation figurent dans les lignes directrices 4/2019 de l'EDPB

[34] 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, CEPD, point 32.
[35] Lignes directrices 4/2019 de l'EDPB relatives à l'article 25 du RGPD – Protection des données dès la conception et protection des données par défaut, p. 29.

relatives à l'article 25 du RGPD – Protection des données dès la conception et protection des données par défaut mentionnées ci-dessus.

6.2 Mesures de minimisation des données

62. Les prestataires tiers qui accèdent à des données de comptes de paiement pour fournir les services requis doivent aussi tenir compte du principe de minimisation et doivent uniquement collecter les données à caractère personnel nécessaires pour fournir les services de paiement requis par l'utilisateur de services de paiement. En principe, l'accès aux données à caractère personnel devrait être limité à ce qui est nécessaire aux fins de la fourniture des services de paiement. Comme on l'a montré au chapitre 2, la DSP2 impose aux PSPGC de partager les informations de l'utilisateur de services de paiement à la demande de ce dernier, lorsque ledit utilisateur de services de paiement souhaite recourir à un service d'initiation de paiement ou à un service d'information sur les comptes.

63. Lorsque l'exécution d'un contrat ne nécessite pas l'intégralité des données relatives au compte de paiement, le PSIC devrait sélectionner les catégories de données pertinentes avant leur collecte. Par exemple, les catégories de données qui peuvent ne pas être nécessaires peuvent être l'identité de la partie silencieuse et les caractéristiques de l'opération. En outre, à moins que le droit de l'État membre ou de l'Union ne l'exige, il peut ne pas être nécessaire d'afficher l'IBAN du compte bancaire de la partie silencieuse.

64. À cet égard, l'application potentielle de mesures techniques visant à permettre aux PT de s'acquitter de leur obligation d'accéder et d'extraire uniquement les données à caractère personnel nécessaires aux fins de la fourniture de leurs services ou à les aider dans cette tâche pourrait être envisagée dans le contexte de la mise en œuvre de politiques de protection des données adéquates, conformément à l'article 24, paragraphe 2, du RGPD. À cet égard, l'EDPB recommande de recourir à des outils numériques pour aider les PSIC à s'acquitter de leur obligation de collecter uniquement les données à caractère personnel qui sont nécessaires aux fins pour lesquelles elles sont traitées. Par exemple, lorsqu'un prestataire de services n'a pas besoin des caractéristiques de l'opération (dans le champ descriptif des relevés des opérations) aux fins de la fourniture de son service, un outil de sélection numérique pourrait constituer un moyen pour les PT d'exclure ce champ de leurs opérations de traitement globales.

Exemple 2:

HappyPayments, notre prestataire de services d'information sur les comptes de l'exemple 1, veut s'assurer de traiter uniquement les données à caractère personnel des comptes de paiement qui intéressent ses utilisateurs. L'accès à d'autres données sur les comptes de paiement ne serait pas nécessaire aux fins de la fourniture du service. Il permet donc aux utilisateurs de sélectionner les types d'informations qui les intéressent.

L'utilisateur A veut un aperçu de ses dépenses au cours des deux derniers mois. Il demande donc, pour ses deux comptes bancaires, auprès de deux PSPGC différents, les informations concernant toutes les opérations effectuées au cours des deux derniers mois, le montant des opérations, la date d'exécution et le nom du bénéficiaire, et il coche les cases correspondantes dans l'interface utilisateur de HappyPayments.

HappyPayments commence alors à demander aux différents PSPGC uniquement les informations correspondant aux champs définis par l'utilisateur A et uniquement pour les deux derniers mois. Des informations telles que la «communication» liée au virement ou même l'IBAN ne sont pas requises, car l'utilisateur A n'a pas demandé ces informations.

Pour permettre à HappyPayments de se conformer à ses obligations de minimisation des données, les PSPGC autorisent HappyPayments à requérir des champs bien précis pour une plage de dates.

65. Il est aussi à noter, à cet égard, qu'en vertu de la DSP2, les PSPGC sont uniquement autorisés à donner accès aux informations sur les comptes de paiement. Il n'existe pas de base juridique au titre de la DSP2 permettant de donner accès aux données à caractère personnel contenues dans d'autres comptes, tels que les comptes d'épargne, hypothécaires ou d'investissement. En conséquence, en vertu de la DSP2, des mesures techniques doivent être prises afin de garantir que l'accès est limité aux informations sur les comptes de paiement nécessaires.

66. En plus de collecter aussi peu de données que possible, le prestataire de services doit aussi mettre en œuvre des périodes de conservation limitées. Le prestataire de services ne devrait pas conserver les données à caractère personnel plus longtemps que nécessaire aux fins requises par l'utilisateur de services de paiement.

67. Si le contrat entre la personne concernée et le PSIC exige la transmission de données à caractère personnel à des tiers, alors seules les données à caractère personnel qui sont nécessaires aux fins de l'exécution du contrat peuvent être transmises. Les personnes concernées devraient aussi être expressément informées au sujet de la transmission et des données à caractère personnel qui vont être transmises à ce tiers.

6.3 Sécurité

68. L'EDPB a déjà souligné que la violation des données à caractère personnel financières «*aurait clairement des incidences graves dans la vie quotidienne de la personne concernée*» et cite comme exemple les risques de paiements frauduleux[36].

69. Lorsqu'une violation de données concerne des données financières, la personne concernée peut être exposée à des risques considérables. Selon les informations qui ont été divulguées, les personnes concernées peuvent être exposées à un risque d'usurpation d'identité ou de vol des fonds présents sur leurs comptes et d'autres actifs. En outre, la possibilité existe que la divulgation de données sur les opérations s'accompagne de risques considérables pour la protection de la vie privée, car les données sur les opérations peuvent contenir des références à tous les aspects de la vie privée d'une personne concernée. Dans le même temps, les données financières présentent un intérêt évident pour les criminels et sont donc une cible de choix.

70. En qualité de responsables du traitement, les prestataires de services de paiement sont tenus de prendre les mesures adéquates pour protéger les données à caractère personnel des personnes concernées (article 24, paragraphe 1, du RGPD). Plus les risques liés à l'activité de traitement exécutée par le responsable du traitement sont grands, plus les normes de sécurité appliquées doivent être élevées. Comme le traitement des données financières est lié à plusieurs risques graves, les mesures de sécurité devraient être proportionnellement élevées.

71. Les prestataires de services devraient être tenus d'appliquer des normes élevées, y compris des mécanismes d'authentification forte du client et des normes de sécurité élevées pour l'équipement technique[37]. D'autres procédures, telles que la vérification des normes de sécurité

[36] Lignes directrices du groupe de travail «Article 29» 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, WP248 rev.01 – approuvées par l'EDPB.
[37] Voir NTR.

des sous-traitants et la mise en œuvre de procédures contre l'accès non autorisé, sont tout aussi importantes.

6.4 Transparence et responsabilité

72. La transparence et la responsabilité sont deux principes fondamentaux du RGPD.

73. En ce qui concerne la transparence [article 5, paragraphe 1, point a), du RGPD], l'article 12 du RGPD précise que les responsables du traitement prennent des mesures appropriées pour fournir toute information visée aux articles 13 et 14 du règlement. Cela nécessite en outre que l'information ou la communication concernant le traitement des données à caractère personnel soit concise, transparente, compréhensible et aisément accessible. Les informations doivent être formulées en des termes clairs et simples et par écrit « ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique». Les lignes directrices du groupe de travail « Article 29» sur la transparence au sens du règlement (UE) 2016/679, telles qu'approuvées par l'EDPB, donnent des orientations spécifiques en vue de se conformer au principe de transparence dans les environnements numériques.

74. Conformément aux lignes directrices susmentionnées sur la transparence au sens du règlement (UE) 2016/679, l'article 11 du RGPD devrait être interprété comme un moyen de faire appliquer une véritable minimisation des données sans entraver l'exercice des droits des personnes concernées. Un tel exercice doit être rendu possible grâce aux informations complémentaires fournies par les personnes concernées. Des situations peuvent se présenter où un responsable du traitement traite des données à caractère personnel qui ne requièrent pas d'identifier une personne concernée (par exemple, des données pseudonymisées). Dans de tels cas, l'article 11, paragraphe 1, peut également être pertinent puisqu'il dispose qu'un responsable du traitement n'est pas tenu de conserver, d'obtenir ou de traiter des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter le RGPD.

75. Pour les services au titre de la DSP2, l'article 13 du RGPD est applicable aux données à caractère personnel collectées auprès de la personne concernée et l'article 14 est applicable lorsque les données à caractère personnel n'ont pas été obtenues de la personne concernée.

76. En particulier, la personne concernée doit être informée de la durée pendant laquelle les données à caractère personnel seront conservées ou, si ce n'est pas possible, des critères utilisés pour déterminer cette durée et, le cas échéant, des intérêts légitimes poursuivis par le responsable du traitement ou par un éventuel tiers. Lorsque le traitement est fondé sur le consentement visé à l'article 6, paragraphe 1, point a), du RGPD ou sur le consentement explicite visé à l'article 9, paragraphe 2, point a), du RGPD, la personne concernée doit être informée de son droit de retirer son consentement à tout moment.

77. Le responsable du traitement fournit les informations à la personne concernée, compte tenu des circonstances particulières dans lesquelles les données à caractère personnel sont traitées. Si les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée[38], ce qui sera probablement le cas pour les PSIC, les informations doivent être fournies au plus tard au moment de la première communication à ladite personne. Si des données à caractère personnel doivent être divulguées à un autre destinataire, les informations doivent être fournies au plus tard lorsque les données sont divulguées pour la première fois.

[38] Article 14, paragraphe 3, point b), du RGPD.

78. En ce qui concerne les services de paiement en ligne, les lignes directrices susmentionnées précisent que les responsables du traitement peuvent adopter une approche à plusieurs niveaux, par laquelle ils choisissent d'utiliser plusieurs méthodes pour garantir la transparence. Il est en particulier recommandé que les notes/chartes de protection des données personnelles soient structurées en plusieurs couches/niveaux afin de relier entre elles les différentes catégories d'informations à fournir à la personne concernée, au lieu d'afficher toutes ces informations sur une seule et même page, afin d'éviter de noyer d'informations la personne concernée tout en garantissant l'efficacité de l'information.

79. Les lignes directrices susmentionnées précisent aussi que les responsables du traitement peuvent choisir d'utiliser des outils de transparence supplémentaires pour fournir des informations à la personne concernée, tels que des tableaux de bord sur la protection de la vie privée. Un tableau de bord sur la protection de la vie privée est un lieu unique depuis lequel les personnes concernées peuvent visualiser les informations relatives à la confidentialité et gérer leurs préférences en permettant ou en empêchant que leurs données soient utilisées de certaines façons par le responsable du traitement en question[39]. Un tel tableau de bord peut donner une vue d'ensemble des PT qui ont obtenu le consentement explicite des personnes concernées et peut aussi fournir des informations utiles sur la nature et la quantité des données à caractère personnel auxquelles les PT ont eu accès. En principe, un PSPGC peut donner à l'utilisateur la possibilité de retirer son consentement explicite au titre de la DSP2[40] par l'intermédiaire du tableau de bord, ce qui se traduirait par un refus d'accéder à leurs comptes de paiement pour un ou plusieurs PT. L'utilisateur peut aussi demander à un PSPGC de refuser l'accès à leur(s) compte(s) de paiement à un ou plusieurs PT donnés[41], car l'utilisateur est en droit de (ne pas) recourir à un service d'information sur les comptes. Si des tableaux de bord sur la protection de la vie privée sont utilisés pour donner ou retirer un consentement explicite, ils devraient être conçus et appliqués dans le respect de la loi et, en particulier, pour empêcher la création d'obstacles au droit des PT de fournir des services conformément à la DSP2. À cet égard et conformément aux dispositions applicables au titre de la DSP2, un PT a la possibilité d'obtenir à nouveau le consentement explicite de l'utilisateur après que ce consentement ait été retiré.

80. Le principe de responsabilité impose au responsable du traitement de définir des mesures techniques et organisationnelles appropriées pour garantir et être en mesure de démontrer que le traitement est effectué conformément au RGPD, en particulier aux grands principes de protection des données prévus à l'article 5, paragraphe 1. Ces mesures devraient tenir compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que du risque que celui-ci présente pour les droits et libertés des personnes physiques, et doivent être révisées et mises à jour si nécessaire[42].

[39] Selon les lignes directrices du groupe de travail « Article 29 » sur la transparence au sens du règlement (UE) 2016/679 – approuvées par le CEPD, les tableaux de bord sur la protection de la vie privée sont particulièrement utiles lorsqu'un même service est utilisé par les personnes concernées sur une pluralité d'appareils différents, car cela leur donne accès à leurs données à caractère personnel et leur permet de les gérer sans égard à la façon dont elles utilisent le service. Permettre aux personnes concernées de régler manuellement leurs paramètres de confidentialité au moyen d'un tableau de bord sur la protection de la vie privée peut également faciliter la personnalisation d'un avis ou d'une déclaration sur la protection de la vie privée, en reflétant uniquement les types de traitement ayant lieu précisément pour cette personne concernée.

[40] Voir, par exemple, le «consentement explicite» mentionné à l'article 67, paragraphe 2, point a), de la DSP2.

[41] Voir également EBA/OP/2020/10, point 45.

[42] Article 5, paragraphe 2, et article 24 du RGPD.

6.5 Profilage

81. Le traitement des données à caractère personnel par des prestataires de services de paiement peut s'accompagner d'un « profilage » tel que visé à l'article 4, point 4), du RGPD. Par exemple, les PSIC peuvent s'en remettre au traitement automatique des données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique. La situation financière personnelle d'une personne concernée peut être évaluée, en fonction des spécificités du service. Les services d'information sur les comptes, à fournir sur demande des utilisateurs, peuvent nécessiter une évaluation approfondie des données sur les comptes de paiement personnels.

82. Le responsable du traitement doit aussi être transparent vis-à-vis de la personne concernée au sujet de l'existence d'une prise de décision automatisée, y compris un profilage. Dans ces cas, le responsable du traitement doit fournir des informations utiles concernant la logique sous-jacente, ainsi que l'importance des conséquences prévues de ce traitement pour la personne concernée [article 13, paragraphe 2, point f), et article 14, paragraphe 2, point g), et considérant 60][43]. De même, en vertu de l'article 15 du RGPD, la personne concernée a le droit de demander et d'obtenir du responsable du traitement des informations sur l'existence d'une prise de décision automatisée, y compris un profilage, sur la logique sous-jacente, ainsi que sur les conséquences pour la personne concernée et, dans certaines circonstances, sur le droit de s'opposer au profilage, indépendamment du fait qu'il s'agisse ou non d'une prise de décision individuelle exclusivement automatisée fondée sur le profilage[44].

83. En outre, un autre élément également pertinent dans ce contexte est le droit de la personne concernée de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire, tel que prévu par l'article 22 du RGPD. Cette norme inclut aussi, dans certaines circonstances, la nécessité pour les responsables du traitement, de mettre en place des mesures appropriées pour sauvegarder les droits de la personne concernée tels qu'une information spécifique de la personne concernée, le droit d'obtenir une intervention humaine dans le contexte de la prise de décision et d'exprimer son point de vue et de contester la décision. Comme également indiqué au considérant 71 du RGPD, cela signifie, entre autres, que les personnes concernées ont le droit de ne pas faire l'objet d'une décision, comme le rejet automatique d'une demande de crédit en ligne sans aucune intervention humaine[45].

84. La prise de décision automatisée qui implique des catégories particulières de données à caractère personnel n'est autorisée que dans les conditions cumulatives prévues à l'article 22, paragraphe 4, du RGPD:

- il existe une exception applicable en vertu de l'article 22, paragraphe 2;

[43] Lignes directrices sur la transparence au sens du règlement (UE) 2016/679, WP260rev.01 – approuvées par l'EDPB.
[44] Lignes directrices du groupe de travail «Article 29» relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, WP251rev.01
[45] Considérant 71 du RGPD.

- et le point a) ou g) de l'article 9, paragraphe 2, du RGPD s'applique. Dans les deux cas, le responsable du traitement doit mettre en place des mesures appropriées pour sauvegarder les droits et libertés de la personne concernée ainsi que ses intérêts légitimes[46].

85. Les exigences applicables au traitement ultérieur, telles qu'indiquées dans les présentes lignes directrices, devraient aussi être respectées. Les précisions et les instructions sur la prise de décision individuelle automatisée et le profilage fournies par les lignes directrices du groupe de travail « Article 29 » relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, telles qu'approuvées par l'EDPB, sont tout à fait pertinentes dans le contexte des services de paiement et devraient donc être dûment prises en considération.

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)

[46] Lignes directrices du groupe de travail «Article 29» relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, WP251rev.01, p. 24.