PROJET DE RECOMMANDATION

RELATIVE À L'EXERCICE DES DROITS PAR L'INTERMÉDIAIRE D'UN MANDATAIRE

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. La présente recommandation vise à proposer des modalités pratiques d'exercice des droits conférés par le Règlement (UE) 2016/679 (« RGPD ») par le bais de sociétés étant mandatées par les personnes (ci-après « les mandataires »), auprès d'organismes détenant ces données (ci-après « les responsables de traitement détenteurs des données » ou « responsables de traitement »).

2. Cette recommandation, notamment les exemples qui y sont proposés, n'est ni prescriptive ni exhaustive, et a pour seul objectif d'aider les mandataires et responsables de traitement dans leur démarche de mise en conformité. D'autres méthodes pour la mise en œuvre de l'exercice de droits par l'intermédiaire de sociétés mandatées peuvent être mises en œuvre, sous réserve qu'elles permettent d'être conforme aux textes en vigueur.

3. Cette recommandation est susceptible de faire l'objet de mises à jour et d'enrichissements afin d'intégrer, au fil du temps, les développements technologiques et les réponses aux questionnements exprimés tant par les organismes que par les personnes concernées.

Article 1er
Périmètre de la recommandation

1.1 – Normes juridiques et droits concernés

4. L'article 77 du décret d'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après « Informatique et Libertés ») prévoit qu'une demande d'exercice des droits peut être présentée par une personne spécialement mandatée à cet effet par le demandeur, si celle-ci justifie de son identité et de l'identité du mandant, de son mandat, ainsi que de la durée et de l'objet précis de celui-ci.

5. Les exemples donnés dans la présente recommandation sont plus spécifiquement relatifs à l'exercice du droit à la portabilité (article 20 du RGPD) et du droit d'accès (article 15 du RGPD). Toutefois, la Commission invite les mandataires qui choisiraient de proposer des services d'exercice d'autres droits conférés par le RGPD à se référer également à la présente recommandation, pour les parties qui s'appliqueraient à leur activité.

6. Les acteurs assujettis à la directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (ci-après « DSP2 ») peuvent également se référer à la présente recommandation, dans les conditions présentées ci-dessous.

1.2 – Traitements et acteurs concernés

7. La présente recommandation concerne tous les traitements tels que définis par l'article 4 du RGPD, qui sont mis en œuvre dans le cadre d'une demande d'exercice de droits par le biais d'un mandataire.

8. Une demande d'exercice de droits par le biais d'un mandataire se déroule en général en quatre ou cinq étapes :

- la création d'une relation contractuelle entre la personne concernée (le mandant) et le mandataire ;
- l'établissement d'un mandat spécifique, ainsi que la transmission de la demande d'exercice de droits au responsable de traitement;

- la transmission des données par le responsable de traitement à la personne concernée ou au mandataire ;
- la transmission des données par le mandataire à la personne concernée, ou à un autre responsable de traitement (dans le cadre d'une demande de portabilité), ou le stockage des données ; et
- le cas échéant, la réutilisation par le mandataire des données ainsi obtenues.

9. La présente recommandation concerne, en premier lieu, l'ensemble des responsables de traitement détenteurs des données qui reçoivent des demandes d'exercice des droits par le biais de sociétés mandatées.

10. Ces responsables peuvent être des entités publiques ou privées, pouvant être soumises à des réglementations sectorielles particulières venant préciser certaines caractéristiques de leurs traitements.

11.A cet égard, la Commission a été interrogée sur l'interaction entre les dispositions de la DPS2 relatives aux conditions de mise en œuvre de certains traitements de données à caractère personnel, par rapport aux dispositions générales du RGPD.

12. La Commission relève que la DSP2 précise les conditions dans lesquelles les acteurs assujettis doivent mettre à disposition et transmettre certaines données, pour les activités entrant dans son champ d'application. Plus précisément, si une demande est adressée à un prestataire gestionnaire de compte par un prestataire d'information sur les comptes ou un prestataire d'initiation de paiement pour accéder à des données de paiement, les modalités d'accès et de transmission sont prévues par la DSP2. Si, dans ce cas, la DSP2 est pleinement applicable aux opérations qu'elle vise spécifiquement, le RGPD aura vocation à s'appliquer aux traitements de données à caractère personnel mis en œuvre pour tous les aspects sur lesquels la DSP2 reste silencieuse.

13. Par ailleurs, dans les cas où l'ensemble des critères d'application de la DSP2 (liés aux acteurs concernés, aux données sur lesquelles porte la demande, et à la nature du service fourni) n'est pas réuni, le RGPD et, par là-même, la présente recommandation, trouveront à pleinement s'appliquer.

14. En second lieu, la présente recommandation concerne les mandataires qui proposent aux personnes concernées d'exercer les droits qui leur sont conférés par le RGPD par leur intermédiaire. Ne sont donc pas directement concernés les acteurs proposant des outils facilitateurs d'exercice de droits (par exemple ceux fournissant une plateforme sur laquelle les personnes concernées ont accès à des demandes pré-rédigées qu'elles envoient elles-mêmes), ou ceux qui jouent le rôle de connecteurs et de facilitateurs de transmission dans le cadre d'une demande de portabilité.

Article 2
Qualification des rôles et responsabilités

15. La Commission rappelle que les acteurs doivent effectuer une analyse préalable à la mise en œuvre du traitement quant à la qualification de leur rôle. Elle invite les acteurs à se référer aux documents publiés par le Comité européen sur la protection des données (CEPD) sur la notion de responsable de traitement et de sous-traitant.

16. La Commission constate que, d'une manière générale, chaque acteur, qu'il soit un responsable de traitement recevant une demande d'exercice de droit, ou une société mandatée par la personne concernée, est un responsable de traitement séparé, à moins que les acteurs déterminent ensemble les moyens et les finalités du traitement : dans ce cas spécifique, une responsabilité conjointe peut être dégagée.

17. Enfin, la Commission invite les acteurs à collaborer autant que possible, afin de faciliter l'exercice des droits des personnes et à ne pas créer de conditions additionnelles, dépourvues de fondement juridique, qui feraient obstacle à l'aboutissement d'une demande d'exercice de droits.

Article 3
L'entrée en relation contractuelle entre la personne concernée et le mandataire

18. Comme dans toute entrée en relation contractuelle entre un organisme et une personne concernée, un certain nombre de traitements ayant pour finalité la gestion contractuelle sont mis en œuvre. La Commission considère qu'il n'existe pas pour cette étape de spécificités liées à la collecte et à la conservation de ces données lorsque le mandataire propose des services d'exercice des droits.

19. La Commission rappelle que si le mandataire estime devoir s'assurer de l'identité de la personne concernée avant d'entrer en relation commerciale avec elle, la consultation d'un justificatif suffit généralement, sans que cette donnée soit nécessairement stockée. Toutefois, le mandataire peut exceptionnellement conserver la pièce d'identité afin d'anticiper les cas spécifiques où le responsable de traitement aurait des doutes raisonnables sur l'identité de la personne. Pour la conservation de cette donnée, la Commission recommande de déployer de mesures de sécurité renforcées, telles que :

- la conservation sous une forme adaptée, par exemple en limitant la qualité de l'image numérisée, en intégrant un filigrane comportant la date de collecte et l'identité du responsable de traitement ou en mettant en place des mécanismes de chiffrement des pièces d'identité numérisées ;
- une gestion stricte des habilitations (accès uniquement aux contrôleurs de gestion ou service de recouvrement, par exemple) ;
- la mise en place de mécanismes d'authentification des utilisateurs ;
- la mise en place d'un système de journalisation des accès aux pièces d'identité, conservant pendant une durée de six mois glissants l'identifiant du collaborateur ayant accédé à une pièce d'identité, la référence de la pièce d'identité consultée, ainsi que l'horodatage de la consultation, associés à des mécanismes d'analyse automatiques afin de détecter des accès non autorisés ; et
- l'utilisation d'un logiciel spécialisé de destruction des données lors de leur suppression.

Article 4
Sur l'établissement du mandat et sur son contenu

20. La Commission rappelle que conformément à l'article 77 du décret « Informatique et libertés », le mandataire doit être « spécialement mandaté » par la personne concernée,

sachant que la durée et l'objet précis du mandat doivent être spécifiés, et que le mandataire doit être en mesure de justifier de son mandat.

21. Ainsi, bien que certains aspects d'une demande d'exercice de droits par le biais d'un mandataire puissent être traités dans le cadre de conditions générales d'utilisation (comme par exemple la durée de conservation, les droits que le mandataire propose d'exercer par son intermédiaire, etc.), la Commission relève qu'une clause générale risquerait d'être insuffisante, en principe, pour répondre au caractère spécifique du mandat en ce qui concerne (i) les données visées par la demande ; (ii) les responsables de traitement destinataires de la demande ; (iii) les données d'identification transmises au responsable de traitement ; (iv) les droits exercés ; et (v) la durée du mandat. Afin d'aider les mandataires dans la formalisation de leurs mandats, la Commission tient à leur disposition sur son site web un exemple de mandat-type, auquel les mandataires, ainsi que les responsables de traitement détenteurs de données peuvent se référer.

22. Par ailleurs, la Commission rappelle que les responsables de traitement auxquels une demande est adressée ne doivent pas procéder à la transmission des données sans s'être assurés au préalable de sa validité. Il leur incombe ainsi de s'assurer de l'identité de la personne concernée et de la véracité du mandat.

23. Par conséquent, afin de faciliter la mise en œuvre de cette obligation, la Commission recommande au mandataire de s'assurer que le mandat contienne tous les éléments permettant aux responsables de traitement (i) d'identifier la personne à l'origine de la demande d'exercice du droit ; (ii) de s'assurer de l'authenticité du mandat ; et (iii) d'identifier le destinataire auquel les données doivent être transmises.

24. Enfin, la Commission rappelle que le mandataire doit porter une attention particulière au respect du principe de minimisation des données, en vertu de l'article 5 du RGPD. Le mandataire doit ainsi procéder à une analyse en amont en vue de s'assurer de la pertinence des données transmises au responsable de traitement dans le mandat. Dans cette perspective, la Commission propose que les mandataires se réfèrent aux paragraphes ci-dessous, ainsi qu'au mandat-type mis en ligne sur le site web de la Commission.

4.1 – Les données permettant au responsable de traitement d'identifier la personne concernée

25. La Commission recommande de laisser dans le mandat le champ libre à la personne concernée afin qu'elle renseigne elle-même les données qu'elle considère comme pertinentes pour permettre au responsable de traitement de l'identifier (identifiant, date de naissance, date de dernière connexion, par exemple).

26. La Commission préconise par ailleurs que le mandat rappelle à la personne concernée que sa pièce d'identité ne devrait être transmise à l'appui de la demande que si le responsable de traitement la connait sous son identité régalienne (par exemple, dans le cadre d'une relation avec une banque). En d'autres termes, la Commission est d'avis que si le responsable de traitement connaît la personne sous un pseudonyme, la transmission de la pièce d'identité avec la demande de mandat pourrait ne pas être justifiée.

4.2 – Les données permettant au responsable de traitement de s'assurer de l'authenticité, de l'étendue et de la durée du mandat

27. Dans la mesure où il incombe au responsable de traitement détenteur des données de s'assurer de l'authenticité du mandat, il est recommandé que des mesures lui permettant de mettre en œuvre cette obligation soient prises en amont par les mandataires.

28. Dans certains cas, le recours à la signature électronique simple peut être envisagé afin de vérifier l'identité et la volonté de la personne concernée d'établir le mandat. Elle permet également de garantir que le mandat n'a subi aucune modification depuis sa signature par la personne concernée.

29. Le responsable de traitement doit également être en mesure d'identifier, à travers le mandat, les données faisant l'objet de la demande, la nature des droits exercés et la durée du mandat.

30. Le mandat peut ainsi inviter expressément la personne concernée à préciser sa demande, en fonction notamment des catégories de données faisant l'objet de l'exercice du droit (par exemple, toutes les données relatives à ses interactions avec le service-client), ou en fonction des finalités du traitement (par exemple, toutes les données collectées pour faciliter le paiement), ou par service fourni par le responsable de traitement (par exemple, un service de billetterie), ou par droit qu'elle souhaite exercer (si le mandataire le propose parmi ses services).

31. Enfin, conformément à l'article 77 du décret « Informatique et Libertés », la durée du mandat doit être indiquée, ce qui implique que l'échéance à laquelle le mandat prend fin doit être déterminée ou déterminable. Ainsi, la Commission considère qu'un mandat établi pour une durée indéfinie ne répond pas à l'exigence de l'article 77 du décret. Par exemple, les missions devant être accomplies par le mandataire peuvent être précisément listées, et il peut être indiqué que l'accomplissement de ces dernières entrainera la résiliation automatique du mandat. Par ailleurs, la Commission rappelle qu'en application de l'article 2004 du code civil, la personne concernée a le droit de révoquer le mandat à tout moment. La Commission recommande que lorsque la personne concernée révoque son mandat, le mandataire avise les responsables de traitement auprès desquels des demandes d'exercice des droits ont été adressées et qui sont toujours en cours de traitement.

4.3 – Les données permettant au responsable de traitement d'identifier les destinataires des données

32. Le mandat doit préciser si le mandataire peut être rendu destinataire des données, conformément à l'article 77 du décret. Pour assurer une transmission fluide des données, l'adresse (postale ou électronique) vers laquelle les données doivent être acheminées peut également être précisée.

33. Dans les cas où le destinataire des données n'est pas précisé dans le mandat, la Commission recommande que les données soient transmises par défaut à la personne concernée.

Article 5
Sur les demandes d'exercice de droit par voie électronique

34. L'article 12 alinéa 3 du RGPD prévoit que lorsque la personne concernée présente sa demande sous une forme électronique, les informations sont fournies par voie électronique si cela est possible, à moins que la personne concernée ne demande qu'il en soit autrement.

Cet article implique que la personne concernée dispose d'une certaine maîtrise sur le canal par lequel elle choisit de présenter sa demande. Par conséquent, si cela lui est techniquement faisable, la Commission recommande que le mandataire offre à la personne concernée la possibilité de choisir le canal par lequel elle souhaite exercer sa demande (c'est-à-dire par voie postale ou par voie électronique), sachant que la voie électronique peut être considérée comme la voie par défaut.

35. Par ailleurs, la Commission note que dans le cas d'une demande par voie électronique, les mandataires peuvent souhaiter avoir recours aux API ou à la technique dite d'« aspiration » (« scraping »). Dans ce contexte, la Commission recommande les principes édictés ci-dessous.

5.1 - Les demandes d'exercice de droit *via* l'utilisation d'une API

36. La Commission constate que les demandes d'exercice de droit par le biais d'un mandataire peuvent être réalisées par le biais d'une interface de programmation applicative (ci-après « API »).

37. La Commission constate que les API permettent de réduire considérablement la charge des responsables de traitement dans le traitement des demandes d'exercice de droits. La Commission encourage ainsi les responsables de traitement détenteurs de données et les mandataires à avoir recours à cette technique, notamment lorsqu'ils doivent traiter une quantité importante de demandes d'exercice de droits, dans la mesure où elle permet une transmission fluide de données à caractère personnel.

38. Par ailleurs, quand les responsables de traitement fournissent un accès par API, la Commission recommande que l'accès à l'API soit stable, qu'elle ait un niveau de disponibilité élevé, et que des mesures de sécurité adaptées aux risques soient mises en œuvre.

39. Le recours à une API peut être particulièrement pertinent si une mise à jour régulière des données est nécessaire pour que le mandataire puisse fournir le service à la personne concernée (par exemple, dans le cadre d'un service d'alerte à l'arrivée d'une nouvelle facture téléphonique).

40. Enfin, lorsque des API sont développées afin de se conformer aux exigences du règlement délégué (UE) 2018/389, la Commission encourage les acteurs assujettis à la DSP2 à étendre leur usage aux données n'entrant pas dans le champ de la DSP2, afin de pouvoir répondre de manière sécurisée et avec plus de fluidité aux demandes d'exercice des droits qu'ils pourraient recevoir.

5.2 – Les demandes d'exercice de droit via l'utilisation de la technique d'« aspiration » (« *scraping* »)

41. De manière générale, la Commission recommande que les mandataires s'abstiennent de récupérer auprès de la personne concernée son identifiant et son mot de passe en vue d'extraire des données la concernant qui sont affichées sur le site du responsable de traitement. En effet, cette technique peut poser des problèmes en matière de sécurisation des échanges de données, de limitation et de pertinence des données extraites.

42. Toutefois, dans certaines situations, le responsable de traitement peut exceptionnellement décider de permettre l'accès aux données affichées sur son site par

aspiration. Dans ce cas, la Commission recommande qu'en amont de l'exercice du droit, le responsable de traitement et le mandataire procèdent à une analyse de risques afin d'évaluer la sensibilité des données et des opérations qui peuvent être menées sur leur site web, et de mettre en œuvre les mesures de sécurité adéquate afin que ces risques soient maitrisés.

43. Par exemple, ces mesures peuvent consister en la mise en place d'une authentification dédiée au mandataire, la mise à disposition d'une version dégradée du site contenant uniquement les informations auxquelles le mandataire doit avoir accès, ou l'usage d'un mot de passe temporaire sur le compte utilisateur dédiée au mandataire.

44. Enfin, s'il s'avère que les mandataires ne sont pas en mesure de répondre aux missions qui leur ont été confiées par la personne concernée (par exemple, si les responsables de traitement détenteurs de données ne répondent pas à une demande effectuée à plusieurs reprises), la Commission considère qu'ils peuvent exceptionnellement avoir recours à l'aspiration (« *scraping* »), en mettant en place les dispositifs suivants : (i) le mandat doit prévoir le recueil d'un consentement explicite de la personne concernée au recours à cette technique ; (ii) la personne concernée doit avoir été pleinement informée des risques encourus ; (iii) le responsable de traitement devrait avoir été prévenu en amont qu'une aspiration va être mise en œuvre ; (iv) le mandataire devrait être en mesure de fournir le mandat au responsable de traitement si ce dernier en fait la demande, et ce, même si les données ont déjà été transmises ; et (v) le mot de passe utilisé ordinairement par l'utilisateur ne devrait pas être transmis au mandataire. Pour veiller au respect de la condition (v), la Commission recommande aux mandataires de mettre en place un système permettant que l'aspiration soit réalisée *via* le navigateur de la personne concernée (par exemple, par une extension spécifique dans le navigateur) ou, à défaut, qu'il fasse remplacer le mot de passe de l'utilisateur par un mot de passe temporaire, avant et après l'accès à son compte.

Article 6
Sur la réponse apportée par le responsable de traitement à la demande d'exercice de droits

6.1 – Sur la prorogation du délai de réponse lorsqu'une demande est complexe

45. Conformément à l'article 12 alinéa 3 du RGPD, le responsable du traitement doit informer la personne sur les mesures prises pour répondre à sa demande, dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande. Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes.

46. La Commission rappelle que le responsable de traitement doit être en mesure de démontrer la complexité de la demande, et considère que le simple fait qu'une demande est exercée par le biais d'un mandataire ne suffit pas à proroger automatiquement le délai de réponse.

47. Par ailleurs, la Commission considère que le mandataire devrait jouer pleinement son rôle d'intermédiaire entre le responsable de traitement et la personne concernée. Par exemple, si le responsable de traitement accuse réception de la demande, ou s'il répond en informant qu'une prolongation de deux mois est nécessaire, le mandataire devrait transmettre ces informations à la personne concernée.

6.2 – Sur la transmission des données du responsable de traitement au mandataire

48. En ce qui concerne le format technique des données, la Commission rappelle que l'article 20 du RGPD énonce que les données doivent être transmises dans un format couramment utilisé, c'est-à-dire dans un format que des systèmes doivent être en mesure de traiter de manière automatisée. Bien que cet article ne soit relatif qu'aux données faisant l'objet d'une demande de portabilité, la Commission encourage les responsables de traitement et les mandataires à avoir recours à des formats standards globaux ou à l'échelle d'un secteur, et de préférence ouverts et documentés (par exemple XML, JSON, CSV, assortis de métadonnées utiles au meilleur niveau de granularité possible, tout en maintenant un niveau d'abstraction élevé) pour répondre aux demandes d'exercice des droits.

49. En ce qui concerne le canal de transmission, l'article 12 du RGPD énonce que lorsque la personne concernée présente sa demande sous une forme électronique, les informations sont fournies par voie électronique. La Commission constate ainsi que le RGPD pose un principe de parallélisme des formes. Ainsi, si le mandataire a mis en place des mesures permettant à la personne concernée d'exercer sa demande par voie postale, des mesures similaires devraient être prises permettant de recevoir les données par ce même canal.

Article 7
Sur le refus de faire droit à une demande d'exercice de droits par le biais d'un mandataire

7.1 - Lorsque la demande est manifestement infondée ou excessive

50. L'article 12 alinéa 5 b) du RGPD énonce que lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le responsable de traitement peut refuser de donner suite à ces demandes. La Commission considère que le caractère excessif ou infondé d'une demande devrait faire l'objet d'une appréciation au cas par cas par le responsable de traitement détenteur des données, et que le terme « manifestement » implique que le caractère excessif ou infondé soit indéniable et évident.

51. Sur le caractère manifestement infondé, la Commission estime que le simple fait qu'une demande est effectuée par le biais d'un mandataire ne suffit pas à considérer qu'elle est infondée. Par ailleurs, la Commission rappelle que les responsables de traitement détenteurs des données ne sont pas responsables des utilisations ultérieures que feraient les mandataires une fois que les données ont été transmises. En d'autres termes, le caractère infondé ne devrait pas être caractérisé par ces réutilisations qui relèvent entièrement de la responsabilité du mandataire.

52. Sur le caractère manifestement excessif, la Commission rappelle que la quantité de données faisant l'objet de la demande ne constitue pas, en soi, une justification suffisante pour considérer qu'une demande est manifestement excessive.

53. En outre, la Commission a été interrogée sur le point de savoir si le caractère répétitif de demandes d'exercice de droits pouvait être considéré comme étant manifestement excessif. La Commission rappelle sur ce point que le CEPD considère dans ses lignes directrices relatives au droit à la portabilité que les cas dans lesquels le responsable de traitement peut refuser de fournir les informations demandées devraient être très rares, même lorsqu'il est

question de demandes multiples. La Commission estime que ce principe pourrait être applicable à l'exercice des autres droits conférés par le RGPD.

54. Plus précisément, la Commission considère que le renouvellement d'une demande d'exercice de droits pourrait être considéré comme excessif si une demande rigoureusement similaire a déjà été adressée au responsable de traitement détenteur des données, alors que (i) cette demande porte sur le même ensemble de données et les mêmes droits ; (ii) qu'aucune réponse n'a encore été délivrée et que (iii) le délai de réponse (un mois pouvant être prorogé de deux mois) dont dispose le responsable de traitement n'est pas encore écoulé.

55. En revanche, le renouvellement d'une demande qui porte sur le même ensemble de données et sur les mêmes droits ne devrait pas être considéré comme excessif si le délai de réponse est écoulé et que le responsable de traitement n'a pas répondu à la demande, ou qu'il a répondu de manière insatisfaisante (par exemple, il n'a pas correctement rectifié les données, ou n'a pas procédé au transfert de l'ensemble des données portables).

56. S'il a déjà été donné entièrement satisfaction à une première demande par le responsable de traitement, les conditions dans lesquelles une demande relative au même ensemble de données et pour les mêmes droits peut être renouvelée sont généralement liées à des évènements ponctuels, comme par exemple :

- le souhait de la personne concernée d'ajouter un nouveau destinataire à sa demande de portabilité des données ; ou
- lorsque la personne concernée peut raisonnablement considérer que de nouvelles données sont apparues ou que les modalités de traitement ont évolué, comme l'indique le considérant 63 du RGPD.

57. En ce qui concerne l'ajout d'un nouveau destinataire dans le cadre d'une demande de portabilité, la Commission encourage le mandataire à mettre en place un mécanisme permettant à la personne concernée d'ajouter directement sur sa plateforme un nouveau destinataire, si les données ont été conservées par le mandataire, afin d'éviter de renouveler la demande de portabilité auprès du responsable de traitement.

58. Dans tous les cas, la Commission recommande que la personne concernée puisse déterminer librement l'étendue de sa demande et renouveler, par le biais d'un nouveau mandat, ses demandes d'exercice de droits auprès du mandataire, si elle le souhaite. En tant que bonne pratique, le mandataire peut lui conseiller de cibler sa demande de renouvellement (par exemple, sur une nouvelle fenêtre temporelle) ou de préciser les raisons pour lesquelles elle estime qu'un renouvellement est nécessaire.

59. D'une manière générale, la Commission recommande de ne pas prévoir de renouvellement par défaut ou de périodicité d'un mandat, sauf si :

- la nature du traitement permet d'anticiper que des modifications seront régulièrement apportées et que le mandataire propose un service de mise à jour périodique des données ; ou si
- la transmission des données se fait par l'intermédiaire d'une API. En effet, comme expliqué dans l'article 5 de la présente recommandation, le recours à une API permet de réduire considérablement la charge relative au traitement de demandes d'exercice de droits répétitives et réduit la probabilité que des demandes puissent être considérées comme imposant une charge excessive.

60. Enfin, la Commission rappelle que si le responsable de traitement refuse de faire droit à la demande d'exercice de droits, il devra, en application de l'article 12 alinéa 6 du RGPD, justifier des motifs de son refus. Cette justification pourra s'effectuer auprès du mandataire, qui devra en informer la personne concernée. La personne concernée pourra alors déposer une plainte auprès de la Commission ou former un recours juridictionnel si elle considère que ce refus est injustifié.

7.2 - Lorsque le responsable de traitement a des doutes raisonnables sur l'identité de la personne concernée

61. De manière générale, la Commission rappelle que le fait qu'une demande soit exercée par l'intermédiaire d'un mandataire ne doit pas, en principe, conduire à considérer *a priori* qu'il existe des doutes raisonnables quant à l'identité de la personne. Ainsi, si les informations préalablement fournies dans le mandat sont suffisantes, il n'est en principe pas nécessaire de collecter des informations supplémentaires. En revanche, ces doutes raisonnables peuvent par exemple être caractérisés en cas d'homonymie.

62. Dans les cas spécifiques où le responsable de traitement aurait des doutes raisonnables sur l'identité de la personne, notamment lorsque la personne a recours à un pseudonyme qui ne concorde pas avec les informations détenues par le responsable de traitement, ce dernier peut collecter des informations supplémentaires pour confirmer son identité, sachant qu'une attention spécifique doit être portée au principe de pertinence des données. Par exemple, si le responsable de traitement ne connait pas la personne sous son identité régalienne, la collecte de la pièce d'identité pour procéder à des vérifications supplémentaires n'est en principe pas pertinente.

63. Par ailleurs, la Commission relève que le responsable de traitement peut aussi bien se tourner vers le mandataire que vers la personne concernée pour la collecte d'informations supplémentaires. Elle invite dans ce dernier cas le responsable de traitement à veiller à tenir le mandataire informé de cette démarche. Par exemple, il peut mettre en place des mécanismes d'authentification permettant à la personne concernée de se connecter au service en ligne avec ses identifiants et lui demander de confirmer que la demande émane bien d'elle. Le responsable de traitement peut également la contacter directement en vue de vérifier la concordance avec des informations dont il dispose déjà (historique d'achats, numéro de carte de fidélité, etc…).

64. Enfin, dans le champ d'application de la DSP2, la Commission considère que la mise en œuvre des obligations relatives aux modalités d'accès aux données et de transmission des données, telles qu'exigées par le Règlement Délégué (UE) 2018/389 de la Commission du 27 novembre 2017, sont suffisantes pour que le prestataire gestionnaire de compte n'ait pas de doute raisonnable sur l'identité de la personne concernée.

7.3 - Sur le motif que la réponse à la demande d'exercice de droits ne serait pas techniquement possible

65. La Commission constate que lorsque la réponse est fournie sous une forme électronique, la transmission des données peut se faire soit par le biais d'une transmission directe, soit par le biais d'outils automatisés permettant l'extraction des données pertinentes (comme par exemple les API).

66. La Commission encourage les responsables de traitement et les mandataires à développer des systèmes standardisés, afin de réduire les entraves techniques qui font obstacle à la transmission directe des données. L'adoption des technologies standardisées peut se faire à plusieurs niveaux :

- au niveau du transfert des données, notamment dans le cadre de la portabilité des données lors de l'établissement du protocole de communication entre les responsables de traitement (des protocoles largement utilisés sont recommandés, comme REST HTTP/S, SOAP, etc.) ;
- au niveau du format des données, afin que le contenu de celles-ci puisse être aisément interprétable par un autre responsable de traitement ;
- au niveau de la sémantique des données, c'est-à-dire de leur signification dans un contexte en particulier. Afin de faciliter la compréhension du modèle des données, de la documentation, des documentations et des langages sémantiques ou de modélisation (tels qu'UML) peuvent être utilisés.

67. La Commission considère que le simple fait que le mandataire et le responsable de traitement n'ont pas développé des mécanismes de transmission similaires (directe ou par outil automatisé) ne suffit pas à conclure que l'exercice de droit est techniquement impossible. Il conviendra ainsi que le mandataire et le responsable de traitement déploient des efforts raisonnables en vue de trouver des solutions techniques permettant la bonne transmission des données.

68. Enfin, la Commission relève que dès lors que des API ont été développées afin de se conformer aux exigences de la DSP2 et qu'elles sont en état de fonctionnement, la transmission directe de données d'une banque vers un prestataire des services d'information sur les comptes et d'initiation de paiement paraît « techniquement possible », y compris dans les cas spécifiques où la DSP2 ne s'applique pas.

Article 8
Sur les traitements mis en œuvre par le mandataire lorsque les données ont été transmises par le responsable de traitement

8.1 - Sur la restructuration/réorganisation des données

69. En ce qui concerne la possibilité pour le mandataire de restructurer les données avant de les transmettre à la personne concernée, la Commission invite les mandataires à informer clairement les personnes, en précisant dans le contrat conclu avec la personne concernée si cette réorganisation fait partie intégrante du service proposé ou si la personne concernée peut recevoir les données brutes.

8.2. - Sur la conservation des données par le mandataire

70. En ce qui concerne les durées de conservation des données transmises par le responsable de traitement dans le cadre de l'exercice du droit, elles doivent en principe être supprimées, une fois la finalité du traitement découlant du mandat atteinte, ce qui correspond en principe à la transmission des données à la personne concernée ou à un autre responsable de traitement (notamment dans le cadre d'une demande de portabilité).

71. Toutefois, les données peuvent être conservées si une telle conservation fait partie intégrante du service ou si une réutilisation est prévue dans les conditions posées par l'article 9 ci-dessous.

72. De manière générale, la Commission recommande que les mesures suivantes soient prises pour les modalités de conservation des données :

- mettre en place une politique de gestion du contrôle d'accès aux données, qui doit être garanti aux seules personnes autorisées, afin de se prémunir contre la destruction, la violation et la modification par des personnes malveillantes ;
- mettre en place la journalisation des accès et modifications apportées ;
- si les données sont de nature sensible, garantir leur confidentialité par des mesures de chiffrement avec une gestion de clés sous l'unique contrôle de l'utilisateur ;
- si les données sont importantes, garantir leur disponibilité et mettre en place des mécanismes de réplication afin de pouvoir les restaurer en cas de perte ;
- mettre en place une politique de suppression une fois que la durée de conservation prévue sera atteinte.

Article 9
Sur la réutilisation des données transmises au mandataire

73. Tout d'abord, la Commission rappelle que les responsables de traitement répondant à des demandes d'exercice de droits ne sont pas responsables des traitements subséquents effectués par le mandataire.

74. Si le mandataire souhaite réutiliser les données, la Commission estime que cette réutilisation s'apparente à un traitement ayant une finalité propre, qu'il conviendra de distinguer des traitements mis en œuvre dans le cadre de l'exercice des droits. La Commission rappelle que ce nouveau traitement devra être licite et conforme à toutes les dispositions du RGPD.

75. Le mandataire devra notamment fournir à la personne concernée, avant de mettre en œuvre les traitements, toutes les informations pertinentes et utiles sur ces nouveaux traitements, d'une manière claire, concise et transparente, en application de l'article 13 du RGPD. Ainsi, la personne devra être en mesure de comprendre précisément ce qui sera fait des données la concernant.

76. La Commission encourage également les mandataires à proposer un choix granulaire, par type de données et d'utilisation. Ainsi, la personne concernée devrait avoir le choix de décider au cas par cas des réutilisations qu'elle permet. En tant que bonne pratique, la Commission recommande que ce soit le mandat qui prévoie si la personne est d'accord qu'une réutilisation des données soit faite, à condition que cette réutilisation soit faite conformément aux exigences du RGPD.

77. Si cette réutilisation n'a pas été prévue dès l'entrée en relation contractuelle entre la personne concernée et le mandataire, ce dernier devra procéder à une analyse de compatibilité entre les finalités en application de l'article 6(4) du RGPD et disposer d'une base légale valable. Ainsi, la Commission estime que dans la grande majorité des cas, le consentement valable de la personne sera nécessaire avant de procéder à toute réutilisation des données transmises dans le cadre de l'exercice de droit, à moins que cette réutilisation ait

un lien fort avec cet exercice (par exemple, si le mandataire propose à la personne de centraliser toutes les données transmises par différents responsables de traitement dans un espace personnel), et que les autres critères de compatibilité énumérés à l'article 6(4) soient remplis.

78. Par ailleurs, la Commission rappelle qu'il appartient aux mandataires de s'assurer qu'ils respectent les autres réglementations périphériques au RGPD qui peuvent par ailleurs trouver à s'appliquer, notamment le droit de la concurrence ou le droit des producteurs de bases de données.

79. Enfin, la Commission rappelle que le droit d'obtenir une copie des données ne doit pas porter atteinte aux droits et libertés d'autrui (article 15 alinéa 4 du RGPD), et que le droit à la portabilité ne porte pas atteinte aux droits et libertés de tiers (article 20 alinéa 4 du RGPD). A ce titre, le CEPD considère que les droits et libertés des tiers ne sont pas respectés si le nouveau responsable du traitement utilise leurs données à des fins qui lui sont propres. Ainsi, la Commission estime que les mandataires ne devraient pas réutiliser les données relatives à des tiers pour leurs propres finalités.

Article 10
Sur la sécurité de la transmission des données

80. En ce qui concerne la sécurité des données transmises directement aux utilisateurs finaux, la Commission recommande que les mesures suivantes soient mises en œuvre par l'entité expéditrice (responsable du traitement ou mandataire) :

- assurer la confidentialité des données échangées lors de leur transmission, par exemple en chiffrant les communications avec des algorithmes et des clés à l'état de l'art ;
- assurer que seule la personne concernée peut accéder à ses données. Cela peut se traduire par la possibilité d'accéder aux données depuis un compte utilisateur accessible uniquement après authentification, ou par le partage d'un secret par un canal de communication différent de celui par lequel les données sont transmises, permettant de déchiffrer les données lorsqu'elles sont accessibles depuis un environnement non authentifié ;
- mettre en œuvre un mécanisme de traçabilité illustrant le parcours des données.

81. En ce qui concerne les mesures de sécurité lorsque les données sont transmises au mandataire ou à un responsable de traitement tiers, la Commission recommande que les mesures suivantes soient mises en œuvre :

- assurer la confidentialité des données échangées lors de leur transmission en chiffrant les communications avec des algorithmes et des clés à l'état de l'art ;
- mettre en place des mécanismes d'authentification mutuelle des entités concernées ;
- avoir recours à des mécanismes d'authentification forte pour l'authentification des personnels habilités à accéder aux données ;
- mettre en place des mécanismes de traçabilité des accès aux données, associés à une conservation des journaux de traçabilité pendant une durée de 6 mois et à des mécanismes d'analyse automatique de ces données.