GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

16/FR
WP 242 rev.01

Lignes directrices relatives au droit à la portabilité des données

Adoptées le 13 décembre 2016
Version révisée et adoptée le 5 avril 2017

TABLE DES MATIÈRES

Synthèse

L'article 20 du règlement général sur la protection des données crée un nouveau droit à la portabilité des données, qui est étroitement lié au droit d'accès aux données, tout en différant de celui-ci à de nombreux égards. Il confère aux personnes concernées le droit de recevoir les données à caractère personnel qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et de les transmettre à un autre responsable du traitement. Ce nouveau droit a pour objectif de responsabiliser les personnes concernées et de leur permettre de contrôler davantage les données à caractère personnel les concernant.

Dans la mesure où il permet la transmission directe des données à caractère personnel d'un responsable du traitement à un autre, le droit à la portabilité des données constitue également un instrument important qui facilitera la libre circulation des données à caractère personnel dans l'Union et qui stimulera la concurrence entre les responsables du traitement. Il facilitera le passage d'un prestataire de services à un autre et encouragera dès lors la mise au point de nouveaux services dans le contexte de la stratégie pour un marché unique numérique.

Le présent avis fournit des orientations sur la manière d'interpréter et de mettre en œuvre le droit à la portabilité des données, tel qu'il a été introduit par le règlement général sur la protection des données. Il a pour objet d'examiner la question du droit à la portabilité des données et son champ d'application. Il précise les conditions dans lesquelles ce nouveau droit s'applique compte tenu de la base juridique du traitement des données (soit le consentement de la personne concernée, soit la nécessité d'exécuter un contrat) et du fait que ce droit est limité aux données à caractère personnel fournies par la personne concernée. Le présent avis fournit également des exemples et des critères concrets pour expliquer les circonstances dans lesquelles ce droit s'applique. À cet égard, le groupe de travail «Article 29» considère que le droit à la portabilité des données couvre les données fournies sciemment et activement par la personne concernée, ainsi que les données à caractère personnel générées par son activité. Ce nouveau droit ne peut être remis en cause et limité aux informations à caractère personnel que la personne concernée communique directement, par exemple sur un formulaire en ligne.

À titre de bonne pratique, les responsables du traitement devraient commencer à élaborer les moyens qui contribueront à répondre aux demandes de portabilité des données, comme des outils de téléchargement et des interfaces de programme d'application. Ils devraient garantir que les données à caractère personnel sont transmises dans un format structuré, couramment utilisé et lisible par machine et doivent être encouragés à garantir l'interopérabilité du format de données fourni dans le cadre de l'exercice d'une demande de portabilité des données.

Le présent avis aide également les responsables du traitement à comprendre clairement leurs obligations respectives et recommande des bonnes pratiques et des outils visant à soutenir le respect du droit à la portabilité des données. Enfin, il recommande que les parties prenantes du secteur et les associations professionnelles travaillent de concert sur une série commune de normes et de formats interopérables afin de satisfaire aux exigences liées au droit à la portabilité des données.

I. Introduction

L'article 20 du règlement général sur la protection des données (RGPD) introduit un nouveau droit à la portabilité des données. Ce droit permet aux personnes concernées de recevoir les données à caractère personnel qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et de les transmettre sans obstacle à un autre responsable du traitement. Ce droit, qui s'applique sous réserve de certaines conditions, encourage le choix et le contrôle de l'utilisateur, ainsi que sa responsabilisation.

Les personnes exerçant leur droit d'accès au titre de la directive 95/46/CE relative à la protection des données étaient limitées par le format choisi par le responsable du traitement lors de la fourniture des informations demandées. **Le nouveau droit à la portabilité des données vise à responsabiliser les personnes concernées au sujet de leurs données à caractère personnel, car il facilite leur capacité à déplacer, à copier ou à transmettre facilement des données à caractère personnel d'un environnement informatique vers un autre** (qu'il s'agisse de leur propre système, du système de tiers de confiance ou de celui de nouveaux responsables du traitement).

En affirmant les droits et le contrôle personnels des particuliers sur les données à caractère personnel les concernant, la portabilité des données représente également une occasion de «rééquilibrer» la relation entre les personnes concernées et les responsables du traitement[1].

Si le droit à la portabilité des données à caractère personnel peut également favoriser la concurrence entre les services (en facilitant le passage d'un service à l'autre), le RGPD réglemente les données à caractère personnel et non la concurrence. En particulier, l'article 20 ne limite pas les données portables à celles qui sont nécessaires ou utiles pour le changement de services[2].

Bien que la portabilité des données soit un nouveau droit, d'autres types de portabilité existent déjà ou sont en cours de discussion dans d'autres domaines de la législation (par exemple, dans le contexte de la résiliation d'un contrat, de l'itinérance des services de communication et de l'accès transfrontière aux services[3]). Certaines synergies, voire des avantages pour les particuliers, peuvent découler de ces différents types de portabilité si ces services sont fournis dans le cadre d'une approche combinée, même si les analogies doivent être traitées avec prudence.

Le présent avis fournit des orientations aux responsables du traitement afin qu'ils puissent mettre à jour leurs pratiques, leurs processus et leurs stratégies, et clarifie la signification de la portabilité des données afin de permettre aux personnes concernées d'exercer efficacement leur nouveau droit.

---

[1] L'objectif premier de la portabilité des données est de renforcer le contrôle des particuliers sur les données à caractère personnel les concernant et de veiller à ce qu'ils jouent un rôle actif dans l'écosystème des données.

[2] Par exemple, ce droit peut permettre aux banques de proposer des services complémentaires, sous le contrôle de l'utilisateur, en utilisant des données à caractère personnel initialement recueillies dans le cadre d'un service d'approvisionnement en énergie.

[3] Voir le programme de la Commission européenne pour un marché unique numérique: https://ec.europa.eu/digital-agenda/en/digital-single-market, en particulier le premier pilier stratégique intitulé «Améliorer l'accès aux biens et services numériques».

II. Quels sont les principaux éléments de la portabilité des données?

À son article 20, paragraphe 1, le règlement général sur la protection des données définit le droit à la portabilité des données comme suit:

> *Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle […]*

- Le droit de recevoir des données à caractère personnel

Premièrement, la portabilité des données est un **droit des personnes concernées à recevoir un sous-ensemble de données à caractère personnel** les concernant traitées par un responsable du traitement et à les sauvegarder en vue d'un usage personnel ultérieur. Cette sauvegarde peut se faire sur un dispositif privé ou un nuage privé, sans que les données soient nécessairement transmises à un autre responsable du traitement.

À cet égard, la portabilité des données complète le droit d'accès. Une particularité de la portabilité des données réside dans le fait qu'elle offre aux personnes concernées un moyen aisé de gérer et de réutiliser elles-mêmes les données à caractère personnel les concernant. Ces données doivent être reçues «*dans un format structuré, couramment utilisé et lisible par machine*». Par exemple, une personne concernée pourrait vouloir extraire sa liste de chansons actuelle (ou un historique des titres écoutés) d'un service de diffusion en flux de musique afin de voir le nombre de fois qu'elle a écouté certaines chansons ou de décider quelle musique elle souhaite acheter ou écouter sur une autre plate-forme. De la même manière, elle pourrait aussi souhaiter extraire la liste de ses contacts de son application de messagerie, par exemple, pour établir une liste de mariage ou obtenir des informations sur des achats effectués en utilisant différentes cartes de fidélité, ou pour évaluer son empreinte carbone[4].

- Le droit de transmettre les données à caractère personnel d'un responsable du traitement à un autre responsable du traitement

Deuxièmement, l'article 20, paragraphe 1, confère aux personnes concernées le **droit de transmettre les données à caractère personnel d'un responsable du traitement à un autre responsable du traitement** sans que le premier «y fasse obstacle». Les données peuvent aussi être transmises directement d'un responsable du traitement à un autre à la demande de la personne concernée, lorsque cela est techniquement possible (article 20, paragraphe 2). À cet égard, le considérant 68 énonce qu'[i]l y a lieu d'encourager les responsables du traitement à mettre au point des formats interopérables permettant la portabilité des données[5], mais sans créer, pour les responsables du traitement, d'obligation

[4] Dans ces cas, le traitement des données effectué par la personne concernée peut relever des activités domestiques lorsque le traitement est entièrement effectué sous le seul contrôle de la personne concernée ou être réalisé par une autre partie, au nom de la personne concernée. Dans ce dernier cas, l'autre partie doit être considérée comme le responsable du traitement, y compris aux seules fins de la conservation des données à caractère personnel, et doit respecter les principes et obligations énoncés dans le règlement général.

[5] Voir également la section V.

d'adopter ou de maintenir des systèmes de traitement qui sont techniquement compatibles[6]. Le règlement général sur la protection des données interdit toutefois aux responsables du traitement d'entraver la transmission.

En substance, cet aspect de la portabilité des données habilite les personnes concernées non seulement à obtenir et à réutiliser les données qu'elles ont fournies, mais aussi à les transmettre à un autre prestataire de services (dans le même secteur d'activité ou dans un autre). En plus de responsabiliser le consommateur en empêchant un «verrouillage» des données, le droit à la portabilité des données devrait renforcer les possibilités d'innovation et de partage des données à caractère personnel entre les responsables du traitement de manière sûre et sécurisée, sous le contrôle de la personne concernée[7]. La portabilité des données peut encourager le partage contrôlé et limité par les utilisateurs de données à caractère personnel entre organisations et, partant, enrichir les services et les expériences clients[8]. La portabilité des données peut faciliter la transmission et la réutilisation de données à caractère personnel concernant les utilisateurs entre les différents services qui les intéressent.

[6] Une attention particulière doit par conséquent être accordée au format des données transmises pour garantir que les données peuvent être réutilisées, avec un minimum d'effort, par la personne concernée ou un autre responsable du traitement. Voir également la section V.

[7] Voir plusieurs applications expérimentales en Europe, par exemple MiData au Royaume-Uni ou MesInfos / SelfData par FING en France.

[8] Les industries appartenant aux mouvements du «Quantified Self» et de l'«Internet of Things» ont démontré l'avantage (et les risques) découlant de la mise en relation des données à caractère personnel provenant de différents aspects de la vie d'une personne, comme la forme physique, l'activité sportive et l'absorption de calories, afin de fournir une image plus complète de la vie d'une personne en un seul fichier.

- **Responsabilité**

La portabilité des données garantit le droit de recevoir des données à caractère personnel et de les traiter selon les souhaits de la personne concernée[9].

Les responsables du traitement qui répondent à des demandes de portabilité des données, dans les conditions établies à l'article 20, ne sont pas responsables du traitement effectué par la personne concernée ou par une autre société qui reçoit les données à caractère personnel. Ils agissent au nom de la personne concernée, y compris lorsque les données à caractère personnel sont directement transmises à un autre responsable du traitement. À cet égard, le responsable des données n'est pas responsable de la conformité du responsable du traitement destinataire avec la législation relative à la protection des données, étant donné que ce n'est pas le responsable du traitement émetteur qui choisit le destinataire. En même temps, le responsable du traitement devrait fixer des garanties pour s'assurer qu'il agit réellement au nom de la personne concernée. Il peut par exemple mettre en place des procédures pour s'assurer que le type de données à caractère personnel transmises est effectivement celui que la personne concernée souhaite transmettre. À cet effet, il est possible d'obtenir la confirmation de la personne concernée avant la transmission ou plus tôt, lorsque le consentement original au traitement est donné ou lors de la finalisation du contrat.

Les responsables du traitement répondant à une demande de portabilité des données n'ont aucune obligation particulière de contrôler et de vérifier la qualité des données avant de les transmettre. Bien entendu, ces données doivent déjà être exactes et tenues à jour, conformément aux principes énoncés à l'article 5, paragraphe 1, du règlement général sur la protection des données. La portabilité des données n'oblige par ailleurs pas le responsable du traitement à conserver des données à caractère personnel plus longtemps que nécessaire ou au-delà d'une période de conservation spécifiée[10]. Il est important de noter qu'il n'existe aucune exigence supplémentaire concernant la conservation des données au-delà des périodes de conservation applicables par ailleurs, simplement pour pouvoir répondre de manière positive à toute éventuelle demande future de portabilité des données.

Lorsque les données à caractère personnel demandées sont traitées par un sous-traitant, le contrat conclu en vertu de l'article 28 du règlement général sur la protection des données doit inclure l'obligation d'aider «le responsable du traitement, par des mesures techniques et organisationnelles appropriées, [à] donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits». Le responsable du traitement devrait donc mettre en œuvre des procédures spécifiques en coopération avec ses sous-traitants pour répondre aux demandes de portabilité des données. En cas de responsabilité conjointe, le contrat devrait clairement répartir les responsabilités entre chaque responsable du traitement en ce qui concerne le traitement des demandes de portabilité des données.

Par ailleurs, un responsable du traitement destinataire [11] est chargé de garantir que les données portables fournies sont pertinentes et ne sont pas excessives au regard du nouveau traitement

[9] Le droit à la portabilité des données ne se limite pas aux données à caractère personnel qui sont utiles et pertinentes pour des services similaires fournis par des concurrents du responsable du traitement.

[10] Dans l'exemple ci-dessus, si le responsable du traitement des données ne conserve aucune liste des chansons écoutées par un utilisateur, ces données à caractère personnel ne peuvent être incluses dans une demande de portabilité des données.

[11] C'est-à-dire le responsable du traitement qui reçoit les données à caractère personnel à la suite d'une demande de portabilité des données introduite par la personne concernée auprès d'un autre responsable du traitement.

des données. Par exemple, dans le cas d'une demande de portabilité des données auprès d'un service de messagerie par laquelle la personne concernée souhaite récupérer des courriers électroniques et les envoyer vers une plate-forme d'archivage sécurisée, le nouveau responsable du traitement ne doit pas traiter les coordonnées des correspondants de la personne concernée. Si ces informations ne sont pas pertinentes au regard de la finalité du nouveau traitement, elles ne doivent pas être conservées ni traitées. Dans tous les cas, les responsables du traitement destinataires ne sont pas tenus d'accepter de traiter les données à caractère personnel transmises à la suite d'une demande de portabilité des données. De la même manière, lorsqu'une personne concernée demande à transmettre les détails de ses transactions bancaires à un service qui l'aide à gérer son budget, le responsable du traitement destinataire ne doit pas accepter toutes les données ni conserver tous les détails des transactions une fois qu'elles ont été caractérisées aux fins du nouveau service. En d'autres termes, les données acceptées et conservées devraient se limiter à celles qui sont nécessaires et pertinentes au service fourni par le responsable du traitement destinataire.

Une organisation «destinataire» devient un nouveau responsable du traitement pour ces données à caractère personnel et doit respecter les principes énoncés à l'article 5 du règlement général sur la protection des données. Par conséquent, le «nouveau» responsable du traitement destinataire doit indiquer clairement et directement la finalité du nouveau traitement avant toute demande de transmission des données portables, conformément aux exigences en matière de transparence établies à l'article 14[12]. Comme pour tout traitement de données effectué sous sa responsabilité, le responsable du traitement doit appliquer les principes énoncés à l'article 5, tels que la licéité, la loyauté et la transparence, la limitation des finalités, la minimisation des données, l'exactitude, l'intégrité et la confidentialité, la limitation de la conservation et la responsabilité[13].

Les responsables du traitement détenant des données à caractère personnel doivent être prêts à faciliter l'exercice du droit à la portabilité des données par leurs personnes concernées. Les responsables du traitement peuvent également choisir d'accepter des données provenant d'une personne concernée, mais ils n'y sont pas tenus.

- **Portabilité des données au regard des autres droits des personnes concernées**

Lorsqu'une personne exerce son droit à la portabilité des données, elle le fait sans porter atteinte à aucun autre droit (comme c'est le cas pour tout autre droit prévu par le règlement général sur la protection des données). Une personne concernée peut continuer à utiliser le service du responsable du traitement et à en bénéficier même après une opération de portabilité des données. La portabilité des données ne déclenche pas automatiquement l'effacement des données[14] des systèmes du responsable du traitement et n'a pas d'incidence sur la période de conservation initiale qui s'applique aux données transmises. La personne

[12] En outre, le nouveau responsable du traitement ne doit pas traiter de données à caractère personnel qui ne sont pas pertinentes et le traitement doit être limité à ce qui est nécessaire au regard des nouvelles finalités, même si les données à caractère personnel font partie d'une série de données plus globale transmise au moyen d'un processus de portabilité. Les données à caractère personnel qui ne sont pas nécessaires pour réaliser la finalité du nouveau traitement doivent être supprimées dans les meilleurs délais.

[13] Une fois reçues par le responsable du traitement, les données à caractère personnel envoyées dans le cadre du droit à la portabilité des données peuvent être considérées comme ayant été «fournies» par la personne concernée et être retransmises conformément à ce droit, dans la mesure où les autres conditions applicables à celui-ci (c'est-à-dire la base juridique du traitement, etc.) sont remplies.

[14] Comme indiqué à l'article 17 du règlement général sur la protection des données.

concernée peut exercer ses droits aussi longtemps que le responsable du traitement continue de traiter les données.

De la même manière, si la personne concernée souhaite exercer son droit à l'effacement de ses données («droit à l'oubli» établi à l'article 17), la portabilité des données ne peut être utilisée par un responsable du traitement comme moyen de reporter ou de refuser cet effacement.

Si une personne concernée venait à découvrir que des données à caractère personnel demandées dans le cadre du droit à la portabilité des données ne répondent pas totalement à sa demande, toute autre demande de données à caractère personnel au titre du droit d'accès doit être accueillie complètement, conformément à l'article 15 du règlement général sur la protection des données.

Par ailleurs, lorsqu'un acte législatif spécifique de l'Union ou d'un État membre dans un autre domaine prévoit également une certaine forme de portabilité des données concernées, les conditions établies par ces législations spécifiques doivent aussi être prises en considération lorsqu'il est donné suite à une demande de portabilité des données au titre du règlement général sur la protection des données. S'il ressort clairement de la demande formulée par la personne concernée que son intention n'est pas d'exercer ses droits au titre du règlement général sur la protection des données mais plutôt au titre de la législation sectorielle uniquement, alors, les dispositions du règlement général sur la protection des données relatives à la portabilité des données ne s'appliquent pas à cette demande[15]. Si, en revanche, la demande concerne la portabilité au titre du règlement général sur la protection des données, l'existence de cette législation spécifique est sans préjudice de l'application générale du principe de portabilité des données à tout responsable du traitement, comme le prévoit ledit règlement. Il convient plutôt d'évaluer, au cas par cas, comment cette législation spécifique peut, éventuellement, affecter le droit à la portabilité des données.

III. Quand la portabilité des données s'applique-t-elle?

- Quelles sont les opérations de traitement couvertes par le droit à la portabilité des données?

Le respect du règlement général sur la protection des données exige des responsables du traitement qu'ils se fondent sur une base juridique claire pour le traitement des données à caractère personnel.

Conformément à l'article 20, paragraphe 1, point a), du règlement général sur la protection des données, **pour relever du champ d'application de la portabilité des données**, les opérations de traitement doivent être fondées:

[15] Par exemple, si, par sa demande, la personne concernée cherche spécifiquement à donner accès à l'historique de son compte bancaire à un prestataire de services d'information sur les comptes aux fins énoncées dans la directive sur les services de paiement 2 (DSP2), cet accès doit être octroyé conformément aux dispositions de cette directive.

- sur le consentement de la personne concernée [en application de l'article 6, paragraphe 1, point a), ou de l'article 9, paragraphe 2, point a), s'agissant de catégories particulières de données à caractère personnel];

- ou sur un contrat auquel la personne concernée est partie en application de l'article 6, paragraphe 1, point b).

Les titres de livres achetés par une personne sur une librairie en ligne ou les chansons écoutées via un service de diffusion en flux de musique sont des exemples de données à caractère personnel qui relèvent généralement du champ d'application de la portabilité des données, parce qu'elles sont traitées sur la base de l'exécution d'un contrat auquel la personne concernée est partie.

Le règlement général sur la protection des données n'établit aucun droit général à la portabilité des données dans les cas où le traitement des données à caractère personnel ne se fonde pas sur le consentement ou sur un contrat[16]. Par exemple, les établissements financiers n'ont pas l'obligation de donner suite à une demande de portabilité des données concernant les données à caractère personnel traitées dans le cadre de leurs obligations en matière de prévention et de détection du blanchiment d'argent et d'autres formes de criminalité financière. De même, la portabilité des données ne couvre pas les coordonnées professionnelles traitées dans le cadre d'une relation d'entreprise à entreprise lorsque le traitement n'est fondé ni sur le consentement de la personne concernée ni sur un contrat auquel cette personne est partie.

S'agissant des données des employés, le droit à la portabilité des données ne s'applique généralement que si le traitement se fonde sur un contrat auquel la personne concernée est partie. Dans de nombreux cas, le consentement ne sera pas considéré comme ayant été donné librement dans ce contexte, en raison du déséquilibre des pouvoirs entre l'employeur et l'employé[17]. Certains traitements relevant des ressources humaines se fondent plutôt sur la base juridique de l'intérêt légitime, ou sont nécessaires au respect d'obligations juridiques spécifiques dans le domaine de l'emploi. Dans la pratique, le droit à la portabilité des données dans le domaine des ressources humaines concernera incontestablement certaines opérations de traitement (tels que les services de paiement et d'indemnisation ou le recrutement interne), mais dans de nombreuses autres situations, une approche au cas par cas sera nécessaire pour déterminer si toutes les conditions régissant le droit à la portabilité des données sont remplies.

[16] Voir le considérant 68 et l'article 20, paragraphe 3, du règlement général sur la protection des données. L'article 20, paragraphe 3, et le considérant 68 disposent que la portabilité des données ne s'applique pas si le traitement des données 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 ou si un responsable du traitement exerce ses missions publiques ou respecte une obligation légale. Dès lors, les responsables du traitement ne sont pas obligés de prévoir la portabilité dans ces cas. Toutefois, une bonne pratique consiste à mettre au point des processus visant à répondre automatiquement à des demandes de portabilité, en suivant les principes régissant le droit à la portabilité des données. Un exemple serait un service public fournissant un service de téléchargement facile des précédentes déclarations des revenus des particuliers. Concernant la portabilité des données en tant que bonne pratique dans le cas d'un traitement fondé sur la base juridique de la nécessité d'un intérêt légitime et de régimes volontaires existants, voir les pages 53 et 54 de l'avis 6/2014 du groupe de travail «Article 29» concernant les intérêts légitimes (WP 217).

[17] Comme le groupe de travail «Article 29» l'a souligné dans son avis 8/2001 du 13 septembre 2001 (WP 48).

Enfin, le droit à la portabilité des données s'applique uniquement si le traitement des données «est effectué à l'aide de procédés automatisés» et, par conséquent, ne couvre pas la plupart des dossiers papier.

- **Quelles sont les données à caractère personnel à inclure?**

Conformément à l'article 20, paragraphe 1, les personnes concernées ont le droit de recevoir les données:

- à caractère personnel les concernant et
- qu'elles ont *fournies* à un responsable du traitement.

L'article 20, paragraphe 4, dispose également que le respect de ce droit ne porte pas atteinte aux droits et libertés de tiers.

Première condition: données à caractère personnel relatives à la personne concernée

Seules les données à caractère personnel peuvent faire l'objet d'une demande de portabilité. Par conséquent, toute donnée anonyme[18] ou ne se rapportant pas la personne concernée est exclue du champ d'application. Toutefois, les données pseudonymisées qui peuvent clairement être liées à la personne concernée (par exemple, lorsque la personne concernée fournit l'identifiant correspondant, voir l'article 11, paragraphe 2) relèvent du champ d'application.

Dans de nombreuses circonstances, les responsables du traitement traiteront des informations qui contiennent les données à caractère personnel de plusieurs personnes concernées. Dans un tel cas, les responsables du traitement ne devraient pas interpréter de manière trop restrictive l'expression «données à caractère personnel les concernant [relatives à la personne concernée]». À titre d'exemple, les registres des services de téléphonie, de messagerie interpersonnelle ou de VoIP peuvent inclure (dans l'historique du compte de l'abonné) les coordonnées de tiers concernés par des appels entrants et sortants. Même si les registres contiennent dès lors des données à caractère personnel relatives à plusieurs personnes, les abonnés devraient pouvoir recevoir ceux-ci en réponse à leurs demandes de portabilité des données, étant donné que les registres se rapportent (également) à la personne concernée. Toutefois, lorsque ces registres sont ensuite transmis à un nouveau responsable du traitement, ce dernier ne doit pas les traiter pour une finalité qui porterait atteinte aux droits et libertés de tiers (voir ci-dessous: troisième condition).

Deuxième condition: données fournies par la personne concernée

La deuxième condition restreint le champ d'application aux données «fournies» par la personne concernée.

Il existe de nombreux exemples de données à caractère personnel qui sont sciemment et activement «fournies» par la personne concernée, comme les données relatives à un compte (par exemple, adresse postale, nom d'utilisateur, âge) transmises via des formulaires en ligne. Néanmoins, les données «fournies» par la personne concernée peuvent également découler de l'observation de l'activité de cette dernière. Par conséquent, le groupe de travail «Article 29»

[18] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf

considère que pour donner tout son effet à ce nouveau droit, il convient que le terme «fournies» couvre également les données personnelles qui sont observées dans le cadre des activités des utilisateurs, telles que les données brutes traitées par un compteur intelligent ou d'autres types d'objets connectés[19], les journaux d'activités, l'historique d'utilisation d'un site web ou des activités de recherche.

Cette dernière catégorie de données n'inclut pas les données qui sont générées par le responsable du traitement (au moyen des données observées ou directement fournies comme intrants), telles qu'un profil d'utilisateur créé par l'analyse des données brutes collectées à partir d'un compteur intelligent.

Une distinction peut être opérée entre différentes catégories de données, en fonction de leur origine, afin de déterminer si elles sont couvertes par le droit à la portabilité des données. Les catégories suivantes peuvent être qualifiées de données «fournies par la personne concernée»:

- **les données activement et sciemment fournies par la personne concernée** (par exemple, adresse postale, nom d'utilisateur, âge, etc.);
- **les données observées fournies par la personne concernée grâce à l'utilisation du service ou du dispositif**. Ces données peuvent inclure, par exemple, l'historique de recherche, les données relatives au trafic et les données de localisation d'une personne. Elles peuvent aussi inclure d'autres données brutes comme le rythme cardiaque enregistré par un dispositif portable.

En revanche, les données déduites et les données dérivées sont créées par le responsable du traitement sur la base des données «fournies par la personne concernée». Par exemple, le résultat d'une appréciation relative à la santé d'un utilisateur ou un profil créé dans le contexte des règlementations relatives à la gestion des risques et de la réglementation financière (par ex., pour attribuer une cote de solvabilité ou respecter les règles en matière de lutte contre le blanchiment d'argent) ne peuvent pas être considérés en soi comme ayant été «fournis» par la personne concernée. Bien que ces données puissent faire partie d'un profil conservé par un responsable du traitement et soient déduites ou dérivées d'une analyse des données fournies par la personne concernée (par ses actions, par exemple), ces données ne seront généralement pas considérées comme étant «fournies par la personne concernée» et ne relèveront dès lors pas du champ d'application de ce nouveau droit[20].

En général, compte tenu des objectifs stratégiques du droit à la portabilité des données, l'expression «fournies par la personne concernée» doit être interprétée au sens large, et devrait exclure les «données déduites» et les «données dérivées», qui incluent les données à caractère personnel qui sont créées par un prestataire de services (par exemple, des résultats algorithmiques). Un responsable du traitement peut exclure ces données déduites, mais doit

[19] En ayant la possibilité d'extraire les données résultant de l'observation de son activité, la personne concernée pourra également disposer d'un meilleur aperçu des choix de mise en œuvre posés par le responsable du traitement en ce qui concerne la portée des données observées et sera plus à même de choisir les données qu'elle est prête à fournir pour obtenir un service similaire, de même qu'elle saura dans quelle mesure son droit à la vie privée est respecté.

[20] Néanmoins, la personne concernée peut continuer à exercer son «droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel», ainsi que son droit d'accès à des informations concernant «l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée», conformément à l'article 15 du règlement général sur la protection des données (qui fait référence au droit d'accès).

inclure toutes les autres données à caractère personnel fournies par la personne concernée via les moyens techniques mis à disposition par le responsable du traitement[21].

Par conséquent, l'expression «fournies par» englobe les données à caractère personnel qui se rapportent à l'activité de la personne concernée ou qui résultent de l'observation du comportement d'une personne, mais exclut les données résultant d'une analyse subséquente de ce comportement. En revanche, les données à caractère personnel qui ont été créées par le responsable du traitement dans le cadre du traitement des données, par exemple, par un processus de personnalisation ou de recommandation, par catégorisation ou profilage des utilisateurs, sont des données qui sont dérivées ou déduites des données à caractère personnel fournies par la personne concernée et elles ne sont pas couvertes par le droit à la portabilité des données.

Troisième condition: le droit à la portabilité des données ne doit pas porter atteinte aux droits et libertés de tiers

En ce qui concerne les données à caractère personnel relatives à d'autres personnes concernées:

La troisième condition vise à empêcher l'extraction et la transmission de données contenant les données à caractère personnel d'autres personnes concernées (non consentantes) à un nouveau responsable du traitement dans le cas où ces données sont susceptibles d'être traitées d'une manière qui porterait atteinte aux droits et aux libertés des autres personnes concernées (article 20, paragraphe 4, du règlement général sur la protection des données)[22].

Une telle atteinte interviendrait, par exemple, si la transmission de données d'un responsable du traitement à un autre empêchait des tiers d'exercer leurs droits en tant que personnes concernées en vertu du règlement général sur la protection des données (comme le droit à l'information, le droit d'accès, etc.).

La personne concernée qui initie la transmission des données la concernant à un autre responsable du traitement soit donne son consentement au nouveau responsable du traitement aux fins du traitement de ses données, soit conclut un contrat avec ce dernier. Lorsque des données à caractère personnel de tiers sont comprises dans l'ensemble de données, une autre base juridique doit être définie pour le traitement. Par exemple, un intérêt légitime peut être poursuivi par le responsable du traitement au titre de l'article 6, paragraphe 1, point f), en particulier lorsque l'objectif du responsable du traitement est de fournir à la personne concernée un service qui permet à cette dernière de traiter des données à caractère personnel dans le cadre d'une activité purement personnelle ou domestique. L'opération de traitement initiée par la personne concernée dans le cadre d'une activité personnelle qui concerne et

[21] Sont incluses toutes les données observées au sujet de la personne concernée durant les activités pour lesquelles les données sont collectées, comme l'historique des transactions ou le protocole des accès. Les données collectées au moyen du suivi et de l'enregistrement de la personne concernée (comme une application enregistrant le rythme cardiaque ou une technologie utilisée pour suivre le comportement de navigation sur le web) doivent également être considérées comme étant «fournies par» la personne concernée, même si les données ne sont pas activement ou sciemment transmises.

[22] Le considérant 68 dispose que «[l]orsque, dans un ensemble de données à caractère personnel, plusieurs personnes sont concernées, le droit de recevoir les données à caractère personnel devrait s'entendre sans préjudice des droits et libertés des autres personnes concernées conformément au présent règlement».

affecte potentiellement des tiers reste de sa responsabilité dans la mesure où ce traitement n'est, en aucune manière, décidé par le responsable du traitement.

Par exemple, un service de messagerie peut permettre la création d'un répertoire de contacts, d'amis, de parents, de membres de la famille et de connaissances plus éloignées d'une personne concernée. Dans la mesure où ces données concernent la personne identifiable qui souhaite exercer son droit à la portabilité des données (et sont créées par celle-ci), les responsables du traitement doivent transmettre à cette personne concernée l'ensemble du répertoire des courriers électroniques entrants et sortants.

De même, le compte bancaire d'une personne concernée peut contenir des données à caractère personnel relatives aux transactions non seulement du titulaire du compte, mais aussi d'autres personnes (par exemple en cas de virement d'argent au titulaire du compte). Il est peu probable que les droits et libertés de ces tiers soient compromis par la transmission des informations concernant le compte bancaire au titulaire du compte dans le cadre d'une demande de portabilité, pour autant que, dans les deux exemples, les données soient utilisées à la même fin (c'est-à-dire, une adresse de contact utilisée uniquement par la personne concernée ou l'historique du compte bancaire de la personne concernée).

À l'inverse, les droits et libertés des tiers ne seront pas respectés si le nouveau responsable du traitement utilise les données à caractère personnel à d'autres fins, par exemple, si le responsable du traitement destinataire des données utilise les données à caractère personnel d'autres personnes figurant dans le carnet d'adresses de la personne concernée à des fins de marketing.

Par conséquent, afin d'éviter qu'il soit porté atteinte aux tiers concernés, le traitement de ces données à caractère personnel par un autre responsable du traitement est permis uniquement dans la mesure où les données sont conservées sous le seul contrôle de l'utilisateur demandeur et sont gérées uniquement à des fins purement personnelles ou domestiques. Un «nouveau» responsable du traitement destinataire (auquel les données peuvent être transmises à la demande de l'utilisateur) ne peut pas utiliser les données de tiers qui lui sont transmises à des fins qui lui sont propres, par exemple pour proposer des produits et services de marketing à ces autres tierces personnes concernées. Par exemple, ces informations ne doivent pas être utilisées pour enrichir le profil de la tierce personne concernée et reconstruire son environnement social, sans qu'elle en soit informée et qu'elle y ait consenti[23]. Elles ne peuvent pas non plus être utilisées pour extraire des informations concernant ces tiers et créer des profils spécifiques, même si le responsable du traitement est déjà en possession de leurs données à caractère personnel. Dans le cas contraire, ce traitement est susceptible d'être illicite et abusif, en particulier si les tiers concernés ne sont pas informés et ne peuvent exercer leurs droits en tant que personnes concernées.

Par ailleurs, il est de bonne pratique pour tous les responsables du traitement (qu'il s'agisse de la partie émettrice ou destinataire des données) de mettre en œuvre des outils permettant aux personnes concernées de choisir les données qu'elles souhaitent recevoir et transmettre et d'exclure, le cas échéant, les données d'autres personnes. Cette manière de procéder

[23] Un service de réseaux sociaux ne doit pas enrichir le profil de ses membres en utilisant des données à caractère personnel transmises par une personne concernée dans le cadre de son droit à la portabilité des données sans respecter le principe de transparence et veiller à ce que ce traitement spécifique repose sur une base juridique appropriée.

contribuera à réduire les risques pour les tiers dont les données à caractère personnel pourraient être concernées par la portabilité.

Par ailleurs, les responsables du traitement devraient mettre en place des mécanismes de consentement applicables à d'autres personnes concernées, afin de faciliter la transmission de données dans les cas où ces parties veulent donner leur consentement, par exemple si celles-ci veulent également transférer leurs données à un autre responsable du traitement. Cette situation peut se produire, par exemple, dans le cas des réseaux sociaux, mais il appartient aux responsables du traitement de décider de la meilleure pratique à suivre.

En ce qui concerne les données couvertes par la propriété intellectuelle et le secret des affaires:
Les droits et libertés d'autrui sont mentionnés à l'article 20, paragraphe 4. Bien qu'elle ne soit pas directement liée à la portabilité, cette notion peut s'entendre comme incluant le «secret des affaires ou [...] la propriété intellectuelle, notamment [le] droit d'auteur protégeant le logiciel». Toutefois, s'il convient de prendre en considération ces droits avant de répondre à une demande de portabilité des données, «ces considérations ne devraient pas aboutir à refuser toute communication d'informations à la personne concernée». En outre, le responsable du traitement ne doit pas rejeter une demande de portabilité des données sur la base d'une violation d'un autre droit contractuel (par exemple, une dette en suspens ou un litige commercial avec la personne concernée).

Le droit à la portabilité des données n'est pas un droit permettant à une personne d'abuser des informations d'une manière qui pourrait être qualifiée de déloyale ou qui constituerait une violation des droits de propriété intellectuelle.

Toutefois, un risque commercial potentiel ne saurait, en soi, motiver un refus de répondre à la demande de portabilité et les responsables du traitement peuvent transmettre les données à caractère personnel fournies par les personnes concernées sous une forme qui ne divulgue pas des informations couvertes par le secret des affaires ou par des droits de propriété intellectuelle.

IV. De quelle manière les règles générales régissant l'exercice des droits de la personne concernée s'appliquent-elles à la portabilité des données?

- **Quelles sont les informations préalables à fournir à la personne concernée?**

Afin de respecter le nouveau droit à la portabilité des données, les responsables du traitement doivent informer les personnes concernées de l'existence de ce nouveau droit. Lorsque les données à caractère personnel concernées sont collectées directement auprès de la personne concernée, cette information doit avoir lieu «au moment où les données en question sont obtenues». Si les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, le responsable du traitement doit fournir les informations requises par l'article 13, paragraphe 2, point b), et l'article 14, paragraphe 2, point c).

«Lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée», l'article 14, paragraphe 3, exige que les informations soient fournies dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas

un mois, au moment de la première communication avec la personne concernée ou lorsque les données à caractère personnel sont communiquées à des tiers[24].

Lorsqu'ils fournissent les informations requises, les responsables du traitement doivent veiller à opérer une distinction entre le droit à la portabilité des données et les autres droits. Par conséquent, le groupe de travail «Article 29» recommande en particulier que les responsables du traitement expliquent clairement la différence entre les types de données qu'une personne concernée peut recevoir en exerçant son droit d'accès et son droit à la portabilité.

En outre, le groupe de travail recommande que les responsables du traitement incluent toujours des informations concernant le droit à la portabilité des données avant toute clôture de compte par une personne concernée. Cette mesure permet aux utilisateurs de faire le point sur leurs données à caractère personnel et de les transférer facilement vers leur propre dispositif ou tout autre prestataire avant la résiliation d'un contrat.

Enfin, en tant que meilleure pratique pour les responsables du traitement «destinataires», le groupe de travail «Article 29» recommande que les personnes concernées reçoivent des informations complètes sur la nature des données à caractère personnel qui sont pertinentes aux fins de l'exécution des services considérés. Outre qu'elle renforce le caractère loyal du traitement, cette pratique permet aux utilisateurs de limiter les risques pour les tiers, ainsi que toute autre duplication inutile de données à caractère personnel, même lorsqu'aucune autre personne n'est concernée.

- **De quelle manière le responsable du traitement peut-il identifier la personne concernée avant de répondre à sa demande?**

Le règlement général sur la protection des données ne contient aucune prescription normative concernant la manière d'authentifier la personne concernée. Néanmoins, l'article 12, paragraphe 2, dudit règlement dispose que le responsable du traitement ne peut pas refuser de donner suite à la demande de la personne concernée d'exercer ses droits (y compris le droit à la portabilité des données), à moins qu'il ne traite des données à caractère personnel pour une finalité qui n'exige pas l'identification d'une personne concernée et qu'il puisse démontrer qu'il n'est pas en mesure d'identifier la personne concernée. Toutefois, conformément à l'article 11, paragraphe 2, en pareils cas, la personne concernée peut fournir des informations complémentaires qui permettent de l'identifier. Par ailleurs, l'article 12, paragraphe 6, dispose que lorsque le responsable du traitement a des doutes raisonnables quant à l'identité de la personne concernée, il peut demander que lui soient fournies des informations supplémentaires nécessaires pour confirmer l'identité de la personne concernée. Lorsqu'une personne concernée fournit des informations complémentaires permettant de l'identifier, le responsable du traitement ne peut refuser de donner suite à la demande. Lorsque les informations et données collectées en ligne sont liées à des pseudonymes ou à des identifiants uniques, les responsables du traitement peuvent appliquer des procédures appropriées permettant à une personne de présenter une demande de portabilité des données et de recevoir des données la concernant. En tout état de cause, les responsables du traitement doivent appliquer une procédure d'authentification afin d'établir avec certitude l'identité de la

[24] L'article 12 exige que le responsable du traitement procède à «toute communication […] d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant.»

personne concernée demandant ses données à caractère personnel ou, plus généralement, exerçant les droits conférés par le règlement général sur la protection des données.

Ces procédures existent déjà souvent. À l'heure actuelle, les personnes concernées sont souvent déjà authentifiées par le responsable du traitement avant la conclusion d'un contrat ou la collecte de leur consentement au traitement. Par conséquent, les données à caractère personnel utilisées pour enregistrer la personne concernée par le traitement peuvent également être utilisées comme preuves pour l'authentification de cette personne aux fins de la portabilité[25].

Si, en pareils cas, l'identification préalable des personnes concernées peut nécessiter une demande de preuve de leur identité légale, cette vérification peut ne pas être pertinente pour évaluer le lien entre les données et la personne concernée, étant donné que ce lien est sans rapport avec l'identité officielle ou légale. Fondamentalement, la possibilité, pour le responsable du traitement, de demander à la personne concernée des informations complémentaires destinées à vérifier son identité ne peut donner lieu à des exigences excessives ni à la collecte de données à caractère personnel qui ne sont pas pertinentes ni nécessaires au renforcement du lien entre la personne et les données à caractère personnel demandées.

Dans de nombreux cas, de telles procédures d'authentification sont déjà en place. Par exemple, les noms d'utilisateur et les mots de passe sont souvent utilisés pour permettre à des personnes d'accéder à leurs données contenues dans leurs comptes de messagerie, leurs comptes sur des réseaux sociaux et les comptes utilisés pour différents services, que certaines personnes choisissent d'utiliser sans révéler leurs identité et nom complets.

Si le volume des données demandées par la personne concernée rend la transmission via l'internet problématique, au lieu de prévoir éventuellement une prolongation de délai de maximum trois mois afin de répondre à cette demande[26], le responsable du traitement pourrait également devoir envisager d'autres moyens de transmettre les données, notamment en utilisant la diffusion en flux ou le stockage sur un CD, un DVD ou d'autres supports physiques ou en autorisant que les données à caractère personnel soient transmises directement à un autre responsable du traitement (conformément à l'article 20, paragraphe 2, du règlement général sur la protection des données, lorsque cela est techniquement possible).

- **Quel est le délai imparti pour répondre à une demande de portabilité?**

L'article 12, paragraphe 3, requiert que le responsable du traitement fournisse à la personne concernée «des informations sur les mesures prises» «dans les meilleurs délais» et en tout état de cause «dans un délai d'un mois à compter de la réception de la demande». Ce délai d'un mois peut être prolongé à un maximum de trois mois pour les affaires complexes, à condition que la personne concernée ait été informée des motifs de cette prolongation dans un délai d'un mois à compter de la réception de la demande initiale.

Les responsables du traitement fournissant des services informatiques sont susceptibles d'être mieux équipés pour pouvoir répondre à des demandes dans un délai très court. Afin de

[25] Par exemple, lorsque le traitement des données est lié à un compte d'utilisateur, la communication de l'identifiant et du mot de passe correspondant à ce compte peut suffire à identifier la personne concernée.
[26] Article 12, paragraphe 3: «Le responsable du traitement fournit des informations sur les mesures prises à la suite d'une demande».

répondre aux attentes de l'utilisateur, une bonne pratique consiste à définir le délai dans lequel une réponse peut d'ordinaire être donnée à une demande de portabilité de données et à communiquer cette information aux personnes concernées.

Le responsable du traitement qui ne donne pas suite à une demande de portabilité informe la personne concernée, conformément à l'article 12, paragraphe 4, «des motifs de son inaction et de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel», dans un délai maximal d'un mois à compter de la réception de la demande.

Les responsables du traitement doivent respecter l'obligation de répondre à la demande dans les conditions prescrites, même s'il s'agit de signifier un refus. En d'autres termes, le responsable du traitement est tenu de répondre à une demande de portabilité des données.

- **Dans quels cas une demande de portabilité des données peut-elle être rejetée ou subordonnée au paiement de frais?**

L'article 12 interdit au responsable du traitement d'exiger un paiement pour fournir les données à caractère personnel, à moins qu'il puisse démontrer que les demandes sont manifestement infondées ou excessives, «notamment en raison de leur caractère répétitif». Pour les services de la société de l'information spécialisés dans le traitement automatisé de données à caractère personnel, la mise en œuvre de systèmes automatisés, tels que des interfaces de programme d'application (API)[27], peut faciliter les échanges avec les personnes concernées et donc alléger la charge potentielle découlant de demandes répétées. Par conséquent, les cas dans lesquels le responsable du traitement peut justifier un refus de fournir les informations demandées devraient être très rares, même lorsqu'il est question de demandes multiples de portabilité des données.

En outre, le coût global des processus créés pour répondre aux demandes de portabilité des données ne devrait pas être pris en considération pour déterminer le caractère excessif d'une demande. En effet, l'article 12 du règlement général sur la protection des données se concentre sur les demandes introduites par une personne concernée et non sur le nombre total de demandes reçues par le responsable du traitement. En conséquence, les coûts totaux liés à la mise en œuvre du système ne devraient pas être imputés aux personnes concernées ni invoqués pour justifier un refus de répondre à des demandes de portabilité.

V. De quelle manière les données portables doivent-elles être fournies?

- **Quels sont les moyens que le responsable du traitement est censé mettre en œuvre pour fournir les données?**

L'article 20, paragraphe 1, du règlement général sur la protection des données dispose que les personnes concernées ont le droit de transmettre les données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle.

[27] Le terme «interface de programme d'application» (API) désigne les interfaces d'applications ou les services web mis à disposition par les responsables du traitement de sorte que d'autres systèmes ou applications puissent se mettre en relation avec leurs systèmes et travailler avec ceux-ci.

Il peut s'agir d'entraves juridiques, techniques ou financières mises en place par le responsable du traitement pour empêcher ou ralentir l'accès aux données, leur transmission ou leur réutilisation par la personne concernée ou par un autre responsable du traitement, par exemple, des frais demandés pour la fourniture des données; un manque d'interopérabilité ou l'absence d'accès à un format de données ou à une interface de programme d'application ou le format fourni; des délais ou une complexité excessifs pour extraire l'intégralité de l'ensemble de données; l'obscurcissement délibéré de l'ensemble de données; ou encore une normalisation sectorielle ou des exigences en matière d'accréditation spécifiques et abusives ou excessives[28].

L'article 20, paragraphe 2, fait également obligation aux responsables du traitement de transmettre directement les données portables à d'autres responsables du traitement «lorsque cela est techniquement possible».

La possibilité technique de la transmission de responsable du traitement à responsable du traitement, sous le contrôle de la personne concernée, doit être évaluée au cas par cas. Le considérant 68 précise les limites de ce qui est «techniquement possible», indiquant que ce droit «ne devrait pas créer, pour les responsables du traitement, d'obligation d'adopter ou de maintenir des systèmes de traitement qui sont techniquement compatibles».

Les responsables du traitement sont censés transmettre les données à caractère personnel dans un format interopérable, bien que cela n'oblige pas les autres responsables du traitement à prendre en charge ces formats. La transmission directe d'un responsable du traitement à un autre peut par conséquent avoir lieu lorsque la communication entre deux systèmes est possible, de manière sécurisée[29], et lorsque le système récepteur est techniquement en mesure de recevoir les données entrantes. Si des entraves techniques empêchent la transmission directe, le responsable du traitement doit expliquer celles-ci à la personne concernée, car, dans le cas contraire, sa décision sera considérée comme semblable, dans ses effets, à un refus de donner suite à la demande formulée par la personne concernée (article 12, paragraphe 4).

Du point de vue technique, les responsables du traitement devraient envisager et évaluer deux modes différents et complémentaires pour mettre les données portables à la disposition des personnes concernées ou d'autres responsables du traitement:

- une transmission directe de l'intégralité de l'ensemble de données portables (ou plusieurs extraits de parties de l'ensemble global de données);
- un outil automatisé permettant l'extraction des données pertinentes.

Le deuxième mode de transmission peut être privilégié par les responsables du traitement dans les cas impliquant des ensembles de données volumineux et complexes, étant donné qu'il permet l'extraction de toute partie de l'ensemble de données pertinente pour la personne concernée dans le cadre de sa demande, peut contribuer à réduire le risque au minimum et

[28] Certaines entraves légitimes peuvent survenir, par exemple celles qui sont liées aux droits et libertés de tiers visés à l'article 20, paragraphe 4, ou celles qui ont trait à la sécurité des propres systèmes des responsables du traitement. Il incombe au responsable du traitement de justifier en quoi ces entraves sont justifiées et pourquoi il ne s'agit pas d'obstacles au sens de l'article 20, paragraphe 1.

[29] Par une communication authentifiée présentant le niveau de chiffrement des données nécessaire.

permet éventuellement l'utilisation de mécanismes de synchronisation[30] (par exemple, dans le contexte d'une communication régulière entre responsables du traitement). Il peut s'agir d'une meilleure manière d'assurer la conformité pour le «nouveau» responsable du traitement et constituerait une bonne pratique en ce qui concerne la réduction des risques liés à la confidentialité de la part du responsable du traitement initial.

Ces deux manières différentes et éventuellement complémentaires de fournir les données portables pertinentes pourraient être mises en œuvre par la mise à disposition des données au moyen, par exemple, de messages sécurisés, d'un serveur SFTP, d'une interface de programme d'application web ou d'un portail web sécurisés. Les personnes concernées devraient avoir la possibilité d'utiliser un entrepôt de données personnelles, un système de gestion des informations personnelles[31] ou d'autres types de services de tiers de confiance pour conserver et stocker leurs données à caractère personnel et accorder aux responsables du traitement l'autorisation d'accéder aux données personnelles et de les traiter en tant que de besoin.

- **Quel est le format de données attendu?**

Le règlement général sur la protection des données exige du responsable du traitement qu'il fournisse les données à caractère personnel demandées par la personne concernée dans un format qui permet leur réutilisation. Plus spécifiquement, l'article 20, paragraphe 1, du règlement général sur la protection des données dispose que les données à caractère personnel doivent être fournies «dans un format structuré, couramment utilisé et lisible par machine». Le considérant 68 précise que ce format doit être interopérable, un terme qui est défini[32] comme suit dans l'Union:

> *la capacité de diverses organisations hétérogènes à interagir en vue d'atteindre des objectifs communs, mutuellement avantageux et convenus, impliquant le partage d'informations et de connaissances entre elles, selon les processus d'entreprise qu'elles prennent en charge, par l'échange de données entre leurs systèmes TIC respectifs.*

Les qualificatifs «structuré», «couramment utilisé» et «lisible par machine» constituent une série d'exigences minimales qui devraient faciliter l'interopérabilité du format de données fourni par le responsable du traitement. En ce sens, les termes «structuré, couramment utilisé et lisible par machine» donnent des précisions sur les moyens, tandis que l'interopérabilité est le résultat escompté.

Le considérant 21 de la directive 2013/37/UE[33] [34]définit le format «lisible par machine» comme suit:

[30] Les mécanismes de synchronisation contribuent au respect de l'obligation générale établie à l'article 5 du règlement général sur la protection des données, qui dispose que les données à caractère personnel «doivent être [...] exactes et, si nécessaire, tenues à jour».
[31] Pour les systèmes de gestion des informations personnelles (PIMS), voir, par exemple, l'avis 9/2016 du CEPD, à l'adresse:https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_fr.pdf
[32] Article 2 de la décision nº 922/2009/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant des solutions d'interopérabilité pour les administrations publiques européennes (ISA), JO L 260 du 3.10.2009, p. 20.
[33] Modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public.

un format de fichier structuré de telle manière que des applications logicielles puissent facilement identifier, reconnaître et extraire des données spécifiques, notamment chaque énoncé d'un fait et sa structure interne. Les données encodées présentes dans des fichiers qui sont structurés dans un format lisible par machine sont des données lisibles par machine. Les formats lisibles par machine peuvent être ouverts ou propriétaires; il peut s'agir de normes formelles ou non. Les documents encodés dans un format de fichier qui limite le traitement automatique, en raison du fait que les données ne peuvent pas, ou ne peuvent pas facilement, être extraites de ces documents, ne devraient pas être considérés comme des documents dans des formats lisibles par machine. Les États membres devraient, le cas échéant, encourager l'utilisation de formats ouverts, lisibles par machine.

Compte tenu de la grande variété de types de données potentiels qui pourraient être traités par un responsable du traitement, le règlement général sur la protection des données n'impose pas de recommandations spécifiques quant au format des données à caractère personnel à fournir. Le format le plus approprié différera d'un secteur à l'autre et des formats adéquats peuvent déjà exister, et doivent toujours être choisis de manière à pouvoir être interprétés et offrir à la personne concernée un degré élevé de portabilité. Dès lors, les formats qui sont soumis à des contraintes de licences onéreuses ne sont pas considérés comme relevant d'une approche adéquate.

Le considérant 68 précise que «*[l]e droit de la personne concernée de transmettre ou de recevoir des données à caractère personnel la concernant ne devrait pas créer, pour les responsables du traitement, d'obligation d'adopter ou de maintenir des systèmes de traitement qui sont techniquement compatibles*». **Dès lors, la portabilité vise à produire des systèmes interopérables, et non des systèmes compatibles**[35].

Les données à caractère personnel devraient être fournies dans des formats dont le niveau d'abstraction par rapport à tout format interne ou propriétaire est élevé. En tant que telle, la portabilité des données suppose un traitement des données supplémentaire par les responsables du traitement, afin d'extraire les données des plates-formes et de filtrer les données à caractère personnel hors du champ d'application de la portabilité, comme les données déduites ou les données liées à la sécurité des systèmes. Ainsi, les responsables du traitement sont encouragés à recenser préalablement les données qui relèvent du champ d'application de la portabilité dans leurs propres systèmes. Ce traitement de données supplémentaire sera considéré comme accessoire au traitement des données principal parce qu'il n'est pas effectué pour réaliser une nouvelle finalité définie par le responsable du traitement.

Lorsqu'aucun format n'est d'usage courant dans un secteur ou un contexte donné, **les responsables du traitement devraient fournir les données à caractère personnel au moyen de formats ouverts communément utilisés (par exemple XML, JSON, CSV, etc.), assortis de métadonnées** utiles **au meilleur niveau de granularité possible,** tout en maintenant un niveau d'abstraction élevé. À cet effet, il convient d'utiliser des métadonnées

[34] Le glossaire de l'UE (http://eur-lex.europa.eu/eli-register/glossary.html) fournit davantage de précisions quant aux attentes liées aux notions utilisées dans les présentes lignes directrices, telles que *lisible par machine, interopérabilité, format ouvert, norme* ou *métadonnées.*

[35] La norme ISO/IEC 2382-01 définit l'interopérabilité comme suit: «La possibilité de communiquer, d'exécuter des programmes, ou de transférer des données entre diverses unités fonctionnelles d'une façon qui n'exige que peu, voire aucune connaissance des caractéristiques particulières de ces unités de la part de l'utilisateur».

appropriées afin de décrire précisément la signification des informations échangées. Ces métadonnées devraient être suffisantes pour rendre possibles la fonction et la réutilisation des données, sans, bien entendu, violer le secret des affaires. Il est par conséquent peu probable qu'une version PDF d'une boîte de messagerie électronique fournie à une personne soit suffisamment structurée ou descriptive pour permettre la réutilisation aisée des données de la boîte de messagerie. Les données contenues dans les courriers électroniques devraient plutôt être fournies dans un format qui préserve toutes les métadonnées, afin de permettre une réutilisation efficace des données. À cet effet, lorsqu'il sélectionne un format de données dans lequel fournir les données à caractère personnel, le responsable du traitement doit examiner en quoi ce format pourrait affecter ou entraver le droit de la personne à réutiliser les données. Dans les cas où un responsable du traitement est en mesure de fournir à la personne concernée des choix quant au format de données à caractère personnel qu'elle préfère, il doit expliquer clairement l'incidence de ce choix. Toutefois, le traitement de métadonnées supplémentaires uniquement parce qu'elles pourraient être nécessaires ou souhaitées dans le cadre d'une demande de portabilité des données ne constitue pas un motif légitime pour ce traitement.

Le groupe de travail «Article 29» encourage la coopération entre les parties prenantes de l'industrie et les associations professionnelles afin qu'elles travaillent de concert sur une série commune de normes et de formats interopérables en vue de satisfaire aux exigences liées au droit à la portabilité des données. Ce défi a également été relevé par le cadre d'interopérabilité européen (EIF, European Interoperability Framework), qui a défini une approche commune de l'interopérabilité pour les organisations souhaitant collaborer en vue de la fourniture de services publics. Au sein de son champ d'application, le cadre définit un ensemble d'éléments communs tels que le vocabulaire, les concepts, les principes, les politiques, les lignes directrices, les recommandations, les normes, les spécifications et les pratiques[36].

- **Comment traiter une collecte de données à caractère personnel de grande ampleur ou complexe?**

Le règlement général sur la protection des données n'explique pas comment relever le défi d'une collecte de données de grande ampleur, d'une structure de données complexe ou d'autres problèmes techniques susceptibles de créer des difficultés pour les responsables du traitement ou les personnes concernées.

Toutefois, dans tous les cas, il est capital que la personne soit en mesure de comprendre pleinement la définition, le schéma et la structure des données à caractère personnel qui pourraient être fournies par le responsable du traitement. Par exemple, les données pourraient d'abord être fournies dans un format résumé au moyen de tableaux permettant à la personne concernée de transmettre des sous-ensembles de données à caractère personnel plutôt que l'intégralité de celles-ci. Le responsable du traitement doit fournir un aperçu «d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples» (voir l'article 12, paragraphe 1, du règlement général sur la protection des données), de manière à ce que la personne concernée dispose toujours d'informations claires quant aux données à télécharger ou à transmettre à un autre responsable du traitement en relation avec une finalité donnée. Par exemple, les personnes concernées doivent être en mesure d'utiliser des applications logicielles afin d'identifier, de reconnaître et de traiter facilement des données spécifiques.

[36] Source: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

Comme indiqué ci-dessus, une manière pratique permettant à un responsable du traitement de répondre à des demandes de portabilité des données pourrait consister à offrir une API dûment sécurisée et documentée. Les personnes concernées pourraient ainsi introduire auprès du responsable du traitement des demandes de données à caractère personnel via leur propre logiciel ou le logiciel d'un tiers ou accorder à d'autres (y compris un autre responsable du traitement) la permission de le faire en leur nom, comme précisé à l'article 20, paragraphe 2, du règlement général sur la protection des données. En accordant l'accès à des données par l'intermédiaire d'une interface de programme d'application accessible depuis l'extérieur, il pourrait également être possible de proposer un système d'accès plus sophistiqué permettant aux personnes d'introduire des demandes de données ultérieures, sous la forme soit d'un téléchargement complet, soit d'une fonction delta contenant uniquement les modifications apportées depuis le dernier téléchargement, sans que ces demandes supplémentaires soient onéreuses pour le responsable du traitement.

- **De quelle manière les données portables peuvent-elles être sécurisées?**

En général, conformément à l'article 5, paragraphe 1, point f), du règlement général sur la protection des données, les responsables du traitement doivent garantir la «sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées».

Toutefois, la transmission des données à caractère personnel à la personne concernée peut aussi poser des problèmes de sécurité:

Comment les responsables du traitement peuvent-ils garantir la fourniture sécurisée de données à caractère personnel à la bonne personne?

La portabilité des données étant destinée à extraire des données à caractère personnel du système d'information du responsable du traitement, la transmission peut devenir une source de risque possible pour ces données (en particulier, un risque de violation des données pendant la transmission). Il incombe au responsable du traitement de prendre toutes les mesures de sécurité qui s'imposent afin de garantir non seulement la transmission sécurisée des données à caractère personnel (par exemple, en utilisant le chiffrement de bout en bout ou le cryptage de données) au bon destinataire (par exemple, en utilisant des informations d'authentification fortes), mais aussi de maintenir la protection des données à caractère personnel qui restent dans ses systèmes, ainsi que d'établir des procédures transparentes pour remédier aux éventuelles violations des données[37]. Pour ce faire, il doit évaluer les éventuels risques spécifiques liés à la portabilité des données et prendre les mesures d'atténuation des risques appropriées.

Les mesures d'atténuation des risques précitées pourraient inclure: si la personne concernée doit déjà s'authentifier, l'utilisation d'informations d'authentification supplémentaires, telles qu'un secret partagé ou un autre élément d'authentification comme un mot de passe à usage unique; la suspension ou le gel de la transmission, s'il existe une suspicion de compromission du compte; en cas de transmission directe d'un responsable du traitement à un autre, il convient d'utiliser une authentification par mandat, telle que l'authentification par jeton.

[37] Conformément à la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

De telles mesures de sécurité ne doivent pas être obstructives par nature et ne doivent pas empêcher les utilisateurs d'exercer leurs droits, notamment en imposant des coûts supplémentaires.

Comment aider les utilisateurs à sécuriser le stockage de leurs données à caractère personnel dans leur propre système?

En récupérant leurs données à caractère personnel d'un service en ligne, les utilisateurs courent toujours le risque de stocker ces données dans des systèmes moins sécurisés que celui fourni par le service. Il incombe à la personne concernée demandant les données de définir les bonnes mesures pour sécuriser les données à caractère personnel dans son propre système. Toutefois, la personne concernée doit être informée de ce risque afin de prendre les mesures nécessaires pour protéger les informations qu'elle a reçues. Comme exemple de bonne pratique, les responsables du traitement pourraient aussi recommander des formats, outils de chiffrement ou autres mesures de sécurité appropriés pour aider les personnes concernées à atteindre cet objectif.

* * *

Fait à Bruxelles, le 13 décembre 2016

Pour le groupe de travail,
La présidente
Isabelle FALQUE-PIERROTIN

Version révisée et adoptée le 5 avril 2017

Pour le groupe de travail
La présidente
Isabelle FALQUE-PIERROTIN