COMMISSION
EUROPÉENNE

Bruxelles, le 29.5.2019
COM(2019) 250 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne

Table des matières

Le présent document est publié par les services de la Commission européenne à des fins d'information uniquement. Il ne contient aucune interprétation faisant autorité du règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne et ne constitue ni une décision ni une position de la Commission européenne. Il est sans préjudice de toute décision ou position de la Commission et de la compétence de la Cour de justice de l'Union s'agissant d'interpréter le règlement conformément aux traités de l'Union.

1 Introduction

Dans une économie où les données jouent un rôle toujours plus important, les flux de données sont au cœur des processus opérationnels des entreprises, toutes tailles et tous secteurs confondus. Les nouvelles technologies numériques ouvrent de nouvelles perspectives pour le grand public, les entreprises et les administrations publiques dans l'Union européenne (ci-après l'«UE»).

Pour accroître encore les échanges transfrontières de données et stimuler l'économie des données, le Parlement européen et le Conseil ont adopté en novembre 2018, sur la base d'une proposition de la Commission européenne (ci-après la «Commission») le règlement (UE) 2018/1807 concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne[1] (ci-après le «règlement relatif au libre flux des données à caractère non personnel)». Ce règlement est applicable à partir du 28 mai 2019. Le principe de la libre circulation des données à caractère personnel est déjà inscrit dans le règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE («règlement général sur la protection des données», ci-après le RGPD)[2]. En conséquence, il existe désormais un cadre global englobant un espace européen commun des données et la libre circulation de toutes les données au sein de l'Union européenne[3].

Le règlement relatif au libre flux des données à caractère non personnel donne aux entreprises la sécurité juridique nécessaire pour traiter leurs données à l'endroit de leur choix dans l'UE, renforce la confiance dans les services de traitement des données et contrecarre les pratiques menant à une dépendance à l'égard des fournisseurs. Cela permettra d'élargir le choix offert au client, d'améliorer l'efficacité et de stimuler l'adoption des technologies en nuage avec, à la clé, des économies non négligeables pour les entreprises de l'UE. Une étude montre que les entreprises de l'UE peuvent économiser 20 à 50 % de leurs coûts informatiques en migrant vers le nuage[4].

Ces deux règlements garantissent la libre circulation des données entre les États membres, ce qui permet aux utilisateurs de services de traitement de données de se servir des données recueillies sur différents marchés de l'UE pour améliorer leur productivité et leur compétitivité. Les utilisateurs peuvent donc tirer pleinement parti des économies d'échelle

---

[1] Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, JO L 303 du 28.11.2018, p. 59.

[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

[3] Le RGPD s'applique également à l'Espace économique européen (EEE), qui comprend l'Islande, le Liechtenstein et la Norvège. En outre, le règlement relatif au libre flux des données à caractère non personnel présente un intérêt pour l'EEE.

[4] Deloitte: *Measuring the economic impact of cloud computing in Europe*, SMART 2014/0031, 2016. Disponible (en anglais) en ligne à l'adresse suivante: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

que permet de réaliser le vaste marché de l'UE, en améliorant leur compétitivité à l'échelle mondiale et en renforçant l'interconnectivité de l'économie européenne fondée sur les données.

Le règlement relatif au libre flux des données à caractère non personnel présente trois caractéristiques dignes d'intérêt:

- Il interdit en principe aux États membres d'imposer des exigences en matière de localisation des données. Il ne peut être dérogé à cette règle que pour des motifs de sécurité publique dans le respect du principe de proportionnalité.
- Il établit un mécanisme de coopération visant à garantir que les autorités compétentes continuent d'être en mesure d'exercer tout droit dont elles jouissent en matière d'accès aux données qui sont traitées dans un autre État membre.
- Il encourage les acteurs du secteur à élaborer, avec le soutien de la Commission, des codes de conduite fondés sur l'autorégulation concernant le changement de fournisseurs de services et le portage des données.

Objectif des présentes lignes directrices

Les présentes lignes directrices sont conformes à l'article 8, paragraphe 3, du règlement relatif au libre flux des données à caractère non personnel, qui impose à la Commission de publier des lignes directrices sur l'interaction entre ledit règlement et le RGPD, «en particulier en ce qui concerne les ensembles de données composés à la fois de données à caractère personnel et de données à caractère non personnel».

Ces lignes directrices visent à aider les utilisateurs — en particulier les petites et moyennes entreprises — à comprendre l'interaction entre le règlement relatif au libre flux des données à caractère non personnel et le RGPD[5]. Elles portent donc, plus particulièrement, sur: i) les concepts de données à caractère non personnel et de données à caractère personnel; ii) les principes de libre circulation des données et d'interdiction des exigences de localisation des données en vertu des deux règlements; et iii) la notion de portabilité des données dans le cadre du règlement sur le libre flux des données à caractère non personnel. Elles couvrent également les exigences d'autorégulation établies dans les deux règlements.

Le règlement relatif au libre flux des données à caractère non personnel couvre uniquement les «données autres que les données à caractère personnel» telles que définies par le RGPD. Le RGPD régit le traitement des données à caractère personnel, qui constitue un élément essentiel du cadre de protection des données de l'UE[6]. Il est entré en vigueur dans les États

5 Considérant 37 du règlement relatif au libre flux des données à caractère non personnel.

6
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).
- Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les

membres le 25 mai 2018. Le règlement établit des règles harmonisées pour protéger les personnes dans l'UE/l'EEE en ce qui concerne le traitement de leurs données à caractère personnel et la libre circulation de ces données. Le RGPD: (i) précise quelles informations constituent des données à caractère personnel; (ii) établit les fondements juridiques de leur traitement; et (iii) définit les droits et obligations à respecter lors du traitement de ces données[7], entre autres dispositions. En ce qui concerne le principe de libre circulation des données personnelles, l'article 1er, paragraphe 3 du RGPD dispose que «[l]a libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel».

Dans la pratique, un ensemble de données est, dans la plupart des cas, composé à la fois de données à caractère personnel et de données à caractère non personnel. On parle souvent d'«ensembles de données mixtes». La section 2.2 ci-dessous fournit davantage de précisions sur l'interaction entre le règlement relatif au libre flux des données à caractère non personnel et le RGPD en ce qui concerne les ensembles de données mixtes.

Dans un souci de clarté, il n'y a pas d'obligations contradictoires au titre du RGPD et du règlement relatif à la libre circulation des données à caractère non personnel.

---

institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE, JO L 295 du 21.11.2018, p. 39.

– Directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 du 4.5.2016, p. 89.

– Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»), JO L 201 du 31.7.2002, p. 37 (en cours de révision).

[7] Pour de plus amples informations sur divers aspects du RGPD et la législation européenne sur la protection des données, voir la page web du comité européen de la protection des données, qui a publié, conformément à l'article 70 du RGPD, un certain nombre de lignes directrices disponibles à l'adresse suivante: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en. Cette page web contient également des références à des lignes directrices, à des recommandations et à d'autres documents émanant du groupe de travail «article 29», prédécesseur du comité européen de la protection des données. En outre, pour sensibiliser les particuliers et les entreprises au RGPD, la Commission a publié une communication contenant des orientations relatives à l'application directe du règlement général sur la protection des données [COM(2018) 43 final), disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52018DC0043&from=EN

2 L'interaction entre le règlement relatif au libre flux des données à caractère non personnel et le RGPD en ce qui concerne les ensembles de données mixtes.

2.1 La notion de données à caractère non personnel dans le règlement relatif au libre flux des données à caractère non personnel

Le règlement relatif au libre flux des données à caractère non personnel[8] vise à assurer le libre flux de données autres que les données à caractère personnel. Le terme utilisé dans le texte du règlement est «données», qui doit s'entendre comme «les données autres que des données à caractère personnel au sens de l'article 4, point 1, du règlement (UE) 2016/679 [RGPD]»[9]. Ces données, également appelées «**données à caractère non personnel**» dans le présent document, sont définies par opposition aux données à caractère personnel définies dans le RGPD.

Données à caractère personnel

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

La définition des données à caractère personnel est volontairement large et elle est restée pour l'essentiel inchangée dans le RGPD par rapport à la législation précédente[10]. Ainsi, divers aspects de la définition des données à caractère personnel, tels que «toute information», «concernant» ou «identifié ou identifiable», ont déjà été étudiés par le groupe de travail «article 29»[11] dans son avis 4/2007 sur le concept de données à caractère personnel du 20 juin 2007, WP 136.

Il est de pratique courante, dans des domaines comme la recherche, de pseudonymiser des données à caractère personnel afin de masquer l'identité d'une personne. La

8 Article 1er du règlement relatif au libre flux des données à caractère non personnel.

9 Voir l'article 3, paragraphe 1 du règlement relatif au libre flux des données à caractère non personnel.

10 Voir l'article 2, point a) de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (date de fin de validité: 24 mai 2018, abrogée par le RGPD). Voir également la jurisprudence de la Cour de justice sur la définition des données à caractère personnel, qui reconnaît l'interprétation large d'une telle notion, par exemple les arrêts de la Cour de justice du 29 janvier 2009, *Productores de Música de España (Promusicae)/ Telefónica de España SAU*, C-275/06, ECLI:EU:C:2008:54; du 24 novembre 2011, *Scarlet Extended SA/Société belge des auteurs, compositeurs et auteurs SCRL (SABAM)*, C-70/10, ECLI:EU:C:2011:771; et du 19 octobre 2016, *Patrick Breyer/Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779.

11 Le groupe de travail «article 29» était un organe consultatif qui conseillait la Commission sur les questions de protection des données et qui a contribué à l'élaboration de politiques harmonisées en matière de protection des données dans l'UE. Après l'entrée en vigueur du RGPD le 25 mai 2018, le comité européen de la protection des données a succédé à ce groupe de travail.

pseudonymisation est le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires. Ces informations supplémentaires sont conservées séparément et de manière sûre, en ayant recours à des mesures techniques et organisationnelles (telles que le chiffrement)[12,13]. Néanmoins, les données qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires sont toujours considérées comme des informations concernant une personne physique identifiable[14]. Ces données **constituent des données à caractère personnel** au sens du RGPD.

Données à caractère non personnel

Les données qui ne sont pas des données à caractère personnel au sens du RGPD sont des données à caractère **non personnel**. On peut ranger les données à caractère non personnel dans deux catégories, selon leur origine:

- d'une part, les données qui, au départ, ne concernaient pas une personne physique identifiée ou identifiable, telles que les données relatives aux conditions météorologiques générées par des capteurs installés sur des éoliennes ou les données relatives aux besoins de maintenance des machines industrielles;

- d'autre part, les données qui étaient initialement des données à caractère personnel, mais qui ont ensuite été rendues **anonymes**[15]. L'«anonymisation» des données à caractère personnel est différente de la pseudonymisation (voir ci-dessus), car des données correctement anonymisées ne peuvent être attribuées à une personne donnée, même en utilisant des données supplémentaires[16], et sont donc des données à caractère non personnel.

[12] Voir la définition de «pseudonymisation» à l'article 4, paragraphe 5, du RGPD.

[13] Par exemple, on pourrait considérer qu'une étude de recherche sur les effets d'un nouveau médicament fait l'objet d'une pseudonymisation si les données à caractère personnel des participants à l'étude étaient remplacées par des attributs uniques (par exemple, un numéro ou un code) dans la documentation de recherche et que leurs données à caractère personnel associées aux attributs uniques qui leur sont attribués étaient conservées séparément dans un document sécurisé (par exemple dans une base de données protégée par un mot de passe).

[14] Voir le considérant 26 du RGPD.

[15] Voir le considérant 26 du RGPD, qui dispose qu'«Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable.»

[16] Voir l'arrêt de la Cour de justice du 19 octobre 2016, *Patrick Breyer*/*Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779. La Cour a jugé qu'une adresse IP dynamique peut constituer une donnée à caractère personnel même si un tiers (par exemple, un fournisseur de services internet) dispose des informations supplémentaires nécessaires pour identifier la personne concernée. La possibilité d'identifier la personne doit constituer un moyen raisonnablement susceptible d'être utilisé à cette fin, que ce soit directement ou indirectement.

L'évaluation visant à déterminer si les données sont correctement anonymisées dépend des circonstances spécifiques propres à chaque cas considéré[17]. Plusieurs exemples de réidentification d'ensembles de données prétendument rendues anonymes ont montré qu'une telle évaluation pouvait être ardue[18]. Pour déterminer si une personne est identifiable, il convient d'examiner tous les moyens raisonnablement susceptibles d'être utilisés par un responsable du traitement ou par une autre personne pour identifier une personne, que ce soit directement ou indirectement[19].

Exemples de données à caractère non personnel

- Lorsque des données sont agrégées à un niveau tel que les événements individuels (tels que les déplacements à l'étranger d'une personne ou ses habitudes de voyage qui pourraient constituer des données à caractère personnel) ne sont plus identifiables, ces données peuvent être qualifiées d'anonymes[20].. Les données anonymes sont notamment utilisées dans le domaine des statistiques ou dans les rapports de vente (par exemple pour évaluer la popularité d'un produit et ses caractéristiques).
- Les données relatives à la négociation à haute fréquence dans le secteur financier, ou les données relatives à l'agriculture de précision qui contribuent à contrôler et à optimiser l'utilisation des pesticides, des nutriments et de l'eau.

Toutefois, si un rapport peut, d'une manière ou d'une autre, être établi entre des données à caractère non personnel et une personne, permettant l'identification directe ou indirecte de cette dernière, ces données doivent être considérées comme des données à caractère personnel.

Par exemple, si un rapport de contrôle de la qualité sur une chaîne de production dans une usine permet d'établir un lien entre les données et certains ouvriers (par exemple ceux qui fixent les paramètres de production), les données sont considérées comme des données à

[17] L'anonymisation des données devrait toujours s'effectuer à l'aide des techniques d'anonymisation les plus récentes.

[18] Pour des exemples de réidentification de données prétendument rendues anonymes, voir l'étude sur les flux de données futurs réalisée pour la commission ITRE du Parlement européen par Blackman, C., Forge, S.: Data Flows — Future Scenarios: In-Depth Analysis for the ITRE Committee, 2017, p. 22, Box 2. Disponible (en anglais) en ligne à l'adresse suivante: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf

[19] Voir le considérant 26 du RGPD, qui dispose que «pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci».

[20] Voir l'*avis 05/2014 sur les techniques d'anonymisation* du groupe de travail «Article 29», WP216, adopté le 10 avril 2014, p. 10: «Ce n'est que si les données sont agrégées par le responsable de leur traitement à un niveau où les événements individuels ne sont plus identifiables que l'ensemble de données résultant peut être qualifié d'anonyme. Par exemple: si une organisation collecte des données sur des déplacements individuels, les habitudes de voyage au niveau des événements individuels pourraient encore être considérées comme des données à caractère personnel pour toute partie intéressée, tant que le responsable du traitement des données (ou un tiers) continue à avoir accès aux données brutes originales, même si les identifiants directs ont été supprimés de l'ensemble de données transmis à des tiers. Mais si le responsable du traitement des données efface les données brutes et ne transmet à des tiers que des statistiques agrégées à un niveau supérieur, par exemple "le lundi, sur le trajet X, le nombre de passagers est supérieur de 160 % à celui du mardi", ces données pourraient être qualifiées d'anonymes».

caractère personnel et c'est le RGPD qui s'applique. Il est également applicable lorsque les progrès de la technologie et de l'analyse des données permettent de transformer des données anonymisées en données à caractère personnel[21].

Étant donné que la définition des données à caractère personnel renvoie à des «personnes physiques», les ensembles de données contenant les noms et les coordonnées de personnes morales sont en principe des données à caractère non personnel[22]. Toutefois, dans certaines situations, il peut s'agir de données à caractère personnel[23]. Tel sera le cas, par exemple, si le nom de la personne morale est le même que celui d'une personne physique qui le détient ou si les informations concernent une personne physique identifiée ou identifiable[24].

2.2 Ensembles de données mixtes

Le règlement relatif au libre flux des données à caractère non personnel et le RGPD abordent la question de la libre circulation des données dans l'UE sous deux angles différents.

Le règlement sur le libre flux des données à caractère non personnel prévoit une interdiction générale des exigences de localisation des données à caractère non personnel. L'article 4, paragraphe 1, du règlement interdit les exigences de localisation des données, à moins qu'elles ne soient justifiées par des motifs de sécurité publique, dans le respect du principe de proportionnalité.

En plus d'assurer un niveau élevé de protection des données à caractère personnel, le RGPD garantit la libre circulation de ces données. En vertu de l'article 1er, paragraphe 3, du règlement, la libre circulation des données à caractère personnel au sein de l'Union «n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel». Les deux règlements combinés assurent la libre circulation de «toutes» les données dans l'UE. Les dispositions spécifiques sont examinées plus en détail dans les sections 3.1 et 3.2.

Un ensemble de données mixte comporte à la fois des données à caractère personnel et des données à caractère non personnel. La majorité des ensembles de données utilisés dans

---

[21] Si des données à caractère personnel font l'objet d'un traitement illicite ou si leur traitement constitue, de quelque autre manière, une violation du règlement sur la protection des données, les personnes concernées (personnes physiques) ont le droit, en vertu dudit règlement, d'introduire une réclamation auprès d'une autorité de contrôle nationale (autorité chargée de la protection des données) dans l'Union européenne ou de former un recours juridictionnel effectif devant une juridiction nationale. Les missions, compétences et pouvoirs des autorités de contrôle nationales sont régis par le chapitre VI, section 2, du RGPD.

[22] Le considérant 14 du RGPD dispose que: «Le [..]règlement ne couvre pas le traitement des données à caractère personnel qui concernent les personnes morales, et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale.». Il y a lieu, toutefois, de lire cette disposition à la lumière de la définition des données à caractère personnel figurant à l'article 4, point 1, du RGPD.

[23] Voir l'arrêt de la Cour de justice du 9 novembre 2010 dans les affaires jointes *Volker und Markus Schecke GbR*, C-92/09 et *Hartmut Eifert*, C-93/09 /*Land Hessen*, ECLI:EU:C:2010:662, point 52.

[24] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_en

l'économie des données sont des ensembles de données mixtes. Les applications nées du progrès technologique telles que l'internet des objets (c'est-à-dire les objets connectés numériques), l'intelligence artificielle et les technologies permettant l'analyse des mégadonnées y ont couramment recours.

Exemples d'ensembles de données mixtes

- Le dossier fiscal d'une entreprise, mentionnant le nom et le numéro de téléphone du directeur général de l'entreprise;
- les ensembles de données d'une banque, notamment ceux qui contiennent des informations sur les clients et les détails de transactions, tels que les services de paiement (cartes de crédit et de débit), les applications de gestion des relations avec les partenaires et les conventions de prêt, les documents combinant des données concernant tant des personnes physiques que des personnes morales;
- les données statistiques anonymisées d'un établissement de recherche et les données brutes initialement collectées, telles que les réponses des personnes interrogées à des questionnaires d'enquête;
- une base de données sur les problèmes informatiques d'une entreprise et leurs solutions fondées sur des rapports individuels d'incidents informatiques;
- des données relatives à l'internet des objets, lorsque certaines des données permettent d'émettre des hypothèses sur des individus identifiables (par exemple, présence à une adresse et modalités d'utilisation particulières); ainsi que
- l'analyse des données des journaux d'exploitation d'équipements de production dans l'industrie manufacturière.

Exemple: services de gestion des relations avec la clientèle

Certaines banques utilisent des services de gestion des relations avec la clientèle (CRM) fournis par des tiers qui nécessitent la mise à disposition des données d'un client dans l'environnement CRM. Les données contenues dans le service CRM comprennent toutes les informations nécessaires pour gérer efficacement l'interaction avec le client, telles que son adresse postale et électronique, son numéro de téléphone, les produits et services qu'il achète, et les rapports de vente, y compris des données agrégées. Ces données peuvent comprendre aussi bien des données à caractère personnel qu'à caractère non personnel.

En ce qui concerne les ensembles de données mixtes, le règlement relatif au libre flux des données à caractère non personnel[25] dispose ce qui suit:

«Dans le cas d'un ensemble de données composé à la fois de données à caractère personnel et de données à caractère non personnel, le présent règlement s'applique aux données de l'ensemble à caractère non personnel. Lorsque les données à caractère personnel et les

[25] Article 2, paragraphe 2

données à caractère non personnel d'un ensemble sont inextricablement liées, le présent règlement est sans préjudice de l'application du règlement (UE) 2016/679.»

Par conséquent, lorsqu'un ensemble de données est composé à la fois de données à caractère personnel et de données à caractère non personnel:

- le règlement relatif au libre flux des données à caractère non personnel s'applique aux données à caractère non personnel de l'ensemble;
- la disposition relative à la libre circulation du RGPD[26] s'applique aux données à caractère personnel de l'ensemble de données et
- si les données à caractère non personnel et les données à caractère personnel sont «inextricablement liées», les droits et obligations en matière de protection des données découlant du RGPD s'appliquent pleinement à l'intégralité de l'ensemble de données mixtes, même lorsque les données à caractère personnel ne représentent qu'une petite partie de l'ensemble de données[27].

Cette interprétation est conforme au droit à la protection des données à caractère personnel garanti par la charte des droits fondamentaux de l'Union européenne[28] et au considérant 8 du règlement sur la libre circulation des données à caractère non personnel[29]. Ce considérant 8 dispose que «le cadre juridique [...] relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel [...], en particulier [le règlement général sur la protection des données] [...] et les directives (UE) 2016/680 et 2002/58/CE [...] n'est pas remis en question par le présent règlement».

Exemple pratique:

Une société exerçant ses activités dans l'UE propose ses services par l'intermédiaire d'une plateforme. Les entreprises (clientes) téléchargent sur la plateforme leurs documents, qui contiennent des ensembles de données mixtes. En tant que «responsable du traitement», l'entreprise qui télécharge les documents doit veiller à ce que le traitement soit conforme au RGPD. En traitant l'ensemble de données pour le compte du responsable du traitement, la société qui offre les services (le «sous-traitant») doit conserver et traiter les données conformément au RGPD, par exemple aux fins de garantir un niveau de sécurité approprié des données, y compris au moyen d'un chiffrement.

[26] Article 1er, paragraphe 3, du RGPD. Voir à cet égard la section 3.2 ci-dessous.

[27] Comme le rappelle *l'analyse d'impact accompagnant la proposition de règlement du Parlement européen et du Conseil concernant un cadre applicable à la libre circulation des données à caractère non personnel dans l'Union européenne*, document de travail des services de la Commission [SWD(2017) 304 final], partie 1/2, p. 3, quelle que soit la quantité de données à caractère personnel figurant dans un ensemble de données mixte, il convient de respecter pleinement les dispositions du RGPD en ce qui concerne les données à caractère personnel de l'ensemble.

[28] Charte des droits fondamentaux de l'Union européenne, JO C 362 du 26.10.2012, p. 391.

[29] Considérant 8 dudit règlement.

L'expression «inextricablement liée» n'est définie par aucun des deux règlements[30]. Dans la pratique, elle peut qualifier une situation où un ensemble de données contient des données à caractère personnel ainsi que des données à caractère non personnel et où une séparation entre les deux serait soit impossible, soit considérée comme économiquement inefficace ou techniquement impossible par le responsable du traitement. Par exemple, une entreprise souhaitant acquérir des systèmes de CRM et de rapport des ventes verrait ses coûts doubler si elle achetait des logiciels distincts pour le système CRM (données à caractère personnel) et pour le système de rapport des ventes (données agrégées/à caractère non personnel) faisant appel aux données du CRM.

La séparation des deux types de données risque également de faire nettement diminuer la valeur de l'ensemble de données. En outre, en raison de l'évolution de la nature des données (voir la section 2.1) il devient plus difficile d'établir une distinction claire entre les différentes catégories de données et, partant, de les séparer.

Il est important de noter qu'aucun des deux règlements n'oblige les entreprises à séparer les ensembles de données dont elles sont responsables ou qu'elles transforment.

En conséquence, un ensemble de données mixte sera généralement soumis aux obligations incombant aux responsables du traitement et aux sous-traitants et devra respecter les droits des personnes concernées établis par le RGPD.

Traitement des données concernant la santé

Les données relatives à la santé peuvent faire partie d'un ensemble de données mixte. Il s'agit, par exemple, des dossiers médicaux électroniques, des essais cliniques ou des séries de données collectées par diverses applications de santé et de bien-être mobiles (applications permettant à l'utilisateur de mesurer son état de santé, lui rappelant de prendre ses médicaments ou de suivre l'évolution de son état de forme)[31]. Les progrès technologiques rendent de plus en plus floue la frontière entre les données à caractère personnel et les données à caractère non personnel de ces ensembles. Par conséquent, leur traitement doit respecter les dispositions du RGPD, en particulier (étant donné que les données relatives à la santé constituent une catégorie particulière de données au sens du règlement) celles de l'article 9, qui prévoit une interdiction générale du traitement des catégories particulières de données et des exceptions à cette règle d'interdiction.

Les données contenues dans les ensembles de données mixtes contenant des données relatives à la santé peuvent constituer une précieuse source d'informations, par exemple pour approfondir la recherche médicale, pour mesurer les effets secondaires d'un médicament

[30] Le règlement relatif au libre flux des données à caractère non personnel et le RGPD.

[31] Le développement et l'exploitation d'applications de santé mobiles doivent avoir lieu dans le respect strict des dispositions du RGPD. Ces exigences seront précisées dans le code de conduite relatif à la protection de la vie privée pour les applications de santé mobiles, actuellement en cours d'élaboration. Pour de plus amples informations sur son état d'avancement, voir: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps

prescrit, à des fins de statistiques épidémiologiques ou pour mettre au point de nouveaux services ou traitements de santé. Toutefois, l'exécution des opérations de traitement initial et des opérations de traitement ultérieur des données doit être conforme au RGPD. Par conséquent, tout traitement de données relatives à la santé doit avoir une base juridique valable[32] et une justification appropriée, être sûr et fournir des garanties suffisantes.

Enfin, il est essentiel que les particuliers et les entreprises bénéficient de la sécurité juridique et qu'ils aient confiance dans le traitement des données. C'est également essentiel pour l'économie des données. Ces garanties sont fournies par les deux règlements, lesquels visent également à ne pas empêcher la libre circulation des données.

3 Libre flux des données et suppression des exigences de localisation des données

La présente section explique plus en détail la notion d'exigences de localisation des données au titre du règlement relatif au libre flux des données à caractère non personnel, et le principe de libre circulation figurant dans le RGPD. Bien que ces dispositions ciblent les États membres, il peut être utile pour les entreprises d'avoir une vision plus précise de la manière dont ces deux règlements contribuent à la libre circulation de toutes les données au sein de l'UE.

3.1 Libre flux des données à caractère non personnel

Le règlement relatif au libre flux des données à caractère non personnel[33] dispose que «[l]es exigences de localisation des données sont interdites, sauf si elles sont justifiées par des motifs de sécurité publique dans le respect du principe de proportionnalité».

Les **exigences de localisation des données** sont définies[34] comme «toute obligation, interdiction, condition, limite ou autre exigence prévue par les dispositions législatives, réglementaires ou administratives d'un État membre ou résultant des pratiques administratives générales et cohérentes dans un État membre et les organismes de droit public, notamment dans le domaine des marchés publics, sans préjudice de la directive 2014/24/UE, qui impose le traitement des données sur le territoire d'un État membre donné ou qui entrave le traitement des données dans un autre État membre[35]».

[32] Voir l'article 6, paragraphe 1, du RGPD.

[33] Article 4, paragraphe 1, dudit règlement.

[34] Article 3, paragraphe 5, du règlement relatif au libre flux des données à caractère non personnel.

[35] Il convient de noter que l'absence de sécurité juridique quant à la portée des exigences, légitimes ou non, de localisation des données restreint encore le choix offert aux acteurs du marché et au secteur public concernant la localisation du traitement des données [voir le considérant 4 du règlement relatif au libre flux des données à caractère non personnel].

La définition montre que les mesures restreignant la libre circulation des données au sein de l'UE peuvent prendre différentes formes. Elles peuvent être prévues par des dispositions législatives, réglementaires ou administratives, voire résulter de pratiques administratives générales et cohérentes. En outre, l'interdiction relative aux exigences de localisation des données couvre les mesures tant directes qu'indirectes qui limiteraient la libre circulation des données à caractère non personnel.

Les **exigences directes de localisation des données** peuvent être, par exemple, l'obligation de stocker les données à un emplacement géographique précis (par exemple, les serveurs doivent être situés dans un État membre donné) ou l'obligation de respecter des exigences techniques propres à un État membre (par exemple, les données doivent répondre à des formats nationaux spécifiques).

Les **exigences indirectes de localisation des données**, qui entraveraient le traitement des données à caractère non personnel dans un autre État membre, peuvent revêtir diverses formes. Elles peuvent inclure l'exigence d'utiliser des moyens techniques qui sont certifiés ou agréés dans un État membre particulier ou d'autres exigences qui ont pour effet de rendre plus difficile le traitement de données en dehors d'une zone géographique ou d'un territoire précis dans l'Union européenne[36,37].

L'évaluation visant à déterminer si une mesure spécifique constitue une exigence indirecte de localisation des données doit tenir compte des circonstances particulières de chaque cas.

Le règlement relatif au libre flux des données à caractère non personnel[38] fait référence à la notion de **sécurité publique** telle que définie par la jurisprudence de la Cour de justice de l'Union européenne. La sécurité publique «englobe à la fois la sécurité intérieure et extérieure d'un État membre[39], mais aussi les questions de sûreté publique, afin, en particulier, de faciliter la détection des infractions pénales, les enquêtes et les poursuites en la matière. [Elle] présuppose l'existence d'une menace réelle et suffisamment grave portant atteinte à l'un des intérêts fondamentaux de la société[40], telle qu'une menace pour le fonctionnement des institutions et des services publics essentiels et pour la survie de la population, ainsi que le

---

[36] Considérant 4 du règlement relatif au libre flux des données à caractère non personnel.

[37] Voir deux études sur les exigences de localisation des données réalisées avant l'adoption du règlement relatif au libre flux des données à caractère non personnel: (1) Godel, M. et al.: *Facilitating cross border data flows in the Digital Single Marke*t, SMART number 2015/2016. Disponible en ligne à l'adresse suivante: http://ec.europa.eu/newsroom/document.cfm?doc_id=41185 et (2) Time.lex, Spark Legal Network et Tech4i2: *Cross-border data flow in the digital single market: study on data localisation restrictions*. SMART number 2015/0054. Disponible en ligne à l'adresse suivante: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695

[38] Considérant 19 dudit règlement.

[39] Voir par exemple l'arrêt de la Cour de justice du 23 novembre 2010, *Land Baden-Württemberg*/*Tsakouridis*, C-145/09, ECLI:EU:C:2010:708, point 43, et l'arrêt du 4 avril 2017, *Sahar Fahimian*/*Bundesrepublik Deutschland*, C-544/15, ECLI:EU:C:2017:225, point 39.

[40] Voir par exemple l'arrêt de la Cour de justice du 22 décembre 2008, *Commission des Communautés européennes*/*République d'Autriche*, C-161/07, ECLI:EU:C:2008:759, point 35, et la jurisprudence citée, ainsi que l'arrêt du 26 mars 2009, *Commission des Communautés européennes*/*République italienne*, C-326/07, ECLI:EC:C:2009:193, point 70, et la jurisprudence citée.

risque d'une perturbation grave des relations extérieures ou de la coexistence pacifique des nations, ou un risque pour les intérêts militaires».

Par ailleurs, toute exigence de localisation des données qui se justifie par des motifs de sécurité publique doit être proportionnelle. Conformément à la jurisprudence de la Cour de justice de l'Union européenne, le principe de proportionnalité exige que les mesures adoptées soient appropriées pour garantir la réalisation de l'objectif poursuivi et n'aillent pas au-delà de ce qui est nécessaire pour atteindre cet objectif[41].

Par souci de clarté, l'interdiction relative aux exigences de localisation des données est sans préjudice des restrictions déjà existantes imposées par le droit de l'Union[42].

En outre, le règlement relatif au libre flux des données à caractère non personnel n'impose aucune obligation aux entreprises ni ne limite leur liberté contractuelle de décider du lieu où leurs données doivent être traitées.

Les États membres sont tenus de publier les détails de toutes les exigences de localisation des données applicables sur leur territoire par l'intermédiaire d'un **point d'information unique en ligne national** (site web national). Ils doivent tenir ce point d'information à jour ou fournir des détails actualisés à un point d'information central établi au titre d'un autre acte de l'Union[43]. Pour plus de facilité pour les entreprises et afin de leur offrir un accès aisé aux informations pertinentes dans toute l'UE, la Commission publiera les liens vers ces points d'information sur le portail «L'Europe est à vous»[44].

3.2 Libre flux des données à caractère personnel

Le RGPD[45] dispose que «[l]a libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel».

Si un État membre impose des exigences de localisation des données à caractère personnel pour des raisons autres que la protection des données à caractère personnel, ces exigences devront être évaluées à l'aune des dispositions relatives aux libertés fondamentales et des motifs permettant de déroger à ces libertés figurant dans le traité sur le fonctionnement de

41 Voir par exemple l'arrêt de la Cour de justice du 8 juillet 2010, *Afton Chemical Limited/Secretary of State for Transport*, C-343/09, ECLI:EU:C:2010:419, point 45, et la jurisprudence citée.

42 Voir par exemple l'article 245, paragraphe 2, de la directive 2006/112/CE du 28 novembre 2006 relative au système commun de taxe sur la valeur ajoutée, qui dispose que «[l]es États membres peuvent imposer aux assujettis établis sur leur territoire l'obligation de leur déclarer le lieu de stockage lorsque celui-ci est situé en dehors de leur territoire». Cette exigence doit toutefois être lue conformément à l'article 249, qui dispose que: «[l]orsqu'un assujetti stocke les factures qu'il émet ou qu'il reçoit par une voie électronique garantissant un accès en ligne aux données et que le lieu de stockage est situé dans un État membre autre que celui dans lequel il est établi, les autorités compétentes de l'État membre dans lequel il est établi ont, aux fins de la présente directive, le droit d'accéder à ces factures par voie électronique, de les télécharger et de les utiliser, dans les limites fixées par la réglementation de l'État membre d'établissement de l'assujetti et dans la mesure où cela leur est nécessaire aux fins de contrôle».

43 Article 4, paragraphe 4, du règlement relatif au libre flux des données à caractère non personnel.

44 https://europa.eu/youreurope/index.htm

45 Article 1er, paragraphe 3, du RGPD.

l'Union européenne[46,47] et dans la législation applicable de l'UE, telle que la directive Services[48] et la directive sur le commerce électronique[49].

Exemple:

Une législation nationale impose que les comptes salaires soient situés dans un État membre donné pour des raisons liées au contrôle réglementaire, par exemple par l'autorité fiscale nationale. Une telle disposition nationale ne relèverait pas du champ d'application de l'article 1er, paragraphe 3, du RGPD, les raisons étant autres que la protection des données à caractère personnel. Cette exigence devrait être évaluée à l'aune des dispositions relatives aux libertés fondamentales et des motifs permettant de déroger à ces libertés figurant dans le traité sur le fonctionnement de l'Union européenne.

Le RGPD[50] reconnaît que les États membres peuvent imposer des conditions, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé. Toutefois, comme indiqué au considérant 53, cela ne devrait pas entraver le libre flux des données à caractère personnel au sein de l'Union lorsque ces conditions s'appliquent au traitement transfrontalier de ces données. Cette approche est conforme à l'article 16 du traité sur le fonctionnement de l'Union européenne, qui constitue la base juridique pour l'adoption de règles relatives au droit à la protection des données à caractère personnel et de règles relatives à la libre circulation de ces données.

3.3 Champ d'application du règlement relatif au libre flux des données à caractère non personnel

Ainsi que cela a déjà été indiqué, le règlement relatif au libre flux des données à caractère non personnel vise à assurer le libre flux de données à caractère non personnel «au sein de l'Union»[51]. Il ne s'applique donc pas aux opérations de traitement ayant lieu en dehors de l'UE ni aux exigences de localisation des données relatives à ce traitement[52,53].

---

46 Version consolidée du traité sur le fonctionnement de l'Union européenne (JO C 326 du 26.10.2012, p. 47).

47 Voir également l'arrêt de la Cour de justice du 19 juin 2008, *Commission des Communautés européennes/Grand-Duché de Luxembourg*, C-319/06, ECLI:EU:C:2008:350, points 90-91: la Cour a estimé qu'une obligation de tenir à disposition et de conserver certains documents dans un État membre donné constituait une restriction à la libre prestation des services; une justification selon laquelle cette obligation est «de nature à faciliter en général l'accomplissement de la mission de contrôle des autorités» n'est pas suffisante.

48 Directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur (JO L 376 du 27.12.2006, p. 36).

49 Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»), JO L 178 du 17.7.2000, p. 1.

50 Article 9, paragraphe 4, du règlement (UE) 2016/679 du RGPD.

51 Voir l'article 1er du règlement relatif au libre flux des données à caractère non personnel.

52 Voir le considérant 15 du règlement relatif au libre flux des données à caractère non personnel.

Conformément à l'article 2, paragraphe 1, du règlement, le champ d'application de ce dernier est donc limité au traitement de données électroniques à caractère non personnel dans l'Union, qui est:

(a) fourni en tant que service aux utilisateurs résidant ou disposant d'un établissement dans l'Union, par un fournisseur de services établi ou non dans l'Union; ou
(b) effectué par une personne physique ou morale résidant ou disposant d'un établissement dans l'Union pour ses propres besoins.

Exemples:

Article 2, paragraphe 1, point a), du règlement relatif au libre flux des données à caractère non personnel:

- Un fournisseur de services en nuage établi aux États-Unis fournit ses services de traitement à des clients résidant ou établis dans l'UE. Il gère ses activités par l'intermédiaire de serveurs situés sur le territoire de l'UE, où les données de ses clients européens sont conservées ou traitées d'une autre manière. Le fournisseur de services en nuage n'est pas tenu de posséder d'infrastructures propres à l'UE, mais peut par exemple aussi louer un espace sur un serveur dans l'UE. Le règlement relatif au libre flux des données à caractère non personnel s'applique à ce traitement des données.
- Un fournisseur de services en nuage établi au Japon propose ses services à des clients européens. Les capacités de traitement du fournisseur sont situées au Japon et toutes les activités de traitement y sont menées. Le règlement relatif au libre flux des données à caractère non personnel ne s'applique pas en l'espèce, si toutes les activités de traitement ont lieu en dehors de l'UE[54].

Article 2, paragraphe 1, point b), du règlement relatif au libre flux des données à caractère non personnel:

- Une petite start-up européenne d'un État membre A décide de développer ses activités en ouvrant un établissement dans l'État membre B. Pour réduire les coûts au minimum, elle choisit de centraliser le stockage et le traitement des données du nouvel établissement sur son serveur situé dans l'État membre A. Les États membres ne peuvent pas interdire ces efforts de centralisation informatique, à moins que cela ne soit

[53] Le terme «traitement» est défini au sens large [article 3, paragraphe 2, du règlement relatif au libre flux des données à caractère non personnel] et, comme le souligne le considérant 17, le règlement devrait s'appliquer au traitement des données au sens le plus large, quel que soit le type de système informatique utilisé.

[54] Il convient de noter que le règlement relatif au libre flux des données à caractère non personnel ne concerne pas les exigences de localisation des données imposées par les États membres, et éventuellement présentes dans leur ordre juridique national, en ce qui concerne le stockage de données à caractère non personnel dans des pays tiers. Par souci de clarté, le RGPD s'applique au traitement des données à caractère personnel des personnes concernées qui se trouvent dans l'UE par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement se rapportent: a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou b) au suivi de leur comportement, dans la mesure où celui-ci a lieu au sein de l'Union (voir l'article 3, paragraphe 2, du RGPD).

justifié pour des raisons de sécurité publique dans le respect du principe de proportionnalité.

Bien que le règlement relatif au libre flux des données à caractère non personnel ne s'applique pas si toutes les activités de traitement des données à caractère non personnel sont effectuées en dehors de l'UE, le RGPD doit être respecté lorsque des données à caractère personnel font partie de l'ensemble de données considéré. En particulier, les règles relatives aux transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales en vertu du RGPD doivent être respectées en tout état de cause[55].

3.4 Activités liées à l'organisation interne des États membres

Le règlement relatif au libre flux des données à caractère non personnel n'oblige pas les États membres à externaliser la prestation de services liés aux données à caractère non personnel qu'ils souhaitent fournir eux-mêmes ou organiser autrement que par des marchés publics[56].

L'article 2, paragraphe 3, deuxième alinéa, du règlement relatif au libre flux des données à caractère non personnel dispose ce qui suit:

«Le présent règlement est sans préjudice des dispositions législatives, réglementaires et administratives qui concernent **l'organisation interne** des États membres et qui attribuent aux autorités publiques et aux organismes de droit public au sens de l'article 2, paragraphe 1, point 4), de la directive 2014/24/UE[57], des pouvoirs et des responsabilités en matière de **traitement des données sans rémunération contractuelle de parties privées**, ainsi que des dispositions législatives, réglementaires et administratives des États membres qui prévoient la mise en œuvre de ces pouvoirs et responsabilités»[58].

Il peut y avoir des intérêts légitimes qui justifieraient le choix de ce type d'«autoprestation» de services de traitement des données, comme l'«internalisation» ou des arrangements

---

[55] Pour ce qui est des transferts de données à caractère personnel vers des pays tiers, consulter la page web de la Commission: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en et la *communication de la Commission au Parlement européen et au Conseil — Échange et protection de données à caractère personnel à l'ère de la mondialisation*, COM(2017) 7 final, disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017 %3A7 %3AFIN. En ce qui concerne le Japon, la Commission a adopté sa décision d'adéquation le 23 janvier 2019, permettant ainsi la libre circulation des données à caractère personnel entre les deux économies moyennant de solides garanties en matière de protection.

[56] Considérant 14 du règlement relatif au libre flux des données à caractère non personnel.

[57] L'article 2, paragraphe 1, point 4, de la directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE (JO L 94 du 28.3.2014, p. 65) dispose qu'«on entend par "organisme de droit public" tout organisme présentant toutes les caractéristiques suivantes: a) il a été créé pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial; b) il est doté de la personnalité juridique; et c) soit il est financé majoritairement par l'État, les autorités régionales ou locales ou par d'autres organismes de droit public, soit sa gestion est soumise à un contrôle de ces autorités ou organismes, soit son organe d'administration, de direction ou de surveillance est composé de membres dont plus de la moitié sont désignés par l'État, les autorités régionales ou locales ou d'autres organismes de droit public».

[58] Le considérant 13 du règlement relatif au libre flux des données à caractère non personnel précise que le règlement est sans préjudice de la directive 2014/24/UE.

mutuels entre administrations publiques. L'utilisation d'un «nuage propre au gouvernement» ou le recours, par le gouvernement, à une agence informatique centralisée pour fournir des services de traitement des données aux institutions et aux organismes publics constituent des exemples types.

Cependant, le règlement relatif au libre flux des données à caractère non personnel encourage les États membres à prendre en considération les avantages économiques et autres bienfaits de l'externalisation vers des prestataires de services extérieurs[59,60]. Dès que les autorités nationales commencent à «externaliser» le traitement des données avec rémunération contractuelle de parties privées et que le traitement a lieu au sein de l'UE, ce dernier est couvert par le règlement relatif au libre flux des données à caractère non personnel, ce qui signifie que le principe du libre flux des données à caractère non personnel s'applique aux pratiques générales et administratives des autorités nationales. Lesdites autorités doivent notamment s'abstenir de prendre des mesures restrictives en matière de localisation des données, par exemple dans le cadre d'appels d'offres relatifs à des marchés publics[61].

4 Approches autorégulatrices soutenant le libre flux des données

L'autorégulation contribue à l'innovation et à l'instauration d'un climat de confiance entre les acteurs du marché et offre la possibilité de tenir davantage compte des évolutions du marché. La présente section donne un aperçu des initiatives d'autorégulation pour le traitement tant des données à caractère personnel que des données à caractère non personnel.

4.1 Portage des données et changement de fournisseur de services en nuage

L'un des objectifs du règlement relatif au libre flux des données à caractère non personnel est d'éviter les pratiques menant à une dépendance à l'égard de fournisseurs. Ces pratiques existent lorsque les utilisateurs ne peuvent pas changer de fournisseur de services parce que leurs données sont «verrouillées» dans le système du fournisseur, par exemple en raison d'un format de données spécifiques ou de dispositions contractuelles, et ne peuvent être transférées en dehors du système informatique du fournisseur. Le portage des données sans entraves est important pour permettre aux utilisateurs de choisir librement entre les fournisseurs de services de traitement des données, et donc pour garantir une concurrence effective sur le marché.

La portabilité des données entre les entreprises gagne en importance dans toute une série de secteurs numériques, dont les services en nuage.

Conformément à l'article 6 du règlement relatif au libre flux des données à caractère non personnel, la Commission encourage et facilite l'élaboration de codes de conduite par autorégulation au niveau de l'Union (ci-après «codes de conduite») afin de contribuer à une

[59] Considérant 14 du règlement relatif au libre flux des données à caractère non personnel.

[60] Un prestataire de services extérieur serait toute entité qui n'est pas un «organisme de droit public» au sens de l'article 2, paragraphe 1, point 4, de la directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE (JO L 94 du 28.3.2014, p. 65).

[61] Considérant 13 du règlement relatif au libre flux des données à caractère non personnel.

économie des données compétitive. Elle fournit une base permettant à l'industrie d'élaborer des codes de conduite par autorégulation concernant le changement de fournisseur de services et le portage des données entre différents systèmes informatiques.

Un certain nombre d'aspects devraient être pris en compte lors de l'élaboration de ces codes de conduite sur le portage des données, notamment:

- les **bonnes pratiques** qui facilitent le changement de fournisseur de services et le portage des données dans des formats structurés, usuels et lisibles par machine;
- les **exigences minimales d'information** afin que les utilisateurs professionnels disposent, préalablement à la conclusion d'un contrat, d'informations suffisamment détaillées et claires en ce qui concerne les processus, les exigences techniques, les délais et les frais qui s'appliquent dans le cas où un utilisateur professionnel souhaite changer de fournisseur de services ou transférer ses données pour les rapatrier vers ses propres systèmes informatiques;
- les **approches en matière de dispositifs de certification** afin de faciliter la comparabilité des services en nuage; ainsi que
- les **feuilles de route de communication** afin d'informer sur les codes de conduite.

Au sein du marché des services en nuage, la Commission a commencé à faciliter les travaux des groupes de travail des parties prenantes sur l'informatique en nuage dans le marché unique numérique (MUN), qui réunit des experts de l'informatique en nuage et des utilisateurs professionnels, dont des petites et moyennes entreprises. À ce stade, un sous-groupe élabore des codes de conduite par autorégulation sur le portage des données et le changement de fournisseur de services en nuage (groupe de travail SWIPO)[62] et un autre sous-groupe travaille sur la mise en place d'une certification de la sécurité de l'informatique en nuage (groupe de travail CSPCERT)[63].

Le groupe de travail SWIPO élabore des codes de conduite couvrant l'ensemble des services en nuage: infrastructure à la demande, plateforme à la demande et logiciel à la demande.

La Commission s'attend à ce que les différents codes de conduite soient complétés par des **clauses contractuelles types**[64]. Celles-ci permettront de disposer d'une spécificité technique et juridique suffisante en ce qui concerne la mise en œuvre et l'application concrètes des codes de conduite, qui seront particulièrement importantes pour les petites et moyennes entreprises. La rédaction des clauses contractuelles types est prévue après l'élaboration des codes de conduite (qui devrait être achevée pour le 29 novembre 2019).

Conformément à l'article 8 du règlement relatif au libre flux des données à caractère non personnel, la Commission évaluera la mise en œuvre du règlement d'ici au 29 novembre

[62] Cloud Switching and Porting Data Working Group (groupe de travail «changement de fournisseur de services en nuage et portage des données»).

[63] European Cloud Service Provider Certification Working Group (groupe de travail «certification européenne des fournisseurs de services en nuage»). Voir également la section 4.3.

[64] Voir le considérant 30 du règlement relatif au libre flux des données à caractère non personnel.

2022. Cette évaluation portera sur: i) l'incidence sur le libre flux des données en Europe; ii) l'application du règlement, en particulier aux ensembles de données mixtes; iii) la mesure dans laquelle les États membres ont effectivement abrogé les mesures restrictives existantes injustifiées en matière de localisation des données; et iv) l'efficacité sur le marché des codes de conduite en ce qui concerne le portage des données et le changement de fournisseur de services en nuage.

La notion de portabilité et l'interaction avec le RGPD

Les deux règlements[65] font référence à la portabilité des données et à l'objectif de faciliter le transfert des données d'un environnement informatique à un autre, que ce soit vers les systèmes d'un autre fournisseur ou vers des systèmes sur site. Cela permet d'éviter la dépendance à l'égard de fournisseurs et favorise la concurrence entre fournisseurs de services. Toutefois, les règlements se distinguent par leur approche de la portabilité en ce qui concerne la relation entre les groupes d'intérêt ciblés ainsi que la nature juridique des dispositions.

Le droit à la portabilité des données à caractère personnel en vertu de l'article 20 du RGPD se concentre sur la relation entre la personne concernée et le responsable du traitement. Il porte sur le droit de la personne concernée à recevoir les données à caractère personnel qu'elle a fournies au responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et à transmettre ces données à un autre responsable du traitement ou à les transférer vers ses propres capacités de stockage sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle[66]. Généralement, les personnes concernées dans cette relation sont les consommateurs de différents services en ligne qui souhaitent changer de fournisseur de services.

L'article 6 du règlement relatif au libre flux des données à caractère non personnel ne prévoit pas le droit pour les utilisateurs professionnels de transférer les données, mais a une approche autorégulatrice, avec des codes de conduite volontaires pour les entreprises. Dans le même temps, il vise une situation où un utilisateur professionnel a externalisé le traitement de ses données à un tiers proposant des services de traitement des données[67]. Conformément à l'article 3, paragraphe 8, du règlement relatif au libre flux des données à caractère non personnel, un «utilisateur professionnel» peut inclure «une personne physique ou morale, y compris une autorité publique ou un organisme de droit public, qui utilise ou demande un service de traitement des données à des fins liées à son activité commerciale, industrielle, artisanale, libérale ou à sa mission».

Dans la pratique, la portabilité prévue à l'article 6 du règlement relatif au libre flux des données à caractère non personnel concerne les interactions interentreprises entre un

[65] Article 6 du règlement relatif au libre flux des données à caractère non personnel et article 20 du RGPD.

[66] Voir le groupe de travail «Article 29»: *lignes directrices relatives au droit à la portabilité des données*. WP 242 rév.01, adoptées le 13 décembre 2016, telles que révisées, et adoptées le 5 avril 2017.

[67] Le considérant 29 du règlement relatif au libre flux des données à caractère non personnel dispose ce qui suit: «Alors que les consommateurs individuels bénéficient du droit de l'Union en vigueur [à savoir, le RGPD], il n'existe pas de mesures facilitant le changement de fournisseur de services pour les utilisateurs intervenant dans le cadre de leurs activités commerciales ou professionnelles».

utilisateur professionnel (pouvant, dans des cas tels que le traitement des données à caractère personnel, être qualifié de «responsable du traitement» conformément au RGPD) et un fournisseur de services (pouvant également être qualifié de «sous-traitant» dans certains cas).

Malgré les différences, il peut se présenter des situations dans lesquelles le portage des données serait couvert à la fois par le règlement relatif au libre flux des données à caractère non personnel et par le RGPD, en ce qui concerne les ensembles de données mixtes.

Exemple:

Une entreprise utilisant des services en nuage décide de changer de fournisseur de services en nuage et de transférer toutes les données vers un nouveau fournisseur. Le changement de fournisseur de services et le portage des données sont couverts par le contrat entre le client et le fournisseur de services en nuage. Si l'ancien fournisseur de services en nuage adhère aux codes de conduite élaborés dans le cadre du règlement relatif au libre flux des données à caractère non personnel, le portage des données doit avoir lieu dans le respect des exigences qui y sont spécifiées.

Si les données à caractère personnel font également partie des ensembles de données transférés, le portage doit respecter toutes les dispositions pertinentes du RGPD et il convient de veiller en particulier à ce que le nouveau fournisseur de services en nuage se conforme aux exigences applicables, notamment en matière de sécurité[68].

Exemple:

Dans le cas où une banque décide de changer de fournisseur de gestion de la relation avec la clientèle (CRM), certaines données (à caractère personnel et non personnel) pourraient devoir être transférées de l'ancien fournisseur vers le nouveau. Ces données seront alors soumises à des exigences réglementaires distinctes, certaines découlant du RGPD et d'autres du règlement relatif au libre flux des données à caractère non personnel.

4.2 Codes de conduite et mécanismes de certification en matière de protection des données à caractère personnel

Des codes de conduite et des mécanismes de certification peuvent être utilisés pour démontrer le respect des obligations prévues par le RGPD (voir article 24, paragraphe 3, et article 28, paragraphe 5).

Conformément à l'article 40, paragraphe 1, et à l'article 42, paragraphe 1, du RGPD, les États membres, les autorités de contrôle, le Comité européen de la protection des données et la Commission devraient encourager l'industrie à élaborer des codes de conduite et à mettre en place des mécanismes de certification en matière de protection des données.

[68] Voir le groupe de travail «Article 29»: *avis 05/2012 sur l'informatique en nuage* adopté le 1er juillet 2012, WP196, qui précise la position et les obligations des utilisateurs de services en nuage et des fournisseurs de services en nuage en ce qui concerne le traitement des données à caractère personnel.

Les associations ou d'autres organismes représentant une catégorie particulière de responsables du traitement ou de sous-traitants peuvent élaborer un code de conduite pour le secteur concerné. Le projet de code doit être soumis à l'autorité de contrôle compétente respective pour approbation[69]. Si le projet de code de conduite porte sur des activités de traitement dans plusieurs États membres, l'autorité de contrôle doit le soumettre au Comité européen de la protection des données avant de l'approuver. Ledit comité se prononce alors sur la question de savoir si le projet de code est conforme au RGPD.

Le Comité européen de la protection des données a publié ses lignes directrices 1/2019 relatives aux codes de conduite et aux organismes de suivi au titre du RGPD[70]. Les lignes directrices comprennent des informations sur l'élaboration des codes de conduite, les critères d'approbation de ceux-ci et d'autres informations utiles. De même, les lignes directrices 1/2018 du Comité européen de la protection des données relatives à l'agrément et à la détermination des critères d'agrément conformément aux articles 42 et 43 du RGPD fournissent des informations sur la certification au titre dudit règlement ainsi que sur l'élaboration et l'approbation des critères de certification[71].

Exemples de codes de conduite élaborés par le secteur de l'informatique en nuage:

Le code de conduite de l'UE sur l'informatique en nuage (EU Cloud Code of Conduct), dont l'élaboration a été facilitée par la Commission, a été rédigé en collaboration avec le Cloud Select Industry Group (C-SIG) sur la base de la directive sur la protection des données[72] puis du RGPD. Ce code de conduite couvre tout l'éventail des services en nuage — logiciel à la demande, plateforme à la demande et infrastructure à la demande[73].

Le code de conduite des prestataires de services d'infrastructure en nuage en Europe (Cloud Infrastructure Services Providers in Europe, CISPE)[74] est axé sur les fournisseurs d'infrastructure à la demande. Il comprend des exigences concernant les fournisseurs d'infrastructure à la demande agissant comme sous-traitants au titre du RGPD. Il contient également des dispositions relatives à la structure de gouvernance pour la mise en œuvre et l'application du code.

69 Voir l'article 40, paragraphe 5, et l'article 55 du RGPD.

70 Comité européen de la protection des données: *Lignes directrices 1/2019 relatives aux codes de conduite et aux organismes de suivi au titre du règlement (UE) 2016/679*, adoptées le 12 février 2019, version pour consultation publique, disponible en ligne à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en

71 Comité européen de la protection des données: *Lignes directrices 1/2018 relatives à l'agrément et à la détermination des critères d'agrément conformément aux articles 42 et 43 du règlement (UE) 2016/679*, adoptées le 23 janvier 2019, disponibles en ligne à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en

72 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (date de fin de validité: 24 mai 2018).

73 Pour de plus amples informations sur le code de conduite de l'UE sur l'informatique en nuage, voir: https://eucoc.cloud/en/home.html

74 Pour de plus amples informations sur le code de conduite CISPE, voir: https://cispe.cloud/code-of-conduct/

Le code de conduite de la Cloud Security Alliance pour le respect du RGPD s'adresse à toutes les parties prenantes dans les domaines de l'informatique en nuage et de la législation européenne relative aux données à caractère personnel, telles que les fournisseurs de services en nuage, les clients faisant appel à ces services et les clients potentiels, les auditeurs de l'informatique en nuage et les courtiers de l'informatique en nuage. Il couvre l'ensemble des fournisseurs de services en nuage[75].

4.3 Renforcer la confiance dans le traitement transfrontière des données – certification de la sécurité

Comme indiqué au considérant 33 du règlement relatif au libre flux des données à caractère non personnel, le renforcement de la confiance dans la sécurité du traitement transfrontière des données devrait réduire la propension des acteurs du marché et du secteur public à utiliser la localisation des données en lieu et place d'une assurance de sécurité des données. Parallèlement au train de mesures sur la cybersécurité proposé par la Commission en 2017[76], le groupe de travail CSPCERT élabore actuellement des recommandations aux fins de la mise en place d'un dispositif européen de certification de l'informatique en nuage qui seront présentées à la Commission. Un tel dispositif est susceptible de faciliter la libre circulation des données, de permettre une meilleure comparabilité des services en nuage et de promouvoir l'adoption de ces services. La Commission peut demander à l'ENISA (Agence de l'Union européenne pour la cybersécurité) de concevoir un système candidat conformément aux dispositions applicables du règlement sur la cybersécurité[77]. Ce système peut porter à la fois sur les données à caractère personnel et sur les données à caractère non personnel. Outre le règlement sur la cybersécurité, et comme souligné au point 4.2, le RGPD peut également être utilisé pour démontrer l'existence de garanties appropriées en matière de sécurité des données[78].

Remarques finales

La sécurité juridique et la confiance dans le traitement des données sont essentielles pour que l'UE puisse exploiter pleinement les données et que des chaînes de valeur puissent être créées dans tous les secteurs et par-delà les frontières. Les deux règlements garantissent cela et poursuivent tous deux l'objectif de la libre circulation des données. Ensemble, le règlement relatif au libre flux des données à caractère non personnel et le RGPD jettent les bases du libre flux de toutes les données au sein de l'Union européenne et d'une économie européenne fondée sur les données hautement compétitive.

---

[75] Pour de plus amples informations sur le code de conduite de la Cloud Security Alliance, voir: https://gdpr.cloudsecurityalliance.org/

[76] Pour en savoir plus, voir: https://ec.europa.eu/digital-single-market/en/cyber-security

[77] Règlement du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification des technologies de l'information et des communications en matière de cybersécurité et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité).

[78] Voir le considérant 74 du règlement sur la cybersécurité.