# Le droit à la portabilité des données à caractère personnel

Knockaert, Manon; Colin, Jean-Noël

*Published in:*
DPO news

*Publication date:*
2019

*Document Version*
le PDF de l'éditeur

Dossier

# Le droit à la portabilité des données à caractère personnel : coup d'œil juridique et technique

*À la suite de l'entrée en application du RGPD, la personne concernée bénéficie d'un nouveau droit : le droit à la portabilité. Quelles dispositions légales encadrent la portabilité, et quelles sont leurs implications techniques ?*

## Coup d'œil juridique

### Définition

Le droit à la portabilité s'inscrit dans la droite ligne du droit d'accès aux données et relève de l'objectif du législateur européen de renforcer la maîtrise des individus sur leurs données à caractère personnel[1]. Lorsque le traitement des données à caractère personnel se fonde sur le consentement de la personne concernée ou sur la nécessité d'exécuter un contrat ou des mesures précontractuelles, l'article 20 consacre le droit à la portabilité[2]. Dorénavant, la personne concernée dispose de la possibilité de recevoir ses données à caractère personnel dans un format structuré, couramment utilisé et lisible par machine et de les copier ou de les transférer d'un environnement *IT* à un autre[3]. Pour ce faire, deux options s'offrent à elle. La première lui permet de s'adresser au responsable du traitement initial pour obtenir ses données à caractère personnel et ainsi les transmettre elle-même à un autre responsable du traitement. La seconde lui permet de directement demander au responsable du traitement initial d'envoyer les informations au second responsable du traitement[4]. À cet égard, mentionnons que, sensible aux difficultés techniques, le RGPD n'emporte pas une obligation de développer des systèmes interopérables[5] entre responsables de traitement. En conséquence, le responsable de traitement se voit confier le rôle de « facilitateur »[6]. Cependant, et même si une telle obligation d'interopérabilité n'existe pas comme telle, elle risque de s'imposer *de facto* au responsable du traitement pour qu'il puisse répondre aux demandes de portabilité. Le considérant 68 ne dit rien d'autre en encourageant « les responsables du traitement à mettre au point des formats interopérables permettant la portabilité des données »[7].

Par ailleurs, eu égard à l'article 12 du RGPD, l'exercice, par la personne concernée, de son droit à la portabilité doit être gratuit.

### Conditions

Pour bénéficier du droit à la portabilité, deux conditions doivent être respectées.

Premièrement, le traitement des données doit être fondé sur le consentement de la personne concernée ou sur un contrat auquel elle est partie. Dès lors, il revient au responsable de traitement de faire la part des choses entre les traitements de données pour lesquels la base de légitimation entraîne un droit à la portabilité et les traitements de données reposant sur un fondement autre que le consentement ou le contrat. À cet égard, le Groupe de travail « Article 29 » mentionne expressément l'exemple des données relatives aux employés, pouvant reposer tantôt sur le consentement, tantôt sur une obligation légale ou un intérêt légitime[8].

Deuxièmement, le droit à la portabilité a vocation à s'appliquer aux traitements effectués à l'aide de procédés automatisés.

### Données portables

De manière laconique, l'article 20 dispose que les données qualifiées de portables sont de deux catégories. Il s'agit, premièrement, des données qui concernent la personne exerçant son droit. Pouvant être liées sans ambiguïté à la personne concernée, les données pseudonymisées relèvent de cette notion. *A contrario*, les données à caractère non personnel ainsi que les données anonymisées n'entraînent pas l'application du droit à la portabilité[9].

Deuxièmement, les données fournies par la personne concernée au responsable de traitement sont également des données portables. La portée exacte de ces notions est précisée par les lignes directrices du Groupe de travail « Article 29 ». Cette dernière catégorie comprend, en réalité, deux types d'informations. En premier lieu, les données activement et sciemment fournies au responsable de traitement par la personne concernée. Il s'agira notamment des informations communiquées lors d'une inscription et pour bénéficier adéquatement du service proposé (nom et prénom, adresse de contact, âge, etc.). En second et dernier lieu, le Groupe de travail « Article 29 » précise que rentrent dans la notion de données fournies par la personne concernée les informations à caractère personnel observées par le responsable de traitement grâce à l'utilisation du service ou du dispositif. Cela inclut notamment l'historique de recherche, le nombre de pas effectués au cours d'une journée ou encore les données de localisation[10].

### Données non portables

En revanche, le droit à la portabilité des données ne s'applique pas aux données concernant les utilisateurs, établies par le responsable du traitement sur la base des données à caractère personnel fournies par la personne

[1] Considérant 68 du RGPD.

[2] L'article 20 dispose que : « 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 ».

[3] Groupe de travail « Article 29 », *Lignes directrices relatives au droit à la portabilité des données*, WP 242 rev. 01, 5 avril 2017, p. 4 (ci-après, *Lignes directrices « Article 29 »*). Il importe peu que cet environnement IT soit le système propre de la personne concernée, le système d'un tiers de confiance ou celui d'un autre responsable de traitement.

[4] *Lignes directrices « Article 29 »*, pp. 5-6.

[5] Par systèmes interopérables, nous entendons des transferts de données à caractère personnel directement entre deux responsables de traitement sans intervention manuelle et sans perte d'information.

[6] Précisons qu'aux yeux du Groupe de travail « Article 29 », si la portabilité entraîne un traitement ultérieur des données, celui-ci est considéré comme un traitement accessoire et ne constitue pas en tant que tel la poursuite d'une nouvelle finalité ; *Lignes directrices « Article 29 »*, p. 21.

[7] Considérant 68 du RGPD.

[8] *Lignes directrices « Article 29 »*, p. 10.

[9] *Lignes directives « Article 29 »*.

[10] *Ibid.*, pp. 11-13 ; Th. Tombal, « Les droits de la personne concernée dans le RGPD », in *Le règlement général sur la protection des données (RGPD/GDPR)*, sous la dir. de C. de Terwangne et K. Rosier, Bruxelles, Larcier, 2018, pp. 487 et s.

concernée, principalement par un usage répété du service. Par conséquent, le RGPD semble ainsi faire la distinction entre, d'une part, les données fournies directement ou indirectement par la personne concernée pour l'utilisation du service et lors de son utilisation et, d'autre part, les données issues des opérations de traitement algorithmique permettant d'obtenir des informations additionnelles – par lesquelles un responsable de traitement peut se distinguer d'un autre – sur les utilisateurs. En ce sens, ne sont pas des « données portables » les profils utilisateurs ou le bilan de santé dressé par une montre intelligente. En d'autres termes sont exclues les données déduites et les données dérivées créées par le responsable du traitement sur la base des données fournies par la personne concernée[11].

### Responsabilité du responsable de traitement initial

Du droit à la portabilité découlent d'autres obligations pour un responsable de traitement.

Premièrement, il incombe au responsable de traitement de pouvoir informer adéquatement la personne concernée. Le Groupe de travail « Article 29 » lui recommande d'opérer une distinction explicite entre le droit à la portabilité des données et les autres droits accordés par le RGPD à la personne concernée. En outre, le responsable de traitement doit indiquer clairement les données pouvant être portées à la connaissance de la personne concernée en vertu du droit à la portabilité et celles en application du droit d'accès[12].

Deuxièmement, le Groupe de travail « Article 29 » souligne également que, lors de la fermeture du compte utilisateur, la personne concernée doit à nouveau être informée des possibilités offertes par le droit à la portabilité. Il précise ainsi que « 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 »[13].

Troisièmement, le responsable du traitement devra mettre au point une procédure permettant l'exercice du droit à la portabilité des données. Il est recommandé que cette procédure soit accompagnée d'un mécanisme d'authentification permettant de vérifier l'identité de la personne concernée[14].

Quatrièmement, l'article 12 du RGPD exige que le responsable du traitement réponde, dans un délai raisonnable, à la demande formulée par la personne concernée. Les données à caractère personnel doivent dès lors être fournies sans retard injustifié et, en tout état de cause, dans un délai d'un mois à compter de la réception de la demande. Pour les cas complexes, le délai peut s'étendre jusqu'à trois mois. Dans cette hypothèse, le responsable du traitement doit informer la personne concernée de ce retard dans un délai d'un mois à compter de la demande initiale. Le rejet d'une demande de portabilité doit être accompagné d'une justification appropriée[15].

Cinquièmement, si le responsable de traitement original ne peut être lié par les usages effectués ultérieurement par le second responsable de traitement[16], il doit toutefois prendre toutes les mesures de sécurité nécessaires pour assurer une transmission sécurisée des données et également veiller à l'envoi des données soit à la personne concernée correctement identifiée, soit au responsable de traitement désigné par cette dernière[17].

Sixièmement et enfin, les données à caractère personnel doivent être exactes et tenues à jour. Néanmoins, le droit à la portabilité n'entraîne pas une exigence de contrôle et de vérification de la qualité des données avant transmission à un responsable de traitement ou à la personne concernée. Relevons également que le droit à la portabilité n'emporte pas l'obligation de conserver les données pour une durée excédant celle nécessaire à l'accomplissement des finalités[18].

### Implication du sous-traitant

En vertu de l'article 28 du RGPD, le sous-traitant est tenu d'apporter son aide au responsable de traitement dans l'exercice de leurs droits par les personnes concernées. Lors de la conclusion du contrat de sous-traitance, il est préférable qu'une coopération et que le partage des responsabilités entre le responsable de traitement et le sous-traitant soient explicités pour la mise en œuvre des demandes de portabilité[19].

### Conclusion

Ce droit nouvellement consacré par le RGPD impose au responsable de traitement d'opérer une distinction entre les données à caractère personnel portables et non portables. Par ailleurs, un tel droit ne peut se concevoir sans une information claire et précise envers la personne concernée, tant au moment de l'ouverture d'un compte qu'à sa fermeture. La mise en place d'une procédure permettant d'identifier valablement la personne concernée et de répondre adéquatement à une demande de portabilité semble participer à l'obligation de développer un système *privacy by design*[20].

## Coup d'œil technique

Le droit à la portabilité des données visant à une plus grande interopérabilité, sans entrave, entre des systèmes informatiques, sa prise en compte dans ces systèmes soulève des questions à plusieurs niveaux :

- le format dans lequel les données seront transmises ;
- le moyen technique par lequel elles pourront être obtenues ;
- l'authentification de la personne concernée ;
- la sécurité apportée à la transmission des informations.

Concernant **le format des données**, le règlement prescrit « un format structuré, couramment utilisé et lisible par la machine ». L'objectif sous-jacent est que l'information puisse être aisément extraite, soit par la personne concernée, soit par le responsable de traitement auquel les données sont transmises. Nombre de formats standards de données existent pour les types de données courants, tels que les documents bureautiques, multimédia (image,

[11] *Lignes directrices « Article 29 »*, pp. 12-13 ; Th. Tombal, « Les droits de la personne concernée dans le RGPD », *op. cit.*, pp. 490-492.
Notons que le Groupe de travail « Article 29 » appelle à une interprétation large de la notion de « données fournies par la personne concernée » : *Lignes directrices « Article 29 »*, p. 12.

[12] *Ibid.*, pp. 7 et 15.

[13] *Ibid.*, p. 16.

[14] *Ibid.*, pp. 16-17.

[15] *Ibid.*, pp. 17-18.

[16] Sur le point de la responsabilité du responsable de traitement recevant les données portées, voy. *Lignes directrices « Article 29 »*, pp. 7-8.

[17] *Ibid.*, p. 23.

[18] *Ibid.*, p. 7.

[19] *Ibid.*, p. 7.

[20] Art. 25 du RGPD.

son, vidéo), mais aussi courrier électronique. Ces formats peuvent être ouverts ou propriétaires. Dès qu'un format courant est disponible, il devrait être utilisé, en donnant la préférence aux formats ouverts. Dans d'autres cas, des standards sectoriels permettent aussi de structurer des données de manière interopérable (HL7 par exemple dans le domaine de la santé). Là où de tels formats n'existent pas, il faut alors recourir à des extractions brutes de bas niveau et utiliser des formats structurés tels que csv (*comma-separated values*), xml ou json. Ces formats permettent de structurer des données de manière plus ou moins détaillée et sémantiquement riche. Dans tous les cas, la communication des données devrait être accompagnée d'une description la plus détaillée possible du format utilisé.

Au-delà du simple format de données, il nous semble important de permettre à la personne concernée de reconstituer l'ensemble du contexte informationnel et pas seulement les données ; ainsi, pour un service d'hébergement de photos, il nous paraît peu approprié de permettre à l'utilisateur de récupérer ses photos sans, en même temps, récupérer la structure des dossiers et albums utilisés. Il faut qu'il puisse, à partir des données récupérées, reconstituer le contexte informationnel à l'identique.

La granularité des données à récupérer devrait être laissée au choix de la personne concernée ; plutôt que de lui proposer de récupérer toutes les données faisant l'objet du droit à la portabilité, il serait plus judicieux de lui permettre de sélectionner les données et catégories de données qu'elle souhaite obtenir, rendant ainsi la réutilisation plus aisée et limitant le risque de transmission de données de tiers vers un nouveau responsable de traitement[21].

Pour ce qui est du **moyen technique** par lequel les données peuvent être mises à disposition, il faut réaliser que l'extraction des données du système d'information est un processus pouvant être long, nécessitant l'analyse de plusieurs sources et supports. Il est donc nécessaire de prévoir un mécanisme asynchrone permettant à la personne concernée de soumettre sa demande, et de la notifier lorsque les données ont été rendues disponibles.

Une solution simple pour rendre les données accessibles est de permettre leur téléchargement, soit depuis une page web, soit à partir d'un serveur (sftp par exemple). Pour limiter les problèmes de transmission, il est prudent, en cas de données volumineuses, de les diviser en plusieurs archives à récupérer individuellement. Dans certaines situations où le téléchargement ne peut être proposé, la remise via un support physique (CD, DVD) est une alternative. Dans les deux cas, il faut informer la personne concernée des risques liés au moyen choisi, par exemple la durée de vie du support matériel.

Une autre manière de permettre la récupération des données pour un responsable de traitement est d'offrir un service automatisé, sous la forme d'une interface de type web service ou API – *Application Programming Interface*, permettant cette fois à un logiciel d'extraire les données souhaitées de manière automatique. Ce mode de transfert est de nature à faciliter le transfert direct entre responsables de traitement, mais il convient de protéger correctement l'accès à ce service afin qu'il ne puisse en être fait un usage abusif.

Dans une perspective de transfert direct entre responsables de traitement, il faut que le responsable destinataire mette aussi en œuvre des mécanismes d'importation des données. À cet égard, il est utile qu'il précise les formats qu'il peut traiter afin de permettre à la personne concernée de définir la marche à suivre pour l'extraction et la réinjection de ses données.

Notons enfin qu'il serait prudent de limiter dans le temps la mise à disposition des données ; en effet, l'extraction et la mise à disposition occupent des ressources non négligeables, qu'il convient de libérer dès lors que la personne concernée a obtenu les données souhaitées ou au-delà d'un délai raisonnable dont elle aura été informée.

Une des conditions pour autoriser le transfert est l'**authentification** de la personne concernée[22]. De nombreux systèmes exigent déjà une authentification de l'utilisateur avant de lui permettre l'accès. Cette authentification peut être utilisée pour permettre la demande de données ou l'accès aux données extraites. Le cas échéant, une ré-authentification peut être demandée afin de renforcer la sécurité d'accès. En tout état de cause, l'identité de la personne concernée doit être établie avant de lui permettre d'exercer les droits conférés par le RGPD ; si un doute subsiste sur l'identité de la personne ou son lien avec les données, le responsable de traitement peut demander des informations complémentaires afin d'établir son identité[23].

Enfin, il importe que la **sécurité** des données garanties par le règlement ne soit à aucun moment compromise, et en particulier lors de l'exercice du droit à la portabilité. Il convient donc que la transmission des données soit protégée contre l'interception ou la manipulation. L'usage de canaux sécurisés par des moyens cryptographiques s'impose donc, que ce soit lors du transfert entre responsable de traitement et personne concernée ou entre responsables de traitement. Les fichiers transférés peuvent aussi être protégés par un mot de passe afin de ne permettre qu'à leur destinataire d'accéder à leur contenu.

Au vu de ce qui précède, il est clair que pour permettre l'exercice de ce nouveau droit, une organisation doit mettre en place des moyens techniques potentiellement importants, que ce soit pour permettre l'extraction, le transfert, la réception et le traitement des données, de manière sécurisée et après avoir correctement établi l'identité de la personne concernée et son lien avec les données. De nombreuses sources proposent des lignes directrices pour mettre ces aspects en pratique, telles que l'Autorité de protection des données belge[24], le Groupe de travail « Article 29 »[25], ou encore la CNIL[26].

*Jean-Noël Colin*
Professeur à l'Université de Namur
Membre du NaDI[27]

*Manon Knockaert*
Chercheuse au CRIDS
Membre du NaDI

[21] L'article 20, § 4, du RGPD dispose que : « Le droit visé au paragraphe 1 ne porte pas atteinte aux droits et libertés de tiers. »

[22] Art. 12 et 20 du RGPD et *Lignes directrices « Article 29 »*, p. 16.

[23] Art. 12, § 6, du RGPD et *Lignes directrices « Article 29 »*, p. 16.

[24] Commission de la protection de la vie privée, *RGPD : Vade-mecum pour les PME*, janvier 2018, disponible sur https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/PME_FR_0.pdf.

[25] *Lignes directrices « Article 29 »*.

[26] Commission nationale de l'informatique et des libertés (CNIL), *Le droit à la portabilité en questions*, 22 mai 2017, disponible sur https://www.cnil.fr/fr/le-droit-la-portabilite-en-questions.

[27] Namur Digital Institute, https://nadi.unamur.be.