Délibération n° 2021-070 du 27 mai 2021 portant adoption d'une recommandation relative à l'exercice des droits par l'intermédiaire d'un mandataire

La Commission nationale de l'informatique et des libertés,

Vu le 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 (« RGPD ») ;

Vu la directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE (« DSP2 ») ;

Vu le 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 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Après avoir entendu le rapport de Mme Anne DEBET, commissaire, et les observations de M. Benjamin TOUZANNE, commissaire du Gouvernement,

Formule les observations suivantes :

1. La présente recommandation vise à proposer des modalités pratiques d'exercice des droits conférés par le RGPD par le biais de personnes physiques ou morales (les mandataires) mandatées par les personnes souhaitant exercer ces droits (les mandants) auprès d'organismes détenant ces données (les responsables de traitement détenteurs des données).

2. Cette recommandation, notamment les exemples qui y sont proposés, n'est ni prescriptive ni exhaustive et a pour 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 mandataires peuvent être envisagées si elles sont conformes aux textes en vigueur.

Les données personnelles nécessaires à l'accomplissement des missions de la CNIL sont traitées dans des fichiers destinés à son usage exclusif.
Les personnes concernées peuvent exercer leurs droits Informatique et Libertés en s'adressant au délégué à la protection des données (DPO) de la CNIL via un formulaire en ligne ou par courrier postal. Pour en savoir plus : www.cnil.fr/donnees-personnelles.

Article 1er
Périmètre de la recommandation

1.1 – Normes juridiques et droits concernés

3. 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 loi « Informatique et Libertés ») prévoit qu'une demande d'exercice des droits (information, accès, rectification, effacement, limitation du traitement, portabilité et/ou opposition) 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.

4. Les exemples donnés dans la 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.

1.2 – Traitements et acteurs concernés

5. La 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.

6. Une demande d'exercice de droits par le biais d'un mandataire se déroule en général en six, voire sept étapes :

- la création d'une relation contractuelle entre la personne concernée (le mandant) et le mandataire ;
- l'établissement d'un mandat spécifique ;
- la transmission par le mandataire 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 ;
- le cas échéant, la conservation par le mandataire des données ainsi obtenues dans un espace accessible à la personne concernée ;
- l'éventuelle réutilisation de ces données par le mandataire.

7. La 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 mandataires.

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

9. Concernant l'interaction entre les dispositions de la DSP2 relatives aux conditions de mise en œuvre de certains traitements de données à caractère personnel et les

dispositions du RGPD, si une demande est adressée à un prestataire gestionnaire de compte par un prestataire d'information sur les comptes, les modalités d'accès et de transmission de ces données sont celles prévues par la DSP2. Elles impliquent notamment l'exigence d'un agrément délivré par l'ACPR et le respect d'obligations spécifiques en matière de sécurité.

10. L'article L. 314-1 du code monétaire et financier liste les services de paiement soumis à cette réglementation, dont le service d'information sur les comptes. Ce dernier est défini comme un service en ligne consistant à fournir des informations consolidées concernant un ou plusieurs comptes de paiement détenus par l'utilisateur de services de paiement, soit auprès d'un autre prestataire de services de paiement, soit auprès de plus d'un prestataire de services de paiement. Cette restitution implique un traitement dépassant la simple transmission de données brutes. Un organisme souhaitant fournir un tel service est donc tenu de respecter les modalités d'accès et de transmission prévues par la DSP2, et ne peut exercer à cette fin les droits prévus par le RGPD, tels que le droit à la portabilité ou le droit d'accès.

11. Il est en revanche possible pour un mandataire, même lorsque ce dernier est par ailleurs prestataire de service d'information sur les comptes, d'exercer les droits d'accès et de portabilité prévus par le RGPD, en qualité de mandataire, auprès d'un prestataire gestionnaire de compte, si la DSP2 n'a pas vocation à s'appliquer à cette opération. Ce serait par exemple le cas si l'accès aux données est réalisé dans le cadre de la fourniture d'un service non soumis à la DSP2, ou si les données auxquelles on accède ne proviennent pas d'un compte de paiement au sens de la DSP2.

12. En tout état de cause, les traitements de données à caractère personnel mis en œuvre par ces organismes sont soumis au respect du RGPD, qu'ils soient ou non opérés dans le cadre de la fourniture des services soumis à la DSP2.

13. Enfin, la recommandation ne vise pas les services mis à disposition par des acteurs proposant des outils facilitateurs d'exercice de droit (par exemple, ceux fournissant une plateforme sur laquelle les personnes concernées ont accès à des demandes prérédigées 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 sans exercer ces droits au nom et pour le compte des personnes concernées.

Article 2
Qualification des rôles et responsabilités

14. Les acteurs doivent effectuer une analyse préalable quant à la qualification de leur rôle, notamment à la lumière de la jurisprudence de la Cour de justice de l'Union européenne et des documents publiés par le Comité européen sur la protection des données (CEPD) sur la notion de responsable de traitement et de sous-traitant.

15. Chaque acteur, qu'il soit un responsable de traitement recevant une demande d'exercice de droit ou un mandataire mandaté par la personne concernée, est un responsable de traitement distinct, à moins que les acteurs déterminent ensemble les moyens et les finalités du traitement : dans ce cas spécifique, une responsabilité conjointe peut être retenue.

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

16. Comme dans toute entrée en relation contractuelle entre un organisme et une personne concernée recourant aux services de ce dernier, plusieurs traitements sont nécessaires à l'exécution du contrat auquel la personne concernée est partie au sens de l'article 6 du RGPD. Dans ce cadre contractuel, le mandataire joue son rôle d'intermédiaire entre la personne concernée et les responsables de traitement auprès desquels cette dernière souhaite exercer ses droits. L'exercice des droits nécessite notamment de prouver que la personne est bien titulaire des droits qu'elle entend exercer, c'est-à-dire qu'elle est bien la personne connue par le responsable de traitement auprès duquel la demande est formulée. L'article 77 du décret dispose que la personne concernée justifie de son identité par tout moyen, et notamment en utilisant des données d'identité numériques lorsque ces données sont nécessaires et estimées suffisantes par le responsable du traitement pour authentifier ses utilisateurs. Le mandataire ne pourra donc collecter et transmettre que les données d'authentification ou d'identification pertinentes, ce qui ne nécessite pas un traitement systématique de justificatifs de l'identité régalienne. L'article 77 du décret précise par ailleurs que la photocopie d'un titre d'identité portant la signature du titulaire ne peut être demandée qu'en cas de doutes raisonnables quant à l'identité de cette personne, lorsque la situation l'exige.

17. Si le mandataire estime qu'il doit s'assurer de l'identité de la personne concernée avant d'entrer en relation commerciale avec elle, la Commission rappelle que la consultation d'un justificatif suffit généralement, sans que cette donnée soit nécessairement stockée. Toutefois, sur le fondement de son intérêt légitime, le mandataire peut exceptionnellement conserver les données permettant de justifier de l'identité de la personne concernée afin d'anticiper les cas spécifiques où le responsable de traitement aurait des doutes raisonnables sur l'identité de la personne, à condition que ces données soient pertinentes au regard de la vérification opérée. Dans l'hypothèse où la personne concernée serait connue par le responsable de traitement sous son identité régalienne, et que le mandataire souhaiterait en conserver un justificatif, la Commission recommande de déployer des 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 salarié ayant accédé à une pièce d'identité, la référence interne de la pièce d'identité consultée, ainsi que l'horodatage de la consultation, associée 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

18. Conformément à l'article 77 du décret, le mandataire doit être « spécialement mandaté » par la personne concernée ; la durée et l'objet précis du mandat doivent être spécifiés et le mandataire doit être en mesure de justifier de son mandat.

19. 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 estime qu'une telle clause générale semble insuffisante pour répondre au caractère spécifique du mandat en ce qui concerne (i) les données visées par la demande ; (ii) le responsable de traitement destinataire de la demande ; (iii) les données d'identification transmises au responsable de traitement ; (iv) les droits exercés ; et (v) la durée du mandat. La Commission tient à la disposition des mandataires sur son site web un exemple de mandat-type, auquel les mandataires ainsi que les responsables de traitement détenteurs de données peuvent se référer.

20. Les responsables de traitement auxquels les demandes sont adressées ne doivent pas procéder à la transmission des données sans s'être assurés au préalable de leur validité : il leur incombe de s'assurer de l'identité de la personne concernée et de la véracité du mandat.

21. La Commission recommande au mandataire de s'assurer que le mandat contienne tous les éléments permettant (i) d'identifier le titulaire du droit exercé et la personne à l'origine de la demande, en cas de représentation légale de la personne concernée ; (ii) de s'assurer de l'authenticité du mandat ; (iii) d'identifier le destinataire à qui les données doivent être transmises (à savoir la personne concernée, le mandataire ou l'éventuel nouveau responsable de traitement dans le cadre du transfert direct, permis par le droit à la portabilité) ; et (iv) d'identifier le responsable de traitement auprès duquel les droits doivent être exercés.

22. Dans l'hypothèse où le mandataire exerce les droits de la personne concernée auprès de plusieurs responsables de traitement, la Commission recommande qu'un contrat de mandat propre à chaque responsable de traitement soit conclu afin d'éviter que le mandat ne contienne des informations non nécessaires ou non pertinentes telles que des informations d'identification uniquement valables auprès d'un responsable de traitement ou que ne soit pas révélé à un responsable de traitement l'identité d'un autre responsable détenant les données à caractère personnel de la personne concernée.

23. Enfin, 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 dans le mandat au responsable de traitement. 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

24. 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). Le mandataire, dans son rôle d'intermédiaire, peut conseiller la personne concernée quant aux informations permettant au responsable de traitement de l'identifier, afin que ne soient collectées et transmises que des informations pertinentes et nécessaires.

25. A cet égard, le mandat devrait rappeler 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). 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

26. 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.

27. 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. Cette signature pourrait également permettre de garantir que le mandat n'a subi aucune modification depuis sa signature par la personne concernée.

28. 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.

29. La Commission recommande que le mandat invite expressément la personne concernée à préciser sa demande avec, par exemple, les catégories de données faisant l'objet de l'exercice du droit (par exemple, toutes les données relatives à ses interactions avec le service client), les finalités du traitement (par exemple, toutes les données collectées pour faciliter le paiement), le service fourni par le responsable de traitement (par exemple, un service de billetterie) ou encore par droit qu'elle souhaite exercer (si le mandataire le propose parmi ses services).

30. Enfin, 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 prévu que l'accomplissement de ces dernières entraînera la résiliation automatique du mandat, notamment à la réception des données dans le cadre de l'exercice d'un droit à la

portabilité des données. 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 le mandat se renouvelle tacitement, la personne concernée en soit informée et puisse user de son droit de rétractation à tout moment. Lorsque la personne révoque son mandat, l'exercice des droits par le biais du mandataire doit cesser. Ce dernier doit donc notifier les responsables de traitement auprès desquels des demandes d'exercice des droits ont été adressées et qui sont toujours en cours de traitement, sans préjudice de l'éventuelle information de cette révocation à l'initiative de la personne concernée elle-même.

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

31. Le mandat doit expressément 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 peuvent être acheminées peut également être précisée, de même que tout autre moyen technique permettant que les données soient reçues et utilisables au plus vite par l'entité destinataire, comme une clef d'accès à une interface de programmation d'application (« *application programming interface* » ou API) ou encore une URL dédiée, dès lors que la transmission par ces moyens s'opère de manière sécurisée et que leur utilisation par le responsable du traitement ne nécessite pas d'efforts additionnels.

32. 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

33. 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. Si cela 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.

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

34. Les demandes d'exercice de droit par le biais d'un mandataire peuvent être réalisées par le biais d'une interface de programmation d'application.

35. 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.

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

37. 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).

38. 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 de données (« *scraping* »)

39. Les mandataires peuvent solliciter auprès de la personne concernée ses identifiant et mot de passe en vue d'extraire des données la concernant accessibles depuis le site du responsable de traitement (technique dite d'aspiration de données ou « *scraping* »).

40. L'utilisation des données d'authentification avec l'accord de la personne concernée dans cette optique n'est pas interdite par principe par le RGPD.

41. Toutefois, compte tenu des risques importants qu'elle comporte pour les personnes concernées, notamment au regard de la préservation du niveau de sécurité apporté par les mécanismes d'authentification reposant sur l'utilisation de mots de passe, le recours à cette technique devrait être strictement limité et systématiquement soumis au recueil d'un consentement valable de la personne concernée (c'est-à-dire libre d'être donné ou refusé, indépendamment de la conclusion du mandat et susceptible d'être retiré à tout moment).

42. De même, le mandataire deviendrait dans cette hypothèse responsable des traitements des données permettant l'authentification de la personne concernée, et serait alors tenu de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

43. Le premier cas d'usage est celui dans lequel le responsable de traitement permet l'accès aux données par aspiration en l'indiquant de manière univoque dans sa réponse à la demande qui lui est adressée. Dans ce cas, le responsable du traitement et le mandataire sont tenus d'adapter les mesures de sécurité et devraient, en amont de l'exercice du droit d'accès, procéder à une analyse de risques afin de mettre en œuvre les mesures de sécurité adéquates afin que ces risques soient maîtrisés.

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

45. Le second correspond au cas où un responsable de traitement ne répond pas à une demande effectuée à plusieurs reprises, au-delà des délais prévus par le RGPD.

46. Dans cette hypothèse, la Commission recommande que le mandataire mette en place les dispositifs suivants : (i) la personne concernée a été pleinement informée des risques encourus dans le cadre du recueil de son consentement ; (ii) le responsable de traitement a été prévenu en amont qu'une aspiration va être mise en œuvre avec les informations lui permettant d'identifier les accès par le mandataire (telles que l'adresse IP de ce dernier, la date, l'heure et la durée de sa connexion, etc.) ; (iii) le mandataire est en mesure de fournir un mandat valide au responsable de traitement si ce dernier en fait la demande, et ce, même si les données ont déjà été collectées ; (iv) le mandataire ne collecte pas de données dont il n'a pas à connaître au regard du mandat, notamment en permettant au mandant de vérifier, de rectifier ou supprimer tout ou partie des données collectées par ce biais ; et (v) le mot de passe utilisé ordinairement par l'utilisateur n'est pas transmis au mandataire. A cette fin, les mandataires devraient 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). A défaut, la Commission recommande au mandataire d'informer la personne concernée de la nécessité de changer son mot de passe pour en créer un temporaire permettant d'accéder à son compte, puis de le modifier à nouveau une fois cet accès réalisé par le mandataire.

47. La Commission recommande en tout état de cause que, dans l'hypothèse exceptionnelle où le mandataire utilise un mot de passe, dédié ou temporaire, celui-ci ne soit accessible à aucun membre de son personnel et soit supprimé immédiatement après l'accès aux données. Si l'aspiration est utilisée de manière récurrente, le mandataire doit informer régulièrement la personne de l'existence de cet accès et lui demander de confirmer son souhait de poursuivre la collecte.

48. La Commission rappelle également que les mandataires envisageant de recourir à cette technique d'aspiration des données ne peuvent exiger la désactivation de mesures de sécurité légitimes mises en place par les responsables de traitement, telles que les systèmes de blocage d'accès aux contenus par des robots comme l'usage de « *captchas* » ou de système de suspension d'accès à certaines adresses IP représentant un risque de sécurité avéré.

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

49. La Commission encourage les acteurs à collaborer autant que possible afin de faciliter l'exercice des droits des personnes et leur rappelle qu'ils ne peuvent créer de conditions additionnelles, dépourvues de fondement juridique, qui feraient obstacle à l'aboutissement d'une demande d'exercice de droit.

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

50. 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.

51. Le responsable de traitement doit être en mesure de démontrer la complexité de la demande ; le simple fait qu'une demande est exercée par le biais d'un mandataire ne suffit pas à proroger automatiquement le délai de réponse.

52. 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, confirme sa prise en compte (notamment dans le cas d'une demande de rectification ou de suppression) ou s'il répond en informant qu'une prolongation de deux mois est nécessaire, le mandataire devrait transmettre ces informations à la personne concernée. A cet égard, la Commission recommande que la personne concernée puisse suivre l'avancement de la mission du mandataire, et ce à tout moment de sa réalisation (sans préjudice des obligations de transparence et d'exercice des droits relatives aux traitements de ses données à caractère personnel par ledit mandataire).

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

53. En ce qui concerne le format technique des données, 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.

54. 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, lorsque cela est possible, à moins que la personne concernée ne demande qu'il en soit autrement. La Commission constate ainsi que le RGPD pose un principe de parallélisme des formes. Aussi, 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.

55. La transmission directe des données au mandataire par le responsable de traitement peut être exigée dans le cadre du droit à la portabilité, lorsque cela est techniquement possible et que le mandat le prévoit.

56. Dans le cadre d'un droit d'accès, la Commission encourage les responsables de traitement à adresser les données au mandataire lorsque ce dernier est désigné comme destinataire par la personne concernée dans le mandat.

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

7.1 - Lorsque la demande est manifestement infondée ou excessive

57. 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 manifestement infondé ou excessif 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 infondé soit indéniable et évident.

58. La Commission estime que le fait qu'une demande soit effectuée par le biais d'un mandataire ne permet pas de considérer qu'elle est manifestement infondée. De plus, la Commission rappelle que les responsables de traitement détenteurs des données ne sont pas responsables des utilisations ultérieures que feraient les mandataires une fois les données transmises : le caractère manifestement infondé ne peut pas être caractérisé par d'éventuelles réutilisations, qui relèvent entièrement de la responsabilité du mandataire.

59. La Commission rappelle que la quantité de données faisant l'objet de la demande ne constitue pas une justification suffisante pour considérer qu'une demande est excessive.

60. Enfin le CEPD a considéré 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. Dans cet esprit, la Commission estime que le caractère répétitif de demandes d'exercice de droits ne suffit pas à lui seul pour les considérer comme excessives.

61. Toutefois, la Commission estime que le renouvellement d'une demande d'exercice de droits pourrait être considérée 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.

62. A l'inverse, 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 respecté ses obligations en ne répondant pas à la demande, ou qu'il a répondu de manière insatisfaisante (si, par exemple, il n'a pas correctement rectifié les données ou n'a pas procédé au transfert de l'ensemble des données portables).

63. 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.

64. 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.

65. Dans tous les cas, la Commission recommande que la personne concernée puisse déterminer librement l'étendue de sa demande et puisse choisir de renouveler un même mandat. En tant que bonne pratique, le mandataire peut lui conseiller de cibler sa demande de renouvellement ou de préciser les raisons pour lesquelles elle estime qu'un renouvellement est nécessaire.

66. 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 aux données concernées 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, le recours à une API permet de réduire considérablement la charge relative au traitement de demandes d'exercices de droit répétitives et réduit la probabilité que des demandes puissent être considérées comme imposant une charge excessive.

67. Enfin, le responsable de traitement ne peut garder le silence lorsqu'il reçoit une demande d'exercice de droits. S'il refuse d'y faire droit, il devra, en application de l'article 12 alinéa 6 du RGPD, justifier des motifs de son refus. Cette justification pourra se faire auprès du mandataire, qui devra en informer la personne concernée. A défaut, le responsable de traitement s'expose, au dépôt d'une plainte auprès de la Commission ou à un recours juridictionnel si la personne concernée souhaite contester le refus implicite ou explicite de prise en compte de sa demande.

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

68. Le fait qu'une demande d'exercice de droits soit exercée par l'intermédiaire d'un mandataire ne doit pas 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.

69. Dans les cas 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 lui-même, il peut collecter des informations supplémentaires pour confirmer l'identité, sachant qu'une attention spécifique doit être portée au principe de pertinence des données. Par exemple, si le responsable de traitement ne connaît 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. A cet égard, la Commission encourage l'adoption de protocoles d'authentification partagés entre le mandataire et le responsable de traitement, afin que ce dernier puisse s'assurer que la personne concernée est bien celle qu'elle prétend être, et de faciliter la transmission directe des données.

70. Pour la collecte d'informations supplémentaires, le responsable de traitement peut se tourner aussi bien vers le mandataire que vers la personne concernée. Dans ce dernier cas, la Commission invite les responsables de traitement à veiller et 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'achat, numéro de carte de fidélité, etc.).

7.3 - Sur la possibilité de refuser une demande en raison d'une impossibilité technique

71. Lorsque la réponse est fournie sous une forme électronique, la transmission des données peut se faire par le biais d'une transmission directe ou d'outils automatisés permettant l'extraction des données pertinentes (comme par exemple des API).

72. 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 langages sémantiques ou de modélisation (tels qu'UML) peuvent être utilisés.

73. La Commission considère que le simple fait que le mandataire et le responsable de traitement n'ont pas développé des mécanismes de transmission similaire (directe ou par outil automatisé) ne suffit pas à conclure que l'exercice des droits 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.

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

74. 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 si cette restructuration fait partie intégrante du service proposé ou si la personne concernée conserve la possibilité de recevoir les données brutes. Le traitement de données réalisé dans ce cadre peut être fondé sur l'exécution du contrat auquel la personne concernée est partie, dès lors que la restructuration opérée fait partie intégrante du service demandé et attendu par la personne concernée.

8.2. - Sur la conservation des données par le mandataire

75. Les données transmises au mandataire par le responsable de traitement 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.

76. Toutefois, le mandataire peut proposer une fonctionnalité permettant à la personne concernée de conserver les données sur un espace de stockage dédié qu'il met à sa disposition pour qu'elle puisse y accéder à tout moment. . Dans un tel cas, la personne concernée doit être en mesure de définir la durée de conservation des données et de décider à tout moment de leur suppression.

77. 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, le vol 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

78. Les responsables de traitement répondant à des demandes d'exercice de droits ne sont pas responsables des traitements effectués par le mandataire. Seuls les mandataires sont responsables de ces traitements et doivent, à ce titre, s'assurer de leur licéité, tant au regard du RGPD que d'autres réglementations.

79. L'objet du mandat visé par le dernier alinéa de l'article 77 du décret d'application de la loi « Informatique et Libertés » est exclusivement d'exercer les droits de la personne concernée en son nom et pour son compte. Il n'autorise donc pas en tant que telle la réutilisation des données personnelles collectées dans ce cadre par le mandataire pour son propre compte. Une telle réutilisation doit être envisagée de manière distincte, en tant que traitement de données à caractère personnel autonome pleinement soumis au respect de l'ensemble des dispositions du RGPD. Ce traitement doit notamment répondre à une ou des finalités déterminées, explicites et légitimes et être mis en œuvre sous le contrôle de la personne concernée.

80. A titre d'exemple, le mandataire peut proposer à la personne concernée un service additionnel reposant sur la réutilisation de ses données, auquel elle peut librement souscrire. Dans ce cas, seules les données nécessaires à la fourniture du service explicitement demandé par la personne peuvent être utilisées et cette dernière doit pouvoir revenir à tout moment sur son choix et demander la suppression des données la concernant.

81. De manière générale, si les données collectées par le biais du mandat venaient à faire l'objet d'un traitement allant au-delà de leur transmission, par le mandataire ou tout autre tiers auquel la personne concernée les aurait confiées, ce traitement devrait être pleinement conforme à toutes les dispositions du RGPD et devrait notamment disposer d'une base légale valable au titre de son article 6. A cet égard, le recueil du consentement spécifique, libre et éclairé des personnes concernées doit être privilégié, et sera souvent obligatoire, préalablement à toute réutilisation de leurs données pour des fins étrangères au mandat d'exercice des droits, dès lors qu'une telle réutilisation ne peut reposer sur l'exécution du contrat de mandat conclu avec la personne concernée et n'apparait pas entrer, de manière générale, dans ses attentes raisonnables.

82. 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 des 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, une forme de consentement 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, et que les autres critères de compatibilité énumérés à l'article 6(4) soient remplis.

83. La Commission encourage les mandataires à proposer, le cas échéant, 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.

84. Le mandataire doit par ailleurs fournir à la personne concernée toutes les informations pertinentes et utiles sur les nouveaux traitements qu'il envisage de mettre en œuvre, d'une manière claire, concise et transparente, en application de l'article 13 du RGPD. Ainsi, la personne doit être en mesure de comprendre précisément ce qui sera fait des données la concernant.

85. Il appartient également aux mandataires de s'assurer qu'ils respectent les autres réglementations qui peuvent s'appliquer, notamment le droit de la concurrence, le droit des producteurs de bases de données ou encore la théorie civile de l'abus de droit.

86. Enfin, 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).

87. Si le droit à la portabilité ne porte pas atteinte aux droits et libertés de tiers (article 20 alinéa 4 du RGPD) dès lors que les données concernant des tiers se rapportent également à la personne concernée à l'origine de la demande, le traitement de données de tiers par un nouveau responsable de traitement doit faire l'objet d'une vigilance particulière. A ce titre, le CEPD considère que le nouveau responsable de traitement peut avoir un intérêt légitime à traiter les données de ces tiers afin de fournir un service à la personne concernée lui permettant de traiter ces données pour son usage personnel, et uniquement pour cet usage. A l'inverse, les droits et libertés des tiers ne semblent pas respectés si le mandataire utilise leurs données à des fins qui lui sont propres. Ainsi, la Commission estime que les mandataires devraient s'abstenir de réutiliser les données relatives à des tiers pour leurs propres finalités.

Article 10
Sur la sécurité de la transmission des données

88. 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.

89. 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 et à des mécanismes d'analyse automatique de ces données conformément à la recommandation relative à la journalisation adoptée par la Commission le 29 avril 2021.

La présidente

Marie-Laure DENIS