

# COM (2020) 767 final

ASSEMBLÉE NATIONALE

QUINZIÈME LÉGISLATURE

SÉNAT

SESSION ORDINAIRE DE 2020-2021

---

---

Reçu à la Présidence de l'Assemblée nationale  
le 26 novembre 2020

---

---

Enregistré à la Présidence du Sénat  
le 26 novembre 2020

## TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,  
À L'ASSEMBLÉE NATIONALE ET AU SÉNAT.

**Proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données)**



Bruxelles, le 25 novembre 2020  
(OR. en)

13351/20

---

---

**Dossier interinstitutionnel:  
2020/0340(COD)**

---

---

**TELECOM 227  
COMPET 592  
MI 521  
DATAPROTECT 135  
JAI 1021  
CODEC 1215  
IA 95**

#### **NOTE DE TRANSMISSION**

---

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	25 novembre 2020
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	COM(2020) 767 final
Objet:	Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL sur la gouvernance européenne des données (acte sur la gouvernance des données)

---

Les délégations trouveront ci-joint le document COM(2020) 767 final.

p.j.: COM(2020) 767 final



Bruxelles, le 25.11.2020  
COM(2020) 767 final

2020/0340 (COD)

Proposition de

**RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL**

**sur la gouvernance européenne des données  
(acte sur la gouvernance des données)**

(Texte présentant de l'intérêt pour l'EEE)

{SEC(2020) 405 final} - {SWD(2020) 295 final} - {SWD(2020) 296 final}

## EXPOSÉ DES MOTIFS

### 1. CONTEXTE DE LA PROPOSITION

#### • **Justification et objectifs de la proposition**

Le présent exposé des motifs accompagne la proposition de règlement du Parlement européen et du Conseil<sup>1</sup> relatif à la gouvernance des données. Cette proposition est la première d'une série de mesures annoncées dans le cadre de la stratégie européenne pour les données de 2020<sup>2</sup>. L'instrument vise à favoriser la disponibilité de données en vue de leur utilisation, en augmentant la confiance dans les intermédiaires de données et en renforçant les mécanismes de partage de données dans l'ensemble de l'UE. L'instrument répondrait aux situations suivantes:

- la mise à disposition de données du secteur public en vue d'une réutilisation, lorsque de telles données sont soumises à des droits d'autrui<sup>3</sup>;
- le partage de données entre entreprises, contre rémunération sous quelque forme que ce soit;
- permettre l'utilisation de données à caractère personnel avec l'aide d'un «intermédiaire de partage de données à caractère personnel», conçu pour aider les personnes physiques à exercer leurs droits au titre du règlement général sur la protection des données (RGPD);
- permettre l'utilisation de données pour des motifs altruistes.

#### • **Cohérence avec les dispositions existantes dans le domaine d'action**

L'initiative actuelle couvre différents types d'intermédiaires de données, traitant à la fois des données à caractère personnel et des données à caractère non personnel. Par conséquent, l'interaction avec la législation relative aux données à caractère personnel est particulièrement importante. Avec le règlement général sur la protection des données (RGPD)<sup>4</sup> et la directive «vie privée et communications électroniques»<sup>5</sup>, l'Union a mis en place un cadre juridique solide et fiable pour la protection des données à caractère personnel et des normes qui font référence au niveau mondial.

La présente proposition complète la directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (directive sur les données ouvertes)<sup>6</sup>. Elle porte sur les données détenues par des organismes du secteur public qui sont soumises à des droits d'autrui et ne relèvent donc pas du champ d'application de cette directive. La proposition présente des liens logiques et cohérents avec les autres initiatives annoncées dans la stratégie européenne pour les données. Elle vise à faciliter le partage de données, notamment en renforçant la confiance dans les intermédiaires de partage de données auxquels il devrait être fait appel dans les différents espaces de données. Elle ne vise pas à accorder, modifier ou supprimer les droits substantiels

---

<sup>1</sup> Le contenu de l'instrument déterminera la forme définitive de l'acte juridique.

<sup>2</sup> [COM/2020/66 final](#).

<sup>3</sup> Les «données dont l'utilisation dépend de droits d'autrui» ou «les données soumises à des droits d'autrui» englobent les données qui pourraient être soumises à la législation en matière de protection des données, à des droits de propriété intellectuelle ou qui contiennent des secrets d'affaires ou d'autres informations commercialement sensibles;

<sup>4</sup> [JO L 119 du 4.5.2016](#), p. 1.

<sup>5</sup> [JO L 201 du 31.7.2002](#), p. 37.

<sup>6</sup> [JO L 172 du 26.6.2019](#), p. 56.

d'accès aux données et d'utilisation de ces dernières. Ce type de mesure est envisagé dans la perspective d'une éventuelle loi sur les données (2021)<sup>7</sup>.

L'instrument s'inspire des principes de gestion et de réutilisation des données élaborés pour les données de la recherche. Les principes FAIR pour les données<sup>8</sup> stipulent que celles-ci doivent, en principe, être faciles à trouver, accessibles, interopérables et réutilisables.

- **Cohérence avec les autres politiques de l'Union**

Une législation sectorielle en matière d'accès aux données est en place et/ou en cours d'élaboration afin de remédier aux défaillances du marché recensées dans des domaines tels que l'automobile<sup>9</sup>, les prestataires de services de paiement<sup>10</sup>, les informations provenant de compteurs intelligents<sup>11</sup>, les données relatives au réseau d'électricité<sup>12</sup>, les systèmes de transport intelligents<sup>13</sup>, les informations environnementales<sup>14</sup>, les informations spatiales<sup>15</sup> et le secteur de la santé<sup>16</sup>. La présente proposition soutient l'utilisation de données mises à disposition en vertu des règles existantes sans modifier ces règles ni créer de nouvelles obligations sectorielles.

De même, la proposition est sans préjudice du droit de la concurrence, et est conçue conformément aux articles 101 et 102 du TFUE. Elle est également sans préjudice des dispositions de la directive n° 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<sup>17</sup>.

## **2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ**

- **Base juridique**

L'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE) constitue la base juridique pertinente du présent règlement. En vertu de cet article, l'UE doit adopter des mesures relatives au rapprochement des dispositions législatives, réglementaires et administratives des États membres qui ont pour objet l'établissement et le fonctionnement du marché intérieur. La présente initiative s'inscrit dans le cadre de la stratégie européenne pour les données de 2020, qui vise à renforcer le marché unique des données. Compte tenu de la numérisation croissante de l'économie et de la société, le risque existe que les États membres légifèrent de plus en plus de manière non coordonnée sur les questions liées aux données, ce qui intensifierait la fragmentation du marché unique. La mise en place de structures et de mécanismes de gouvernance qui formeront une approche coordonnée de l'utilisation des données dans l'ensemble des secteurs et des États membres aiderait les acteurs de l'économie fondée sur les données à tirer parti de l'échelle du marché unique. Cela contribuera à la mise

---

<sup>7</sup> Voir [COM\(2020\) 66 final](#).

<sup>8</sup> <https://www.force11.org/group/fairgroup/fairprinciples>

<sup>9</sup> [JO L 188 du 18.7.2009](#), p. 1, tel que modifié par le [JO L 151 du 14.6.2018](#), p. 1.

<sup>10</sup> [JO L 337 du 23.12.2015](#), p. 35.

<sup>11</sup> [JO L 158 du 14.6.2019](#), p. 125; [JO L 211 du 14.8.2009](#), p. 94.

<sup>12</sup> [JO L 220 du 25.8.2017](#), p. 1; [JO L 113 du 1.5.2015](#), p. 13.

<sup>13</sup> [JO L 207 du 6.8.2010](#), p. 1.

<sup>14</sup> [JO L 41 du 14.2.2003](#), p. 26.

<sup>15</sup> [JO L 108 du 25.4.2007](#), p. 1.

<sup>16</sup> Une proposition législative relative à l'espace européen des données de santé est envisagée pour le quatrième trimestre de 2021. [https://eur-lex.europa.eu/resource.html?uri=cellar%3A91ce5c0f-12b6-11eb-9a54-01aa75ed71a1.0001.02/DOC\\_2&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar%3A91ce5c0f-12b6-11eb-9a54-01aa75ed71a1.0001.02/DOC_2&format=PDF)

<sup>17</sup> [JO L 178 du 17.7.2000](#), p. 1.

en place du marché unique des données, en garantissant l'émergence et le fonctionnement transfrontière de services innovants au moyen d'un ensemble de dispositions harmonisées.

Les politiques numériques sont une compétence partagée entre l'UE et ses États membres. L'article 4, paragraphes 2 et 3 du TFUE, précise que, dans le domaine du marché unique et du développement technologique, l'Union peut mener des actions spécifiques, sans préjudice de la liberté des États membres d'agir dans les mêmes domaines.

- **Subsidiarité (en cas de compétence non exclusive)**

Les entreprises ont souvent besoin de données provenant de plusieurs États membres afin de pouvoir mettre au point des produits et des services à l'échelle de l'UE, étant donné que les échantillons de données disponibles dans un État membre en particulier ne recèlent souvent pas la richesse et la diversité qui permettent la reconnaissance de formes ou l'apprentissage automatique fondés sur les mégadonnées. En outre, les produits et services fondés sur des données qui sont mis au point dans un État membre peuvent nécessiter une adaptation aux préférences des clients d'un autre État membre, ce qui exige la disponibilité de données locales au niveau des États membres. Il faut dès lors que les données puissent circuler facilement au sein de chaînes de valeur transsectorielles et à l'échelle de l'UE, pour lesquelles un environnement législatif hautement harmonisé s'avère essentiel. En outre, seule une action au niveau de l'Union peut garantir l'essor d'un modèle européen de partage des données, comprenant des intermédiaires de données fiables pour le partage de données entre entreprises (B2B) et les espaces de données à caractère personnel, compte tenu de la nature transfrontière du partage de données et de l'importance d'une telle activité.

Un marché unique des données devrait garantir que des données du secteur public, des entreprises et des citoyens puissent être consultées et utilisées de la manière la plus efficace et la plus responsable possible, tandis que les entreprises et les citoyens conserveraient le contrôle des données qu'ils généreraient et que les investissements réalisés dans leur collecte seraient préservés. Un accès accru aux données aurait pour conséquence que des entreprises et des organismes de recherche feraient progresser des avancées scientifiques représentatives et l'innovation sur le marché dans l'ensemble de l'UE, un aspect particulièrement important dans les situations où une action coordonnée de l'UE s'avère nécessaire, telles que la crise de la COVID-19.

- **Proportionnalité**

L'initiative est proportionnée aux objectifs poursuivis. L'acte législatif proposé crée un cadre propice qui ne va pas au-delà de ce qui est nécessaire pour atteindre les objectifs. Il harmonise une série de pratiques de partage de données, tout en respectant la prérogative des États membres d'organiser leur administration et de légiférer sur l'accès aux informations du secteur public. Le cadre de notification concernant les intermédiaires de données, ainsi que les mécanismes relatifs à l'altruisme en matière de données, permettent d'accroître la confiance dans ces services, sans restreindre inutilement ces activités, et contribuent au développement d'un marché intérieur de l'échange de ce type de données. L'initiative laissera également une large marge de manœuvre en vue d'une application au niveau sectoriel, y compris pour le développement futur des espaces européens des données.

Le règlement proposé engendrera des coûts financiers et administratifs, qui devront être supportés principalement par les autorités nationales, tandis que les utilisateurs de données et les prestataires de services de partage de données supporteront certains coûts afin de garantir le respect des obligations énoncées dans le présent règlement. Toutefois, l'examen des

différentes options et de leurs coûts et avantages escomptés a permis de concevoir l'instrument de manière équilibrée. Ce dernier laissera suffisamment de souplesse aux autorités nationales pour décider du niveau des investissements financiers et examiner les possibilités de recouvrer ces coûts au moyen de redevances ou de frais administratifs, tout en offrant une coordination globale au niveau de l'UE. De même, les coûts supportés par les utilisateurs de données et les prestataires de services de partage seront compensés par la valeur qui découlera d'un accès et d'une utilisation plus larges des données, ainsi que par la pénétration de services innovants sur le marché.

- **Choix de l'instrument**

Le choix du règlement en tant qu'instrument juridique se justifie par la prédominance d'éléments qui requièrent une application uniforme ne laissant aucune marge de mise en œuvre aux États membres et créant un cadre entièrement horizontal. Parmi ces éléments figurent la notification concernant les prestataires de services de partage de données, les mécanismes d'altruisme en matière de données, les principes de base s'appliquant à la réutilisation de données du secteur public qui ne peuvent pas être mises à disposition en tant que données ouvertes ou qui ne sont pas soumises à une législation sectorielle de l'UE, ainsi que la mise en place de structures de coordination au niveau européen. L'applicabilité directe du règlement éviterait un délai et un processus de mise en œuvre aux États membres, tout en permettant la création des espaces européens communs des données dans un avenir proche, conformément au plan de relance de l'UE<sup>18</sup>.

Dans le même temps, les dispositions du règlement ne sont pas excessivement contraignantes et laissent aux États membres la possibilité d'agir à divers niveaux pour les éléments qui ne compromettent pas les objectifs de l'initiative, en particulier l'organisation des organismes compétents qui soutiennent les organismes du secteur public dans leurs tâches liées à la réutilisation de certaines catégories de données du secteur public.

### **3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT**

- **Consultation des parties intéressées**

Une consultation publique en ligne a été lancée le 19 février 2020, le jour de l'adoption de la stratégie européenne pour les données<sup>19</sup>, et s'est achevée le 31 mai 2020. La consultation a explicitement indiqué qu'elle avait pour objet de préparer la présente initiative, et elle a abordé les différents éléments de l'initiative au moyen de sections et de questions portant spécifiquement sur chacun d'eux. La consultation s'adressait à toutes les catégories de parties prenantes.

Au total, la Commission a reçu 806 contributions, dont 219 émanaient d'entreprises, 119 d'associations d'entreprises, 201 de citoyens de l'UE, 98 d'établissements universitaires/de recherche et 57 de pouvoirs publics. La voix des consommateurs était représentée par 7 participants, tandis que 54 participants étaient des organisations non gouvernementales (dont 2 organisations environnementales). Parmi les 219 entreprises/organisations d'entreprises, 43,4 % étaient des PME. Au total, 92,2 % des réponses provenaient de l'UE à 27. Très peu de participants ont précisé la portée locale, régionale, nationale ou internationale de leur organisation.

---

<sup>18</sup> [COM\(2020\) 456 final.](#)

<sup>19</sup> [COM/2020/66 final.](#)



230 documents de prise de position ont été présentés, soit en tant que pièce jointe aux réponses au questionnaire (210), soit en tant que contribution indépendante (20). Les documents ont apporté différents points de vue sur les sujets couverts par le questionnaire en ligne, en particulier en ce qui concerne la gouvernance des espaces communs de données. Ils ont fourni des avis sur les principes clés applicables à ces espaces et ont exprimé un large soutien à une hiérarchisation des normes ainsi qu'à la notion d'altruisme en matière de données. Ils ont également indiqué la nécessité de prévoir des garanties dans le cadre de l'élaboration de mesures relatives aux intermédiaires de données.

- **Obtention et utilisation d'expertise**

Afin d'explorer avec les experts compétents les conditions-cadres de la création d'espaces européens communs des données dans les secteurs recensés, une série de 10 ateliers consacrés aux espaces européens communs des données ont eu lieu en 2019 et un autre atelier a été organisé en mai 2020. Rassemblant au total plus de 300 parties prenantes, provenant principalement des secteurs privé et public, les ateliers ont couvert différents secteurs (agriculture, santé, secteur financier/bancaire, énergie, transports, durabilité/environnement, services publics, fabrication intelligente) et des aspects plus transversaux (éthique des données, marchés de données). Les services de la Commission chargés de ces secteurs ont participé aux ateliers. Les ateliers sectoriels ont permis d'identifier les éléments communs à tous les secteurs qui doivent être couverts par la mise en place d'un cadre horizontal de gouvernance.

- **Analyse d'impact**

Une analyse d'impact a été réalisée pour la présente proposition. Le 9 septembre 2020, le comité d'examen de la réglementation a émis un avis négatif. Le 5 octobre 2020, le comité a émis un avis favorable, assorti de réserves.

L'analyse d'impact examine les scénarios de référence, les options stratégiques et leurs incidences pour quatre domaines d'intervention, à savoir a) les mécanismes permettant une utilisation accrue des données du secteur public qui ne peuvent être mises à disposition en tant que données ouvertes, b) un cadre de certification ou de labellisation concernant les intermédiaires de données, c) des mesures favorisant l'altruisme en matière de données et d) des mécanismes de coordination et d'orientation des aspects horizontaux de la gouvernance sous la forme d'une structure au niveau de l'UE.

Pour tous les domaines d'intervention, l'option 1 consistant à assurer une coordination au niveau de l'UE avec des mesures réglementaires non contraignantes a été jugée insuffisante, car elle ne modifierait pas sensiblement la situation par rapport au scénario de référence. L'analyse s'est donc principalement concentrée sur les options 2 et 3, qui impliquaient une intervention réglementaire à faible et à forte intensité, respectivement. L'option privilégiée s'est avérée être une combinaison d'interventions réglementaires à plus faible et à plus forte intensité. Elle se présente comme suit:

En ce qui concerne les mécanismes visant à renforcer l'utilisation de certaines données du secteur public, dont l'utilisation est soumise à des droits d'autrui, tant l'option à faible intensité que l'option à forte intensité introduiraient des règles à l'échelle de l'UE pour la réutilisation de ces informations (notamment en ce qui concerne la non-exclusivité). L'intervention réglementaire à faible intensité nécessiterait que les organismes du secteur public particuliers qui permettent ce type de réutilisation soient techniquement équipés pour garantir une pleine préservation de la protection des données, de la vie privée et de la confidentialité. Elle comporterait également l'obligation pour les États membres de prévoir au

moins un mécanisme de guichet unique pour les demandes d'accès à ce type de données, sans déterminer la forme institutionnelle et administrative exacte que ce mécanisme devrait prendre. L'option à forte intensité aurait prévu la création d'un seul organisme d'autorisation des données par État membre. Compte tenu des coûts et des questions de faisabilité liés à l'option à forte intensité, l'option privilégiée est l'intervention réglementaire à faible intensité.

En ce qui concerne la certification ou la labellisation d'intermédiaires de données fiables, une intervention réglementaire à plus faible intensité a été envisagée sous la forme d'un mécanisme de labellisation facultatif plus souple, dans le cadre duquel les autorités compétentes désignées par les États membres (qui peuvent également être les mécanismes de guichet unique également mis en place pour améliorer la réutilisation des données du secteur public) effectueraient un bilan de qualité du respect des exigences requises pour l'obtention et l'octroi du label. L'intervention réglementaire à forte intensité consistait en un système de certification obligatoire géré par des organismes privés d'évaluation de la conformité. Étant donné qu'un système obligatoire engendrerait des coûts plus élevés, l'effet sur les PME et les jeunes pousses pourrait être prohibitif, et le marché n'est pas suffisamment mature pour un tel système; l'intervention réglementaire à plus faible intensité a dès lors été définie comme l'option stratégique privilégiée. Toutefois, l'intervention réglementaire à plus forte intensité, consistant en un système obligatoire, a également été considérée comme une solution alternative possible, car elle renforcerait considérablement la confiance dans le fonctionnement des intermédiaires de données et établirait des règles claires quant à la manière dont ces intermédiaires sont censés agir sur le marché européen des données. Une solution intermédiaire a été retenue à l'issue de nouvelles discussions au sein de la Commission. Elle consiste en une obligation de notification assortie d'un contrôle a posteriori du respect des exigences relatives à l'exercice des activités réalisé par les autorités compétentes des États membres. La solution présente les avantages d'un système obligatoire, tout en limitant la charge réglementaire pesant sur les acteurs du marché.

En ce qui concerne l'altruisme en matière de données, l'intervention réglementaire à faible intensité consistait en un cadre de certification volontaire pour les organisations désireuses d'offrir ce type de services, tandis que l'intervention réglementaire à forte intensité prévoyait un cadre d'autorisation obligatoire. Étant donné que la dernière option garantirait un niveau plus élevé de confiance dans la mise à disposition des données, ce qui pourrait contribuer à ce qu'un plus grand nombre de données soient mises à disposition par les personnes concernées et les entreprises et à accroître ainsi le niveau de développement et de recherche, tout en générant des coûts similaires, l'analyse d'impact l'a identifiée comme l'option privilégiée pour ce domaine d'intervention. Les discussions menées ultérieurement au sein de la Commission ont toutefois fait apparaître de nouvelles préoccupations quant à la charge administrative susceptible de peser sur les organisations altruistes en matière de données et au lien des obligations avec de futures initiatives sectorielles relatives à l'altruisme en matière de données. Une solution alternative a dès lors été retenue; elle donne aux organisations altruistes en matière de données la possibilité de s'enregistrer en tant qu'«organisation altruiste en matière de données reconnue dans l'UE». Ce mécanisme volontaire contribuera à accroître la confiance, tout en réduisant la charge administrative par rapport à un cadre d'autorisation obligatoire et à un cadre de certification volontaire.

Enfin, pour le mécanisme de gouvernance horizontal européen, l'intervention réglementaire à faible intensité prévoyait la création d'un groupe d'experts, tandis que l'intervention réglementaire à forte intensité consistait à créer une structure indépendante dotée de la personnalité juridique (semblable au comité européen de la protection des données). Compte

tenu des coûts élevés et du faible niveau de faisabilité politique de la mise en place de l'option à plus forte intensité, c'est l'option à faible intensité qui a été retenue.

Selon l'étude<sup>20</sup> réalisée à l'appui de l'analyse d'impact, si, dans le scénario de référence, l'économie fondée sur les données et la valeur économique du partage des données devraient augmenter pour atteindre 510 milliards à 533 milliards d'EUR (3,87 % du PIB) selon les estimations, celles-ci atteindraient 540,7 milliards à 544,4 milliards d'EUR (3,92 % à 3,95 % du PIB) selon l'option prête à l'emploi privilégiée. Ces montants ne tiennent compte que dans une mesure limitée des avantages en aval en termes d'amélioration des produits, d'augmentation de la productivité et de nouveaux moyens de relever les défis de société (par exemple, le changement climatique). En effet, ces avantages sont susceptibles d'être nettement plus importants que les avantages directs.

Dans le même temps, cette option stratégique prête à l'emploi permettrait de créer un modèle européen de partage des données qui offrirait une approche alternative au modèle commercial actuel des plateformes technologiques intégrées, grâce à l'émergence d'intermédiaires de données neutres. La présente initiative peut faire la différence pour l'économie fondée sur les données en instaurant la confiance dans le partage des données et en encourageant le développement d'espaces européens communs des données, au sein desquels les personnes physiques et morales contrôlent les données qu'elles génèrent.

- **Droits fondamentaux**

Étant donné que les données à caractère personnel relèvent du champ d'application de certains éléments du règlement, les mesures sont conçues de manière à respecter pleinement les dispositions législatives en matière de protection des données et à renforcer en pratique le contrôle que les personnes physiques exercent sur les données qu'elles génèrent.

En ce qui concerne la réutilisation accrue des données du secteur public, les droits fondamentaux que constituent la protection des données, le respect de la vie privée et la propriété (en l'occurrence les droits de propriété sur certaines données, qui sont par exemple commercialement confidentielles ou protégées par des droits de propriété intellectuelle) seront respectés. De même, les prestataires de services de partage de données qui proposent des services aux personnes concernées devront respecter les règles applicables en matière de protection des données.

Le cadre de notification des intermédiaires de données toucherait à la liberté d'entreprendre, dans la mesure où il introduirait certaines restrictions sous la forme de diverses exigences en tant que préalable au fonctionnement de telles entités.

#### **4. INCIDENCE BUDGÉTAIRE**

La présente proposition n'a aucune incidence budgétaire.

#### **5. AUTRES ÉLÉMENTS**

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

En raison du caractère dynamique de l'économie fondée sur les données, le suivi de l'évolution des incidences constitue un élément clé de l'intervention dans ce domaine. Afin de garantir que les mesures retenues produisent véritablement les résultats escomptés et de

---

<sup>20</sup> Commission européenne (2020, à paraître). *Support Study to this Impact Assessment*, SMART 2019/0024, élaborée par Deloitte.

faciliter d'éventuelles révisions futures, il est nécessaire de procéder au suivi et à l'évaluation de la mise en œuvre du présent règlement.

Le contrôle la réalisation des objectifs spécifiques et du respect des obligations réglementaires se fera à l'aide d'enquêtes représentatives menées auprès des parties prenantes, des travaux du centre de soutien pour le partage des données, des archives du comité européen de l'innovation dans le domaine des données sur les différents domaines d'intervention signalés par les autorités nationales concernées et d'une étude d'évaluation visant à faciliter la révision de l'acte.

- **Explication détaillée des différentes dispositions de la proposition**

Le **chapitre I** définit l'objet du règlement et énonce les définitions utilisées dans l'ensemble de l'acte.

Le **chapitre II** crée un mécanisme de réutilisation de certaines catégories de données protégées du secteur public, qui est subordonné au respect des droits d'autrui (notamment pour des motifs de protection des données à caractère personnel, mais aussi de protection des droits de propriété intellectuelle et de confidentialité des informations commerciales). Ce mécanisme est sans préjudice de la législation sectorielle de l'UE sur l'accès à ces données et sur leur réutilisation. La réutilisation de ces données ne relève pas du champ d'application de la directive (UE) 2019/1024 (directive sur les données ouvertes). Si les dispositions du présent chapitre ne créent aucun droit de réutilisation de ces données, elles définissent cependant un ensemble de conditions de base harmonisées dont le respect autoriserait une telle réutilisation (l'exigence de non-exclusivité, par exemple). Les organismes du secteur public autorisant ce type de réutilisation devraient être équipés sur le plan technique afin que la protection des données, le respect de la vie privée et la confidentialité soient pleinement préservés. Les États membres devront mettre en place un point de contact unique pour aider les chercheurs et les entreprises innovantes à sélectionner des données appropriées, et ils seront tenus de mettre en place des structures qui soutiendront les organismes du secteur public par des moyens techniques et une assistance juridique.

Le **chapitre III** vise à accroître la confiance dans le partage de données à caractère personnel et non personnel et à réduire les coûts de transaction liés au partage de données entre entreprises (B2B) ainsi qu'entre particuliers et entreprises (C2B) grâce à la création d'un régime de notification pour les prestataires de services de partage de données. Ces prestataires devront respecter un certain nombre d'exigences, notamment l'obligation de rester neutres en ce qui concerne les données échangées. Ils ne peuvent pas utiliser ces données à d'autres fins. Lorsque des prestataires de services de partage de données proposent des services à des personnes physiques, le critère supplémentaire d'assumer un devoir de loyauté à l'égard des personnes qui utilisent ces données devra également être rempli.

Le but de cette approche est de permettre aux services de partage de données de fonctionner de manière ouverte et collaborative, tout en donnant aux personnes physiques et morales les moyens d'agir grâce à une meilleure vue d'ensemble et à un meilleur contrôle de leurs données. Une autorité compétente désignée par les États membres sera chargée de contrôler le respect des exigences liées à la fourniture de ces services.

Le **chapitre IV** facilite l'altruisme des données (données mises volontairement à disposition par des particuliers ou des entreprises, pour le bien commun). Il prévoit la possibilité, pour les organisations qui pratiquent l'altruisme des données, de s'enregistrer en tant qu'«organisation

altruiste en matière de données reconnue dans l'UE» afin de renforcer la confiance dans leurs activités. Par ailleurs, un formulaire européen commun de consentement à l'altruisme des données sera élaboré afin de réduire les coûts liés au recueil du consentement et de faciliter la portabilité des données (lorsque les données à mettre à disposition ne sont pas détenues par la personne).

Le **chapitre V** énonce les exigences relatives au fonctionnement des autorités compétentes désignées pour surveiller et mettre en œuvre le cadre de notification pour les prestataires de services de partage de données et les entités altruistes en matière de données. Il contient également des dispositions relatives au droit d'introduire une réclamation contre les décisions de ces organes et aux voies de recours juridictionnel.

Le **chapitre VI** crée un groupe d'experts formel (le «comité européen de l'innovation dans le domaine des données»), qui facilitera l'émergence de bonnes pratiques par les autorités des États membres, notamment en matière de traitement des demandes de réutilisation de données, qui sont soumises aux droits d'autrui (chapitre II), de développement d'une pratique cohérente en ce qui concerne le cadre de notification pour les prestataires de services de partage de données (chapitre III) et d'altruisme des données (chapitre IV). Par ailleurs, le groupe d'experts formel assistera et conseillera la Commission sur la gouvernance de la normalisation intersectorielle et l'élaboration de demandes stratégiques de normalisation intersectorielle. Ce chapitre définit également la composition du conseil d'administration et en organise le fonctionnement.

Le **chapitre VII** autorise la Commission à adopter des actes d'exécution concernant le formulaire européen de consentement à l'altruisme en matière de données.

Le **chapitre VIII** contient des dispositions transitoires relatives au fonctionnement du régime d'autorisation générale pour les prestataires de partage de données et contient les dispositions finales.

Proposition de

**RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL****sur la gouvernance européenne des données  
(acte sur la gouvernance des données)**

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,  
vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,  
vu la proposition de la Commission européenne,  
après transmission du projet d'acte législatif aux parlements nationaux,  
vu l'avis du Comité économique et social européen<sup>21</sup>,  
vu l'avis du Comité des régions<sup>22</sup>,  
statuant conformément à la procédure législative ordinaire,  
considérant ce qui suit:

- (1) Le traité sur le fonctionnement de l'Union européenne (TFUE) prévoit l'établissement d'un marché intérieur ainsi que l'instauration d'un régime assurant que la concurrence n'est pas faussée sur le marché intérieur. La mise en place de règles et de pratiques communes dans les États membres en ce qui concerne l'élaboration d'un cadre de gouvernance des données devrait contribuer à la réalisation de ces objectifs.
- (2) Ces dernières années, les technologies numériques ont transformé l'économie et la société, touchant tous les secteurs d'activité et la vie quotidienne. Les données sont au cœur de cette transformation: l'innovation fondée sur les données apportera des avantages énormes aux particuliers, notamment par une amélioration de la médecine personnalisée, une mobilité nouvelle et une contribution au pacte vert pour l'Europe<sup>23</sup>. Dans sa stratégie pour les données<sup>24</sup>, la Commission a décrit la vision d'un espace européen commun des données, à savoir un marché unique des données dans lequel les données pourraient être utilisées quel que soit le lieu de leur stockage physique dans l'Union, conformément au droit applicable. Elle a également plaidé en faveur de la libre circulation sécurisée des données avec les pays tiers, sous réserve des exceptions et des restrictions en matière de sécurité publique, d'ordre public et d'autres objectifs légitimes de politique publique de l'Union européenne, conformément aux obligations internationales. Afin que cette vision devienne réalité, elle propose de mettre en place des espaces européens communs des données spécifiques à certains domaines, qui

---

<sup>21</sup> JO C du , p. .

<sup>22</sup> JO C du , p. .

<sup>23</sup> Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «Le pacte vert pour l'Europe», du 11.12.2019 [COM(2019) 640 final].

<sup>24</sup> COM(2020) 66 final.



constitueront le cadre concret du partage de données et de la mise en commun de données. Ainsi que le prévoit ladite stratégie, ces espaces européens communs des données peuvent couvrir des domaines tels que la santé, la mobilité, l'industrie manufacturière, les services financiers, l'énergie ou l'agriculture, ou des domaines thématiques tels que le pacte vert pour l'Europe, l'administration publique ou les compétences.

- (3) Il est nécessaire d'améliorer les conditions du partage des données dans le marché intérieur, en créant un cadre harmonisé pour les échanges de données. La législation sectorielle peut élaborer, adapter et proposer des éléments nouveaux et complémentaires, en fonction des spécificités du secteur, à l'instar de la législation envisagée sur l'espace européen des données de santé<sup>25</sup> et sur l'accès aux données relatives aux véhicules. En outre, certains secteurs de l'économie sont déjà réglementés par des volets sectoriels du droit de l'Union qui comprennent des règles relatives au partage de données ou à l'accès aux données, au niveau transfrontalier ou à l'échelle de l'Union<sup>26</sup>. Le présent règlement est donc sans préjudice du règlement (UE) 2016/679 du Parlement européen et du Conseil<sup>27</sup>, son application n'empêchant en particulier pas les transferts transfrontaliers de données conformément au chapitre V du règlement (UE) 2016/679, de la directive (UE) 2016/680 du Parlement européen et du Conseil<sup>28</sup>, de la directive (UE) 2016/943 du Parlement européen et du Conseil<sup>29</sup>, du règlement (UE) 2018/1807 du Parlement européen et du Conseil<sup>30</sup>, du règlement (CE) n° 223/2009 du Parlement européen et du Conseil<sup>31</sup>, de la directive 2000/31/CE du Parlement européen et du Conseil<sup>32</sup>, de la directive 2001/29/CE du

---

<sup>25</sup> Voir les annexes de la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur le programme de travail de la Commission pour 2021 [COM(2020) 690 final].

<sup>26</sup> Par exemple, la directive 2011/24/UE dans le contexte de l'espace européen des données de santé, et la législation pertinente en matière de transports, notamment la directive 2010/40/UE, le règlement (UE) 2019/1239 et le règlement (UE) 2020/1056, dans le contexte de l'espace européen des données relatives à la mobilité.

<sup>27</sup> 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).

<sup>28</sup> Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 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).

<sup>29</sup> Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (JO L 157 du 15.6.2016, p. 1).

<sup>30</sup> 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).

<sup>31</sup> Règlement (CE) n° 223/2009 du Parlement européen et du Conseil du 11 mars 2009 relatif aux statistiques européennes et abrogeant le règlement (CE, Euratom) n° 1101/2008 relatif à la transmission à l'Office statistique des Communautés européennes d'informations statistiques couvertes par le secret, le règlement (CE) n° 322/97 du Conseil relatif à la statistique communautaire et la décision 89/382/CEE, Euratom du Conseil instituant un comité du programme statistique des Communautés européennes (JO L 87 du 31.3.2009, p. 164).

<sup>32</sup> 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).

Parlement européen et du Conseil<sup>33</sup>, de la directive (UE) 2019/790 du Parlement européen et du Conseil<sup>34</sup>, de la directive 2004/48/CE du Parlement européen et du Conseil<sup>35</sup>, de la directive (UE) 2019/1024 du Parlement européen et du Conseil<sup>36</sup>, ainsi que du règlement (UE) 2018/858 du Parlement européen et du Conseil<sup>37</sup>, de la directive 2010/40/UE du Parlement européen et du Conseil<sup>38</sup> et des règlements délégués adoptés en vertu de cette dernière, et de toute autre législation sectorielle de l'Union régissant l'accès aux données et leur réutilisation. Le présent règlement ne devrait préjuger en rien de l'accès aux données et de leur utilisation à des fins de coopération internationale dans le cadre de la prévention et de la détection des infractions pénales, des enquêtes et des poursuites en la matière ou de l'exécution de sanctions pénales. Il convient d'établir un régime horizontal pour la réutilisation de certaines catégories de données protégées détenues par des organismes du secteur public et pour la fourniture de services de partage de données et de services fondés sur l'altruisme en matière de données dans l'Union. Les caractéristiques spécifiques des différents secteurs peuvent rendre nécessaire la conception de systèmes sectoriels fondés sur les données, tout en s'appuyant sur les exigences du présent règlement. Lorsqu'un acte juridique sectoriel de l'Union impose aux organismes du secteur public, aux prestataires de services de partage de données ou aux entités enregistrées fournissant des services d'altruisme en matière de données de respecter des exigences techniques, administratives ou organisationnelles particulières supplémentaires, y compris au moyen d'un régime d'autorisation ou de certification, les dispositions de cet acte juridique sectoriel de l'Union devraient s'appliquer également.

- (4) Une action au niveau de l'Union est nécessaire pour lever les obstacles au bon fonctionnement de l'économie fondée sur les données et créer un cadre de gouvernance à l'échelle de l'Union pour l'accès aux données et leur utilisation, en particulier en ce qui concerne la réutilisation de certains types de données détenues par le secteur public, la fourniture de services aux entreprises utilisatrices et aux personnes concernées par les prestataires de services de partage de données, ainsi que la collecte et le traitement des données mises à disposition à des fins altruistes par les personnes physiques et morales.
- (5) L'idée selon laquelle les données produites aux frais des budgets publics devraient profiter à la société est depuis longtemps présente dans la politique de l'Union. La directive (UE) 2019/1024 ainsi que la législation sectorielle garantissent que le secteur public rend facilement accessibles davantage des données qu'il produit, en vue de leur

---

<sup>33</sup> Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (JO L 167 du 22.6.2001, p. 10).

<sup>34</sup> Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE (JO L 130 du 17.5.2019, p. 92).

<sup>35</sup> Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle. (JO L 157 du 30.4.2004, p. 45).

<sup>36</sup> Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (JO L 172 du 26.6.2019, p. 56).

<sup>37</sup> Règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) n° 715/2007 et (CE) n° 595/2009 et abrogeant la directive 2007/46/CE (JO L 151 du 14.6.2018, p. 1).

<sup>38</sup> Directive 2010/40/UE du Parlement européen et du Conseil du 7 juillet 2010 concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport (JO L 207 du 6.8.2010, p. 1).



utilisation et de leur réutilisation. Toutefois, il arrive souvent que certaines catégories de données [données commerciales confidentielles, données couvertes par le secret statistique, données protégées par des droits de propriété intellectuelle détenus par des tiers, y compris les secrets d'affaires et les données à caractère personnel non accessibles en vertu d'une législation nationale ou de l'Union particulière, comme le règlement (UE) 2016/679 et la directive (UE) 2016/680] figurant dans des bases de données publiques ne soient pas rendues accessibles, même pour des activités de recherche ou d'innovation. En raison du caractère sensible de ces données, il faut satisfaire à certaines exigences procédurales de nature technique et juridique avant leur mise à disposition, afin de garantir le respect des droits que d'autres personnes détiennent sur ces données. Le respect de ces exigences requiert généralement beaucoup de temps et de connaissances, ce qui a entraîné la sous-utilisation de ces données. Si certains États membres mettent en place des structures, des processus et, parfois, des législations pour faciliter ce type de réutilisation, ce n'est pas le cas dans l'ensemble de l'Union.

- (6) Il existe des techniques permettant d'effectuer des analyses respectueuses de la vie privée dans les bases de données contenant des données à caractère personnel, notamment l'anonymisation, la pseudonymisation, la confidentialité différentielle, la généralisation ou la suppression et la randomisation. Le recours à ces technologies renforçant la protection de la vie privée, ainsi qu'à des approches globales de la protection des données, devrait garantir la réutilisation sûre des données à caractère personnel et des données commerciales confidentielles à des fins de recherche, d'innovation et de statistiques. Dans de nombreux cas, cela suppose que l'utilisation et la réutilisation des données dans ce contexte ne puissent se faire que dans un environnement de traitement sécurisé mis en place et supervisé par le secteur public. Il existe, au niveau de l'Union, une certaine expérience de tels environnements de traitement sécurisés, qui sont utilisés pour la recherche sur les microdonnées statistiques au titre du règlement (UE) n° 557/2013 de la Commission<sup>39</sup>. D'une manière générale, dans la mesure où des données à caractère personnel sont concernées, leur traitement devrait se fonder sur un ou plusieurs des motifs de traitement prévus à l'article 6 du règlement (UE) 2016/679.
- (7) Les catégories de données détenues par des organismes du secteur public qui devraient faire l'objet d'une réutilisation en vertu du présent règlement ne relèvent pas du champ d'application de la directive (UE) 2019/1024, qui exclut les données qui ne sont pas accessibles pour des raisons de confidentialité commerciale ou statistique et les données dont des tiers détiennent les droits de propriété intellectuelle. Les données à caractère personnel ne relèvent pas du champ d'application de la directive (UE) 2019/1024 dans la mesure où les règles d'accès excluent ou limitent l'accès à ces données pour des motifs de protection des données, de protection de la vie privée et d'intégrité de la personne concernée, en particulier au regard des règles relatives à la protection des données. La réutilisation de données susceptibles de contenir des secrets d'affaires devrait se faire sans préjudice de la directive (UE) 2016/943<sup>40</sup>, qui fixe le cadre pour l'obtention, l'utilisation ou la divulgation licites des secrets d'affaires. Le présent règlement est sans préjudice des obligations plus spécifiques que le droit

---

<sup>39</sup> Règlement (UE) n° 557/2013 de la Commission du 17 juin 2013 mettant en œuvre le règlement (CE) n° 223/2009 du Parlement européen et du Conseil relatif aux statistiques européennes en ce qui concerne l'accès aux données confidentielles à des fins scientifiques et abrogeant le règlement (CE) n° 831/2002 de la Commission (JO L 164 du 18.6.2013, p. 16).

<sup>40</sup> JO L 157 du 15.6.2016, p. 1.

sectoriel national ou de l'Union impose aux organismes du secteur public pour autoriser la réutilisation de données, et il complète ces obligations.

- (8) Le régime de réutilisation prévu par le présent règlement devrait s'appliquer aux données dont la fourniture est une activité qui relève des missions de service public dévolues aux organismes du secteur public concernés en vertu de la loi ou d'autres règles contraignantes en vigueur dans les États membres. En l'absence de telles règles, les missions de service public devraient être définies conformément aux pratiques administratives courantes dans les États membres, sous réserve que l'objet de ces missions soit transparent et soumis à réexamen. Les missions de service public pourraient être définies à titre général ou au cas par cas pour les différents organismes du secteur public. Étant donné que les entreprises publiques ne relèvent pas de la définition des organismes du secteur public, les données qu'elles détiennent ne devraient pas être soumises au présent règlement. Les données détenues par les établissements culturels et éducatifs, pour lesquelles les droits de propriété intellectuelle ne sont pas accessoires mais qui sont principalement contenues dans des œuvres et d'autres documents protégés par de tels droits de propriété intellectuelle, ne relèvent pas du présent règlement.
- (9) Les organismes du secteur public devraient se conformer au droit de la concurrence lorsqu'ils établissent les principes de la réutilisation des données qu'ils détiennent, en évitant autant que possible la conclusion d'accords qui pourraient avoir pour objet ou pour effet de créer des droits exclusifs pour la réutilisation de certaines données. De tels accords ne devraient être possibles que lorsque cela est justifié et nécessaire en vue de la fourniture d'un service d'intérêt général. Tel peut être le cas lorsque l'utilisation exclusive des données est le seul moyen de maximiser les avantages sociétaux des données en question, par exemple lorsqu'il n'existe qu'une seule entité (spécialisée dans le traitement d'un ensemble de données particulier) capable d'exécuter le service ou de réaliser le produit permettant à l'organisme du secteur public de fournir un service numérique avancé dans l'intérêt général. De tels accords devraient toutefois être conclus dans le respect des règles en matière de marchés publics et faire l'objet d'un réexamen régulier sur la base d'une analyse de marché, afin de déterminer si cette exclusivité reste nécessaire. En outre, ils devraient être conformes aux règles applicables en matière d'aides d'État, le cas échéant, et être conclus pour une période limitée ne dépassant pas trois ans. Dans un souci de transparence, ces accords exclusifs devraient être publiés en ligne, indépendamment de l'éventuelle publication de l'attribution d'un marché public.
- (10) Lorsqu'ils ont été conclus ou étaient déjà en place avant l'entrée en vigueur du présent règlement, les accords exclusifs dorénavant interdits et les autres pratiques ou arrangements entre détenteurs et réutilisateurs de données qui ne confèrent pas expressément de droits exclusifs mais dont on peut raisonnablement s'attendre à ce qu'ils restreignent la disponibilité des données à des fins de réutilisation ne devraient pas être renouvelés à leur terme. Dans le cas d'accords à durée indéterminée ou à long terme, la résiliation devrait intervenir dans un délai de trois ans à compter de la date d'entrée en vigueur du présent règlement.
- (11) Il convient de fixer les conditions de réutilisation des données protégées qui s'appliquent aux organismes du secteur public compétents en vertu du droit national pour autoriser la réutilisation, sans que ces conditions portent atteinte à des droits ou obligations concernant l'accès à ces données. Ces conditions devraient être non discriminatoires, proportionnées et objectivement justifiées, sans restreindre la concurrence. En particulier, les organismes du secteur public autorisant la réutilisation

devraient disposer des moyens techniques nécessaires pour assurer la protection des droits et intérêts des tiers. Les conditions liées à la réutilisation des données devraient être limitées à ce qui est nécessaire pour préserver les droits et intérêts d'autrui en ce qui concerne les données, ainsi que l'intégrité des systèmes informatiques et de communication des organismes du secteur public. Ces derniers devraient appliquer des conditions qui servent au mieux les intérêts du réutilisateur sans entraîner d'efforts disproportionnés pour le secteur public. Selon le cas, avant leur transmission, les données à caractère personnel devraient être totalement anonymisées, de manière à empêcher définitivement l'identification des personnes concernées, et les données contenant des informations commerciales confidentielles devraient être modifiées de telle sorte qu'aucune information confidentielle ne soit divulguée. Dans le cas où la fourniture de données anonymisées ou modifiées ne permettrait pas de répondre aux besoins du réutilisateur, la réutilisation des données dans un environnement de traitement sécurisé, sur place ou à distance, pourrait être autorisée. L'analyse des données dans ces environnements de traitement sécurisés devrait être supervisée par l'organisme du secteur public, afin de protéger les droits et intérêts d'autrui. En particulier, des données à caractère personnel ne devraient être transmises à un tiers en vue de leur réutilisation que lorsqu'une base juridique le permet. L'organisme du secteur public pourrait subordonner l'utilisation d'un tel environnement de traitement sécurisé à la signature par le réutilisateur d'un accord de confidentialité interdisant la divulgation de toute information compromettant les droits et intérêts de tiers que le réutilisateur aurait pu acquérir malgré les garanties mises en place. Les organismes du secteur public devraient, le cas échéant, faciliter la réutilisation des données fondée sur le consentement des personnes concernées ou l'autorisation des personnes morales quant à la réutilisation des données les concernant, par des moyens techniques appropriés. À cet égard, l'organisme du secteur public devrait aider les réutilisateurs potentiels à solliciter un tel consentement, en mettant en place des mécanismes techniques permettant la transmission des demandes de consentement des réutilisateurs, lorsque cela est réalisable en pratique. Les coordonnées permettant de prendre directement contact avec les personnes concernées ou les entreprises ne devraient pas être communiquées aux réutilisateurs.

- (12) Le présent règlement ne devrait pas affecter les droits de propriété intellectuelle détenus par des tiers. Le présent règlement ne devrait pas non plus affecter l'existence des droits de propriété intellectuelle détenus par des organismes du secteur public ou la qualité de titulaires de tels droits reconnue à ces organismes, de même qu'il ne devrait restreindre en aucune manière l'exercice de ces droits en dehors des limites qu'il fixe. Les obligations imposées conformément au présent règlement ne devraient s'appliquer que dans la mesure où elles sont compatibles avec les accords internationaux sur la protection des droits de propriété intellectuelle, notamment la convention de Berne pour la protection des œuvres littéraires et artistiques (convention de Berne), l'accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (accord sur les ADPIC) et le traité de l'OMPI sur le droit d'auteur. Les organismes du secteur public devraient, toutefois, exercer leurs droits d'auteur de façon à faciliter la réutilisation des données.
- (13) Les données faisant l'objet de droits de propriété intellectuelle ou contenant des secrets d'affaires ne devraient être transmises à un tiers que si cette transmission est licite en vertu du droit de l'Union ou du droit national ou avec l'accord du titulaire des droits. Lorsque les organismes du secteur public sont titulaires du droit prévu à l'article 7, paragraphe 1, de la directive n° 96/9/CE du Parlement européen et du

Conseil<sup>41</sup>, ils ne devraient pas exercer ce droit dans le but de prévenir la réutilisation des données ou de restreindre la réutilisation au-delà des limites fixées par le présent règlement.

- (14) Les entreprises et les personnes concernées devraient pouvoir avoir la certitude que la réutilisation de certaines catégories de données protégées détenues par le secteur public se fera dans le respect de leurs droits et intérêts. Des garanties supplémentaires devraient donc être mises en place pour les situations dans lesquelles la réutilisation de telles données du secteur public est fondée sur un traitement des données en dehors du secteur public. Une garantie supplémentaire de cet ordre pourrait consister à exiger des organismes du secteur public qu'ils tiennent pleinement compte des droits et intérêts des personnes physiques et morales (en particulier de la protection des données à caractère personnel, des données commercialement sensibles et des droits de propriété intellectuelle) dans le cas où ces données sont transférées vers des pays tiers.
- (15) En outre, il importe de protéger les données commercialement sensibles à caractère non personnel, notamment les secrets d'affaires, mais aussi les données à caractère non personnel représentant des contenus protégés par des droits de propriété intellectuelle contre un accès illicite susceptible de constituer un vol de propriété intellectuelle ou de l'espionnage industriel. Afin de garantir la protection des droits fondamentaux ou des intérêts des détenteurs de données, les données à caractère non personnel qui doivent être protégées contre un accès illicite ou non autorisé en vertu du droit de l'Union ou du droit national et qui sont détenues par des organismes du secteur public ne devraient être transférées que vers des pays tiers dans lesquels des garanties appropriées sont prévues pour l'utilisation des données. Il devrait être considéré que de telles garanties appropriées existent lorsque, dans le pays tiers concerné, des mesures équivalentes garantissent que les données à caractère non personnel bénéficient d'un niveau de protection similaire à celui qui est applicable en vertu du droit de l'Union ou du droit national, notamment en ce qui concerne la protection des secrets d'affaires et la protection des droits de propriété intellectuelle. À cette fin, la Commission peut adopter des actes d'exécution établissant qu'un pays tiers offre un niveau de protection essentiellement équivalent à celui prévu par le droit de l'Union ou le droit national. Pour évaluer le niveau de protection offert dans un tel pays tiers, il convient en particulier de prendre en considération la législation applicable, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal relatif à l'accès aux données à caractère non personnel et à leur protection, tout accès par les autorités publiques de ce pays tiers aux données transférées, l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes qui sont chargées dans le pays tiers d'assurer et de faire respecter le régime juridique garantissant l'accès à ces données, ou les engagements internationaux pris par le pays tiers concerné en ce qui concerne la protection des données, ou d'autres obligations découlant de conventions ou instruments juridiquement contraignants ainsi que de la participation à des systèmes multilatéraux ou régionaux. L'existence de voies de droit effectives pour les détenteurs de données, les organismes du secteur public ou les prestataires de services de partage de données dans le pays tiers concerné revêt une importance particulière dans le contexte du transfert de données à caractère non personnel vers ce pays tiers. Ces garanties devraient donc inclure l'existence de droits opposables et de voies de droit effectives.

---

<sup>41</sup> Directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 concernant la protection juridique des bases de données (JO L 77 du 27.3.1996, p. 20).

- (16) Dans les cas où la Commission n'a pas adopté d'acte d'exécution établissant qu'un pays tiers offre, en particulier en ce qui concerne la protection des données commercialement sensibles et la protection des droits de propriété intellectuelle, un niveau de protection essentiellement équivalent à celui prévu par le droit de l'Union ou le droit national, l'organisme du secteur public ne devrait transmettre des données protégées à un réutilisateur que si ce dernier prend certains engagements dans l'intérêt de la protection des données. Le réutilisateur souhaitant transférer les données à un tel pays tiers devrait s'engager à respecter les obligations prévues dans le présent règlement, même après le transfert. Afin de garantir la bonne exécution de ces obligations, le réutilisateur devrait également admettre, pour le règlement judiciaire des litiges, la compétence de l'État membre de l'organisme du secteur public qui a autorisé la réutilisation.
- (17) Certains pays tiers adoptent des lois, des règlements et d'autres actes juridiques qui visent à transférer directement des données à caractère non personnel, ou à donner accès à de telles données dans l'Union, sous le contrôle de personnes physiques et morales relevant de la compétence des États membres. Les décisions de juridictions ou d'autorités administratives de pays tiers qui exigent un tel transfert ou accès concernant des données à caractère non personnel devraient être exécutoires lorsqu'elles sont fondées sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre. Dans certains cas, il peut arriver que l'obligation découlant du droit d'un pays tiers de transférer des données à caractère non personnel ou de donner accès à de telles données soit incompatible avec une obligation concurrente de protéger ces données en vertu du droit de l'Union ou du droit national, en particulier en ce qui concerne la protection des données commercialement sensibles et la protection des droits de propriété intellectuelle, et y compris les engagements contractuels pris en matière de confidentialité conformément à ce droit. En l'absence d'accords internationaux régissant ces questions, il convient de n'autoriser le transfert ou l'accès que sous certaines conditions: en particulier, le système du pays tiers devrait exiger que les motifs et la proportionnalité de la décision soient exposés, la décision judiciaire ou administrative devrait avoir un caractère spécifique et l'objection motivée du destinataire devrait faire l'objet d'un contrôle dans le pays tiers par une juridiction compétente habilitée à tenir dûment compte des intérêts juridiques pertinents du fournisseur de ces données.
- (18) Afin d'empêcher l'accès illicite à des données à caractère non personnel, les organismes du secteur public, les personnes physiques ou morales auxquelles le droit de réutilisation des données a été accordé, les prestataires de services de partage de données et les entités inscrites au registre des organisations altruistes en matière de données reconnues devraient prendre toutes les mesures raisonnables pour empêcher l'accès aux systèmes dans lesquels des données à caractère non personnel sont stockées, y compris le cryptage des données ou des politiques internes.
- (19) Afin de renforcer la confiance dans les mécanismes de réutilisation, il peut être nécessaire d'assortir de conditions plus strictes certains types de données à caractère non personnel dont le caractère hautement sensible a été constaté, en ce qui concerne le transfert vers des pays tiers, si un tel transfert risque de compromettre des objectifs de politique publique, conformément aux engagements internationaux. Par exemple, dans le domaine de la santé, certains ensembles de données détenus par des acteurs du système de santé publique, tels que les hôpitaux publics, pourraient être considérés comme des données de santé hautement sensibles. Afin de garantir l'harmonisation



des pratiques dans l'ensemble de l'Union, ces types de données publiques à caractère non personnel hautement sensibles devraient être définis par le droit de l'Union, par exemple dans le contexte de l'espace européen des données de santé ou d'une autre législation sectorielle. Les conditions de transfert de ces données vers des pays tiers devraient être fixées dans des actes délégués. Elles devraient être proportionnées, non discriminatoires et nécessaires pour protéger les objectifs légitimes de politique publique définis, tels que la protection de la santé publique, l'ordre public, la sécurité, l'environnement, la moralité publique, la protection des consommateurs, la protection de la vie privée et la protection des données à caractère personnel. Ces conditions devraient correspondre aux risques mis en évidence en ce qui concerne la sensibilité de ces données, y compris le risque de réidentification des personnes. Elles pourraient comprendre des conditions applicables au transfert ou des arrangements techniques, notamment l'obligation d'utiliser un environnement de traitement sécurisé, des limitations en ce qui concerne la réutilisation des données dans des pays tiers ou les catégories de personnes habilitées à transférer ces données vers des pays tiers ou pouvant y avoir accès dans des pays tiers. Dans des cas exceptionnels, elles pourraient également inclure des restrictions quant au transfert des données vers des pays tiers afin de protéger l'intérêt public.

- (20) Les organismes du secteur public devraient avoir la possibilité de percevoir des redevances pour la réutilisation des données, mais aussi de décider de rendre ces données disponibles à un coût inférieur ou gratuitement, par exemple pour certaines catégories de réutilisations telles que la réutilisation à des fins non commerciales ou la réutilisation par des petites et moyennes entreprises, de manière à encourager cette réutilisation pour stimuler la recherche et l'innovation et soutenir des entreprises qui représentent une source importante d'innovation et ont généralement plus de difficultés à collecter elles-mêmes des données pertinentes, conformément aux règles en matière d'aides d'État. Ces redevances devraient être raisonnables, transparentes, publiées en ligne et non discriminatoires.
- (21) Afin d'encourager la réutilisation de ces catégories de données, les États membres devraient mettre en place un point d'information unique servant d'interface principale pour les réutilisateurs qui souhaitent réutiliser les données détenues par les organismes du secteur public. Sa mission devrait s'étendre à plusieurs secteurs et compléter, si nécessaire, les dispositions prises au niveau sectoriel. En outre, les États membres devraient désigner, établir ou contribuer à établir des organismes compétents pour soutenir les activités des organismes du secteur public autorisant la réutilisation de certaines catégories de données protégées. L'une des tâches confiées à ces organismes compétents peut être d'accorder l'accès aux données, lorsque la législation sectorielle de l'Union ou des États membres l'exige. Ces organismes compétents devraient fournir un soutien aux organismes du secteur public en recourant à des techniques de pointe, notamment des environnements de traitement des données sécurisés, qui permettent d'analyser les données d'une manière qui préserve la confidentialité des informations. Une telle structure de soutien pourrait assister les détenteurs de données dans la gestion du consentement, y compris en ce qui concerne certains domaines de la recherche scientifique, dans le respect des normes éthiques reconnues en matière de recherche scientifique. Le traitement des données devrait être réalisé sous la responsabilité de l'organisme du secteur public chargé du registre contenant les données, qui reste un responsable du traitement des données au sens du règlement (UE) 2016/679 en ce qui concerne les données à caractère personnel. Les États membres peuvent se doter d'un ou de plusieurs organismes compétents agissant dans différents secteurs.

(22) Les prestataires de services de partage de données (intermédiaires de données) sont appelés à jouer un rôle clé dans l'économie fondée sur les données, en tant qu'instruments facilitant l'agrégation et l'échange de quantités substantielles de données pertinentes. Les intermédiaires de données qui proposent des services mettant en relation les différents acteurs contribuent potentiellement à la mise en commun efficace des données ainsi qu'à la facilitation du partage bilatéral des données. Des intermédiaires de données spécialisés qui sont indépendants à la fois des détenteurs de données et des utilisateurs de données peuvent jouer un rôle de facilitation dans l'émergence de nouveaux écosystèmes fondés sur les données qui soient indépendants de tout acteur jouissant d'une puissance significative sur le marché. Le présent règlement ne devrait concerner que les prestataires de services de partage de données qui ont pour principal objectif d'établir une relation commerciale, juridique et éventuellement technique entre, d'une part, des détenteurs de données, y compris des personnes concernées et, d'autre part, des utilisateurs potentiels et d'aider l'une et l'autre parties dans leurs transactions réciproques d'actifs de données. Il ne devrait couvrir que les services visant à assurer une intermédiation entre un nombre indéterminé de détenteurs de données et un nombre indéterminé d'utilisateurs de données, à l'exclusion des services de partage de données destinés à être utilisés par un groupe fermé de détenteurs et d'utilisateurs de données. Les prestataires de services en nuage devraient être exclus, de même que les prestataires de services qui obtiennent des données auprès de détenteurs de données, les agrègent, les enrichissent ou les transforment et accordent à des utilisateurs de données des licences d'utilisation pour les données qui en résultent, sans établir de relation directe entre les détenteurs de données et les utilisateurs de données, par exemple, les courtiers en publicité ou courtiers de données, les cabinets de conseil en données, les fournisseurs de produits de données résultant de la valeur ajoutée aux données par le prestataire de services. Par ailleurs, les prestataires de services de partage de données devraient être autorisés à apporter des adaptations aux données échangées, telles que leur conversion dans des formats spécifiques, dans la mesure où cela facilite leur utilisation par l'utilisateur de données et si ce dernier le souhaite. En outre, les services axés sur l'intermédiation de contenus, en particulier les contenus protégés par le droit d'auteur, ne devraient pas être couverts par le présent règlement. Les plateformes d'échange de données qui sont à l'usage exclusif d'un seul détenteur de données pour lui permettre d'utiliser les données qu'il détient, ainsi que les plateformes développées dans le contexte d'objets et de dispositifs connectés à l'internet des objets, qui ont pour principal objectif de garantir les fonctionnalités de l'objet ou du dispositif connecté et d'autoriser des services à valeur ajoutée, ne devraient pas être couvertes par le présent règlement. Les «fournisseurs de système consolidé de publication» au sens de l'article 4, paragraphe 1, point 53, de la directive 2014/65/UE du Parlement européen et du Conseil<sup>42</sup> ainsi que les «prestataires de services d'information sur les comptes» au sens de l'article 4, point 19, de la directive (UE) 2015/2366 du Parlement européen et du Conseil<sup>43</sup> ne devraient pas être considérés comme des prestataires de services de partage de données aux fins du présent règlement. Les entités qui limitent leurs activités à faciliter l'utilisation de données mises à disposition selon le principe de

---

<sup>42</sup> Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE (JO L 173 du 12.6.2014, p. 349).

<sup>43</sup> Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35).

l'altruisme en matière de données et qui agissent dans un but non lucratif ne devraient pas être couvertes par le chapitre III du présent règlement, étant donné que cette activité sert des finalités d'intérêt général en augmentant le volume des données disponibles à ces fins.

- (23) Les prestataires de services de partage de données qui proposent leurs services à des personnes concernées, au sens du règlement (UE) 2016/679, constituent une catégorie spécifique d'intermédiaires de données. Ces prestataires s'intéressent exclusivement aux données à caractère personnel et cherchent à renforcer la capacité d'action individuelle et le contrôle des individus sur les données les concernant. Ils devraient aider les personnes à exercer leurs droits au titre du règlement (UE) 2016/679, notamment la gestion de leur consentement au traitement des données, le droit d'accès à leurs propres données, le droit de rectification des données à caractère personnel inexacts, le droit à l'effacement ou «droit à l'oubli», le droit à la limitation du traitement et le droit à la portabilité des données, qui permet aux personnes concernées de transférer leurs données à caractère personnel d'un responsable du traitement à un autre. Dans ce contexte, il importe que leur modèle commercial garantisse qu'il n'existe pas d'incitations inadéquates poussant les personnes à mettre à disposition en vue d'un traitement davantage de données qu'elles ne devraient le faire dans leur propre intérêt. Les prestataires pourraient notamment conseiller les personnes sur les utilisations potentielles de leurs données et vérifier que les utilisateurs de données font preuve d'une diligence suffisante avant de les autoriser à contacter les personnes concernées, afin d'éviter les pratiques frauduleuses. Dans certaines circonstances, il pourrait être souhaitable de compiler des données réelles dans un espace de stockage de données à caractère personnel, ou «espace de données à caractère personnel», de sorte que le traitement puisse avoir lieu dans cet espace sans que les données à caractère personnel soient transmises à des tiers, afin d'assurer une protection maximale des données à caractère personnel et de la vie privée.
- (24) Les coopératives de données visent à renforcer la position des personnes physiques en leur permettant de poser des choix en connaissance de cause avant de donner leur consentement à l'utilisation des données, en influant sur les conditions et modalités appliquées à l'utilisation des données par les organisations d'utilisateurs de données ou en réglant, le cas échéant, les litiges nés entre les membres d'un groupe sur la manière d'utiliser les données lorsque celles-ci portent sur plusieurs personnes concernées au sein de ce groupe. Dans ce contexte, il est important de tenir compte du fait que les droits consacrés par le règlement (UE) 2016/679 ne peuvent être exercés que par des personnes à titre individuel et ne peuvent être conférés ou délégués à une coopérative de données. Les coopératives de données pourraient également constituer un outil utile pour les entreprises unipersonnelles, les microentreprises, les petites et moyennes entreprises, qui sont souvent comparables à des personnes physiques en termes de connaissance du partage des données.
- (25) Afin d'accroître la confiance dans ces services de partage de données, notamment en ce qui concerne l'utilisation des données et le respect des conditions imposées par les détenteurs de données, il est nécessaire de créer un cadre réglementaire à l'échelle de l'Union qui définisse des exigences largement harmonisées concernant la prestation fiable de ces services de partage de données. Cela contribuera à pourvoir les détenteurs et les utilisateurs de données d'un meilleur contrôle sur l'accès à leurs données et leur utilisation, conformément au droit de l'Union. Tant dans les contextes où le partage de données intervient entre entreprises que dans ceux où il se produit entre entreprises et consommateurs, les prestataires de services de partage de données devraient proposer



une nouvelle gouvernance des données «à l'européenne», en prévoyant une séparation, dans l'économie fondée sur les données, entre fourniture, intermédiation et utilisation. Les prestataires de services de partage de données peuvent également mettre à disposition une infrastructure technique spécifique pour l'interconnexion des détenteurs de données et des utilisateurs de données.

- (26) La neutralité des prestataires de services de partage de données à l'égard des données échangées entre les détenteurs et les utilisateurs de données est fondamentale pour instaurer la confiance et accroître le contrôle des détenteurs et des utilisateurs de données. Il est donc nécessaire que les prestataires de services de partage de données agissent uniquement en tant qu'intermédiaires dans les transactions, et qu'ils n'utilisent les données échangées à aucune autre fin. Dès lors, une séparation structurelle entre le service de partage de données et tout autre service fourni sera également nécessaire, afin d'éviter les conflits d'intérêts. Cela signifie que le service de partage de données devrait être fourni par une entité juridique distincte des autres activités du prestataire. Les prestataires de services de partage de données qui agissent en tant qu'intermédiaires dans l'échange de données entre des personnes physiques qui sont détenteurs de données et des personnes morales devraient, en outre, assumer un devoir de loyauté à l'égard des personnes physiques, de telle sorte qu'ils agissent au mieux des intérêts des détenteurs de données.
- (27) Afin de garantir que les prestataires de services de partage de données respectent les conditions énoncées dans le présent règlement, il convient que ces derniers soient établis dans l'Union. À défaut, lorsqu'un prestataire de services de partage de données qui n'est pas établi dans l'Union propose des services à l'intérieur de l'Union, il devrait désigner un représentant. La désignation d'un représentant est nécessaire, étant donné que ces prestataires de services de partage de données traitent des données à caractère personnel ainsi que des données commerciales confidentielles, ce qui nécessite un contrôle étroit du respect, par ces prestataires de services, des conditions énoncées dans le présent règlement. Afin de déterminer si un tel prestataire de services de partage de données propose des services dans l'Union, il convient d'examiner s'il apparaît qu'il envisage d'offrir des services à des personnes dans un ou plusieurs États membres. La seule accessibilité, dans l'Union, du site internet du prestataire de services de partage de données ou d'une adresse électronique et d'autres coordonnées ou encore l'utilisation d'une langue généralement utilisée dans le pays tiers où le prestataire de services de partage de données est établi devraient être jugés insuffisants aux fins de vérifier si telle est son intention. Cependant, des facteurs tels que l'utilisation d'une langue ou d'une monnaie généralement utilisées dans un ou plusieurs États membres avec la possibilité de commander des services dans cette autre langue ou la mention d'utilisateurs qui se trouvent dans l'Union peuvent indiquer que le prestataire de services de partage de données envisage d'offrir des services dans l'Union. Le représentant devrait agir pour le compte du prestataire de services de partage de données et devrait pouvoir être contacté par les autorités compétentes. Le représentant devrait être désigné par un mandat écrit du prestataire de services de partage de données le chargeant d'agir en son nom pour remplir les obligations qui lui incombent en vertu du présent règlement.
- (28) Le présent règlement est sans préjudice de l'obligation faite aux prestataires de services de partage de données de se conformer au règlement (UE) 2016/679 ni de la responsabilité qui incombe aux autorités de contrôle de veiller au respect dudit règlement. Lorsque les prestataires de services de partage de données sont des responsables du traitement ou des sous-traitants au sens du règlement (UE) 2016/679,

ils sont liés par les dispositions dudit règlement. Le présent règlement est également sans préjudice de l'application du droit de la concurrence.

- (29) Les prestataires de services de partage de données devraient également prendre des mesures pour veiller au respect du droit de la concurrence. Le partage de données peut générer divers gains d'efficacité, mais il peut également entraîner des restrictions de concurrence, en particulier lorsqu'il porte sur des informations sensibles sous l'angle de la concurrence. Cela vaut en particulier dans les situations où le partage de données permet aux entreprises de prendre connaissance des stratégies de marché de leurs concurrents actuels ou potentiels. Parmi ces informations sensibles sous l'angle de la concurrence, on trouve généralement des informations sur les prix futurs, les coûts de production, les quantités, les chiffres d'affaires, les ventes ou les capacités.
- (30) Une procédure de notification pour les services de partage de données devrait être mise en place afin de garantir que la gouvernance des données au sein de l'Union est fondée sur un échange de données digne de confiance. Le meilleur moyen de tirer avantage d'un environnement digne de confiance serait d'imposer un certain nombre d'exigences pour la prestation de services de partage de données sans pour autant qu'une décision expresse ou un acte administratif ne soient exigés à cette fin de l'autorité compétente.
- (31) Afin de favoriser l'efficacité de la prestation transfrontalière de services, le prestataire de services de partage de données devrait être invité à envoyer une notification uniquement à l'autorité compétente désignée de l'État membre dans lequel est situé son établissement principal ou dans lequel se trouve son représentant légal. Une telle notification ne devrait nécessiter qu'une simple déclaration de l'intention de proposer de tels services, uniquement assortie des informations énumérées dans le présent règlement.
- (32) L'établissement principal d'un prestataire de services de partage de données dans l'Union devrait être l'État membre dans lequel se trouve son administration centrale dans l'Union. L'établissement principal d'un prestataire de services de partage de données dans l'Union devrait être déterminé selon des critères objectifs et associé à l'exercice effectif et réel d'activités de gestion.
- (33) Les autorités compétentes désignées pour contrôler le respect des exigences du présent règlement par les services de partage de données devraient être choisies sur la base de leurs capacités et de leur expertise en matière de partage de données horizontal ou sectoriel, et elles devraient être indépendantes, transparentes et impartiales dans l'exercice de leurs tâches. Les États membres devraient notifier à la Commission l'identité des autorités compétentes désignées.
- (34) Le cadre de notification mis en place par le présent règlement ne devrait pas porter atteinte aux règles spécifiques complémentaires applicables à la prestation de services de partage de données en vertu de la législation sectorielle.
- (35) Nombreuses sont les possibilités offertes par l'utilisation à des fins d'intérêt général de données mises à disposition volontairement par des personnes concernées avec leur consentement ou, lorsqu'il s'agit de données à caractère non personnel, mises à disposition par des personnes morales. Ces finalités sont notamment les soins de santé, la lutte contre le changement climatique, l'amélioration de la mobilité, l'établissement plus aisé de statistiques officielles ou l'amélioration de la prestation de services publics. Le soutien à la recherche scientifique, et notamment au développement technologique et à la démonstration, à la recherche fondamentale, à la recherche

appliquée et à la recherche financée par des fonds privés, devrait également être considéré comme une finalité d'intérêt général. Le présent règlement vise à contribuer à l'émergence de réserves de données mises à disposition selon le principe de l'altruisme en matière de données, qui soient d'une taille suffisante pour permettre l'analyse des données et l'apprentissage automatique, y compris au-delà des frontières de l'Union.

- (36) Les entités juridiques qui cherchent à promouvoir des finalités d'intérêt général en mettant à disposition des données pertinentes selon le principe de l'altruisme en matière de données à grande échelle et qui satisfont à certaines exigences devraient pouvoir s'enregistrer en tant qu'«organisation altruiste en matière de données reconnue dans l'Union». Cela pourrait aboutir à la mise en place de référentiels de données. Étant donné que l'enregistrement dans un État membre serait valable dans toute l'Union, cela devrait faciliter l'utilisation transfrontière des données au sein de l'Union et l'émergence de réserves de données couvrant plusieurs États membres. À cet égard, les personnes concernées devraient consentir à des finalités spécifiques du traitement de données, mais pourraient également donner leur consentement au traitement de données dans certains domaines de recherche ou pour certaines parties de projets de recherche, sachant qu'il est souvent impossible de cerner entièrement la finalité d'un traitement de données à caractère personnel à des fins de recherche scientifique au moment de la collecte des données. Les personnes morales pourraient autoriser le traitement de leurs données à caractère non personnel pour une série de finalités non définies au moment où l'autorisation est accordée. Le respect volontaire d'un ensemble d'exigences par ces entités enregistrées devrait susciter la confiance dans le fait que les données mises à disposition à des fins altruistes servent l'intérêt général. Cette confiance devrait s'appuyer notamment sur l'existence d'un lieu d'établissement dans l'Union, ainsi que sur l'obligation pour les entités enregistrées d'avoir un but non lucratif, sur les exigences de transparence imposées et sur les garanties spécifiques mises en place pour protéger les droits et les intérêts des personnes concernées et des entreprises. D'autres garanties devraient inclure la possibilité de traiter les données pertinentes dans un environnement de traitement sécurisé exploité par l'entité enregistrée, des mécanismes de surveillance tels que l'existence de conseils d'éthique afin de garantir que le responsable du traitement respecte des normes rigoureuses en matière d'éthique scientifique, des moyens techniques efficaces pour retirer ou modifier le consentement à tout moment, sur la base des obligations d'information incombant aux sous-traitants en vertu du règlement (UE) 2016/679, ainsi que des moyens permettant aux personnes concernées de rester informées de l'utilisation des données qu'elles ont mises à disposition.
- (37) Le présent règlement est sans préjudice de l'établissement, de l'organisation et du fonctionnement des entités qui souhaitent s'engager dans l'altruisme en matière de données en vertu du droit national. Il s'inspire des exigences imposées par le droit national pour agir légalement dans un État membre en tant qu'organisation à but non lucratif. Les entités qui satisfont aux exigences du présent règlement devraient pouvoir utiliser la dénomination «organisation altruiste en matière de données reconnue dans l'Union».
- (38) Les organisations altruistes en matière de données reconnues dans l'Union devraient être en mesure de collecter des données pertinentes directement auprès de personnes physiques et morales ou de traiter les données collectées par d'autres. En règle générale, l'altruisme en matière de données devrait reposer sur le consentement des personnes concernées au sens de l'article 6, paragraphe 1, point a), et de l'article 9,

paragraphe 2, point a), du règlement (UE) 2016/679 et conformément aux exigences régissant un consentement licite énoncées à l'article 7 du même règlement. Conformément au règlement (UE) 2016/679, le consentement accordé en ce qui concerne certains domaines de recherche scientifique, dans le respect des normes éthiques reconnues en matière de recherche scientifique, ou uniquement en ce qui concerne certains domaines de recherche ou certaines parties de projets de recherche, peut servir la promotion de finalités de la recherche scientifique. L'article 5, paragraphe 1, point b), du règlement (UE) 2016/679 précise que le traitement ultérieur à des fins de recherche scientifique ou historique ou à des fins statistiques ne devrait pas être considéré, conformément à l'article 89, paragraphe 1, de ce règlement, comme incompatible avec les finalités initiales.

- (39) Afin d'entourer le consentement et son retrait d'un degré supplémentaire de sécurité juridique, en particulier dans le contexte de la recherche scientifique et de l'utilisation statistique des données mises à disposition sur une base altruiste, il convient d'élaborer et d'utiliser un formulaire de consentement européen à l'altruisme en matière de données en cas de partage de données altruiste. Un tel formulaire devrait contribuer à accroître la transparence à l'égard des personnes concernées quant au fait que leurs données seront consultées et utilisées conformément à leur consentement et dans le plein respect des règles en matière de protection des données. Il pourrait également être utilisé pour rationaliser l'altruisme en matière de données pratiqué par les entreprises et fournir un mécanisme permettant à ces entreprises de retirer leur autorisation d'utiliser les données. Afin de tenir compte des spécificités de chaque secteur, y compris sur le plan de la protection des données, il devrait être possible d'apporter des adaptations sectorielles au formulaire de consentement européen à l'altruisme en matière de données.
- (40) Afin de mettre en œuvre avec succès le cadre de gouvernance des données, il convient d'instaurer un comité européen de l'innovation dans le domaine des données, sous la forme d'un groupe d'experts. Le comité devrait être composé de représentants des États membres, de la Commission et de représentants des espaces de données pertinents et de secteurs particuliers (tels que la santé, l'agriculture, les transports et les statistiques). Le comité européen de la protection des données devrait être invité à désigner un représentant auprès du comité européen de l'innovation dans le domaine des données.
- (41) Le comité devrait aider la Commission à coordonner les pratiques et les politiques nationales sur les thèmes couverts par le présent règlement et à promouvoir l'utilisation intersectorielle des données moyennant le respect des principes du cadre d'interopérabilité européen (EIF) et l'application de normes et de spécifications (telles que les vocabulaires de base<sup>44</sup> et les blocs constitutifs du MIE<sup>45</sup>), sans préjudice des travaux de normalisation menés dans des secteurs ou domaines spécifiques. Les travaux de normalisation technique peuvent inclure la définition de priorités pour l'élaboration de normes et la création et l'actualisation d'un ensemble de normes techniques et juridiques régissant la transmission de données entre deux environnements de traitement afin d'organiser des espaces de données sans recourir à un intermédiaire. Le comité devrait coopérer avec des organismes, des réseaux ou des groupes d'experts sectoriels, ou toute autre organisation intersectorielle intervenant dans la réutilisation des données. En ce qui concerne l'altruisme en matière de données, le comité devrait aider la Commission à élaborer le formulaire de

<sup>44</sup> <https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/core-vocabularies>

<sup>45</sup> <https://joinup.ec.europa.eu/collection/connecting-europe-facility-cef>

consentement européen, en consultation avec le comité européen de la protection des données.

- (42) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission pour lui permettre d'élaborer le formulaire de consentement européen à l'altruisme en matière de données. Ces compétences devraient être exercées en conformité avec le règlement (UE) n° 182/2011 du Parlement européen et du Conseil<sup>46</sup>.
- (43) Afin de tenir compte de la nature spécifique de certaines catégories de données, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du TFUE pour définir les conditions particulières applicables aux transferts vers des pays tiers de certaines catégories de données à caractère non personnel considérées comme hautement sensibles dans certains actes de l'Union adoptés par procédure législative. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer». En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.
- (44) Le présent règlement ne devrait pas avoir d'incidence sur l'application des règles relatives à la concurrence, en particulier les articles 101 et 102 du traité sur le fonctionnement de l'Union européenne. Les mesures prévues par le présent règlement ne devraient pas être utilisées pour restreindre la concurrence d'une manière qui soit contraire au traité sur le fonctionnement de l'Union européenne. Cela concerne en particulier les règles relatives à l'échange d'informations sensibles du point de vue de la concurrence entre concurrents réels ou potentiels au moyen de services de partage de données.
- (45) Le Contrôleur européen de la protection des données et le comité européen de la protection des données ont été consultés conformément à l'article 42 du règlement (UE) 2018/1725 du Parlement européen et du Conseil<sup>47</sup> et ont rendu un avis le [...].
- (46) Le présent règlement respecte les droits fondamentaux et observe les principes reconnus en particulier par la charte des droits fondamentaux de l'Union européenne, notamment le respect de la vie privée, la protection des données à caractère personnel, la liberté d'entreprise, le droit de propriété et l'intégration des personnes handicapées,

---

<sup>46</sup> Règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

<sup>47</sup> 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 institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).



ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

## **CHAPITRE I**

### **DISPOSITIONS GÉNÉRALES**

#### *Article premier*

#### *Objet et champ d'application*

- (1) Le présent règlement établit:
  - (a) les conditions de réutilisation, au sein de l'Union, de certaines catégories de données détenues par des organismes du secteur public;
  - (b) un cadre de notification et de surveillance pour la fourniture de services de partage de données;
  - (c) un cadre pour l'enregistrement volontaire des entités qui collectent et traitent les données mises à disposition à des fins altruistes.
- (2) Le présent règlement est sans préjudice des dispositions particulières d'autres actes juridiques de l'Union concernant l'accès à certaines catégories de données ou leur réutilisation, ou des exigences relatives au traitement de données à caractère personnel ou non. Lorsqu'un acte juridique sectoriel de l'Union impose aux organismes du secteur public, aux prestataires de services de partage de données ou aux entités enregistrées fournissant des services d'altruisme en matière de données de respecter des exigences techniques, administratives ou organisationnelles particulières supplémentaires, notamment au moyen d'un régime d'autorisation ou de certification, les dispositions de cet acte juridique sectoriel de l'Union s'appliquent également.

#### *Article 2*

#### *Définitions*

Aux fins du présent règlement, on entend par:

- (1) «données», toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels;
- (2) «réutilisation», l'utilisation, par des personnes physiques ou morales, de données détenues par des organismes du secteur public, à des fins commerciales ou non commerciales autres que l'objectif initial de la mission de service public pour lequel les données ont été produites, à l'exception de l'échange de données entre des organismes du secteur public aux seules fins de l'exercice de leur mission de service public;
- (3) «données à caractère non personnel», les données autres que les données à caractère personnel au sens de l'article 4, point 1), du règlement (UE) 2016/679;
- (4) «métadonnées», les données collectées sur toute activité d'une personne physique ou morale aux fins de la fourniture d'un service de partage de données, notamment la date, l'heure et les données de géolocalisation, la durée de l'activité et les connexions établies avec d'autres personnes physiques ou morales par la personne qui utilise le service;

- (5) «détenteur de données», une personne morale ou une personne concernée qui, conformément au droit de l'Union ou au droit national applicable, a le droit de donner accès à certaines données à caractère personnel ou à caractère non personnel qu'elle contrôle ou de les partager;
- (6) «utilisateur de données», une personne physique ou morale qui dispose d'un accès licite à certaines données à caractère personnel ou non personnel et qui est autorisée à les utiliser à des fins commerciales ou non commerciales;
- (7) «partage de données», la fourniture de données à un utilisateur de données par un détenteur de données, en vue d'une utilisation conjointe ou individuelle des données partagées, sur la base d'accords volontaires, directement ou via un intermédiaire;
- (8) «accès», le traitement, par un utilisateur de données, de données qui ont été fournies par un détenteur de données conformément à des exigences techniques, juridiques ou organisationnelles particulières, sans que cela implique nécessairement la transmission ou le téléchargement de ces données;
- (9) «établissement principal» d'une entité juridique, le lieu de son administration centrale dans l'Union;
- (10) «altruisme en matière de données», le consentement donné par les personnes concernées au traitement de données à caractère personnel les concernant, ou les autorisations accordées par d'autres titulaires de données pour l'utilisation de leurs données à caractère non personnel sans demander de contrepartie, à des fins d'intérêt général, telles que la recherche scientifique ou l'amélioration des services publics;
- (11) «organismes du secteur public», l'État, les autorités régionales ou locales, les organismes de droit public ou les associations formées par une ou plusieurs de ces autorités ou un ou plusieurs de ces organismes de droit public;
- (12) «organismes de droit public», les organismes présentant les caractéristiques suivantes:
- (a) ils ont été créés pour satisfaire spécifiquement des besoins d'intérêt général et n'ont pas de caractère industriel ou commercial;
  - (b) ils sont dotés de la personnalité juridique;
  - (c) leur activité est financée majoritairement par l'État, les collectivités régionales ou locales ou d'autres organismes de droit public, soit leur gestion est soumise à un contrôle de ces autorités ou organismes, soit leur 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;
- (13) «entreprise publique», toute entreprise sur laquelle les organismes du secteur public peuvent exercer directement ou indirectement une influence dominante du fait de la propriété de l'entreprise, de la participation financière qu'ils y détiennent ou des règles qui la régissent; aux fins de la présente définition, une influence dominante des organismes du secteur public sur l'entreprise est présumée dans tous les cas suivants lorsque ces organismes, directement ou indirectement:
- (a) détiennent la majorité du capital souscrit de l'entreprise;
  - (b) disposent de la majorité des voix attachées aux parts émises par l'entreprise;

- (c) peuvent désigner plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance de l'entreprise;
- (14) «environnement de traitement sécurisé», l'environnement physique ou virtuel et les moyens organisationnels donnant la possibilité de réutiliser les données d'une manière qui permette à l'opérateur de l'environnement de traitement sécurisé de déterminer et de surveiller toutes les opérations de traitement de données, notamment d'afficher, de stocker, de télécharger, d'exporter les données et de calculer les données dérivées au moyen d'algorithmes de calcul;
- (15) «représentant», toute personne physique ou morale établie dans l'Union, expressément désignée pour agir au nom d'un prestataire de services de partage de données ou d'une entité collectant à des fins d'intérêt général des données mises à disposition par des personnes physiques ou morales selon le principe d'altruisme en matière de données, non établis dans l'Union, qui peut être contactée par une autorité compétente nationale à la place du prestataire de services de partage de données ou de l'entité en ce qui concerne les obligations incombant à ce prestataire ou à cette entité en application du présent règlement.

## **CHAPITRE II**

### **REUTILISATION DE CERTAINES CATEGORIES DE DONNEES PROTEGEES DETENUES PAR DES ORGANISMES DU SECTEUR PUBLIC**

#### *Article 3 Catégories de données*

- (1) Le présent chapitre s'applique aux données détenues par des organismes du secteur public, qui sont protégées pour des motifs:
  - (a) de confidentialité des informations commerciales;
  - (b) de confidentialité des données statistiques;
  - (c) de protection des droits de propriété intellectuelle de tiers;
  - (d) de protection des données à caractère personnel.
- (2) Le présent chapitre ne s'applique pas:
  - (a) aux données détenues par des entreprises publiques;
  - (b) aux données détenues par des radiodiffuseurs de service public et leurs filiales et par d'autres organismes ou leurs filiales pour l'accomplissement d'une mission de radiodiffusion de service public;
  - (c) aux données détenues par des établissements culturels et des établissements d'enseignement;
  - (d) aux données protégées pour des raisons de sécurité nationale, de défense ou de sécurité publique;
  - (e) aux données dont la fourniture est une activité qui ne relève pas de la mission de service public dévolue aux organismes du secteur public concernés telle qu'elle est définie par la loi ou d'autres règles contraignantes en vigueur dans l'État membre concerné ou, en l'absence de telles règles, telle qu'elle est définie conformément aux pratiques administratives courantes dans cet État membre,



sous réserve que l'objet des missions de service public soit transparent et soumis à réexamen.

- (3) Les dispositions du présent chapitre ne créent, pour les organismes du secteur public, aucune obligation d'autoriser la réutilisation des données et ne libèrent pas les organismes du secteur public de leurs obligations de confidentialité. Le présent chapitre est sans préjudice du droit de l'Union et du droit national ou des accords internationaux auxquels l'Union ou les États membres sont parties en ce qui concerne la protection des catégories de données énumérées au paragraphe 1. Le présent chapitre est sans préjudice du droit de l'Union et du droit national en matière d'accès aux documents et des obligations incombant aux organismes du secteur public, en application du droit de l'Union et du droit national, en ce qui concerne l'autorisation de la réutilisation des données.

#### *Article 4*

##### *Interdiction des accords d'exclusivité*

- (1) Les accords ou autres pratiques relatifs à la réutilisation de données détenues par des organismes du secteur public contenant des catégories de données énumérées à l'article 3, paragraphe 1, qui octroient des droits exclusifs ou qui ont pour objet ou pour effet d'octroyer de tels droits exclusifs ou de restreindre la disponibilité des données à des fins de réutilisation par des entités autres que les parties à ces accords ou autres pratiques sont interdits.
- (2) Par dérogation au paragraphe 1, un droit exclusif de réutilisation des données visées audit paragraphe peut être accordé dans la mesure nécessaire à la fourniture d'un service ou d'un produit d'intérêt général.
- (3) Ce droit exclusif est accordé dans le cadre d'un contrat de service ou de concession pertinent conformément aux règles applicables en matière d'attribution de marchés publics et de concessions au niveau de l'Union et au niveau national ou, dans le cas d'un contrat d'une valeur pour laquelle ni les règles de l'Union ni les règles nationales en matière d'attribution de marchés publics et de concessions ne sont applicables, dans le respect des principes de transparence, d'égalité de traitement et de non-discrimination en raison de la nationalité.
- (4) Dans tous les cas ne relevant pas du paragraphe 3 et lorsque la finalité d'intérêt général ne peut être atteinte sans l'octroi d'un droit exclusif, les principes de transparence, d'égalité de traitement et de non-discrimination en raison de la nationalité s'appliquent.
- (5) La durée d'exclusivité du droit de réutilisation des données ne dépasse pas trois ans. Si un contrat est conclu, la durée du contrat est la même que la durée d'exclusivité.
- (6) L'octroi d'un droit exclusif en vertu des paragraphes 2 à 5, notamment les raisons pour lesquelles il est nécessaire d'accorder un tel droit, est transparent et fait l'objet d'une publication en ligne, indépendamment d'une éventuelle publication relative à l'attribution d'un marché public ou d'un contrat de concession.
- (7) Les accords ou autres pratiques tombant sous le coup de l'interdiction visée au paragraphe 1, qui ne remplissent pas les conditions énoncées au paragraphe 2, et qui ont fait l'objet d'un contrat conclu avant la date d'entrée en vigueur du présent règlement expirent à la fin du contrat et, en tout état de cause, au plus tard dans un délai de trois ans après la date d'entrée en vigueur du présent règlement.

*Article 5*  
*Conditions applicables à la réutilisation*

- (1) Les organismes du secteur public qui sont compétents en vertu du droit national pour accorder ou refuser l'accès en vue de la réutilisation d'une ou de plusieurs des catégories de données énumérées à l'article 3, paragraphe 1, rendent publiques les conditions d'autorisation de cette réutilisation. Ils peuvent être assistés dans cette tâche par les organismes compétents visés à l'article 7, paragraphe 1.
- (2) Les conditions applicables à la réutilisation sont non discriminatoires, proportionnées et objectivement justifiées en ce qui concerne les catégories de données et les finalités de réutilisation, ainsi que la nature des données pour lesquelles la réutilisation est autorisée. Ces conditions ne sont pas utilisées pour restreindre la concurrence.
- (3) Les organismes du secteur public peuvent exiger que seules soient réutilisées les données ayant fait l'objet d'un prétraitement visant à anonymiser ou à pseudonymiser des données à caractère personnel ou à supprimer des informations commerciales confidentielles, y compris des secrets d'affaires.
- (4) Les organismes du secteur public peuvent imposer des obligations
  - (a) relatives à l'accès aux données et à leur réutilisation dans un environnement de traitement sécurisé fourni et contrôlé par le secteur public;
  - (b) relatives à l'accès aux données et à leur réutilisation dans les locaux où se trouve l'environnement de traitement sécurisé, si l'accès à distance ne peut être autorisé sans qu'il soit porté atteinte aux droits et aux intérêts des tiers.
- (5) Les organismes du secteur public imposent des conditions qui préservent l'intégrité du fonctionnement des systèmes techniques de l'environnement de traitement sécurisé utilisé. Les organismes du secteur public sont en mesure de vérifier tout résultat du traitement de données effectué par le réutilisateur et se réservent le droit d'interdire l'utilisation des résultats qui contiennent des informations portant atteinte aux droits et aux intérêts de tiers.
- (6) Lorsqu'il est impossible d'autoriser la réutilisation des données en respectant les obligations énoncées aux paragraphes 3 à 5 et qu'il n'existe pas d'autre base juridique pour la transmission des données en vertu du règlement (UE) 2016/679, les organismes du secteur public aident les réutilisateurs à demander le consentement des personnes concernées et/ou l'autorisation des entités juridiques dont les droits et intérêts peuvent être affectés par cette réutilisation, lorsque cela est faisable sans coûts disproportionnés pour le secteur public. Ils peuvent être assistés dans cette tâche par les organismes compétents visés à l'article 7, paragraphe 1.
- (7) La réutilisation des données n'est autorisée que dans le respect des droits de propriété intellectuelle. Les organismes du secteur public n'exercent pas le droit prévu à l'article 7, paragraphe 1, de la directive 96/9/CE pour le fabricant d'une base de données aux fins d'empêcher la réutilisation de données ou de limiter celle-ci au-delà des limites fixées par le présent règlement.
- (8) Lorsque les données demandées sont considérées comme confidentielles, conformément au droit de l'Union ou au droit national en matière de confidentialité commerciale, les organismes du secteur public veillent à ce que les informations confidentielles ne soient pas divulguées du fait de leur réutilisation.

- (9) La Commission peut adopter des actes d'exécution établissant que le cadre juridique et le dispositif de surveillance et de mise en œuvre d'un pays tiers:
- (a) assurent la protection de la propriété intellectuelle et des secrets d'affaires d'une manière qui est essentiellement équivalente à la protection assurée par le droit de l'Union;
  - (b) sont effectivement appliqués et leur application est contrôlée; et
  - (c) prévoient un recours juridictionnel effectif.

Ces actes d'exécution sont adoptés en conformité avec la procédure consultative visée à l'article 29, paragraphe 2.

- (10) Les organismes du secteur public ne transmettent des données confidentielles ou des données protégées par des droits de propriété intellectuelle à un réutilisateur qui a l'intention de les transférer vers un pays tiers autre qu'un pays désigné conformément au paragraphe 9 que si le réutilisateur s'engage:
- (a) à respecter les obligations imposées en application des paragraphes 7 et 8, même après le transfert des données vers le pays tiers; et
  - (b) à admettre la compétence des juridictions de l'État membre de l'organisme du secteur public en ce qui concerne tout litige relatif au respect de l'obligation énoncée au point a).
- (11) Lorsque des actes spécifiques de l'Union adoptés conformément à une procédure législative établissent que certaines catégories de données à caractère non personnel détenues par des organismes du secteur public sont considérées comme hautement sensibles aux fins du présent article, la Commission est habilitée à adopter des actes délégués conformément à l'article 28 afin de compléter le présent règlement en fixant des conditions particulières applicables aux transferts vers des pays tiers. Les conditions de transfert vers des pays tiers sont fondées sur la nature des catégories de données identifiées dans l'acte de l'Union et sur les motifs de les considérer comme hautement sensibles, sont non discriminatoires et limitées à ce qui est nécessaire pour atteindre les objectifs de politique publique définis dans l'acte législatif de l'Union, tels que la sécurité et la santé publique, et sont définies en fonction des risques de réidentification de données anonymisées pour les personnes concernées, dans le respect des obligations internationales de l'Union. Il peut s'agir notamment de conditions applicables au transfert ou d'arrangements techniques à cet égard, de limitations en ce qui concerne la réutilisation de données dans des pays tiers ou les catégories de personnes habilitées à transférer ces données vers des pays tiers ou, dans des cas exceptionnels, de restrictions en ce qui concerne les transferts vers des pays tiers.
- (12) La personne physique ou morale à laquelle le droit de réutiliser des données à caractère non personnel a été accordé ne peut transférer ces données que vers les pays tiers pour lesquels il est satisfait aux exigences énoncées aux paragraphes 9 à 11.
- (13) Lorsque le réutilisateur a l'intention de transférer des données à caractère non personnel vers un pays tiers, l'organisme du secteur public informe le détenteur des données du transfert de ces dernières vers ce pays tiers.

*Article 6*  
*Redevances*

- (1) Les organismes du secteur public qui autorisent la réutilisation des catégories de données énumérées à l'article 3, paragraphe 1, peuvent percevoir des redevances pour autoriser la réutilisation de ces données.
- (2) Les redevances sont non discriminatoires, proportionnées et objectivement justifiées et ne restreignent pas la concurrence.
- (3) Les organismes du secteur public font en sorte que ces redevances puissent être acquittées en ligne au moyen de services de paiement transfrontières largement disponibles, sans discrimination fondée sur le lieu d'établissement du prestataire de services de paiement, le lieu d'émission de l'instrument de paiement ou la localisation du compte de paiement dans l'Union.
- (4) Lorsqu'ils appliquent des redevances, les organismes du secteur public prennent des mesures pour encourager la réutilisation des catégories de données énumérées à l'article 3, paragraphe 1, à des fins non commerciales et par les petites et moyennes entreprises conformément aux règles en matière d'aides d'État.
- (5) Les redevances sont calculées sur la base des coûts liés au traitement des demandes de réutilisation des catégories de données énumérées à l'article 3, paragraphe 1. La méthode de calcul des redevances est publiée à l'avance.
- (6) Les organismes du secteur public publient une description des principales catégories de coûts et des règles utilisées pour la répartition des coûts.

*Article 7*  
*Organismes compétents*

- (1) Les États membres désignent un ou plusieurs organismes compétents, éventuellement à caractère sectoriel, pour appuyer les organismes du secteur public qui accordent l'accès pour la réutilisation des catégories de données énumérées à l'article 3, paragraphe 1, dans l'exercice de cette tâche.
- (2) L'appui prévu au paragraphe 1 consiste, le cas échéant:
  - (a) à fournir une assistance technique en mettant à disposition un environnement de traitement sécurisé pour donner accès à la réutilisation de données;
  - (b) à fournir un soutien technique dans l'application de techniques éprouvées garantissant le traitement des données d'une manière qui préserve la confidentialité des informations contenues dans les données dont la réutilisation est autorisée, notamment les techniques de pseudonymisation, d'anonymisation, de généralisation, de suppression et de randomisation des données à caractère personnel;
  - (c) à aider les organismes du secteur public, en tant que de besoin, à obtenir le consentement ou l'autorisation des réutilisateurs en vue d'une réutilisation à des fins altruistes et à d'autres fins conformément aux décisions spécifiques des détenteurs de données, y compris en ce qui concerne le ou les territoires où le traitement des données est prévu;
  - (d) à fournir aux organismes du secteur public une assistance sur l'adéquation des engagements pris par un réutilisateur, conformément à l'article 5, paragraphe 10.

- (3) Les organismes compétents peuvent également être chargés, en application des dispositions du droit de l'Union ou du droit national permettant d'accorder l'accès, d'octroyer cet accès aux catégories de données énumérées à l'article 3, paragraphe 1, en vue d'une réutilisation. Les articles 4, 5 et 6 et l'article 8, paragraphe 3, s'appliquent à ces organismes compétents lorsque ces derniers octroient ou refusent l'accès en vue d'une réutilisation.
- (4) Le ou les organismes compétents doivent disposer des capacités et de l'expertise juridiques et techniques suffisantes pour être en mesure de se conformer au droit de l'Union ou au droit national applicable en ce qui concerne les régimes d'accès pour les catégories de données énumérées à l'article 3, paragraphe 1.
- (5) Les États membres communiquent à la Commission l'identité des organismes compétents désignés en application du paragraphe 1 au plus tard le [date d'application du présent règlement]. Ils communiquent également à la Commission toute modification ultérieure concernant l'identité de ces organismes.

#### *Article 8*

##### *Point d'information unique*

- (1) Les États membres veillent à ce que toutes les informations pertinentes concernant l'application des articles 5 et 6 soient disponibles par l'intermédiaire d'un point d'information unique.
- (2) Le point d'information unique reçoit les demandes de réutilisation des catégories de données visées à l'article 3, paragraphe 1, et les transmet aux organismes du secteur public compétents ou aux organismes compétents visés à l'article 7, paragraphe 1, le cas échéant. Le point d'information unique met à disposition par voie électronique un registre des ressources de données disponibles qui contient des informations pertinentes décrivant la nature des données disponibles.
- (3) Les demandes de réutilisation des catégories de données visées à l'article 3, paragraphe 1, sont acceptées ou refusées par les organismes du secteur public compétents ou les organismes compétents visés à l'article 7, paragraphe 1, dans un délai raisonnable et, en tout état de cause, dans un délai de deux mois à compter de la date de la demande.
- (4) Toute personne physique ou morale affectée par une décision d'un organisme du secteur public ou d'un organisme compétent, selon le cas, dispose d'un droit de recours juridictionnel effectif contre cette décision devant les juridictions de l'État membre dans lequel se trouve ledit organisme.

### **CHAPITRE III**

#### **EXIGENCES APPLICABLES AUX SERVICES DE PARTAGE DE DONNEES**

#### *Article 9*

##### *Prestataires de services de partage de données*

- (1) La fourniture des services de partage de données suivants est soumise à une procédure de notification:
  - (a) les services d'intermédiation entre les détenteurs de données qui sont des personnes morales et les utilisateurs de données potentiels, y compris la mise à disposition des moyens techniques ou autres requis pour permettre la fourniture

desdits services; ces derniers peuvent comprendre des échanges bilatéraux ou multilatéraux de données ou la création de plateformes ou de bases de données permettant l'échange ou l'exploitation conjointe de données, ainsi que la mise en place d'une infrastructure spécifique pour l'interconnexion des détenteurs de données et des utilisateurs de données;

- (b) les services d'intermédiation entre, d'une part, les personnes concernées qui cherchent à mettre à disposition leurs données à caractère personnel et, d'autre part, les utilisateurs de données potentiels, y compris la mise à disposition des moyens techniques ou autres requis pour permettre la fourniture desdits services, en vue de l'exercice des droits prévus par le règlement (UE) 2016/679;
  - (c) les services de coopérative de données, c'est-à-dire les services qui, d'une part, aident les personnes concernées et les entreprises unipersonnelles, microentreprises, petites et moyennes entreprises qui sont membres de la coopérative ou qui confèrent à celle-ci, avant de donner leur consentement, le pouvoir de négocier, les conditions et modalités du traitement des données, à poser des choix en connaissance de cause avant de donner leur consentement au traitement des données, et, d'autre part, prévoient des mécanismes d'échange de vues sur les finalités et les conditions du traitement des données qui représenteraient le mieux les intérêts des personnes concernées ou des personnes morales.
- (2) Le présent chapitre est sans préjudice de l'application d'autres dispositions du droit de l'Union et du droit national aux prestataires de services de partage de données, y compris des pouvoirs conférés aux autorités de contrôle d'assurer le respect du droit applicable, notamment en ce qui concerne la protection des données à caractère personnel et le droit de la concurrence.

#### *Article 10*

##### *Notification des prestataires de services de partage de données*

- (1) Tout prestataire de services de partage de données qui a l'intention de fournir les services visés à l'article 9, paragraphe 1, soumet une notification à l'autorité compétente visée à l'article 12.
- (2) Aux fins du présent règlement, un prestataire de services de partage de données établi dans plusieurs États membres est considéré comme relevant de la compétence de l'État membre dans lequel il a son établissement principal.
- (3) Un prestataire de services de partage de données qui n'est pas établi dans l'Union mais propose les services visés à l'article 9, paragraphe 1, dans l'Union désigne un représentant légal dans l'un des États membres où il propose lesdits services. Le prestataire est considéré comme relevant de la compétence de l'État membre dans lequel son représentant légal est établi.
- (4) Après notification, le prestataire de services de partage de données peut commencer l'activité sous réserve des conditions énoncées au présent chapitre.
- (5) La notification donne au prestataire le droit de fournir des services de partage de données dans tous les États membres.
- (6) La notification comporte les renseignements suivants:
  - (a) le nom du prestataire de services de partage de données;



- (b) le statut et la forme juridiques ainsi que le numéro d'enregistrement du prestataire, le lieu où il est enregistré dans un registre de commerce ou dans un autre registre public similaire;
  - (c) l'adresse de l'éventuel établissement principal du prestataire dans l'Union et, le cas échéant, de toute succursale dans un autre État membre, ou bien l'adresse du représentant légal désigné en application du paragraphe 3;
  - (d) un site web contenant des informations sur le prestataire et ses activités, le cas échéant;
  - (e) les personnes de contact et les coordonnées du prestataire;
  - (f) une description du service que le prestataire a l'intention de fournir;
  - (g) une estimation de la date de lancement de l'activité;
  - (h) les États membres dans lesquels le prestataire a l'intention de fournir des services.
- (7) À la demande du prestataire, l'autorité compétente délivre, dans un délai d'une semaine, une déclaration standardisée confirmant que le prestataire a soumis la notification visée au paragraphe 4.
- (8) L'autorité compétente transmet immédiatement chaque notification aux autorités nationales compétentes des États membres, par voie électronique.
- (9) L'autorité compétente informe la Commission de toute nouvelle notification. La Commission tient un registre des prestataires de services de partage de données.
- (10) L'autorité compétente peut percevoir des redevances. Ces redevances sont proportionnées et objectives et sont fondées sur les coûts administratifs liés au contrôle du respect des dispositions et aux autres activités de contrôle du marché menées par les autorités compétentes en rapport avec les notifications de services de partage de données.
- (11) Lorsqu'un prestataire de services de partage de données cesse ses activités, il le notifie dans un délai de 15 jours à l'autorité compétente concernée, déterminée conformément aux paragraphes 1, 2 et 3. L'autorité compétente transmet immédiatement cette notification aux autorités nationales compétentes des États membres et à la Commission, par voie électronique.

#### *Article 11*

##### *Conditions de fourniture des services de partage de données*

La fourniture des services de partage de données visés à l'article 9, paragraphe 1, est soumise aux conditions suivantes:

- (1) le prestataire ne peut utiliser les données pour lesquelles il fournit des services à d'autres fins que leur mise à disposition des utilisateurs de données, et les services de partage de données sont logés dans une entité juridique distincte;
- (2) les métadonnées collectées dans le cadre de la fourniture d'un service de partage de données ne peuvent être utilisées que pour le développement dudit service;
- (3) le prestataire veille à ce que la procédure d'accès à son service soit équitable, transparente et non discriminatoire à l'égard tant des détenteurs de données que des utilisateurs de données, y compris en ce qui concerne les prix;

- (4) le prestataire facilite l'échange des données au format dans lequel il les reçoit du détenteur des données et convertit les données dans des formats spécifiques uniquement pour améliorer l'interopérabilité intrasectorielle et transsectorielle, ou si l'utilisateur de données le demande, ou lorsque le droit de l'Union l'exige, ou pour assurer l'harmonisation avec des normes internationales ou européennes en matière de données;
- (5) le prestataire met en place des procédures pour prévenir les pratiques frauduleuses ou abusives en matière d'accès aux données auxquelles se livreraient certaines parties en cherchant à obtenir un accès via le service du prestataire;
- (6) le prestataire assure une continuité raisonnable de la fourniture de ses services et, dans le cas de services de stockage des données, met en place des garanties suffisantes pour permettre aux détenteurs de données et aux utilisateurs de données d'avoir accès à leurs données en cas d'insolvabilité;
- (7) le prestataire met en place des mesures techniques, juridiques et organisationnelles appropriées afin d'empêcher le transfert de données à caractère non personnel ou l'accès à celles-ci dans les cas où ils sont illicites au regard du droit de l'Union;
- (8) le prestataire prend des mesures garantissant un niveau de sécurité élevé pour le stockage et la transmission de données à caractère non personnel;
- (9) le prestataire met en place des procédures pour garantir le respect des règles nationales et de l'Union en matière de concurrence;
- (10) le prestataire proposant des services à des personnes concernées agit au mieux de leurs intérêts lorsqu'il facilite l'exercice de leurs droits, notamment en conseillant les personnes concernées sur les utilisations potentielles des données et sur les conditions générales applicables à ces utilisations;
- (11) lorsqu'un prestataire fournit des outils permettant d'obtenir le consentement de personnes concernées ou l'autorisation de traiter des données mises à disposition par des personnes morales, il précise le ou les territoires où l'utilisation des données est prévue.

## *Article 12*

### *Autorités compétentes*

- (1) Chaque État membre désigne sur son territoire une ou plusieurs autorités compétentes pour exécuter les tâches liées au cadre de notification et communique à la Commission l'identité de ces autorités au plus tard le [date d'application du présent règlement]. Il communique également à la Commission toute modification ultérieure.
- (2) Les autorités compétentes désignées se conforment à l'article 23.
- (3) Les autorités compétentes désignées, les autorités chargées de la protection des données, les autorités nationales de la concurrence, les autorités chargées de la cybersécurité et les autres autorités sectorielles concernées échangent les informations qui sont nécessaires à l'accomplissement de leurs tâches en rapport avec les prestataires de services de partage de données.



*Article 13*  
*Contrôle du respect des dispositions*

- (1) L'autorité compétente contrôle et assure le respect des dispositions du présent chapitre.
- (2) L'autorité compétente a le pouvoir d'exiger des prestataires de services de partage de données toutes les informations nécessaires pour vérifier le respect des exigences énoncées aux articles 10 et 11. Toute demande d'information est proportionnée à l'accomplissement de la tâche et est motivée.
- (3) Lorsque l'autorité compétente constate qu'un prestataire de services de partage de données ne respecte pas une ou plusieurs des exigences énoncées à l'article 10 ou à l'article 11, elle notifie ces constatations audit prestataire et lui donne la possibilité d'exposer son point de vue dans un délai raisonnable.
- (4) L'autorité compétente a le pouvoir d'exiger qu'il soit mis fin au manquement visé au paragraphe 3, soit immédiatement soit dans un délai raisonnable, et prend des mesures appropriées et proportionnées pour garantir la mise en conformité. À cet égard, les autorités compétentes peuvent, le cas échéant:
  - (a) imposer des sanctions financières dissuasives, pouvant comporter des astreintes avec effet rétroactif;
  - (b) exiger la cessation ou le report de la fourniture du service de partage de données.
- (5) Les autorités compétentes communiquent immédiatement à l'entité concernée les mesures imposées en vertu du paragraphe 4 et leur motivation et fixent à l'entité concernée un délai raisonnable pour se conformer auxdites mesures.
- (6) Si un prestataire de services de partage de données a son établissement principal ou un représentant légal dans un État membre mais fournit des services dans d'autres États membres, l'autorité compétente de l'État membre où est situé l'établissement principal ou dans lequel se trouve le représentant légal et les autorités compétentes de ces autres États membres coopèrent et se prêtent assistance. Cette assistance et cette coopération peuvent porter sur les échanges d'informations entre les autorités compétentes concernées et sur les invitations à adopter les mesures prévues dans le présent article.

*Article 14*  
*Dérogations*

Le présent chapitre ne s'applique pas aux entités sans but lucratif dont les activités consistent uniquement à collecter, pour des finalités d'intérêt général, des données mises à disposition par des personnes physiques ou morales selon le principe de l'altruisme en matière de données.

## CHAPITRE IV

### ALTRUISME EN MATIERE DE DONNEES

#### *Article 15*

##### *Registre d'organisations altruistes en matière de données reconnues*

- (1) Chaque autorité compétente désignée en application de l'article 20 tient un registre des organisations altruistes en matière de données reconnues.
- (2) La Commission gère un registre de l'Union recensant les organisations altruistes en matière de données reconnues.
- (3) Une entité inscrite dans le registre conformément à l'article 16 peut se présenter en tant qu'«organisation altruiste en matière de données reconnue dans l'Union» dans ses communications écrites et orales.

#### *Article 16*

##### *Conditions générales d'enregistrement*

Pour être admise à l'enregistrement en tant qu'organisation altruiste en matière de données, une entité doit:

- (a) être une entité juridique constituée pour poursuivre des finalités d'intérêt général;
- (b) opérer dans un but non lucratif et être indépendante de toute entité poursuivant un but lucratif;
- (c) mener les activités liées à l'altruisme en matière de données par l'intermédiaire d'une structure juridiquement indépendante, distincte des autres activités qu'elle exerce.

#### *Article 17*

##### *Enregistrement*

- (1) Toute entité qui satisfait aux exigences de l'article 16 peut demander à être inscrite au registre des organisations altruistes en matière de données reconnues tenu par l'autorité compétente, visé à l'article 15, paragraphe 1.
- (2) Aux fins du présent règlement, une entité qui mène des activités fondées sur l'altruisme en matière de données et est établie dans plusieurs États membres procède à son enregistrement dans l'État membre dans lequel elle a son établissement principal.
- (3) Une entité qui n'est pas établie dans l'Union mais qui satisfait aux exigences énoncées à l'article 16 désigne un représentant légal dans l'un des États membres où elle a l'intention de collecter des données selon le principe de l'altruisme en matière de données. Aux fins du respect du présent règlement, cette entité est considérée comme relevant de la compétence de l'État membre dans lequel se trouve son représentant légal.
- (4) La demande d'enregistrement comporte les renseignements suivants:
  - (a) le nom de l'entité;
  - (b) le statut et la forme juridiques de l'entité, son numéro d'enregistrement, le lieu où elle est enregistrée dans un registre public;
  - (c) les statuts de l'entité, le cas échéant;

- (d) les principales sources de revenus de l'entité;
  - (e) l'adresse de l'éventuel établissement principal de l'entité dans l'Union et, le cas échéant, de toute succursale dans un autre État membre, ou bien l'adresse du représentant légal désigné en application du paragraphe 3;
  - (f) un site web contenant des informations sur l'entité et ses activités;
  - (g) les personnes de contact et les coordonnées de l'entité;
  - (h) les finalités d'intérêt général qu'elle entend promouvoir par la collecte de données;
  - (i) tout autre document démontrant qu'il est satisfait aux exigences de l'article 16.
- (5) Lorsque l'entité a fourni tous les renseignements nécessaires conformément au paragraphe 4 et que l'autorité compétente estime que l'entité satisfait aux exigences de l'article 16, elle l'inscrit au registre des organisations altruistes en matière de données reconnues dans un délai de douze semaines à compter de la date de la demande. L'enregistrement vaut pour tous les États membres. Tout enregistrement est communiqué à la Commission en vue de son inclusion dans le registre de l'Union recensant les organisations altruistes en matière de données reconnues.
- (6) Les renseignements prévus au paragraphe 4, points a), b), f), g) et h) sont publiés dans le registre des organisations altruistes en matière de données reconnues.
- (7) Toute entité inscrite au registre des organisations altruistes en matière de données reconnues soumet à l'autorité compétente toute modification des renseignements communiqués conformément au paragraphe 4 dans un délai de 14 jours calendaires à compter de la date de la modification.

### *Article 18*

#### *Exigences de transparence*

- (1) Toute entité inscrite au registre national des organisations altruistes en matière de données reconnues conserve des archives complètes et exactes concernant:
- (a) toutes les personnes physiques ou morales qui se sont vu offrir la possibilité de traiter des données détenues par cette entité;
  - (b) la date ou la durée de ce traitement;
  - (c) la finalité de ce traitement, telle qu'elle a été déclarée par la personne physique ou morale qui s'est vu offrir la possibilité d'effectuer ce traitement;
  - (d) les éventuelles redevances acquittées par les personnes physiques ou morales traitant les données.
- (2) Toute entité inscrite au registre des organisations altruistes en matière de données reconnues établit et transmet à l'autorité nationale compétente un rapport annuel d'activité qui contient au moins les éléments suivants:
- (a) des informations sur les activités de l'entité;
  - (b) une description de la manière dont les finalités d'intérêt général pour lesquelles des données ont été collectées ont été mises en avant pendant l'exercice considéré;
  - (c) une liste de toutes les personnes physiques et morales qui ont été autorisées à utiliser des données qu'elle détient, assortie d'une description sommaire des

finalités d'intérêt général poursuivies par cette utilisation de données et de la description des moyens techniques employés en vue de cette utilisation, y compris une description des techniques appliquées pour préserver la vie privée et la protection des données;

- (d) une synthèse des résultats des utilisations de données autorisées par l'entité, s'il y a lieu;
- (e) des informations sur les sources de recettes de l'entité, en particulier toutes les recettes générées par le fait d'avoir autorisé l'accès aux données, et sur les dépenses.

#### *Article 19*

##### *Exigences spécifiques visant à préserver les droits et intérêts des personnes concernées et des entités juridiques quant à leurs données*

- (1) Toute entité inscrite au registre des organisations altruistes en matière de données reconnues informe les détenteurs de données:
  - (a) d'une manière aisément intelligible, des finalités d'intérêt général pour lesquelles elle permet le traitement de données les concernant par un utilisateur de données;
  - (b) de tout traitement effectué en dehors de l'Union.
- (2) L'entité veille également à ce que les données ne soient pas utilisées à des fins autres que celles d'intérêt général pour lesquelles elle permet le traitement.
- (3) Lorsqu'une entité inscrite au registre des organisations altruistes en matière de données reconnues fournit des outils permettant d'obtenir le consentement de personnes concernées ou l'autorisation de traiter des données mises à disposition par des personnes morales, elle précise le ou les territoires où l'utilisation des données est prévue.

#### *Article 20*

##### *Autorités compétentes pour procéder à l'enregistrement*

- (1) Chaque État membre désigne une ou plusieurs autorités compétentes chargées de tenir le registre des organisations altruistes en matière de données reconnues et de contrôler le respect des exigences du présent chapitre. Les autorités compétentes désignées satisfont aux exigences de l'article 23.
- (2) Chaque État membre informe la Commission de l'identité des autorités désignées.
- (3) L'autorité compétente exécute ses tâches en coopération avec l'autorité chargée de la protection des données, lorsque ces tâches se rapportent au traitement de données à caractère personnel, et avec les organismes sectoriels concernés du même État membre. Pour toute question nécessitant une évaluation du respect du règlement (UE) 2016/679, l'autorité compétente sollicite au préalable un avis ou une décision de l'autorité de contrôle compétente instituée en application dudit règlement et se conforme à cet avis ou à cette décision.

*Article 21*  
*Contrôle du respect des dispositions*

- (1) L'autorité compétente contrôle et assure le respect, par les entités inscrites au registre des organisations altruistes en matière de données reconnues, des conditions énoncées dans le présent chapitre.
- (2) L'autorité compétente a le pouvoir d'exiger des entités inscrites au registre des organisations altruistes en matière de données reconnues les informations qui lui sont nécessaires pour vérifier qu'elles respectent les dispositions du présent chapitre. Toute demande d'information est proportionnée à l'accomplissement de la tâche et est motivée.
- (3) Lorsque l'autorité compétente constate qu'une entité ne respecte pas une ou plusieurs des exigences du présent chapitre, elle notifie ces constatations à ladite entité et lui donne la possibilité d'exposer son point de vue dans un délai raisonnable.
- (4) L'autorité compétente a le pouvoir d'exiger qu'il soit mis fin au manquement visé au paragraphe 3, soit immédiatement soit dans un délai raisonnable, et prend des mesures appropriées et proportionnées pour garantir la mise en conformité.
- (5) Si une entité ne respecte pas une ou plusieurs des exigences du présent chapitre même après en avoir été avisée conformément au paragraphe 3 par l'autorité compétente, l'entité:
  - (a) perd le droit de se présenter en tant qu'«organisation altruiste en matière de données reconnue dans l'Union» dans toute communication écrite et orale;
  - (b) est radiée du registre des organisations altruistes en matière de données reconnues.
- (6) Si une entité inscrite au registre des organisations altruistes en matière de données reconnues a son établissement principal ou son représentant légal dans un État membre mais qu'elle exerce des activités dans d'autres États membres, l'autorité compétente de l'État membre où est situé l'établissement principal ou dans lequel se trouve le représentant légal et les autorités compétentes de ces autres États membres coopèrent et, au besoin, se prêtent assistance. Cette assistance et cette coopération peuvent porter sur les échanges d'informations entre les autorités compétentes concernées et sur les demandes de prise des mesures, prévues par le présent article, visant à assurer le respect des exigences.

*Article 22*  
*Formulaire de consentement européen à l'altruisme en matière de données*

- (1) Afin de faciliter la collecte de données selon le principe de l'altruisme en matière de données, la Commission peut adopter des actes d'exécution établissant un formulaire de consentement européen à l'altruisme en matière de données, qui doit permettre de recueillir le consentement dans tous les États membres selon un format uniforme. Ces actes d'exécution sont adoptés en conformité avec la procédure consultative visée à l'article 29, paragraphe 2.
- (2) Le formulaire de consentement européen à l'altruisme en matière de données est conçu selon une approche modulaire permettant son adaptation à des secteurs particuliers et à des fins différentes.

- (3) Lorsque des données à caractère personnel sont communiquées, le formulaire de consentement européen à l'altruisme en matière de données garantit que les personnes concernées sont en mesure de donner et de retirer leur consentement à une opération particulière de traitement de données en conformité avec les exigences du règlement (UE) 2016/679.
- (4) Le formulaire est disponible de manière à pouvoir être imprimé sur papier et lu par l'homme ainsi que sous une forme électronique lisible par machine.

## **CHAPITRE V**

### **AUTORITES COMPETENTES ET DISPOSITIONS PROCEDURALES**

#### *Article 23*

##### *Exigences relatives aux autorités compétentes*

- (1) Les autorités compétentes désignées en application des articles 12 et 20 sont juridiquement distinctes et fonctionnellement indépendantes de tout prestataire de services de partage de données ou de toute entité inscrite au registre des organisations altruistes en matière de données reconnues.
- (2) Les autorités compétentes s'acquittent de leurs tâches de manière impartiale, transparente, cohérente, fiable et rapide.
- (3) Les cadres supérieurs et le personnel chargé d'exécuter les tâches de l'autorité compétente prévues par le présent règlement ne peuvent être le concepteur, le fabricant, le fournisseur, l'installateur, l'acheteur, le propriétaire, l'utilisateur ou le responsable de la maintenance des services qu'ils évaluent, ni le mandataire d'aucune de ces parties; ils ne peuvent pas non plus les représenter. Cela n'exclut pas l'utilisation de services évalués qui sont nécessaires au fonctionnement de l'autorité compétente, ou l'utilisation de ces services à des fins personnelles.
- (4) Les cadres supérieurs et le personnel ne participent à aucune activité susceptible d'entrer en conflit avec l'indépendance de leur jugement ou leur intégrité dans le cadre des activités d'évaluation qui leur sont confiées.
- (5) Les autorités compétentes disposent des ressources humaines et financières suffisantes, y compris des connaissances et ressources techniques nécessaires, pour mener à bien les tâches qui leur sont assignées.
- (6) Sur demande motivée, les autorités compétentes d'un État membre fournissent à la Commission et aux autorités compétentes des autres États membres les informations nécessaires à l'accomplissement des tâches qui leur incombent en application du présent règlement. Lorsqu'une autorité compétente nationale considère que les informations exigées sont confidentielles selon les règles de l'Union et les règles nationales relatives à la confidentialité commerciale et professionnelle, la Commission et toutes les autres autorités compétentes concernées garantissent cette confidentialité.

#### *Article 24*

##### *Droit d'introduire une réclamation*

- (1) Les personnes physiques et morales ont le droit d'introduire une réclamation auprès de l'autorité compétente nationale concernée contre un prestataire de services de



partage de données ou contre une entité inscrite au registre des organisations altruistes en matière de données reconnues.

- (2) L'autorité auprès de laquelle la réclamation a été introduite informe l'auteur de la réclamation de l'état d'avancement de la procédure et de la décision prise, et l'informe de son droit à un recours juridictionnel effectif prévu par l'article 25.

#### *Article 25*

##### *Droit à un recours juridictionnel effectif*

- (1) Nonobstant tout recours administratif ou tout autre recours non juridictionnel, toute personne physique ou morale lésée dispose du droit à un recours juridictionnel effectif en ce qui concerne:
- (a) une absence de réaction à une réclamation introduite auprès de l'autorité compétente dont il est question aux articles 12 et 20;
  - (b) les décisions des autorités compétentes, mentionnées aux articles 13, 17 et 21, prises dans le domaine de la gestion, du contrôle et de la mise en œuvre du régime de notification pour les prestataires de services de partage de données et les décisions desdites autorités relatives au contrôle des entités inscrites au registre des organisations altruistes en matière de données reconnues.
- (2) Les recours formés en vertu du présent article sont portés devant les juridictions de l'État membre dans lequel se trouve l'autorité contre laquelle le recours juridictionnel a été formé.

## **CHAPITRE VI**

### **COMITE EUROPEEN DE L'INNOVATION DANS LE DOMAINE DES DONNEES**

#### *Article 26*

##### *Comité européen de l'innovation dans le domaine des données*

- (1) La Commission institue un comité européen de l'innovation dans le domaine des données (le «comité») sous la forme d'un groupe d'experts, qui se compose des représentants des autorités compétentes de tous les États membres, du comité européen de la protection des données, de la Commission, des espaces de données pertinents et d'autres représentants d'autorités compétentes dans des secteurs particuliers.
- (2) Les parties prenantes et les tiers concernés peuvent être invités à assister aux réunions du comité et à participer à ses travaux.
- (3) La Commission préside les réunions du comité.
- (4) Le comité est assisté par un secrétariat assuré par la Commission.

#### *Article 27*

##### *Missions du comité*

Le comité s'acquitte des missions suivantes:

- (a) conseiller et assister la Commission dans l'élaboration d'une pratique cohérente des organismes du secteur public et des organismes compétents visés à l'article 7,

paragraphe 1, qui traitent les demandes de réutilisation des catégories de données énumérées à l'article 3, paragraphe 1;

- (b) conseiller et assister la Commission dans l'élaboration d'une pratique cohérente des autorités compétentes quant à l'application des exigences auxquelles sont soumis les prestataires de services de partage de données;
- (c) conseiller la Commission sur la hiérarchisation des normes transsectorielles à utiliser et à mettre au point pour l'utilisation de données et le partage de données entre différents secteurs, la comparaison et l'échange transsectoriels des meilleures pratiques en ce qui concerne les exigences sectorielles de sécurité, les procédures d'accès, tout en tenant compte des activités de normalisation transsectorielle;
- (d) aider la Commission à améliorer l'interopérabilité des données ainsi que les services de partage de données entre les différents secteurs et domaines, en tirant parti des normes européennes, internationales ou nationales existantes;
- (e) faciliter la coopération entre les autorités compétentes nationales dans le cadre du présent règlement par le renforcement des capacités et l'échange d'informations, notamment en établissant des méthodes pour l'échange efficace d'informations relatives, d'une part, à la procédure de notification applicable aux prestataires de services de partage de données et, d'autre part, à l'enregistrement et au contrôle des organisations altruistes en matière de données reconnues.

## **CHAPITRE VII**

### **COMITE ET DELEGATION**

#### *Article 28*

#### *Exercice de la délégation*

- (1) Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.
- (2) Le pouvoir d'adopter des actes délégués prévu à l'article 5, paragraphe 11 est conféré à la Commission pour une durée indéterminée à partir du [...].
- (3) La délégation de pouvoir prévue à l'article 5, paragraphe 11 peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.
- (4) Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer».
- (5) Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.
- (6) Un acte délégué adopté en vertu de l'article 5, paragraphe 11, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de trois mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections.

Ce délai est prolongé de trois mois à l'initiative du Parlement européen ou du Conseil.

#### *Article 29*

##### *Procédure de comité*

- (1) La Commission est assistée par un comité au sens du règlement (UE) n° 182/2011.
- (2) Lorsqu'il est fait référence au présent paragraphe, l'article 4 du règlement (UE) n° 182/2011 s'applique.
- (3) Lorsque l'avis du comité doit être obtenu par procédure écrite, ladite procédure est close sans résultat lorsque, dans le délai pour émettre un avis, le président du comité le décide ou qu'un membre du comité le demande. En pareil cas, le président convoque une réunion du comité dans un délai raisonnable.

## **CHAPITRE VIII DISPOSITIONS FINALES**

#### *Article 30*

##### *Accès international*

- (1) L'organisme du secteur public, la personne physique ou morale à laquelle le droit de réutilisation des données a été accordé en vertu du chapitre 2, le prestataire de services de partage de données ou l'entité inscrite au registre des organisations altruistes en matière de données reconnues, selon le cas, prend toutes les mesures techniques, juridiques et organisationnelles raisonnables afin d'empêcher le transfert de données à caractère non personnel détenues dans l'Union ou l'accès à celles-ci dans les cas où ce transfert ou cet accès serait contraire au droit de l'Union ou au droit de l'État membre concerné, à moins que ce transfert ou cet accès ne soit conforme au paragraphe 2 ou au paragraphe 3.
- (2) Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un organisme du secteur public, d'une personne physique ou morale à laquelle le droit de réutilisation des données a été accordé en vertu du chapitre 2, d'un prestataire de services de partage de données ou d'une entité inscrite au registre des organisations altruistes en matière de données reconnues qu'il ou elle transfère depuis l'Union des données à caractère non personnel soumises au présent règlement ou y donne accès dans l'Union ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou sur tout accord de ce type entre le pays tiers demandeur et un État membre, conclu avant [l'entrée en vigueur du présent règlement].
- (3) Lorsqu'un organisme du secteur public, une personne physique ou morale à laquelle le droit de réutilisation des données a été accordé en vertu du chapitre 2, un prestataire de services de partage de données ou une entité inscrite au registre des organisations altruistes en matière de données reconnues est destinataire d'une décision de transférer depuis l'Union des données à caractère non personnel détenues dans l'Union ou d'y donner accès, prise par une juridiction ou une autorité administrative d'un pays tiers, et lorsque le respect d'une telle décision risquerait de mettre le destinataire en contrariété avec le droit de l'Union ou avec le droit de l'État membre concerné, le transfert de ces données vers cette autorité d'un pays tiers ou

l'accès à ces données par cette même autorité n'a lieu que s'il est satisfait aux conditions suivantes:

- (a) le système du pays tiers exige que les motifs et la proportionnalité de la décision soient exposés et que la décision de justice ou la décision administrative, selon le cas, revête un caractère spécifique, par exemple en établissant un lien suffisant avec certains suspects, ou avec des infractions;
- (b) l'objection motivée du destinataire fait l'objet d'un examen par une juridiction compétente dans le pays tiers; et
- (c) dans ce contexte, la juridiction compétente qui rend la décision de justice ou contrôle la décision d'une autorité administrative est habilitée, en vertu du droit de ce pays, à prendre dûment en compte les intérêts juridiques concernés du fournisseur des données protégées par le droit de l'Union ou par le droit applicable de l'État membre.

Le destinataire de la décision sollicite l'avis des autorités ou organismes compétents concernés, en application du présent règlement, afin de déterminer s'il est satisfait à ces conditions.

- (4) Si les conditions prévues par le paragraphe 2 ou le paragraphe 3 sont réunies, l'organisme du secteur public, la personne physique ou morale à laquelle le droit de réutilisation des données a été accordé en vertu du chapitre 2, le prestataire de services de partage de données ou l'entité inscrite au registre des organisations altruistes en matière de données reconnues, selon le cas, fournit le volume minimal de données admissible en réponse à une demande, en partant d'une interprétation raisonnable de la demande.
- (5) L'organisme du secteur public, la personne physique ou morale à laquelle le droit de réutilisation des données a été accordé en vertu du chapitre 2, le prestataire de services de partage de données et l'entité fournissant des services d'altruisme en matière de données informe le détenteur de données de l'existence d'une demande d'accès à des données le concernant qui émane d'une autorité administrative d'un pays tiers, sauf dans les cas où cette demande sert des fins répressives et aussi longtemps que cela est nécessaire pour préserver l'efficacité de l'action répressive.

### *Article 31* *Sanctions*

Les États membres déterminent le régime des sanctions applicables aux violations des dispositions du présent règlement et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Ces sanctions doivent être effectives, proportionnées et dissuasives. Les États membres informent la Commission au plus tard le [date d'application du présent règlement] du régime ainsi déterminé et des mesures ainsi prises, et lui communiquent immédiatement toute modification ultérieurement apportée à ce régime ou à ces mesures.

### *Article 32* *Évaluation et réexamen*

Au plus tard le [quatre ans après la date d'application du présent règlement], la Commission procède à une évaluation du présent règlement et présente ses principales conclusions dans un rapport au Parlement européen et au Conseil ainsi qu'au Comité économique et social

européen. Les États membres fournissent à la Commission les informations nécessaires à l'établissement de ce rapport.

### *Article 33*

#### *Modification du règlement (UE) 2018/1724*

À l'annexe II du règlement (UE) 2018/1724, la ligne suivante est ajoutée sous l'événement «Démarrage et gestion d'une entreprise, et cessation d'activité»:

Démarrage et gestion d'une entreprise, et cessation d'activité	Notification en qualité de prestataire de services de partage de données	Accusé de réception de la notification
	Enregistrement en tant qu'organisation altruiste en matière de données européenne	Confirmation de l'enregistrement

### *Article 34*

#### *Dispositions transitoires*

Les entités fournissant les services de partage de données prévus à l'article 9, paragraphe 1, à la date d'entrée en vigueur du présent règlement se conforment aux obligations énoncées au chapitre III d'ici au [date - 2 ans après la date d'application du présent règlement] au plus tard.

### *Article 35*

#### *Entrée en vigueur et application*

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Il est applicable à partir du [12 mois après son entrée en vigueur].

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le

*Par le Parlement européen*  
*Le président*

*Par le Conseil*  
*Le président*