COMMISSION
EUROPÉENNE

Bruxelles, le 23.2.2022
COM(2022) 68 final

2022/0047 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données
(règlement sur les données)

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

{SEC(2022) 81 final} - {SWD(2022) 34 final} - {SWD(2022) 35 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 fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données).

Les données sont une composante centrale de l'économie numérique et une ressource essentielle pour assurer les transitions écologique et numérique. Le volume de données générées par les êtres humains et les machines a connu une croissance exponentielle ces dernières années. La plupart de ces données ne sont pourtant pas utilisées, ou leur valeur est concentrée entre les mains d'un nombre relativement réduit de grandes entreprises. Manque de confiance, incitations économiques contradictoires et obstacles technologiques sont autant de facteurs qui empêchent d'exploiter tout le potentiel de l'innovation fondée sur les données. Il est donc primordial de libérer ce potentiel en offrant des possibilités de réutiliser les données, ainsi qu'en supprimant les obstacles au développement de l'économie européenne fondée sur les données, conformément aux règles européennes et dans le plein respect de ses valeurs, et en cohérence avec la mission consistant à réduire la fracture numérique pour que chacun puisse profiter de ces avantages. Faire en sorte que la valeur des données soit répartie de manière mieux équilibrée et compatible avec la nouvelle vague de données industrielles à caractère non personnel et la prolifération des produits connectés à l'internet des objets reviendra à tirer parti de l'énorme potentiel existant pour stimuler une économie durable fondée sur les données en Europe.

Réglementer l'accès aux données et l'utilisation de ces dernières est une condition préalable essentielle à la concrétisation des possibilités offertes par l'ère numérique dans laquelle nous vivons. La présidente de la Commission, Ursula von der Leyen, a déclaré dans ses orientations politiques pour la Commission 2019-2024 que l'Europe doit «*équilibrer le flux et l'utilisation des données tout en préservant un haut degré de protection de la vie privée, de sécurité, de sûreté et d'éthique*»[1]. Le programme de travail de la Commission pour 2020[2] définit plusieurs objectifs stratégiques, parmi lesquels la stratégie européenne pour les données[3], adoptée en février 2020. Celle-ci vise à construire un véritable marché unique des données et à faire de l'Europe un leader mondial de l'économie habile à tirer parti des données. À ce titre, le règlement sur les données est donc un pilier essentiel de la stratégie pour les données et la deuxième grande initiative annoncée dans ce cadre. En particulier, il contribue à la création d'un cadre de gouvernance intersectoriel pour l'accès aux données et l'utilisation de ces dernières en légiférant sur des questions qui ont une incidence sur les relations entre les acteurs de l'économie fondée sur les données, afin d'encourager le partage horizontal des données entre les secteurs.

Dans ses conclusions des 21 et 22 octobre 2021, le Conseil européen a souligné «*qu'il importe de progresser rapidement sur d'autres initiatives existantes et futures, consistant en particulier à valoriser les données en Europe, notamment au moyen d'un cadre réglementaire global qui soit propice à l'innovation, qui contribue à une meilleure portabilité des données et*

---

[1] Ursula von der Leyen, Une Union plus ambitieuse — Mon programme pour l'Europe, Orientations politiques pour la prochaine Commission européenne 2019-2024, 16 juillet 2019

[2] Commission européenne, Annexes au programme de travail de la Commission pour 2020 — Une Union plus ambitieuse, COM (2020) 37, 29 janvier 2020.

[3] COM/2020/66 final.

à un accès équitable aux données et qui assure l'interopérabilité»[4]. Le 25 mars 2021, le Conseil européen a réaffirmé *qu'il importe de mieux exploiter le potentiel que recèlent les données et les technologies numériques dans l'intérêt de la société et de l'économie*[5]. Les 1er et 2 octobre 2020, il a insisté sur «*la nécessité de rendre plus facilement accessibles des données de haute qualité et de favoriser et permettre un meilleur partage et une meilleure mise en commun des données, ainsi que l'interopérabilité*»[6]. En ce qui concerne les services en nuage, les États membres de l'UE ont adopté à l'unanimité, le 15 octobre 2020, une déclaration commune sur la construction de l'informatique en nuage de la prochaine génération pour les entreprises et le secteur public dans l'UE. Cela nécessitera, par exemple, une nouvelle génération d'offres de services informatiques en nuage de l'UE qui répondent aux normes les plus élevées en matière de portabilité et d'interopérabilité[7].

Dans sa résolution du 25 mars 2021 sur une stratégie européenne pour les données, le Parlement européen a invité instamment la Commission à présenter une loi sur les données visant à encourager et à permettre un flux de données plus important et équitable dans tous les secteurs, entre les entreprises, entre les entreprises et les administrations publiques et inversement et entre les administrations publiques elles-mêmes[8]. Dans sa résolution du 25 mars 2021, le Parlement européen a également souligné la nécessité de créer des espaces européens communs des données pour garantir la libre circulation des données à caractère non personnel dans tous les pays et tous les secteurs, ainsi qu'entre les entreprises, les universités, les parties prenantes concernées et le secteur public. De ce point de vue, il a encouragé la Commission à clarifier les droits d'utilisation, notamment dans des contextes de marché interentreprises et entre les entreprises et les administrations. Il a souligné que les déséquilibres du marché résultant de la concentration des données restreignaient la concurrence, multipliaient les entraves à l'entrée sur le marché et limitaient l'accès aux données et leur utilisation.

Dans sa résolution, le Parlement européen note également que les accords contractuels entre entreprises ne garantissent pas nécessairement un accès approprié aux données pour les petites et moyennes entreprises (PME). Cette situation s'explique par des disparités dans l'expertise et le pouvoir de négociation. Le Parlement européen a donc souligné la nécessité que les contrats définissent clairement les obligations et les responsabilités en ce qui concerne l'accès, le traitement, le partage et le stockage des données, afin de limiter leur utilisation abusive.

À ce titre, la Commission et les États membres de l'UE ont été invités à examiner les droits et obligations des acteurs en matière d'accès aux données qu'ils ont contribué à produire et à mieux leur faire connaître ces droits et obligations, en particulier le droit d'accès aux données, de les transférer, d'obliger une autre partie à interrompre leur utilisation, à les rectifier ou à les supprimer, tout en identifiant les titulaires de ces droits et en délimitant la nature de ces droits.

En ce qui concerne les relations entre entreprises et administrations publiques, le Parlement

---

4 Conseil européen, Réunion du Conseil européen (21-22 octobre 2021) – Conclusions, EUCO 17/21, 2021, p. 2.

5 Conseil européen, Déclaration des membres du Conseil européen (réunion du 25 mars 2021) — Déclaration SN 18/21, p. 4.

6 Conseil européen, Réunion du Conseil européen (1er-2 octobre 2020) – Conclusion, EUCO 13/20, 2020, p. 5.

7 Commission européenne (2020). *Commission welcomes Member States' declaration on EU cloud federation*, (La Commission salue la déclaration des États membres sur l'intérêt de fédérer l'informatique en nuage au niveau de l'UE), Communiqué de presse.

8 Résolution du Parlement européen du 25 mars 2021 sur une stratégie européenne pour les données [2020/2217(INI)].

européen a demandé à la Commission de définir, dans quelles circonstances et conditions, et pour quelles incitations, le secteur privé devrait être contraint de mettre des données à la disposition du secteur public, notamment en raison de leur nécessité pour l'organisation de services publics fondés sur les données, et d'examiner également les systèmes de partage obligatoire de données entre les entreprises et les administrations publiques, par exemple en cas de force majeure.

Dans ce contexte, la Commission présente la proposition de **règlement sur les données** dans le **but de garantir l'équité dans la répartition de la valeur produite par les données entre les acteurs de l'économie fondée sur les données et de favoriser l'accès aux données et l'utilisation de ces dernières**.

La proposition contribuera à réaliser les objectifs stratégiques plus larges consistant à faire en sorte que, dans tous les secteurs, les entreprises de l'UE soient en mesure d'innover et de faire face à la concurrence, en donnant aux individus les moyens d'agir efficacement sur leurs données et en mieux équipant les entreprises et les organismes du secteur public d'un mécanisme proportionné et prévisible afin de relever les grands défis politiques et sociétaux, y compris les urgences publiques et autres situations exceptionnelles. Les entreprises pourront facilement changer de fournisseur de services en nuage et d'autres services de traitement de données pour ce qui concerne leurs données et autres actifs numériques. Le partage de données tant au sein des secteurs qu'entre les secteurs de l'économie nécessite la mise en place d'un cadre d'interopérabilité de mesures procédurales et législatives pour renforcer la confiance et améliorer l'efficacité. La création d'espaces européens communs des données pour les secteurs stratégiques de l'économie et les domaines d'intérêt public contribuera à la réalisation d'un véritable marché intérieur des données permettant leur partage et leur utilisation entre tous les secteurs. Le présent règlement contribue donc à ces cadres et infrastructures de gouvernance ainsi qu'au partage des données en dehors des espaces de données.

Les objectifs spécifiques de la proposition sont exposés ci-dessous.

– **Faciliter l'accès aux données et l'utilisation de ces dernières par les consommateurs et les entreprises, tout en préservant les incitations à investir dans les moyens de créer de la valeur à partir des données.** Il s'agit notamment de renforcer la sécurité juridique en matière de partage de données obtenues ou générées par l'utilisation de produits ou de services liés, ainsi que de mettre en œuvre des règles visant à garantir l'équité des contrats de partage de données. La proposition **clarifie** l'application des droits pertinents prévus par la directive 96/9/CE concernant la protection juridique des bases de données (**directive sur les bases de données**)[9] à ses dispositions.

– **Prévoir l'utilisation, par les organismes du secteur public et les institutions, agences ou organes de l'Union, de données détenues par les entreprises dans certaines situations où il est nécessaire, à titre exceptionnel, de disposer de ces données.** Cela concerne principalement les urgences publiques, mais aussi d'autres situations exceptionnelles où le partage obligatoire de données entre les entreprises et les administrations publiques est justifié, afin de soutenir des politiques et services publics fondés sur des données probantes, efficaces, efficients et axés sur les performances.

9 JO L 77 du 27.3.1996, p. 20.

– **Faciliter le passage des services d'informatique en nuage aux services de traitement des données à la périphérie.** L'accès à des services de traitement de données compétitifs et interopérables est indispensable à une économie des données performante, dans laquelle les données peuvent être facilement partagées dans et entre les écosystèmes sectoriels. Le niveau de confiance dans les services de traitement des données est déterminant pour l'adoption de ces services par les utilisateurs dans tous les secteurs de l'économie.

– **Mettre en place des garanties contre le transfert illicite de données, sans notification, par les fournisseurs de services informatiques en nuage**. Cet objectif est lié aux préoccupations exprimées au sujet de l'accès illicite de gouvernements de pays tiers/de l'Espace économique européen (EEE) aux données. Ces garanties devraient renforcer encore la confiance dans les services de traitement des données sur lesquels l'économie européenne fondée sur les données s'appuie de plus en plus.

– **Prévoir l'élaboration de normes d'interopérabilité pour les données destinées à être réutilisées entre les secteurs**, dans le but de supprimer les obstacles au partage des données entre les espaces européens communs des données spécifiques à certains domaines, conformément aux exigences d'interopérabilité sectorielles, et entre d'autres données qui ne relèvent pas d'un espace européen commun spécifique des données. La proposition soutient également la définition de normes pour les «contrats intelligents». Il s'agit de programmes informatiques stockés dans des registres électroniques qui exécutent et règlent des opérations en fonction de conditions prédéterminées. Ils sont susceptibles de garantir aux détenteurs et aux destinataires de données que les conditions relatives au partage des données sont remplies.

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

La présente proposition est cohérente avec les règles existantes concernant le **traitement des données à caractère personnel** [(notamment le règlement général sur la protection des données (RGPD)[10]], la protection de la vie privée et de la **confidentialité des communications**, ainsi que les données (à caractère personnel et non personnel) stockées dans un équipement terminal et accessibles depuis celui-ci (la directive vie privée et communications électroniques[11], qui sera remplacée par le règlement vie privée et communications électroniques, actuellement en cours de négociations au niveau législatif). La présente proposition complète les droits existants, en particulier les droits relatifs aux données générées par le produit d'un utilisateur connecté à un réseau de communications électroniques accessible au public.

Le **règlement relatif au libre flux des données à caractère non personnel**[12] a mis en place un élément fondamental de l'économie européenne fondée sur les données, en garantissant que les données à caractère non personnel peuvent être stockées, traitées et transférées partout dans l'Union. Il a également présenté une approche par autorégulation du problème de la «dépendance à l'égard des fournisseurs» au niveau des fournisseurs de services de traitement des données, en introduisant des codes de conduite pour faciliter les changements de fournisseur de services en nuage [codes de conduite «Switching Cloud Providers and Porting Data» élaborés par le secteur (Changement de fournisseur de services en nuage et portage des données) (SWIPO)»]. La présente proposition s'appuie sur cette approche pour aider les entreprises et les citoyens à tirer le meilleur parti du droit au changement de fournisseurs de

10 JO 119 du 4.5.2016, p. 1.
11 JO L 201 du 31.7.2002, p. 37.
12 JO L 303 du 28.11.2018, p. 59; SWIPO (2021), voir *site internet*.

services informatiques en nuage et au portage des données. Pour ce qui est du droit des contrats, elle est également pleinement conforme à la directive concernant les clauses contractuelles abusives[13]. Quant aux services informatiques en nuage, étant donné que l'approche par autorégulation semble ne pas avoir eu d'incidence significative sur la dynamique du marché, la présente proposition présente une approche réglementaire du problème mis en évidence dans le règlement sur le libre flux des données à caractère non personnel.

Le traitement et le stockage internationaux de données ainsi que les transferts de données sont régis par le RGPD, les engagements commerciaux de l'Organisation mondiale du commerce (OMC), l'accord général sur le commerce des services (AGCS), ainsi que des accords commerciaux bilatéraux.

Le droit de la concurrence[14] s'applique, entre autres, au contrôle des concentrations, au partage de données par des entreprises ou à l'abus de position dominante d'une entreprise.

La **directive sur les bases de données**[15] prévoit la protection *sui generis* des bases de données qui ont été créées à la suite d'un investissement important, même si la base de données elle-même n'est pas une création intellectuelle originale protégée par le droit d'auteur. S'appuyant sur une jurisprudence abondante qui interprète les dispositions de la directive sur les bases de données, la présente proposition lève les incertitudes juridiques persistantes sur la question de savoir si les bases de données qui contiennent des données générées ou obtenues par l'utilisation de produits ou de services liés, tels que des capteurs, ou d'autres types de données générées par des machines, pourraient bénéficier d'une telle protection.

Le **règlement «plateformes-entreprises»**[16] impose des obligations de transparence aux plateformes, qui sont tenues de décrire, dans le cas des utilisateurs professionnels, les données produites par la fourniture du service.

La **directive sur les données ouvertes**[17] fixe des règles minimales concernant la réutilisation des données détenues par le secteur public et des données résultant de la recherche financée au moyen de fonds publics, rendues publiques par l'intermédiaire d'archives.

L'initiative «Une Europe interopérable» vise à instaurer une politique d'interopérabilité coopérative pour moderniser le secteur public. L'initiative est née du programme ISA[2], un programme de financement de l'Union mis en œuvre entre 2016 et 2021, qui a soutenu le développement de solutions numériques visant à permettre une interopérabilité transfrontière et transsectorielle des services publics[18].

La présente proposition complète le **règlement sur la gouvernance des données** récemment adopté, qui vise à faciliter le partage volontaire de données par les personnes physiques et les entreprises et harmonise les conditions d'utilisation de certaines données détenues par le secteur public, sans modifier les droits matériels sur les données ou les droits établis en matière d'accès aux données et d'utilisation de ces dernières[19]. Elle complète également la proposition relative à la **législation sur les marchés numériques**, qui imposera à certains

13 JO 95 du 21.4.1993, p. 29.
14 JO 335 du 18.12.2010, p. 36.
15 JO 77 du 27.3.1996, p. 20.
16 JO 186 du 11.7.2019, p. 57.
17 JO 172 du 26.6.2019, p. 56.
18 JO 318 du 4.12.2015, p. 1.
19 COM/2020/767 final.

fournisseurs de services de plateforme essentiels désignés comme «contrôleurs d'accès» d'assurer, entre autres, une portabilité plus effective des données générées par les activités des entreprises et des utilisateurs finaux[20].

La présente proposition n'a pas d'incidence sur les règles existantes en ce qui concerne la propriété intellectuelle (à l'exception de l'application du droit *sui generis* prévu par la directive sur les bases de données), la concurrence, la justice et les affaires intérieures et la coopération (internationale) dans ces domaines, les obligations liées au commerce, ou la protection juridique des secrets d'affaires.

Des adaptations législatives sont nécessaires dans plusieurs domaines pour promouvoir la transition numérique. Des règles claires concernant l'accès à certaines données nécessaires à la circularité et à la durabilité de certains produits tout au long de leur cycle de vie et dans des situations non exceptionnelles seront établies au titre du passeport numérique européen des produits (dans le cadre de l'initiative relative aux produits durables)[21]. Les règles de droit privé constituent un élément clé du dispositif global. Le présent règlement adapte donc le droit des contrats et d'autres règles afin d'améliorer les conditions de réutilisation des données au sein du marché intérieur et d'empêcher les parties aux contrats de tirer parti abusivement des déséquilibres en matière de pouvoir de négociation au détriment des parties les plus faibles.

En tant que proposition horizontale, **le règlement sur les données** prévoit, en ce qui concerne les droits d'utilisation des données, des **règles de base pour tous les secteurs**, par exemple dans les domaines des machines ou des biens de consommation intelligents. Toutefois, les droits et obligations sur l'accès aux données et l'utilisation de ces dernières ont également été réglementés, à des degrés divers, au niveau sectoriel. Le règlement sur les données ne modifiera aucune législation existante de ce type, mais à l'avenir, toute législation dans ces domaines devrait en principe être alignée sur les principes horizontaux établis par le règlement sur les données. La convergence avec les règles horizontales prévues par le règlement sur les données devrait être évaluée lors du réexamen des instruments sectoriels. La présente proposition autorise l'établissement, par la législation verticale, de règles plus détaillées permettant de réaliser les objectifs réglementaires sectoriels.

En ce qui concerne la création de l'espace des données relatives au pacte vert, la révision[22] de la **directive INSPIRE**[23] permettra, compte tenu de la législation sectorielle existante, d'élargir encore la disponibilité et la réutilisation des données spatiales et environnementales. Cette initiative vise à aider les pouvoirs publics, les entreprises et les citoyens de l'UE à soutenir la transition vers une économie plus verte et neutre en carbone et à réduire la charge administrative. Elle devrait promouvoir les services de données réutilisables à grande échelle afin de contribuer à la collecte, au partage, au traitement et à l'analyse de grands volumes de données utiles pour le respect de la législation environnementale et pour les actions prioritaires définies dans le pacte vert pour l'Europe. L'initiative rationalisera la présentation des rapports et la réduction de la charge grâce à une meilleure réutilisation des données existantes, à la génération automatique de rapports via l'exploration de données, et à la veille économique.

---

20 JO 186 du 11.7.2019, p. 57.
21 COM(2020) 98 final.
22 Initiative GreenData4All (REFIT)| «Train législatif»| Parlement européen (europa.eu)
23 JO L 108 du 25.4.2007, p. 1.

Le **règlement** de l'UE **sur l'électricité**[24] impose aux gestionnaires de réseau de transport de fournir des données aux régulateurs, à des fins de planification de l'adéquation des ressources, tandis que la **directive** de l'UE **sur l'électricité**[25] prévoit un accès transparent et non discriminatoire aux données et charge la Commission de définir des exigences d'interopérabilité et des procédures pour faciliter cet accès. La **deuxième directive sur les services de paiement**[26] prévoit l'accès à certains types d'informations relatives aux opérations de paiement et aux comptes sous certaines conditions, ce qui permet un partage interentreprises de données dans le domaine des technologies financières. Dans le secteur de la mobilité et des transports, les règles en matière d'accès aux données et de partage de ces dernières sont très hétérogènes. Les informations sur la réparation et l'entretien des véhicules à moteur et des véhicules agricoles sont soumises à des obligations spécifiques en matière d'accès aux données/de partage des données en vertu de la **législation relative à la réception par type**[27]. Toutefois, il est nécessaire de prévoir de nouvelles règles pour garantir que la législation existante relative à la réception par type des véhicules est adaptée à l'ère numérique et favorise le développement de véhicules propres, connectés et automatisés. Sur la base du règlement sur les données, qui constitue un cadre pour l'accès aux données et l'utilisation de ces dernières, ces règles permettront de prendre en compte des problèmes sectoriels, notamment l'accès aux fonctions et aux ressources des véhicules.

Dans le cadre de la **directive sur les systèmes de transport intelligents**[28], plusieurs règlements délégués ont été élaborés et continueront de l'être, notamment pour mieux définir l'accessibilité des données pour le transport routier et multimodal de passagers, en particulier par l'intermédiaire des points d'accès nationaux. Dans le domaine de la gestion du trafic aérien, les données non opérationnelles sont importantes pour améliorer l'intermodalité et la connectivité. Les données opérationnelles relatives à la gestion du trafic aérien relèvent du régime spécifique défini dans le cadre du **ciel unique européen**[29]. En ce qui concerne le suivi du trafic des navires, les données relatives aux navires (suivi et localisation) sont importantes pour améliorer l'intermodalité et la connectivité: ces données relèvent du régime spécifique défini dans la directive VTMIS[30]. Elles relèvent également du système et des services maritimes numériques[31]. La proposition de règlement sur le déploiement d'une **infrastructure pour carburants alternatifs**[32] précise les types de données pertinents à mettre à disposition, en synergie avec le cadre général établi dans la directive sur les systèmes de transport intelligents.

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

La présente proposition est conforme aux priorités de la Commission consistant à **adapter l'Europe à l'ère numérique** et à bâtir une économie parée pour l'avenir qui soit au service des personnes[33], dans laquelle la numérisation du marché intérieur se caractérise par un degré élevé de confiance, de sécurité et de sûreté, ainsi que par un large éventail de choix pour les consommateurs. La numérisation du marché intérieur est hautement compétitive grâce à un

24 JO L 158 du 14.6.2019, p. 54.
25 JO L 158 du 14.6.2019, p. 125.
26 JO L 337 du 23.12.2015, p. 35
27 JO L 151 du 14.6.2018, p. 1; JO L 60 du 2.3.2013, p. 1.
28 JO 207 du 6.8.2010, p. 1.
29 JO L 96 du 31.3.2004, p. 1; JO L 96 du 31.3.2004, p. 10; JO L 96 du 31.3.2004, p. 20.
30 JO 308 du 29.10.2014, p. 82.
31 JO 96 du 12.4.2016, p. 46.
32 COM/2021/559 final
33 COM/2020/67 final.

cadre qui favorise la transparence, la concurrence et l'innovation, et qui est neutre sur le plan technologique. La proposition soutient la **facilité pour la reprise et la résilience**[34], tirant les leçons de la pandémie de COVID-19, ainsi que les avantages d'un accès plus facile aux données lorsque cela est nécessaire.

La proposition soutient de diverses manières le rôle essentiel des données dans la réalisation des objectifs du **pacte vert pour l'Europe**. Premièrement, en permettant aux gouvernements, aux entreprises et aux particuliers de mieux comprendre les incidences des produits, des services et des matériaux sur la société et l'économie tout au long des chaînes d'approvisionnement. Deuxièmement, en exploitant la très grande quantité de données pertinentes du secteur privé pour affronter les problèmes liés au climat, à la biodiversité, à la pollution[35] et aux ressources naturelles, conformément aux objectifs du pacte vert pour l'Europe[36], aux conclusions du Conseil[37] et aux positions[38] du Parlement européen en la matière. Troisièmement, en comblant les lacunes dans les connaissances et en gérant les crises connexes par des mesures renforcées d'atténuation, de préparation, de réaction et de rétablissement.

Conformément à la **stratégie industrielle**[39], la proposition porte sur des technologies hautement stratégiques telles que l'informatique en nuage et les systèmes d'intelligence artificielle, des domaines dont l'UE n'a pas encore pleinement exploité le potentiel, à l'aube de la prochaine vague de données industrielles. Elle met en œuvre l'objectif de la **stratégie pour les données**[40], qui vise à ce que les entreprises soient mieux armées pour innover et soutenir la concurrence dans le respect des valeurs de l'UE et du principe de **libre circulation des données au sein du marché intérieur**. Elle est également conforme au **plan d'action en faveur de la propriété intellectuelle**[41], dans lequel la Commission s'est engagée à réviser la directive sur les bases de données.

La présente proposition devrait également être conforme aux principes énoncés dans le plan d'action sur le socle européen des droits sociaux[42] et aux exigences en matière d'accessibilité énoncées dans la directive (UE) 2019/882 relative aux exigences en matière d'accessibilité applicables aux produits et services[43].

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

• Base juridique

La base juridique de la proposition est l'article 114 du traité sur le fonctionnement de l'Union européenne, dont l'objectif est la création et le fonctionnement du marché intérieur en renforçant les mesures relatives au rapprochement des règles nationales.

Cette proposition vise à poursuivre l'achèvement du marché intérieur des données dans lequel

34 JO L 57 du 18.2.2021, p. 17.
35 COM(2021) 400 final
36 COM/2019/640 final
37 La transformation numérique au bénéfice de l'environnement, 11 décembre 2020 , conclusions du Conseil sur le nouveau plan d'action pour une économie circulaire, 11 décembre 2020 , conclusions du Conseil sur la stratégie en faveur de la biodiversité à l'horizon 2030, 16 octobre 2020 , conclusions du Conseil sur l'amélioration de la qualité de l'air, 5 mars 2020
38 Urgence climatique et environnementale - jeudi 28 novembre 2019 (europa.eu)
39 COM/2021/350 final.
40 COM/2020/66 final.
41 COM/2020/760 final.
42 COM/2021/102 final.
43 JO L 151 du 7.6.2019.

les données provenant du secteur public, des entreprises et des particuliers sont utilisées au mieux, tout en respectant les droits relatifs à ces données et les investissements réalisés pour les collecter. Les dispositions relatives au changement de fournisseur de services de traitement des données visent à établir des conditions de marché équitables et concurrentielles pour le marché intérieur des services en nuage, des services à la périphérie et des services connexes.

La protection des données commerciales confidentielles et des secrets d'affaires est un aspect important du bon fonctionnement du marché intérieur, comme dans d'autres contextes dans lesquels les services sont échangés et les biens commercialisés. La proposition garantit le respect des secrets d'affaires dans le cadre de l'utilisation des données entre entreprises ou par les consommateurs. L'initiative permettra à l'Union de tirer parti de l'ampleur du marché intérieur, étant donné que les produits ou services connexes sont souvent développés à partir de données provenant de différents États membres, puis commercialisés dans l'ensemble de l'Union.

Certains États membres ont pris des mesures législatives pour résoudre les problèmes décrits ci-dessus, dans des scénarios interentreprises et entre les entreprises et les administrations publiques, tandis que d'autres ne l'ont pas fait. Cela peut entraîner une fragmentation législative du marché intérieur, avec des règles et des pratiques différentes dans l'Union et des coûts connexes pour les entreprises qui seraient tenues de se conformer à des régimes différents. Il importe donc de veiller à ce que les mesures proposées soient appliquées de manière uniforme dans tous les États membres.

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

Compte tenu de la nature transfrontière de l'utilisation des données et des nombreux domaines d'incidence du règlement sur les données, les questions abordées par la présente proposition ne peuvent être traitées efficacement au niveau des États membres. La fragmentation résultant des disparités entre les règles nationales doit être évitée car elle entraînerait des coûts de transaction plus élevés, un manque de transparence, une insécurité juridique et la recherche indésirable de la juridiction la plus favorable. Il est particulièrement important d'éviter cette fragmentation dans toutes les situations concernant les aspects relatifs aux données des relations interentreprises, y compris les clauses contractuelles équitables et les obligations des fabricants de produits de l'internet des objets ou de services connexes, car ces aspects nécessitent un cadre homogène dans l'ensemble de l'Union.

Une évaluation des aspects transfrontières des flux de données dans le domaine du partage des données entre entreprises et administrations publiques démontre également la nécessité d'agir au niveau de l'Union. De nombreux acteurs privés détenant des données pertinentes sont des entreprises multinationales. Celles-ci ne devraient pas être confrontées à un régime juridique fragmenté.

Les services d'informatique en nuage sont rarement proposés dans un seul État membre. Le traitement transfrontière des données au sein de l'Union est conforme au RGPD et au règlement relatif au libre flux des données à caractère non personnel, qui permettent aux consommateurs et aux entreprises de traiter des données à caractère personnel et non personnel partout où ils le souhaitent dans l'Union. Ce traitement transfrontière est essentiel à l'exercice d'activités commerciales dans le marché intérieur. Il est donc crucial que les dispositions relatives au changement de fournisseur de services de traitement des données soient appliquées au niveau de l'Union, afin d'éviter une fragmentation préjudiciable sur un marché par ailleurs unifié des services de traitement des données.

Seule une action commune au niveau de l'Union peut permettre la réalisation des objectifs

fixés dans la présente proposition, y compris la création de conditions de concurrence équitables et innovantes pour les entreprises axées sur les données et l'autonomisation des citoyens. Cette action commune constitue un pas en avant certain dans la concrétisation du projet de créer un véritable marché intérieur des données.

- **Proportionnalité**

La présente proposition établit un équilibre entre les droits et les intérêts des parties prenantes concernées et l'objectif général de faciliter une utilisation plus large des données pour un vaste éventail d'acteurs. Elle crée un cadre favorable qui ne va pas au-delà de ce qui est nécessaire pour atteindre les objectifs. Elle s'attaque aux obstacles qui empêchent les entreprises, les consommateurs et le secteur public de tirer pleinement parti de la valeur potentielle des données. Elle définit également un cadre pour les futures règles sectorielles afin d'éviter la fragmentation et l'insécurité juridique. Elle clarifie les droits existants et, le cas échéant, fournit des droits d'accès aux données, contribuant ainsi à développer un marché intérieur pour le partage des données. L'initiative laisse une grande marge de manœuvre pour l'application au niveau sectoriel.

Cette proposition entraînera des coûts financiers et administratifs qui seront principalement supportés par les autorités nationales, les fabricants et les fournisseurs de services, afin qu'ils se conforment aux 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. De même, les coûts pour les utilisateurs et les détenteurs de données 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**

L'instrument choisi est un règlement parce qu'il s'agit du meilleur mécanisme pour servir les objectifs politiques plus larges visant à garantir que toutes les entreprises de l'Union soient mises en position d'innover et d'être compétitives, que les consommateurs soient mieux à même de contrôler leurs données et que les institutions, agences et organes de l'Union soient mieux armés pour relever les grands défis politiques, y compris les urgences publiques. Un règlement est nécessaire compte tenu de l'objectif d'harmonisation complète poursuivi par la proposition, afin de garantir la sécurité juridique et la transparence pour les opérateurs économiques, y compris les micro, petites et moyennes entreprises, et d'accorder aux personnes morales et physiques de tous les États membres le même niveau de droits et d'obligations juridiquement exécutoires, de garantir une application homogène dans tous les États membres, ainsi qu'une coopération efficace entre les autorités compétentes des différents États membres.

La proposition renforcera le marché intérieur des données en renforçant la sécurité juridique et en garantissant un cadre juridique uniforme, horizontal et cohérent.

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

- **Évaluations ex post/bilans de qualité de la législation existante**

La présente proposition s'appuie en partie sur la dernière évaluation de la directive sur les bases de données et sur l'étude de la Commission soutenant la révision de la directive[44]. La

[44] COM/2017/09 final SWD(2018) 146 final, section 5.4.2; Étude à l'appui d'une analyse d'impact pour la révision de la directive sur les bases de données.

directive sur les bases de données a introduit, entre autres, un droit «sui generis» spécifique pour protéger les bases de données si le fabricant d'une base de données a investi de manière substantielle dans l'obtention, la vérification et la présentation des données. Depuis sa première adoption, la directive a été évaluée à deux reprises. Ces deux évaluations ont été complétées par des communications de la Commission sur la politique relative à l'économie fondée sur les données[45].

La Cour de justice de l'Union européenne a précisé la notion d'investissements substantiels dans une base de données, en clarifiant que le droit «sui generis» vise à protéger les investissements dans la collecte, et non la création de données[46] en tant que sous-produit d'une autre activité économique. Toutefois, une incertitude demeure quant à l'application accidentelle ou involontaire du droit «sui generis» aux bases de données contenant des données générées par des machines, c'est-à-dire les données obtenues ou générées par l'utilisation de produits ou de services connexes. Il est nécessaire d'équilibrer les objectifs stratégiques de protection de la propriété intellectuelle de ces bases de données dans le contexte de l'économie des données, où l'exclusivité des données en tant que bien non rival est généralement considérée comme un obstacle à l'innovation. Par souci de cohérence avec les interventions réglementaires proposées dans la présente proposition, l'intervention sur le droit «sui generis» traite spécifiquement de l'application problématique identifiée du droit «sui generis» dans le contexte de l'internet des objets. La Commission prépare également actuellement l'évaluation du règlement (UE) 2018/1807, attendue pour novembre 2022. Les premiers rapports des contractants externes font apparaître l'effet limité des codes de conduite SWIPO sur le changement de fournisseur de services en nuage.

- **Consultation des parties intéressées**

Des travaux approfondis ont été entamés au cours du mandat de la précédente Commission afin de recenser les problèmes qui empêchent l'Union d'exploiter pleinement le potentiel de l'innovation fondée sur les données dans l'économie. La proposition s'appuie sur des consultations antérieures, telles que la consultation publique de 2017 à l'appui de la communication de la Commission intitulée «Créer une économie européenne fondée sur les données»[47], la consultation publique de 2017 sur l'évaluation de la directive sur les bases de données, la consultation publique de 2018 sur la révision de la directive concernant la réutilisation des informations du secteur public, la consultation du panel PME de 2018 sur les principes et orientations en matière de partage de données entre entreprises et la consultation ouverte en ligne de la Commission sur la stratégie pour les données[48] de février à mai 2020.

Une analyse d'impact initiale a été publiée sur le portail «Mieux légiférer» le 28 mai 2021 et a recueilli des commentaires pendant 4 semaines. La Commission a reçu 91 contributions sur ce portail[49], principalement de la part d'entreprises.

Une consultation publique en ligne sur le règlement sur les données a ensuite été publiée le 3 juin 2021. Elle a été clôturée le 3 septembre 2021. La consultation a abordé les points couverts par l'initiative avec des sections et des questions pertinentes. Elle ciblait tous les

---

45 COM/2017/09 final COM/2020/66 final; COM/2020/760 final.

46 Fixtures Marketing Ltd contre Oy Veikkaus Ab (C-46/02, 9/11/2004), Fixtures Marketing Ltd contre Svenska Spel Ab (C-338/02, 9/11/2004) British Horseracing Board Ltd contre William Hill (C-203/02, 9/11/2004) Fixtures Marketing Ltd contre OPAP (C-444/02, 9/11/2004)

47 COM/2017/09 final.

48 Commission européenne (2020). *Résultats de la consultation en ligne sur la stratégie européenne pour les données.*

49 *Page web* de la Commission européenne: *Donnez votre avis - Acte législatif sur les données et modification des règles relatives à la protection juridique des bases de données*

types de parties prenantes, recueillant des informations sur le partage, l'accès et l'utilisation des données dans des contextes interentreprises et d'entreprises à administrations publiques, sur l'autonomisation des consommateurs et la portabilité des données, sur le rôle potentiel des mesures techniques telles que les contrats intelligents, sur la capacité des utilisateurs à changer de fournisseur de services en nuage, sur les droits de propriété intellectuelle (c'est-à-dire la protection des bases de données), et sur les garanties pour les données à caractère non personnel au niveau international. Après avoir procédé à une analyse approfondie des réponses, la Commission a publié un rapport de synthèse sur son site web[50].

Au total, 449 contributions ont été reçues en provenance de 32 pays. Les entités commerciales ont constitué le plus grand nombre de contributions, soit 122 associations professionnelles et 105 entreprises/organisations professionnelles. Par ailleurs, 100 répondants étaient des autorités publiques et 58 étaient des particuliers. D'une manière générale, les réponses ont confirmé qu'il existe toute une série d'obstacles à un partage efficace et efficient des données dans tous les types de relations.

Dans le contexte interentreprises, bien que le partage de données entre entreprises soit une pratique courante, les répondants ayant rencontré des difficultés ont mentionné des obstacles de nature technique (formats, absence de normes - 69 %); le refus pur et simple d'accorder l'accès non lié à des problèmes de concurrence (55 %) ou l'abus d'un déséquilibre contractuel (44 %). En ce qui concerne les questions contractuelles, près de la moitié des répondants étaient favorables à l'introduction d'une appréciation du caractère abusif (46 %), tandis que 21 % n'y étaient pas favorables. Les PME ont manifesté un large soutien (50 %) en faveur d'une appréciation du caractère abusif, et un nombre important de grandes entreprises y étaient également favorables (41 %). De même, 46 % des parties prenantes des différents secteurs se sont montrées favorables à des règles générales d'accès fondées sur des conditions équitables, raisonnables et non discriminatoires. 60 % des répondants, en particulier les PME et les microentreprises (78 %), ont convenu que des clauses contractuelles types pourraient contribuer à accroître le partage des données. 70 % des parties prenantes ont exprimé l'opinion que les données générées dans le contexte de l'internet des objets posaient un problème d'équité, et que les fabricants de produits connectés ou de services connexes ne devraient pas pouvoir décider unilatéralement de ce qu'il advient des données générées par ces produits. 79 % des répondants estiment que les contrats intelligents pourraient constituer un outil efficace pour mettre en œuvre techniquement l'accès aux données et leur utilisation dans le contexte des données cogénérées de l'internet des objets.

L'insécurité et les obstacles juridiques, les freins commerciaux et le manque d'infrastructures appropriées figuraient parmi les principaux facteurs entravant le partage de données entre entreprises et administrations publiques signalés par les répondants. Presque toutes les autorités publiques estiment qu'une action (de l'Union ou des États membres) sur le partage de données entre entreprises et administrations publiques est nécessaire, contre 80 % des établissements universitaires/de recherche et 38 % des entreprises/organisations professionnelles/associations. Une nette majorité des parties prenantes (en particulier les citoyens et les administrations publiques) a également exprimé l'opinion que le partage de données entre entreprises et administrations publiques devrait être obligatoire, avec des garanties claires pour les cas d'utilisation spécifiques présentant un intérêt public manifeste dans les situations d'urgence et à des fins de gestion de crise, pour les statistiques officielles, pour la protection de l'environnement et pour une société plus saine en général.

[50] Commission européenne (2021). *Consultation publique relative au règlement sur les données:rapport de synthèse*.

Les répondants ont également confirmé l'utilité d'un droit au changement de fournisseur pour les utilisateurs professionnels de services d'informatique en nuage. En ce qui concerne les garanties relatives aux données à caractère non personnel dans des contextes internationaux, 76 % des répondants perçoivent l'accès potentiel aux données par des autorités étrangères sur la base de la législation étrangère comme un risque pour leur organisation, 19 % indiquant qu'il s'agit d'un risque majeur.

- **Obtention et utilisation d'expertise**

La proposition a été soutenue par plusieurs études, ateliers et autres contributions d'experts:

– **Étude à l'appui de l'analyse d'impact sur l'amélioration de l'utilisation des données en Europe**, incluant des entretiens avec des parties prenantes ciblées, deux ateliers intersectoriels sur le partage de données interentreprises et d'entreprises à administrations publiques, ainsi qu'un atelier final de validation organisé au printemps 2021.

– **Étude sur les clauses contractuelles types, le contrôle de l'équité dans le partage de données et dans les contrats de services en nuage, ainsi que sur les droits d'accès aux données** évaluant, en particulier, les aspects relatifs à l'équité dans les relations de partage de données interentreprises et comprenant des entretiens ciblés avec les parties prenantes et un atelier de validation.

– **Étude sur le préjudice économique causé par des clauses contractuelles abusives ou déséquilibrées concernant l'informatique en nuage** incluant notamment une enquête en ligne auprès d'un échantillon de PME et de jeunes pousses utilisant l'informatique en nuage pour la conduite de leurs activités.

– **Étude sur le changement de fournisseur de services en nuage**, comprenant un atelier intersectoriel au deuxième trimestre de 2017.

– **Étude à l'appui de la révision de la directive sur les bases de données**, incluant des entretiens avec des parties prenantes ciblées. Cette étude a aidé la Commission dans sa préparation de l'analyse d'impact accompagnant la révision de la directive sur les bases de données dans le cadre du règlement sur les données et dans la réalisation de leurs objectifs interdépendants.

– **Soutien méthodologique à l'évaluation de l'incidence de l'utilisation de données détenues par le secteur privé dans les statistiques officielles**. Cet exercice contribue à l'évaluation de l'incidence de la réutilisation des données entre entreprises et administrations publiques dans les statistiques officielles en élaborant une approche méthodologique et en décrivant les avantages et les coûts de la réutilisation des données et de certains cas d'utilisation pour différents domaines statistiques et différents types de données du secteur privé. En outre, il contribue aux recherches et aux délibérations en cours afin de parvenir à une meilleure compréhension du partage des données entre entreprises et administrations publiques.

– **Webinaires sur les plateformes de données à caractère personnel et les plateformes de données industrielles.** Trois webinaires ont été organisés les 6, 7 et 8 mai 2020. Ils ont regroupé les projets de plateformes de données pertinents relevant du portefeuille du partenariat public-privé sur la valeur des mégadonnées (Big DataValue).

– **Rapport du groupe d'experts de haut niveau sur le partage des données entre les entreprises et les administrations publiques.** Le rapport contient une analyse

des problèmes liés au partage des données entre les entreprises et les administrations publiques dans l'Union et formule une série de recommandations visant à garantir un partage des données entre les entreprises et les administrations publiques qui soit modulable, responsable et durable dans l'intérêt public. Outre la recommandation à la Commission d'étudier l'option d'un cadre juridique dans ce domaine, le groupe d'experts a présenté plusieurs moyens d'inciter les entreprises privées à partager leurs données. Il s'agit notamment d'incitations monétaires et non monétaires, par exemple des incitations fiscales, l'investissement de fonds publics pour soutenir le déploiement d'outils techniques fiables et des systèmes de reconnaissance pour le partage des données.

– **Atelier sur les labels/la certification des fournisseurs de solutions techniques pour l'échange de données.** Une centaine de participants issus d'entreprises (y compris de PME), d'institutions européennes et d'universités ont participé à ce webinaire le 12 mai 2020. Son objectif était d'examiner si un système de labellisation ou de certification pouvait stimuler le recours par les entreprises à des intermédiaires de données en renforçant la confiance dans l'écosystème de données.

– **Dix ateliers organisés entre juillet et novembre 2019 ont rassemblé plus de 300 parties prenantes et couvert différents secteurs.** Les ateliers ont porté sur la manière dont l'organisation du **partage des données dans certains domaines**, tels que l'environnement, l'agriculture, l'énergie ou les soins de santé, pourrait profiter à la société dans son ensemble, en aidant les acteurs publics à élaborer des politiques plus adaptées et à améliorer les services publics, ainsi que les acteurs privés à produire des services contribuant à relever les défis de société.

– **Consultation du panel de PME.** Cette consultation, organisée d'octobre 2018 à janvier 2019, visait à recueillir l'avis des PME sur les principes et orientations de la Commission concernant le partage des données entre entreprises, publiés dans la communication intitulée «*Vers un espace européen commun des données*» et accompagnant le document de travail des services de la Commission du 25 avril 2018[51].

– **Dernier Eurobaromètre sur l'incidence de la numérisation.** Cette enquête générale sur la vie quotidienne des Européens comprend des questions sur le contrôle et le partage des informations à caractère personnel par les citoyens. Publiée le 5 mars 2020, elle fournit des informations sur la volonté des citoyens européens de partager leurs informations à caractère personnel, et dans quelles conditions.

– **L'avis du Contrôleur européen de la protection des données** (CEPD) sur la stratégie européenne pour les données[52]. Le 16 juin 2020, le CEPD a adopté l'avis 3/2020 sur la stratégie européenne pour les données. Le CEPD s'est félicité de cette stratégie, estimant que sa mise en œuvre offrait l'occasion de montrer l'exemple pour un autre modèle d'économie fondé sur les données.

• **Analyse d'impact**

La présente proposition est accompagnée d'une analyse d'impact[53], soumise au comité d'examen de la réglementation le 29 septembre 2021 et le 13 décembre 2021. Le 21 janvier 2022, le comité a émis un avis favorable, assorti de réserves.

---

51 COM(2018) 232 final SWD(2018) 125 final du 25.4.2018.

52 Avis 3/2020 du CEPD sur la stratégie européenne pour les données.

53 **[Liens vers le document final et la fiche de synthèse à ajouter].**

- **Réglementation affûtée et simplification**

En précisant que le droit «sui generis» conféré par la directive sur les bases de données (directive 96/9/CE) ne s'applique pas aux bases de données contenant des données générées ou obtenues par l'utilisation de produits ou de services liés, la proposition garantit que le droit «sui generis» n'interfère pas avec les droits des entreprises et des consommateurs d'accéder aux données, d'utiliser les données et de les partager prévus par le présent règlement. La clarification permettra d'aligner l'application du droit «sui generis» sur l'objectif de la proposition législative et aura une incidence positive sur l'application uniforme des règles dans le marché intérieur et sur l'économie des données.

En facilitant l'accès aux données et l'utilisation des données, le règlement sur les données devrait réduire les charges, tant dans le secteur public que pour les entreprises, principalement en raison de la baisse des coûts de transaction et des gains d'efficacité. Dans le cadre de l'approche «un ajout, un retrait»[54], qui vise à réduire au minimum les charges pour les citoyens et les entreprises en ce qui concerne les implications et les coûts de l'application de la législation, la charge administrative nette estimée du règlement sur les données, sur la base de l'analyse d'impact, représente des avantages qui sont susceptibles non seulement de compenser les coûts administratifs associés, mais aussi de l'emporter largement sur ces derniers.

- **Droits fondamentaux**

La proposition est conforme à la législation de l'Union sur la protection des données à caractère personnel et la confidentialité des communications et des équipements terminaux et prévoit des garanties supplémentaires lorsque l'accès aux données à caractère personnel peut être concerné ainsi que dans les cas soumis à des droits de propriété intellectuelle.

Au chapitre II, un niveau élevé de protection des consommateurs est renforcé par le nouveau droit d'accès aux données générées par l'utilisateur dans des situations précédemment non couvertes par le droit de l'Union. Le droit d'utiliser et de disposer des biens acquis légalement est renforcé par un droit d'accès aux données générées par l'utilisation d'un objet de l'internet des objets. De cette manière, le propriétaire peut bénéficier d'une meilleure expérience utilisateur et d'un éventail plus large de services de réparation et d'entretien, par exemple. Dans le contexte de la protection des consommateurs, les droits des enfants en tant que consommateurs vulnérables méritent une attention particulière et les dispositions du règlement sur les données contribueront à clarifier les situations en ce qui concerne l'accès aux données et l'utilisation de ces dernières.

Le droit d'accès aux données de l'internet des objets accordé à des tiers à la demande de l'utilisateur limite la liberté d'entreprise et la liberté contractuelle du fabricant ou du concepteur d'un produit ou d'un service lié. Cette limitation se justifie par la nécessité de renforcer la protection des consommateurs, notamment celle de promouvoir leurs intérêts économiques. Le fabricant ou le concepteur d'un produit ou d'un service lié exerce généralement un contrôle exclusif sur l'utilisation des données générées par l'utilisation d'un produit ou d'un service lié, ce qui contribue à des effets de verrouillage et entrave l'entrée sur le marché d'acteurs proposant des services après-vente. Le droit d'accès aux données de l'internet des objets remédie à cette situation en permettant aux consommateurs qui utilisent des produits ou des services liés de contrôler véritablement la manière dont les données générées par leur utilisation du produit ou du service lié sont utilisées et en permettant l'innovation par un plus grand nombre d'acteurs du marché. Les consommateurs peuvent

[54] SWD(2021) 305 final.

donc bénéficier d'un choix plus large de services après-vente, tels que la réparation et l'entretien, et ne dépendent plus uniquement des services du fabricant. La proposition facilite la portabilité des données de l'utilisateur vers des tiers et permet ainsi une offre concurrentielle de services après-vente, ainsi qu'une innovation plus large fondée sur les données et le développement de produits ou de services non liés à ceux que l'acheteur a initialement achetés ou auxquels il s'est abonné.

La limitation de la liberté du fabricant ou du concepteur de conclure des contrats et d'exercer une activité est proportionnée et atténuée par la faculté inchangée du fabricant ou du concepteur d'utiliser également les données, pour autant que la législation applicable et l'accord conclu avec l'utilisateur soient respectés. En outre, le fabricant ou le concepteur bénéficiera également du droit d'exiger une compensation pour permettre l'accès de tiers. Le droit d'accès est sans préjudice des droits existants en matière d'accès et de portabilité pour les personnes concernées au sens du RGPD. Des garanties supplémentaires permettent de s'assurer d'une utilisation proportionnée des données par le tiers.

Au chapitre IV, un système de protection équitable et efficace contre les clauses contractuelles abusives dans le cadre du partage des données contribuera à la capacité des micro, petites et moyennes entreprises d'exercer une activité. Cette disposition restreint la liberté contractuelle des entreprises dans une mesure limitée, étant donné qu'elle ne s'applique qu'aux clauses contractuelles abusives relatives à l'accès aux données et à l'utilisation des données imposées unilatéralement par une partie contractante à une micro, petite ou moyenne entreprise. Cela se justifie dans la mesure où les PME se trouvent généralement dans une position de négociation plus faible et n'ont souvent pas d'autre choix que d'accepter des clauses contractuelles «à prendre ou à laisser». La liberté contractuelle reste largement inchangée, étant donné que seules les clauses excessives et abusives sont invalidées et que le contrat conclu reste, si possible, valable sans les clauses abusives. En outre, les parties peuvent encore négocier individuellement une clause contractuelle spécifique[55].

Au chapitre V, les dispositions relatives au partage de données entre les entreprises et les administrations publiques sur la base d'un besoin exceptionnel renforceront la capacité des pouvoirs publics à prendre des mesures pour le bien commun, par exemple pour réagir à une urgence publique, prévenir une urgence publique ou contribuer au rétablissement à la suite d'une urgence publique. Le secteur privé tirera également profit de la rationalisation des procédures de demande de données.

Au chapitre VI, les dispositions relatives au changement de fournisseur de traitement de données amélioreront la position des entreprises clientes et préserveront leur possibilité de changer de fournisseur. La restriction du droit d'exercer une activité économique imposée aux fournisseurs de traitement de données est justifiée par le fait que les nouvelles règles s'attaquent au problème de l'effet de verrouillage sur le marché de l'informatique en nuage et à la périphérie et améliorent le choix des services de traitement de données pour les entreprises utilisatrices et les particuliers.

Au chapitre X, l'intervention sur le droit «sui generis» applicable aux bases de données de la directive sur les bases de données ne limite pas la protection de la propriété intellectuelle qui y est prévue. Elle renforce au contraire la sécurité juridique dans les cas où la protection du droit «sui generis» n'était pas claire auparavant.

[55] Pour de plus amples explications sur l'appréciation du caractère abusif et le principe de la liberté contractuelle, voir l'analyse d'impact, annexe 11.

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**

Au niveau sectoriel et macroéconomique, l'étude sur la surveillance du marché des données qui est en cours aidera à suivre l'impact économique de la proposition actuelle sur la croissance du marché des données dans l'Union.

L'impact sur les PME, à savoir leur perception des problèmes liés à l'accès aux données et à leur utilisation, sera évalué dans le cadre d'une consultation d'un panel de PME cinq ans après l'adoption du règlement sur les données.

Compte tenu du rôle central joué par les espaces européens communs des données dans la mise en œuvre de la stratégie européenne pour les données, bon nombre des effets de la présente initiative feront l'objet d'un suivi au niveau des espaces de données sectoriels et des informations recueillies par le centre d'appui aux espaces de données qui devra être financé dans le cadre du programme pour une Europe numérique. L'interaction régulière entre les services de la Commission, le centre d'appui et le comité européen de l'innovation dans le domaine des données (qui sera mis en place après l'entrée en vigueur du règlement sur la gouvernance des données) devrait constituer une source d'information fiable permettant d'évaluer les progrès accomplis.

Enfin, une évaluation sera lancée quatre ans après l'adoption du règlement sur les données afin d'évaluer l'initiative et de préparer d'autres actions si nécessaire.

- **Explication détaillée de certaines dispositions de la proposition**

Le chapitre I définit l'objet et le champ d'application du règlement et énonce les définitions utilisées dans l'ensemble de l'acte.

Le chapitre II renforce la sécurité juridique pour les consommateurs et les entreprises en ce qui concerne l'accès aux données générées par les produits ou les services liés qu'ils possèdent, louent ou donnent en location. Les fabricants et les concepteurs doivent concevoir les produits de telle manière que les données soient facilement accessibles par défaut, et ils devront faire preuve de transparence quant aux données qui seront accessibles et à la manière d'y accéder. Les dispositions de ce chapitre n'affectent pas la possibilité pour les fabricants d'accéder aux données des produits ou des services liés qu'ils proposent et d'utiliser ces données, lorsque cela a été convenu avec l'utilisateur. Le détenteur de données est tenu de mettre ces données à la disposition de tiers à la demande de l'utilisateur. Les utilisateurs auront le droit d'autoriser le détenteur de données à donner accès aux données à des fournisseurs de services tiers, tels que les fournisseurs de services après-vente. Les micro et petites entreprises seront exemptées de ces obligations.

Le chapitre III énonce les règles générales applicables aux obligations de mise à disposition des données. Lorsqu'un détenteur de données est tenu de mettre des données à la disposition d'un destinataire de données conformément au chapitre II ou à d'autres dispositions du droit de l'Union ou de la législation d'un État membre, le cadre général définit les conditions dans lesquelles les données sont mises à disposition et la compensation pour la mise à disposition des données. Toutes ces conditions devront être équitables et non discriminatoires, et toute compensation devra être raisonnable, sans empêcher que d'autres dispositions du droit de

l'Union ou de la législation nationale mettant en œuvre le droit de l'Union n'excluent toute compensation ou ne prévoient une compensation moins élevée pour la mise à disposition des données. Toute compensation fixée pour les PME ne peut excéder les coûts occasionnés par la mise à disposition des données, sauf indication contraire dans les législations sectorielles. Les organismes de règlement des différends certifiés par les États membres peuvent prêter assistance aux parties qui ne sont pas d'accord sur la compensation ou les conditions à respecter pour parvenir à un accord.

Le chapitre IV traite du caractère abusif des clauses contractuelles figurant dans les contrats de partage de données entre entreprises, lorsqu'une clause contractuelle est imposée unilatéralement par une partie à une micro, petite ou moyenne entreprise. Ce chapitre garantit que les accords contractuels relatifs à l'accès aux données et à l'utilisation des données ne tirent pas profit de déséquilibres entre les pouvoirs de négociation des parties contractantes. L'instrument de l'appréciation du caractère abusif comprend une disposition générale définissant le caractère abusif d'une clause contractuelle relative au partage de données, complétée par une liste de clauses qui sont soit toujours abusives soit présumées abusives. Dans des situations de pouvoir de négociation inégal, cette appréciation protège la partie contractuelle la plus faible contre un contrat abusif. Un tel caractère abusif entrave l'utilisation des données par les deux parties au contrat. De ce fait, les dispositions garantissent une répartition plus équitable de la valeur dans l'économie fondée sur les données[56]. Les conditions contractuelles types recommandées par la Commission peuvent aider les parties commerciales à conclure des contrats à des conditions équitables.

Le chapitre V crée un cadre harmonisé pour l'utilisation, par les organismes du secteur public et les institutions, organes et organismes de l'Union, des données détenues par des entreprises lorsqu'il existe un besoin exceptionnel pour les données demandées. Le cadre est fondé sur une obligation de mise à disposition des données et ne s'appliquerait qu'en cas d'urgence publique ou dans des situations où les organismes du secteur public ont un besoin exceptionnel d'utiliser certaines données qui ne peuvent être obtenues sur le marché, en temps utile, par l'adoption d'une nouvelle législation ou au moyen d'obligations existantes en matière de communication de données. En cas de besoin exceptionnel de répondre à une urgence publique, telle qu'une urgence de santé publique ou une catastrophe majeure d'origine naturelle ou humaine, les données seraient mises à disposition gratuitement. Dans d'autres cas de nécessité exceptionnelle, y compris pour prévenir une urgence publique ou pour contribuer au rétablissement à la suite d'une urgence publique, le détenteur de données qui met les données à disposition devrait avoir droit à une compensation correspondant aux coûts liés à la mise à disposition des données concernées, majorés d'une marge raisonnable. Afin que le droit de demander des données ne fasse pas l'objet d'abus et que le secteur public reste responsable de son utilisation, les demandes de données devraient être proportionnées, indiquer clairement l'objectif à atteindre et respecter les intérêts de l'entreprise qui met les données à disposition. Les autorités compétentes garantiraient la transparence et la mise à la disposition du public de toutes les demandes. Elles traiteraient également les éventuelles plaintes qui en résulteraient.

Le chapitre VI introduit des exigences réglementaires minimales de nature contractuelle, commerciale et technique, imposées aux fournisseurs de services d'informatique en nuage, de services à la périphérie et d'autres services de traitement des données, afin de permettre le passage d'un service à l'autre. En particulier, la proposition garantit que les clients maintiennent l'équivalence fonctionnelle (un niveau minimal de fonctionnalité) du service

[56] Pour de plus amples explications sur l'appréciation du caractère abusif, y compris sur le fonctionnement dans la pratique, voir l'annexe 11 de l'analyse d'impact.

après leur passage à un autre fournisseur de services. La proposition prévoit une exception en cas d'impossibilité technique, mais fait peser la charge de la preuve à cet égard sur le fournisseur de services. La proposition ne prévoit pas de normes techniques ou d'interfaces spécifiques. Toutefois, elle exige que les services soient compatibles avec les normes européennes ou les spécifications techniques d'interopérabilité ouvertes lorsqu'elles existent.

Le chapitre VII traite de l'accès illicite de tiers à des données à caractère non personnel détenues dans l'Union par des services de traitement de données proposés sur le marché de l'Union. La proposition n'a aucune incidence sur la base juridique des demandes d'accès aux données introduites pour les données détenues par des citoyens ou des entreprises de l'UE et est sans préjudice du cadre de l'Union en matière de protection des données et de la vie privée. Elle offre des garanties spécifiques, les fournisseurs étant tenus de prendre toutes les mesures techniques, juridiques et organisationnelles raisonnables permettant d'empêcher un accès qui serait incompatible avec des obligations concurrentes de protection des données en vertu du droit de l'Union, à moins que des conditions strictes ne soient remplies. Le règlement respecte les engagements internationaux de l'Union au sein de l'OMC et dans les accords commerciaux bilatéraux.

Le chapitre VIII prévoit des exigences essentielles à respecter en ce qui concerne l'interopérabilité pour les opérateurs d'espaces de données et les fournisseurs de services de traitement des données, ainsi que des exigences essentielles relatives aux contrats intelligents. Ce chapitre permet également de définir des spécifications d'interopérabilité ouvertes et des normes européennes pour l'interopérabilité des services de traitement des données afin de promouvoir un environnement en nuage multifournisseur continu.

Le chapitre IX établit le cadre de mise en œuvre et d'application avec les autorités compétentes de chaque État membre, y compris un mécanisme de traitement des plaintes. La Commission recommande des clauses contractuelles types facultatives concernant l'accès aux données et l'utilisation des données. Des sanctions s'appliquent en cas d'infraction au présent règlement.

Le chapitre X contient une disposition selon laquelle le droit «sui generis» établi dans la directive 96/9/CE ne s'applique pas aux bases de données contenant des données obtenues ou générées par l'utilisation d'un produit ou d'un service lié afin de faire obstacle à l'exercice effectif du droit des utilisateurs d'accéder aux données et d'utiliser les données conformément à l'article 4 du présent règlement ou du droit de partager ces données avec des tiers conformément à l'article 5 du présent règlement.

Le chapitre XI permet à la Commission d'adopter des actes délégués afin d'introduire un mécanisme de suivi des frais de changement imposés aux fournisseurs de services de traitement des données, de préciser davantage les exigences essentielles en matière d'interopérabilité et de publier la référence des spécifications d'interopérabilité ouvertes et des normes européennes pour l'interopérabilité des services de traitement des données. Il prévoit également la procédure de comité pour l'adoption d'actes d'exécution visant à faciliter l'adoption de spécifications communes pour l'interopérabilité et les contrats intelligents lorsqu'il n'existe pas de normes harmonisées ou que les normes harmonisées sont insuffisantes pour garantir la conformité avec les exigences essentielles. La proposition clarifie également la relation avec d'autres actes juridiques de l'Union régissant les droits et obligations en matière de partage des données.

2022/0047 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données
(règlement sur les 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[57],

vu l'avis du Comité des régions[58],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) Ces dernières années, les technologies fondées sur les données ont eu des effets transformateurs sur tous les secteurs de l'économie. La multiplication rapide des produits connectés à l'internet des objets, en particulier, a fait augmenter le volume de données et leur valeur potentielle pour les consommateurs, les entreprises et la société. Des données de qualité et interopérables provenant de différents domaines permettent d'accroître la compétitivité et l'innovation et de garantir une croissance économique pérenne. Un même ensemble de données est susceptible d'être utilisé et réutilisé à diverses fins et de façon illimitée, sans perdre en qualité ni en quantité.

(2) Les obstacles au partage de données empêchent que ces données ne soient réparties de façon optimale dans l'intérêt de la société. Parmi ces obstacles figurent l'absence de mesures incitant les détenteurs de données à conclure volontairement des accords de partage de données, l'incertitude quant aux droits et obligations en matière de données, le coût afférent à l'engagement d'un contractant chargé de mettre en œuvre les interfaces techniques, l'importante fragmentation des informations stockées en silos, une mauvaise gestion des métadonnées, l'absence de normes régissant l'interopérabilité sémantique et technique, les goulets d'étranglement qui entravent l'accès aux données, l'absence de pratiques communes de partage de données et l'exploitation abusive de déséquilibres contractuels en ce qui concerne l'accès aux données et leur utilisation.

(3) Dans les secteurs qui comptent des micro, petites et moyennes entreprises, on constate souvent l'absence de capacités et de compétences numériques pour collecter, analyser

[57] JO C du , p. .
[58] JO C du , p. .

et utiliser des données; l'accès à celles-ci est fréquemment restreint soit parce qu'elles sont détenues par un seul acteur au sein du système soit parce que toute interopérabilité fait défaut entre les données ou entre les services de données ou encore au-delà des frontières.

(4) Afin de répondre aux besoins de l'économie numérique et d'éliminer les obstacles au bon fonctionnement du marché intérieur des données, il est nécessaire d'établir un cadre harmonisé qui précise qui, outre le fabricant ou un autre détenteur de données, dispose d'un droit d'accès aux données générées par les produits ou les services liés, dans quelles conditions et sur quel fondement. En conséquence, les États membres ne devraient pas adopter ou maintenir des exigences nationales supplémentaires pour les questions relevant du champ d'application du présent règlement, sauf disposition expresse de ce dernier, parce que cela porterait atteinte à l'application directe et uniforme du présent règlement.

(5) Il est fait en sorte par le présent règlement que les utilisateurs d'un produit ou d'un service lié dans l'Union puissent avoir accès, en temps utile, aux données générées par l'utilisation de ce produit ou de ce service lié et que ces utilisateurs puissent se servir de ces données, y compris en les partageant avec des tiers de leur choix. Le présent règlement impose au détenteur de données de mettre des données, dans certaines circonstances, à la disposition des utilisateurs et des tiers désignés par ces utilisateurs. Il prévoit également que les détenteurs de données mettent des données à la disposition des destinataires de données dans l'Union dans des conditions équitables, raisonnables et non discriminatoires ainsi que de manière transparente. Les règles de droit privé sont essentielles dans le cadre général du partage de données. En conséquence, le présent règlement adapte les règles du droit des contrats et empêche que ne soient exploités les déséquilibres contractuels qui entravent l'accès équitable aux données et leur utilisation équitable par les micro, petites ou moyennes entreprises au sens de la recommandation 2003/361/CE. Le présent règlement prévoit également qu'en cas de besoin exceptionnel, les détenteurs de données mettent à la disposition des organismes du secteur public des États membres et à celle des institutions, organes et organismes de l'Union les données nécessaires à l'exécution de missions d'intérêt public. Le présent règlement vise en outre à faciliter le passage d'un service de traitement des données à un autre et à améliorer l'interopérabilité des données ainsi que des mécanismes et services de partage de données dans l'Union. Il conviendrait de ne pas interpréter le présent règlement comme reconnaissant ou créant une base juridique permettant au détenteur de données de détenir des données, d'y avoir accès ou d'en effectuer le traitement ou comme lui conférant un droit nouveau d'utiliser les données générées par l'utilisation d'un produit ou d'un service lié. Le présent règlement a plutôt pour point de départ le contrôle dont le détenteur de données jouit effectivement, en fait ou en droit, sur les données générées par des produits ou des services liés.

(6) Des données sont générées sous l'effet des actions d'au moins deux acteurs: le concepteur ou fabricant d'un produit et l'utilisateur de ce produit. La génération de données soulève des questions d'équité dans l'économie numérique parce que les données enregistrées par ces produits ou ces services liés constituent un apport important pour les services après-vente, les services auxiliaires et autres. Afin de concrétiser les avantages économiques considérables que les données, en tant que «bien non rival», présentent pour l'économie et la société, une approche générale de l'attribution des droits d'accès et d'utilisation en matière de données est préférable à l'octroi de droits exclusifs d'accès et d'utilisation.

(7) Le droit fondamental à la protection des données à caractère personnel est garanti notamment par le règlement (UE) 2016/679 et le règlement (UE) 2018/1725. La directive 2002/58/CE protège, quant à elle, la vie privée et la confidentialité des communications en prévoyant notamment des conditions régissant tout stockage de données à caractère personnel et de données à caractère non personnel dans un équipement terminal et l'accès aux unes et aux autres à partir dudit équipement. Ces instruments servent de base à un traitement pérenne et responsable des données, y compris lorsque les ensembles de données contiennent un mélange de données à caractère personnel et de données à caractère non personnel. Le présent règlement complète, sans y porter atteinte, les dispositions de droit de l'Union relatives à la protection des données et à la vie privée, en particulier le règlement (UE) 2016/679 et la directive 2002/58/CE. Aucune disposition du présent règlement ne devrait être appliquée ou interprétée de manière à réduire ou à limiter le droit à la protection des données à caractère personnel ou le droit à la vie privée et à la confidentialité des communications.

(8) Les principes de la minimisation des données ainsi que de la protection des données dès la conception et de la protection des données par défaut sont essentiels lorsque le traitement comporte des risques importants pour les droits fondamentaux des personnes. Compte tenu de l'état des connaissances, toutes les parties au partage de données, y compris lorsque ce partage relève du champ d'application du présent règlement, devraient mettre en œuvre des mesures techniques et organisationnelles pour protéger ces droits. Des mesures de ce type incluent non seulement la pseudonymisation et le cryptage mais aussi le recours à des technologies de plus en plus disponibles qui permettent d'appliquer des algorithmes aux données et d'obtenir des informations précieuses sans transmission de ces données entre les parties ni copie inutile des données brutes ou des données structurées elles-mêmes.

(9) Le présent règlement complète, sans y porter atteinte, le droit de l'Union visant à promouvoir les intérêts des consommateurs et à assurer un niveau élevé de protection de ces derniers, à protéger leur santé, leur sécurité et leurs intérêts économiques, en particulier la directive 2005/29/CE du Parlement européen et du Conseil[59], la directive 2011/83/UE du Parlement européen et du Conseil[60] et la directive 93/13/CEE du Parlement européen et du Conseil[61].

(10) Le présent règlement est sans préjudice des actes juridiques de l'Union qui prévoient le partage de données, l'accès à ces dernières et leur utilisation 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, ou à des fins douanières et fiscales, quelle que soit la

[59] Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) nº 2006/2004 du Parlement européen et du Conseil («directive sur les pratiques commerciales déloyales») (JO L 149 du 11.6.2005, p. 22).

[60] Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil.

[61] Directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs. Directive (UE) 2019/2161 du Parlement européen et du Conseil du 27 novembre 2019 modifiant la directive 93/13/CEE du Conseil et les directives 98/6/CE, 2005/29/CE et 2011/83/UE du Parlement européen et du Conseil en ce qui concerne une meilleure application et une modernisation des règles de l'Union en matière de protection des consommateurs.

base juridique prévue par le traité sur le fonctionnement de l'Union européenne sur laquelle ces actes ont été adoptés. Il s'agit notamment du règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion de contenus à caractère terroriste en ligne, des propositions sur les preuves électroniques [COM(2018) 225 et 226] une fois qu'elles auront été adoptées, du [de la proposition de] règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE, ainsi que de la coopération internationale dans ce domaine fondée, en particulier, sur la convention de 2001 du Conseil de l'Europe sur la cybercriminalité («convention de Budapest»). Le présent règlement est sans préjudice des compétences des États membres en ce qui concerne les activités relatives à la sécurité publique, à la défense et à la sécurité nationale conformément au droit de l'Union, et les activités des autorités douanières relatives à la gestion des risques et, en général, à la vérification du respect du code des douanes par les opérateurs économiques.

(11) Le présent règlement ne devrait pas avoir d'incidence sur les dispositions de droit de l'Union qui fixent des exigences en matière de conception physique et de données que les produits doivent remplir pour pouvoir être mis sur le marché de l'Union.

(12) Le présent règlement complète, sans y porter atteinte, les dispositions de droit de l'Union qui visent à définir les exigences en matière d'accessibilité applicables à certains produits et services, en particulier la directive 2019/882[62].

(13) Le présent règlement est sans préjudice des compétences des États membres en ce qui concerne les activités relatives à la sécurité publique, à la défense et à la sécurité nationale conformément au droit de l'Union, et les activités des autorités douanières relatives à la gestion des risques et, en général, à la vérification du respect du code des douanes par les opérateurs économiques.

(14) Les produits physiques qui, au moyen de leurs composants, obtiennent, génèrent ou recueillent des données concernant leur performance, leur utilisation ou leur environnement et qui sont en mesure de communiquer ces données par l'intermédiaire d'un service de communications électroniques accessible au public (souvent appelé «l'internet des objets») devraient relever du présent règlement. Les services de communications électroniques comprennent les réseaux téléphoniques terrestres, les réseaux câblés de télévision, les réseaux par satellite et les réseaux de communication en champ proche. De tels produits peuvent inclure les véhicules, les équipements domestiques et les biens de consommation, les dispositifs médicaux et sanitaires ou encore les machines agricoles et industrielles. Les données, qui représentent la numérisation des actions de l'utilisateur et des événements concernant l'utilisation que ce dernier fait du produit, devraient, dès lors, être accessibles à l'utilisateur, tandis que les informations obtenues ou déduites de ces données, lorsqu'elles sont détenues légalement, ne devraient pas être considérées comme relevant du champ d'application du présent règlement. De telles données sont potentiellement précieuses pour l'utilisateur et favorisent l'innovation et le développement de services numériques et d'autres services protégeant l'environnement, la santé et l'économie circulaire, notamment en facilitant l'entretien et la réparation des produits en question.

(15) À l'inverse, certains produits qui sont principalement conçus pour afficher ou jouer des contenus, ou pour en enregistrer et en transmettre, entre autres à des fins

[62] Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services (JO L 151 du 7.6.2019, p. 70).

d'utilisation par un service en ligne ne devraient pas relever du présent règlement. De tels produits comprennent, par exemple, les ordinateurs personnels, serveurs, tablettes et smart phones, les caméras, webcams, systèmes d'enregistrement du son et scanners de texte. Ils nécessitent une intervention humaine pour produire diverses formes de contenu, telles que des documents texte, des fichiers sonores, des fichiers vidéo, des jeux et des cartes numériques.

(16) Il est nécessaire d'établir des règles applicables aux produits connectés qui intègrent un service ou sont interconnectés avec celui-ci d'une manière telle que l'absence de ce service empêcherait le produit de remplir ses fonctions. Ces services liés peuvent faire partie du contrat de vente ou de location, ou alors de tels services sont habituellement fournis pour des produits du même type et l'utilisateur pourrait raisonnablement s'attendre à ce qu'ils soient fournis étant donné la nature du produit et compte tenu de toute déclaration publique faite par le vendeur, le bailleur ou d'autres personnes situées en amont de la chaîne de transactions, y compris le fabricant, ou pour leur compte. Ces services liés peuvent eux-mêmes générer des données de valeur pour l'utilisateur indépendamment des capacités de collecte de données du produit avec lequel ils sont interconnectés. Le présent règlement devrait également s'appliquer à un service lié qui n'est pas fourni par le vendeur ou le bailleur lui-même, mais qui est fourni, conformément au contrat de vente ou de location, par un tiers. En cas de doute sur la question de savoir si la fourniture de services fait ou non partie du contrat de vente ou de location, il conviendrait d'appliquer le présent règlement.

(17) Les données générées par l'utilisation d'un produit ou d'un service lié incluent les données enregistrées intentionnellement par l'utilisateur. De telles données comprennent également les données générées en tant que sous-produit de l'action de l'utilisateur, telles que les données de diagnostic, celles générées sans aucune action de la part de l'utilisateur, comme lorsque le produit est en «mode veille», et les données enregistrées pendant les périodes au cours desquelles le produit est éteint. De telles données devraient inclure les données dans la forme et le format dans lesquels elles sont générées par le produit mais elles ne devraient pas concerner les données résultant d'un procédé logiciel qui calcule les données dérivées provenant de telles données parce que ce procédé logiciel est susceptible d'être soumis à des droits de propriété intellectuelle.

(18) Il conviendrait d'entendre par utilisateur d'un produit la personne morale ou physique, telle qu'une entreprise ou un consommateur, qui a acheté ou loué le produit. En fonction du titre juridique en vertu duquel il utilise ce produit, cet utilisateur supporte les risques et bénéficie des avantages que présente l'utilisation du produit connecté et il devrait également avoir accès aux données que ce produit génère. L'utilisateur devrait par conséquent avoir le droit de tirer parti des données générées par ce produit et par tout service lié.

(19) En pratique, les données générées par des produits ou des services liés ne sont pas toutes aisément accessibles à leurs utilisateurs et les possibilités de portabilité des données générées par les produits connectés à l'internet des objets sont souvent limitées. Les utilisateurs ne sont pas en mesure d'obtenir les données nécessaires pour recourir à des fournisseurs de services de réparation et d'autres services, tandis que les entreprises sont dans l'impossibilité de lancer des services innovants, plus efficaces et plus pratiques. Dans de nombreux secteurs, les fabricants peuvent souvent déterminer, par le contrôle qu'ils exercent sur la conception technique du produit ou des services liés, la nature des données générées et les modalités d'accès à ces données, même s'ils n'ont légalement aucun droit sur ces données. Il est par conséquent nécessaire de

veiller à ce que les produits soient conçus et fabriqués et à ce que les services liés soient fournis de telle sorte que les données générées par leur utilisation soient toujours facilement accessibles à l'utilisateur.

(20) Dans le cas où plusieurs personnes ou entités seraient propriétaires d'un produit ou seraient parties à un contrat de location et bénéficieraient de l'accès à un service lié, il conviendrait de consentir des efforts raisonnables en ce qui concerne la conception du produit ou du service lié ou de l'interface correspondante, de sorte que toutes les personnes puissent avoir accès aux données qu'elles génèrent. Les utilisateurs de produits qui génèrent des données ont généralement besoin de créer un compte d'utilisateur. Cela permet l'identification de l'utilisateur par le fabricant et constitue un moyen de communication pour effectuer des demandes d'accès aux données et les traiter. Les fabricants ou concepteurs d'un produit qui est généralement utilisé par plusieurs personnes devraient mettre en place le mécanisme nécessaire permettant la coexistence de comptes d'utilisateur distincts pour différentes personnes, s'il y a lieu, ou permettant à plusieurs personnes d'utiliser le même compte d'utilisateur. L'accès devrait être accordé à l'utilisateur au moyen de mécanismes de simple demande permettant l'exécution automatique, sans que le fabricant ou le détenteur de données ne soit tenu d'examiner ou d'approuver la demande. Cela signifie que les données ne devraient être mises à disposition que lorsque l'utilisateur le souhaite effectivement. Lorsqu'il n'est pas possible de procéder à l'exécution automatique de la demande d'accès aux données, par exemple au moyen d'un compte d'utilisateur ou d'une application mobile fournie avec le produit ou le service, le fabricant devrait informer l'utilisateur des modalités d'accès aux données.

(21) Les produits peuvent être conçus de façon à ce que certaines données soient directement disponibles à partir d'un dispositif de stockage intégré à l'appareil ou d'un serveur distant auquel les données sont communiquées. L'accès à ce dispositif de stockage de données peut être rendu possible par l'intermédiaire de réseaux locaux câblés ou sans fil connectés soit à un service de communications électroniques accessible au public, soit à un réseau mobile. Pour ce qui est du serveur, il peut s'agir de la propre capacité de serveur locale du fabricant ou de celle d'un tiers ou d'un fournisseur de services en nuage qui fait fonction de détenteur de données. Les produits peuvent être conçus pour permettre à l'utilisateur ou à un tiers de traiter les données relatives au produit ou à une instance informatique du fabricant.

(22) Les assistants virtuels jouent un rôle croissant dans la dématérialisation de l'environnement des consommateurs et servent d'interface facile à utiliser pour jouer des contenus, obtenir des informations ou activer des objets physiques connectés à l'internet des objets. Ils peuvent servir de portail unique dans un environnement domestique intelligent, par exemple, et enregistrer des quantités importantes de données utiles sur la manière dont les utilisateurs interagissent avec les produits connectés à l'internet des objets, dont ceux fabriqués par d'autres parties, et ils peuvent remplacer l'utilisation d'interfaces fournies par le fabricant telles que des écrans tactiles ou des applications pour smartphones. L'utilisateur pourrait souhaiter mettre ces données à la disposition de fabricants tiers et ainsi permettre l'avènement de services domotiques nouveaux. Ces assistants virtuels devraient relever du droit d'accès aux données prévu par le présent règlement également en ce qui concerne, d'une part, les données enregistrées avant l'activation de l'assistant virtuel par le mot déclencheur et, d'autre part, les données générées lorsqu'un utilisateur interagit avec un produit par l'intermédiaire d'un assistant virtuel fourni par une entité autre que le fabricant du produit. Toutefois, seules les données provenant de l'interaction entre

l'utilisateur et le produit par l'intermédiaire de l'assistant virtuel relèvent du champ d'application du présent règlement. Les données produites par l'assistant virtuel qui sont sans rapport avec l'utilisation d'un produit ne sont pas l'objet du présent règlement.

(23) Avant la conclusion d'un contrat relatif à l'achat ou à la location d'un produit ou à la fourniture d'un service lié, l'utilisateur devrait recevoir des informations claires et suffisantes sur les modalités d'accès aux données générées. Cette obligation permet de garantir la transparence quant aux données générées et accroît la facilité d'accès pour l'utilisateur. Cette obligation d'information ne porte pas atteinte à l'obligation incombant au responsable du traitement de fournir des informations à la personne concernée en application des articles 12, 13 et 14 du règlement (UE) 2016/679.

(24) Le présent règlement impose aux détenteurs de données de mettre des données à disposition dans certaines circonstances. Dans la mesure où des données à caractère personnel sont traitées, le détenteur de données devrait faire fonction de responsable du traitement au sens du règlement (UE) 2016/679. Lorsque les utilisateurs sont des personnes concernées, les détenteurs de données devraient être tenus de leur donner accès à leurs données et de mettre ces dernières à la disposition de tiers choisis par l'utilisateur conformément au présent règlement. Toutefois, le présent règlement ne crée pas de base juridique fondée sur le règlement (UE) 2016/679 permettant au détenteur de données d'accorder l'accès à des données à caractère personnel ou de mettre celles-ci à la disposition d'un tiers à la demande d'un utilisateur qui n'est pas une personne concernée et il ne devrait pas être interprété comme conférant au détenteur de données un droit nouveau d'utiliser les données générées par l'utilisation d'un produit ou d'un service lié. Cela vaut en particulier lorsque le fabricant est le détenteur de données. Dans ce dernier cas, l'utilisation de données à caractère non personnel par le fabricant devrait être fondée sur un accord contractuel entre le fabricant et l'utilisateur. Cet accord pourrait faire partie du contrat de vente ou de location relatif au produit. Toute clause contractuelle stipulant que le détenteur de données peut utiliser les données générées par l'utilisateur d'un produit ou d'un service lié devrait être transparente pour l'utilisateur, y compris en ce qui concerne la finalité pour laquelle le détenteur de données a l'intention d'utiliser ces données. Le présent règlement ne devrait pas faire obstacle à des conditions contractuelles ayant pour effet d'exclure ou de limiter l'utilisation des données, ou de certaines catégories d'entre elles, par le détenteur de données. Le présent règlement ne devrait pas non plus faire obstacle aux exigences réglementaires sectorielles prévues par le droit de l'Union, ou par le droit national compatible avec le droit de l'Union, qui excluraient ou limiteraient l'utilisation de certaines de ces données par le détenteur de données pour des raisons d'ordre public bien définies.

(25) Dans les secteurs caractérisés par la concentration d'un petit nombre de fabricants qui approvisionnent les utilisateurs finaux, ces derniers ne disposent que d'options limitées pour ce qui est du partage de données avec ces fabricants. En pareilles circonstances, il se peut que les accords contractuels ne suffisent pas pour atteindre l'objectif de responsabilisation des utilisateurs. Les données tendent à rester sous le contrôle des fabricants, de sorte qu'il est difficile pour les utilisateurs d'obtenir de la valeur à partir des données générées par les équipements qu'ils achètent ou qu'ils louent. En conséquence, la possibilité pour les petites entreprises innovantes de proposer des solutions fondées sur les données de manière compétitive et en faveur d'une économie des données diversifiée en Europe est limitée. Le présent règlement devrait par conséquent s'appuyer sur les évolutions récentes survenues dans certains

secteurs, telles que le code de conduite pour le partage des données agricoles par accord contractuel. Des actes législatifs sectoriels pourraient être présentés pour répondre à des besoins et objectifs sectoriels. De surcroît, le détenteur de données ne devrait utiliser aucune donnée générée par l'utilisation du produit ou du service lié afin d'obtenir des informations sur la situation économique, les actifs ou les méthodes de production de l'utilisateur, ou sur l'utilisation d'une quelconque autre manière que ce dernier fait du produit ou du service lié, qui sont susceptibles de porter atteinte à la position commerciale de l'utilisateur sur les marchés où celui-ci est actif. Cela impliquerait, par exemple, d'utiliser des connaissances relatives aux performances globales d'une entreprise ou d'une exploitation agricole à l'occasion de négociations contractuelles avec l'utilisateur sur l'acquisition potentielle de produits ou de produits agricoles de l'utilisateur au détriment de ce dernier ou, par exemple, d'utiliser ces informations pour alimenter des bases de données plus vastes et agrégées relatives à certains marchés (par exemple, des bases de données sur les rendements des cultures pour la prochaine saison de récolte) parce qu'une telle utilisation pourrait avoir des répercussions négatives indirectes sur l'utilisateur. Il conviendrait de doter l'utilisateur de l'interface technique nécessaire pour lui permettre de gérer les autorisations, qui comprendrait de préférence des options d'autorisation par niveau (telles que «autoriser une fois» ou «autoriser lors de l'utilisation de cette application ou de ce service»), y compris l'option de retirer l'autorisation.

(26) En ce qui concerne les contrats conclus entre un détenteur de données et un consommateur en tant qu'utilisateur d'un produit ou d'un service lié générant des données, la directive 93/13/CEE s'applique aux clauses de ces contrats afin de garantir que le consommateur ne soit pas soumis à des clauses contractuelles abusives. Pour ce qui concerne les clauses contractuelles abusives imposées unilatéralement à une micro, petite ou moyenne entreprise au sens de l'article 2 de l'annexe de la recommandation 2003/361/CE[63], le présent règlement prévoit que de telles clauses abusives ne devraient pas lier ladite entreprise.

(27) Le détenteur de données peut exiger une identification appropriée de l'utilisateur pour vérifier que ce dernier a le droit d'accéder aux données. Dans le cas de données à caractère personnel traitées par un sous-traitant pour le compte du responsable du traitement, le détenteur de données devrait veiller à ce que la demande d'accès soit reçue et traitée par le sous-traitant.

(28) L'utilisateur devrait être libre d'utiliser les données à toutes fins licites. Il peut notamment s'agir de transmettre les données que l'utilisateur a reçues en exerçant le droit prévu par le présent règlement à un tiers proposant un service après-vente qui peut être en concurrence avec un service fourni par le détenteur de données, ou de donner instruction au détenteur de données de le faire. Le détenteur de données devrait veiller à ce que les données mises à la disposition du tiers soient aussi exactes, complètes, fiables, pertinentes et à jour que les données auxquelles lui-même a le droit d'avoir accès, ou peut avoir accès, du fait de l'utilisation du produit ou du service lié. Tout secret d'affaires ou droit de propriété intellectuelle devrait être respecté lors du traitement des données. Il importe de préserver les incitations à investir dans des produits dotés de fonctionnalités fondées sur l'utilisation de données provenant de capteurs intégrés dans ces produits. Le présent règlement devrait donc être interprété comme ayant pour objet de favoriser le développement de nouveaux produits et services liés innovants, de stimuler l'innovation sur les marchés de l'après-vente, mais

[63] Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises.

aussi de favoriser le développement de services entièrement nouveaux utilisant les données, y compris sur la base de données provenant de divers produits ou services liés. Il vise dans le même temps à éviter que les incitations à l'investissement soient fragilisées pour le type de produit à partir duquel les données sont obtenues, par exemple du fait de l'utilisation des données pour développer un produit concurrent.

(29) Un tiers auquel des données sont mises à disposition peut être une entreprise, un organisme de recherche ou un organisme à but non lucratif. En mettant les données à la disposition du tiers, le détenteur de données devrait s'abstenir d'abuser de sa position pour rechercher un avantage concurrentiel sur des marchés où lui-même et le tiers peuvent être en concurrence directe. Le détenteur de données ne devrait donc utiliser aucune donnée générée par l'utilisation du produit ou du service lié pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production du tiers, ou sur l'utilisation d'une quelconque autre manière que ce dernier fait du produit ou du service lié, qui sont susceptibles de porter atteinte à la position commerciale du tiers sur les marchés où celui-ci est actif.

(30) L'utilisation d'un produit ou d'un service lié peut, en particulier lorsque l'utilisateur est une personne physique, générer des données se rapportant à une personne physique identifiée ou identifiable (la personne concernée). Le traitement de ces données est soumis aux règles établies par le règlement (UE) 2016/679, y compris lorsque les données à caractère personnel et non personnel figurant dans un ensemble de données sont inextricablement liées[64]. La personne concernée peut être l'utilisateur ou une autre personne physique. Les données à caractère personnel ne peuvent être demandées que par un responsable du traitement ou une personne concernée. Un utilisateur qui est la personne concernée a, dans certaines circonstances, le droit en vertu du règlement (UE) 2016/679 d'accéder aux données à caractère personnel le concernant, et le présent règlement ne porte pas atteinte à ce droit. En vertu du présent règlement, l'utilisateur qui est une personne physique a également le droit d'accéder à toutes les données générées par le produit, qu'elles soient à caractère personnel ou non personnel. Lorsque l'utilisateur n'est pas la personne concernée mais une entreprise, y compris un entrepreneur individuel, sauf en cas d'usage domestique partagé du produit, l'utilisateur sera un responsable du traitement au sens du règlement (UE) 2016/679. En conséquence, un utilisateur, qui, en tant que responsable du traitement, a l'intention de demander des données à caractère personnel générées par l'utilisation d'un produit ou d'un service lié, est tenu de disposer d'une base juridique pour le traitement des données au titre de l'article 6, paragraphe 1, du règlement (UE) 2016/679, comme le consentement de la personne concernée ou un intérêt légitime. Cet utilisateur devrait veiller à ce que la personne concernée soit dûment informée des finalités spécifiées, explicites et légitimes du traitement de ces données et de la manière dont elle peut exercer effectivement ses droits. Lorsque le détenteur de données et l'utilisateur sont des responsables conjoints du traitement au sens de l'article 26 du règlement (UE) 2016/679, ils sont tenus de déterminer, de manière transparente, au moyen d'un accord entre eux, leurs responsabilités respectives quant au respect dudit règlement. Il convient de comprendre qu'un tel utilisateur, une fois que les données ont été mises à sa disposition, peut à son tour devenir détenteur de données s'il remplit les critères prévus par le présent règlement et est donc soumis aux obligations de mise à disposition des données prévues par le présent règlement.

64 JO L 303 du 28.11.2018, p. 59.

(31) Les données générées par l'utilisation d'un produit ou d'un service lié ne devraient être mises à la disposition d'un tiers qu'à la demande de l'utilisateur. Le présent règlement complète donc le droit prévu à l'article 20 du règlement (UE) 2016/679. Ledit article prévoit le droit pour les personnes concernées de recevoir les données à caractère personnel les concernant dans un format structuré, couramment utilisé et lisible par machine, et de les transférer à d'autres responsables du traitement, lorsque ces données sont traitées sur la base de l'article 6, paragraphe 1, point a), ou de l'article 9, paragraphe 2, point a), ou sur la base d'un contrat en application de l'article 6, paragraphe 1, point b). Les personnes concernées ont également le droit de faire transmettre les données à caractère personnel directement d'un responsable du traitement à un autre, mais uniquement lorsque cela est techniquement possible. L'article 20 indique qu'il porte sur les données fournies par la personne concernée, mais ne précise pas si cela nécessite un comportement actif de la part de la personne concernée ou s'il s'applique également aux situations dans lesquelles un produit ou un service lié, par sa conception, observe le comportement d'une personne concernée ou d'autres informations en rapport avec une personne concernée de manière passive. Le droit prévu par le présent règlement complète de plusieurs manières le droit de recevoir et de transférer des données à caractère personnel prévu à l'article 20 du règlement (UE) 2016/679. Il accorde aux utilisateurs le droit d'accéder à toutes données générées par l'utilisation d'un produit ou d'un service lié et de mettre celles-ci à la disposition d'un tiers, quelle que soit leur nature en tant que données à caractère personnel, sans distinction entre les données activement fournies et les données observées passivement, et quelle que soit la base juridique du traitement. À la différence des obligations techniques prévues à l'article 20 du règlement (UE) 2016/679, le présent règlement rend obligatoire et garantit la faisabilité technique de l'accès des tiers à tous les types de données relevant de son champ d'application, qu'elles soient à caractère personnel ou non personnel. Il permet également au détenteur de données de fixer une compensation raisonnable à la charge des tiers, mais pas de l'utilisateur, pour tous frais encourus liés à l'octroi d'un accès direct aux données générées par le produit de l'utilisateur. Si un détenteur de données et un tiers ne sont pas en mesure de s'entendre sur les conditions d'un tel accès direct, la personne concernée ne devrait en aucun cas être empêchée d'exercer les droits prévus par le règlement (UE) 2016/679, y compris le droit à la portabilité des données, en introduisant un recours conformément audit règlement. Il convient de comprendre dans ce contexte que, conformément au règlement (UE) 2016/679, un accord contractuel ne permet pas le traitement de catégories particulières de données à caractère personnel par le détenteur de données ou le tiers.

(32) L'accès à toutes les données stockées dans les équipements terminaux et consultables à partir de ces derniers est soumis à la directive 2002/58/CE et requiert le consentement de l'abonné ou de l'utilisateur au sens de ladite directive, à moins qu'il ne soit strictement nécessaire à la fourniture d'un service de la société de l'information expressément demandé par l'utilisateur ou l'abonné (ou aux seules fins de la transmission d'une communication). La directive 2002/58/CE («directive vie privée et communications électroniques») (et la proposition de règlement «vie privée et communications électroniques») protège l'intégrité de l'équipement terminal de l'utilisateur en ce qui concerne l'utilisation des capacités de traitement et de stockage et la collecte d'informations. Les équipements de l'internet des objets sont considérés comme des équipements terminaux s'ils sont directement ou indirectement connectés à un réseau de communications public.

(33) Afin d'empêcher l'exploitation des utilisateurs, les tiers auxquels des données ont été mises à disposition à la demande de l'utilisateur ne devraient traiter les données aux fins convenues avec l'utilisateur et les partager avec un autre tiers que si cela est nécessaire pour fournir le service demandé par l'utilisateur.

(34) Conformément au principe de minimisation des données, le tiers ne devrait avoir accès qu'aux informations supplémentaires nécessaires à la fourniture du service demandé par l'utilisateur. Après avoir obtenu l'accès aux données, le tiers devrait traiter celles-ci exclusivement aux fins convenues avec l'utilisateur, sans ingérence du détenteur des données. Il devrait être aussi facile pour l'utilisateur de refuser ou d'interrompre l'accès aux données par le tiers que d'autoriser cet accès. Le tiers devrait s'abstenir de contraindre, tromper ou manipuler l'utilisateur de quelque manière que ce soit, en nuisant ou en portant atteinte à l'autonomie, à la prise de décision ou aux choix de l'utilisateur, y compris au moyen d'une interface numérique avec l'utilisateur. Dans ce contexte, les tiers devraient s'abstenir de recourir à des pièges à utilisateurs lors de la conception de leurs interfaces numériques. Ces pièges à utilisateurs sont des techniques de conception qui poussent les consommateurs à prendre des décisions indésirables susceptibles d'avoir des conséquences négatives pour eux ou qui les induisent en erreur à cette fin. L'utilisation de ces techniques de manipulation peut avoir pour but de persuader les utilisateurs, notamment les consommateurs vulnérables, d'adopter des comportements indésirables, de tromper les utilisateurs en les poussant à prendre des décisions relatives aux opérations de divulgation d'informations, ou de biaiser exagérément la décision des utilisateurs du service, d'une manière qui sape ou altère leur autonomie, leur décision et leur choix. Les pratiques commerciales communes et légitimes qui sont conformes au droit de l'Union ne devraient pas en soi être considérées comme des pièges à utilisateurs. Les tiers devraient respecter les obligations qui leur incombent en vertu du droit de l'Union pertinent, en particulier les exigences énoncées dans la directive 2005/29/CE, la directive 2011/83/UE, la directive 2000/31/CE et la directive 98/6/CE.

(35) Le tiers devrait également s'abstenir d'utiliser les données pour identifier des personnes, à moins que les activités de traitement concernées ne soient strictement nécessaires pour fournir le service demandé par l'utilisateur. L'obligation de supprimer les données lorsqu'elles ne sont plus nécessaires à la finalité convenue avec l'utilisateur complète le droit à l'effacement conféré à la personne concernée en application de l'article 17 du règlement (UE) 2016/679. Lorsque le tiers est un fournisseur d'un service d'intermédiation de données au sens de [règlement sur la gouvernance des données], les garanties pour la personne concernée prévues par ledit règlement s'appliquent. Le tiers peut utiliser les données pour développer un produit nouveau et innovant ou un service lié, mais pas pour développer un produit concurrent.

(36) Les start-up, les petites et moyennes entreprises et les entreprises des secteurs traditionnels dont les capacités numériques sont moins poussées peinent à obtenir l'accès aux données pertinentes. Le présent règlement vise à faciliter l'accès de ces entités aux données, tout en veillant à ce que les obligations correspondantes aient une portée aussi proportionnée que possible afin d'éviter tout excès. Dans le même temps, un petit nombre de très grandes entreprises ont vu le jour qui possèdent une puissance économique considérable dans l'économie numérique grâce à l'accumulation et à l'agrégation de volumes considérables de données ainsi qu'à l'infrastructure technologique nécessaire à leur monétisation. Parmi ces entreprises figurent des sociétés qui fournissent des services de plateforme essentiels contrôlant des

écosystèmes de plateformes entiers au sein de l'économie numérique, que les opérateurs du marché existants ou nouveaux sont incapables de concurrencer ou de contester. Le [règlement relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques)] vise à remédier à ces manques d'efficacité et déséquilibres en permettant à la Commission de désigner un fournisseur en tant que «contrôleur d'accès», et impose à ces contrôleurs d'accès désignés un certain nombre d'obligations, dont l'interdiction de combiner certaines données sans consentement, et l'obligation de garantir un droit effectif à la portabilité des données en vertu de l'article 20 du règlement (UE) 2016/679. Conformément au [règlement sur les marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques)], et compte tenu de la capacité sans égale de ces entreprises en matière d'acquisition de données, il ne serait pas nécessaire, pour atteindre l'objectif du présent règlement, et serait donc disproportionné à l'égard des détenteurs de données soumis à de telles obligations, d'inclure ces entreprises désignées contrôleur d'accès parmi les bénéficiaires du droit d'accès aux données. Cela signifie qu'une entreprise fournissant des services de plateforme essentiels qui a été désignée comme contrôleur d'accès ne peut demander ou se voir accorder l'accès aux données des utilisateurs générées par l'utilisation d'un produit ou d'un service lié ou par un assistant virtuel sur la base des dispositions du chapitre II du présent règlement. Une entreprise fournissant des services de plateforme essentiels désignée comme contrôleur d'accès en vertu de la législation sur les marchés numériques devrait s'entendre comme incluant toutes les entités juridiques d'un groupe de sociétés lorsqu'une entité juridique fournit un service de plateforme essentiel. En outre, les tiers auxquels des données sont mises à disposition, à la demande de l'utilisateur, ne peuvent pas mettre celles-ci à la disposition d'un contrôleur d'accès désigné. Par exemple, le tiers ne peut sous-traiter la fourniture d'un service à un contrôleur d'accès. Cela n'empêche toutefois pas que des tiers puissent recourir aux services de traitement de données offerts par un contrôleur d'accès désigné. Cette exclusion des contrôleurs d'accès désignés du champ d'application du droit d'accès prévu par le présent règlement n'empêche pas ces entreprises d'obtenir des données par d'autres moyens licites.

(37) Compte tenu de l'état actuel de la technologie, il serait trop lourd d'imposer d'autres obligations en matière de conception pour les produits fabriqués ou conçus et les services liés fournis par les micro et petites entreprises. Tel n'est toutefois pas le cas lorsqu'une micro ou petite entreprise travaille en sous-traitance pour la fabrication ou la conception d'un produit. Dans ce cas, l'entreprise, qui a pris la micro ou petite entreprise comme sous-traitant, est en mesure d'accorder au sous-traitant une compensation appropriée. Une micro ou petite entreprise peut néanmoins être soumise aux exigences fixées par le présent règlement en tant que détenteur de données, lorsqu'elle n'est pas le fabricant du produit ou un fournisseur de services liés.

(38) Le présent règlement contient des règles générales d'accès applicables chaque fois qu'un détenteur de données est tenu, en vertu de la législation, de mettre des données à la disposition d'un destinataire de données. Cet accès devrait être fondé sur des conditions équitables, raisonnables, non discriminatoires et transparentes afin de garantir la cohérence des pratiques de partage de données dans le marché intérieur, y compris entre les secteurs, et d'encourager et de promouvoir des pratiques équitables de partage des données, même dans les domaines où un tel droit d'accès aux données n'est pas accordé. Ces règles générales d'accès ne s'appliquent pas aux obligations de mise à disposition de données prévues par le règlement (UE) 2016/679. Le partage volontaire de données n'est pas compromis par ces règles.

(39) Sur la base du principe de la liberté contractuelle, les parties devraient rester libres de négocier les conditions précises de mise à disposition de données dans leurs contrats, dans le cadre des règles générales d'accès pour la mise à disposition de données.

(40) Afin de garantir que les conditions d'accès obligatoire aux données soient équitables pour les deux parties, les règles générales relatives aux droits d'accès aux données devraient faire référence à la règle visant à éviter les clauses contractuelles abusives.

(41) Afin de compenser le manque d'informations sur les conditions des différents contrats, qui complique la tâche du destinataire des données s'agissant de déterminer si les conditions de mise à disposition des données sont non discriminatoires, il devrait incomber au détenteur de données de démontrer la nature non discriminatoire d'une clause contractuelle. N'est pas constitutif d'une discrimination illicite le fait qu'un détenteur de données ait recours à des clauses contractuelles différentes pour la mise à disposition des données ou à des compensations différentes, si ces différences sont justifiées par des raisons objectives. Ces obligations sont sans préjudice du règlement (UE) 2016/679.

(42) Afin d'encourager la poursuite des investissements dans la production de données précieuses, y compris dans les outils techniques pertinents, le présent règlement consacre le principe selon lequel le détenteur de données peut demander une compensation raisonnable lorsqu'il est légalement tenu de mettre des données à la disposition du destinataire des données. Ces dispositions ne doivent pas être interprétées comme prévoyant le paiement des données elles-mêmes, mais le paiement, dans le cas des micro, petites et moyennes entreprises, des frais encourus et des investissements nécessaires pour mettre des données à disposition.

(43) Dans des cas justifiés, y compris la nécessité de préserver la participation des consommateurs et la concurrence ou de promouvoir l'innovation sur certains marchés, le droit de l'Union ou la législation nationale mettant en œuvre le droit de l'Union peut imposer une compensation réglementée pour la mise à disposition de types de données spécifiques.

(44) Afin de protéger les micro, petites et moyennes entreprises contre des charges économiques excessives qui les pénaliseraient trop sur le plan commercial pour élaborer et appliquer des modèles d'entreprise innovants, la compensation pour la mise à disposition de données à leur charge ne devrait pas dépasser le coût direct de cette mise à disposition et être non discriminatoire.

(45) Les coûts directs liés à la mise à disposition de données sont les frais encourus pour la reproduction, la diffusion par voie électronique et le stockage des données, mais pas pour la collecte ou la production des données. Les coûts directs liés à la mise à disposition de données devraient être limités à la part imputable aux demandes individuelles, compte tenu du fait que les interfaces techniques nécessaires ou les logiciels et la connectivité connexes devront être installés de manière permanente par le détenteur des données. Des accords à long terme entre les détenteurs de données et les destinataires des données, par exemple au moyen d'un modèle d'abonnement, pourraient réduire les coûts liés à la mise à disposition de données lors d'opérations régulières ou répétitives dans le cadre d'une relation commerciale.

(46) Il n'est pas nécessaire d'intervenir en cas de partage de données entre grandes entreprises ou lorsque le détenteur des données est une petite ou moyenne entreprise et que le destinataire des données est une grande entreprise. Dans ces cas, les entreprises sont considérées comme capables de négocier toute compensation pour autant que

celle-ci soit raisonnable, compte tenu d'éléments tels que le volume, le format, la nature, l'offre et la demande des données ainsi que les coûts liés à la collecte des données et à leur mise à disposition du destinataire des données.

(47) La transparence est un principe important pour garantir que la compensation demandée par le détenteur des données est raisonnable ou, dans le cas où le destinataire des données est une micro, petite ou moyenne entreprise, que la compensation n'excède pas les coûts directement liés à la mise à disposition des données au destinataire des données et est imputable à la demande individuelle. Afin de mettre le destinataire des données en mesure d'évaluer et de vérifier que la compensation satisfait aux exigences du présent règlement, le détenteur des données devrait fournir au destinataire des données les informations nécessaires au calcul de la compensation avec un degré de détail suffisant.

(48) Garantir l'accès à des modes de règlement extrajudiciaire des litiges nationaux et transfrontières liés à la mise à disposition de données devrait profiter aux détenteurs et aux destinataires de données et, partant, renforcer la confiance dans le partage des données. Dans les cas où les parties ne parviennent pas à s'entendre sur des conditions équitables, raisonnables et non discriminatoires de mise à disposition des données, les organismes de règlement des litiges devraient leur proposer une solution simple, rapide et peu coûteuse.

(49) Afin d'éviter que deux ou plusieurs organismes de règlement des litiges ne soient saisis du même litige, en particulier dans un contexte transfrontière, tout organisme de règlement des litiges devrait pouvoir rejeter une demande de règlement d'un litige qui a déjà été portée devant un autre organisme de règlement des litiges ou devant une cour ou un tribunal d'un État membre.

(50) Les parties à une procédure de règlement des litiges ne devraient pas être empêchées d'exercer leurs droits fondamentaux à un recours effectif et à accéder à un tribunal impartial. Par conséquent, la décision de saisir un organisme de règlement des litiges ne devrait pas priver ces parties de leur droit de demander réparation devant une juridiction d'un État membre.

(51) Lorsqu'une partie se trouve dans une position de négociation plus forte, il existe un risque que cette partie puisse exploiter cette position au détriment de l'autre partie contractante lors de la négociation de l'accès aux données et rendre l'accès aux données commercialement moins viable et parfois prohibitif sur le plan économique. Ces déséquilibres contractuels portent particulièrement préjudice aux micro, petites et moyennes entreprises qui ne disposent pas d'une capacité importante pour négocier les conditions d'accès aux données et qui n'ont peut-être pas d'autre choix que d'accepter des clauses contractuelles «à prendre ou à laisser». Par conséquent, les clauses contractuelles abusives régissant l'accès aux données et leur utilisation ou la responsabilité et les voies de recours en cas de violation ou de résiliation des obligations liées aux données ne devraient pas être contraignantes pour les micro, petites et moyennes entreprises lorsqu'elles leur ont été imposées unilatéralement.

(52) Les règles relatives aux clauses contractuelles devraient tenir compte du principe de la liberté contractuelle en tant que concept essentiel dans les relations interentreprises. Par conséquent, toutes les clauses contractuelles ne devraient pas être soumises à une appréciation du caractère abusif, mais uniquement aux clauses qui sont imposées unilatéralement aux micro, petites et moyennes entreprises. Il s'agit des situations du type «à prendre ou à laisser» dans lesquelles une partie fournit une certaine clause contractuelle et où la micro, petite ou moyenne entreprise ne peut pas influencer le

contenu de cette clause malgré une tentative de négociation. Une clause contractuelle qui est simplement fournie par une partie et acceptée par la micro, petite ou moyenne entreprise ou une clause négociée puis convenue sous forme modifiée entre les parties contractantes ne devrait pas être considérée comme imposée unilatéralement.

(53) En outre, les règles relatives aux clauses contractuelles abusives ne devraient s'appliquer qu'aux éléments d'un contrat qui sont liés à la mise à disposition de données, à savoir les clauses contractuelles concernant l'accès aux données et leur utilisation, ainsi que la responsabilité ou les voies de recours en cas de violation et de résiliation des obligations relatives aux données. Les autres parties du même contrat, qui ne sont pas liées à la mise à disposition de données, ne devraient pas être soumises à l'appréciation du caractère abusif prévue par le présent règlement.

(54) Les critères permettant d'identifier les clauses contractuelles abusives ne devraient s'appliquer qu'aux clauses contractuelles excessives, en cas d'abus de pouvoir de négociation supérieur. La grande majorité des clauses contractuelles qui sont commercialement plus favorables à une partie qu'à l'autre, y compris celles qui sont normales dans les contrats interentreprises, sont une expression normale du principe de la liberté contractuelle et continuent de s'appliquer.

(55) Si une clause contractuelle n'est pas incluse dans la liste des clauses qui sont toujours considérées comme abusives ou présumées abusives, la disposition générale sur le caractère abusif s'applique. À cet égard, les clauses énumérées en tant que clauses abusives devraient servir de critère d'interprétation de la disposition générale relative au caractère abusif. Enfin, des clauses contractuelles types pour les contrats de partage de données interentreprises que la Commission doit élaborer et recommander peuvent également être utiles aux parties commerciales lorsqu'elles négocient des contrats.

(56) En cas de besoin exceptionnel, les organismes du secteur public ou les institutions, organes ou organismes de l'Union peuvent être contraints d'utiliser des données détenues par une entreprise pour répondre à des urgences publiques ou dans d'autres cas exceptionnels. Les organismes exerçant une activité de recherche et les organisations finançant une activité de recherche pourraient aussi être organisés comme des organismes du secteur public ou des organismes de droit public. Afin de limiter la charge pesant sur les entreprises, les microentreprises et les petites entreprises devraient être exemptées de l'obligation de fournir des données aux organismes du secteur public et aux institutions, organes ou organismes de l'Union en cas de besoin exceptionnel.

(57) En cas de situations d'urgence publique, telles que les urgences de santé publique, les urgences résultant de la dégradation de l'environnement et les catastrophes naturelles majeures, y compris celles aggravées par le changement climatique, ainsi que les catastrophes majeures d'origine humaine, telles que les incidents majeurs de cybersécurité, l'intérêt public résultant de l'utilisation des données l'emportera sur l'intérêt des détenteurs de données à disposer librement des données qu'ils détiennent. Dans ce cas, les détenteurs de données devraient être tenus de les mettre à la disposition des organismes du secteur public ou des institutions, organes ou organismes de l'Union à leur demande. L'existence d'une urgence publique est déterminée conformément aux procédures respectives des États membres ou des organisations internationales compétentes.

(58) Un besoin exceptionnel peut également se présenter lorsqu'un organisme du secteur public peut démontrer que les données sont nécessaires soit pour prévenir une urgence publique, soit pour contribuer au rétablissement à la suite d'une urgence publique,

dans des circonstances raisonnablement proches de l'urgence publique en question. Lorsque le besoin exceptionnel n'est pas justifié par la nécessité de répondre à une urgence publique, de prévenir une urgence publique ou de contribuer au rétablissement à la suite d'une urgence publique, l'organisme du secteur public ou l'institution, l'organe ou l'organisme de l'Union devrait démontrer que l'absence d'accès en temps utile aux données demandées et d'utilisation de celles-ci les empêche de s'acquitter efficacement d'une mission spécifique d'intérêt public explicitement prévue par la loi. Un tel besoin exceptionnel peut également se produire dans d'autres situations, par exemple en ce qui concerne l'établissement en temps utile de statistiques officielles lorsque les données ne sont pas disponibles par ailleurs ou lorsque la charge pesant sur les répondants aux statistiques s'en trouvera considérablement réduite. Dans le même temps, l'organisme du secteur public ou l'institution, l'organe ou l'organisme de l'Union devrait, en dehors du cas où il s'agit de réagir à une urgence publique, de prévenir une urgence publique ou de contribuer au rétablissement à la suite d'une urgence publique, démontrer qu'il n'existe aucun autre moyen d'obtenir les données demandées et que les données ne peuvent être obtenues en temps utile en fixant les obligations de fourniture de données nécessaires dans la nouvelle législation.

(59) Le présent règlement ne devrait pas s'appliquer aux accords volontaires d'échange de données entre entités privées et publiques, ni s'y substituer. Le présent règlement ne devrait pas avoir d'incidence sur les obligations imposées aux détenteurs de données de fournir des données qui sont motivées par des besoins de nature non exceptionnelle, notamment lorsque l'éventail des données et des détenteurs de données est connu et que l'utilisation des données peut avoir lieu régulièrement, comme dans le cas des obligations de déclaration et des obligations relatives au marché intérieur. Il ne devrait pas non plus avoir d'incidence sur les exigences relatives à l'accès aux données visant à vérifier le respect des règles applicables, y compris dans les cas où des organismes du secteur public confient la tâche de vérification de la conformité à des entités autres que des organismes du secteur public.

(60) Pour l'exercice de leurs missions dans les domaines de la prévention et de la détection des infractions pénales et administratives, des enquêtes et des poursuites en la matière, de l'exécution de sanctions pénales et administratives, ainsi que de la collecte de données à des fins fiscales ou douanières, les organismes du secteur public et les institutions, organes et organismes de l'Union devraient faire valoir les pouvoirs qui leur sont conférés par la législation sectorielle. Le présent règlement ne porte donc pas atteinte aux instruments de partage, d'accès et d'utilisation des données dans ces domaines.

(61) Un cadre proportionné, limité et prévisible au niveau de l'Union est nécessaire pour que les détenteurs de données puissent, en cas de besoins exceptionnels, mettre les données à la disposition des organismes du secteur public et des institutions, organes ou organismes de l'Union, à la fois pour garantir la sécurité juridique et pour réduire au minimum les charges administratives pesant sur les entreprises. À cette fin, les demandes de données adressées par des organismes du secteur public et par des institutions, organes et organismes de l'Union aux détenteurs de données devraient être transparentes et proportionnées en ce qui concerne leur contenu et leur granularité. La finalité de la demande et l'utilisation prévue des données demandées devraient être spécifiques et clairement expliquées, tout en laissant à l'entité demandeuse une souplesse suffisante pour lui permettre d'accomplir ses missions d'intérêt public. La demande devrait également respecter les intérêts légitimes des entreprises auxquelles elle est adressée. La charge pesant sur les détenteurs de données devrait être réduite au

minimum en obligeant les entités requérantes à respecter le principe «une fois pour toutes», qui empêche que les mêmes données soient demandées plus d'une fois par plus d'un organisme du secteur public ou plus d'une institution, d'un organe ou d'un organisme de l'Union lorsque ces données sont nécessaires pour répondre à une urgence publique. Dans un souci de transparence, les demandes de données formulées par des organismes du secteur public et par des institutions, organes ou organismes de l'Union devraient être rendues publiques sans retard injustifié par l'entité qui demande les données et il convient de veiller à ce que toutes les demandes justifiées par une urgence publique soient mises à la disposition du public en ligne.

(62) L'objectif de l'obligation de fournir les données est de faire en sorte que les organismes du secteur public et les institutions, organes ou organismes de l'Union disposent des connaissances nécessaires pour réagir à une urgence publique, prévenir une urgence publique ou contribuer au rétablissement à la suite d'une urgence publique, ou encore maintenir la capacité d'accomplir des missions spécifiques expressément prévues par la loi. Les données obtenues par ces entités peuvent être commercialement sensibles. Par conséquent, la directive (UE) 2019/1024 du Parlement européen et du Conseil[65] ne devrait pas s'appliquer aux données mises à disposition en vertu du présent règlement qui ne devraient pas être considérées comme des données ouvertes disponibles pour une réutilisation par des tiers. Cela ne devrait toutefois pas avoir d'incidence sur l'applicabilité de la directive (UE) 2019/1024 à la réutilisation de statistiques officielles pour la production desquelles les données obtenues en vertu du présent règlement ont été utilisées, à condition que la réutilisation ne comprenne pas les données sous-jacentes. Cela ne devrait pas non plus porter atteinte à la possibilité de partager les données à des fins de recherche ou pour l'établissement de statistiques officielles, pour autant que les conditions énoncées dans le présent règlement soient satisfaites. Les organismes du secteur public devraient également être autorisés à échanger des données obtenues en vertu du présent règlement avec d'autres organismes du secteur public afin de répondre aux besoins exceptionnels pour lesquels les données ont été demandées.

(63) Les détenteurs de données devraient avoir la possibilité de demander soit une modification de la demande présentée par un organisme du secteur public ou une institution, un organe ou un organisme de l'Union, soit son annulation dans un délai de 5 ou 15 jours ouvrables en fonction de la nature du besoin exceptionnel invoqué dans la demande. En cas de demande motivée par une urgence publique, il devrait exister une raison justifiée de ne pas mettre les données à disposition s'il peut être démontré que la demande est similaire ou identique à une demande présentée précédemment pour la même finalité par un autre organisme du secteur public ou par une autre institution ou un autre organe ou organisme de l'Union. Un détenteur de données rejetant la demande ou demandant sa modification devrait communiquer à l'organisme du secteur public ou à l'institution, l'organe ou l'organisme de l'Union demandant les données la justification sous-jacente du refus de la demande. Si le droit *sui generis* lié à la base de données prévu par la directive 96/6/CE du Parlement européen et du Conseil[66] s'applique aux ensembles de données demandés, les détenteurs de données devraient exercer leur droit d'une manière qui n'empêche pas l'organisme du secteur

---

65 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).

66 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).

public et les institutions, organes ou organismes de l'Union d'obtenir les données, ou de les partager, conformément au présent règlement.

(64) Lorsqu'il est strictement nécessaire d'inclure des données à caractère personnel dans les données mises à la disposition d'un organisme du secteur public ou d'une institution, d'un organe ou d'un organisme de l'Union, les règles applicables en matière de protection des données à caractère personnel devraient être respectées et la mise à disposition des données et leur utilisation ultérieure devraient s'accompagner de garanties pour les droits et intérêts des personnes concernées par ces données. L'organisme qui demande les données devrait démontrer la stricte nécessité et les finalités spécifiques et limitées du traitement. Le détenteur de données devrait déployer des efforts raisonnables pour anonymiser les données ou, lorsque cette anonymisation s'avère impossible, il devrait appliquer des moyens technologiques tels que la pseudonymisation et l'agrégation, avant de mettre les données à disposition.

(65) Les données mises à la disposition des organismes du secteur public et des institutions, organes et organismes de l'Union en raison d'un besoin exceptionnel ne devraient être utilisées qu'aux fins pour lesquelles elles ont été demandées, à moins que le détenteur de données qui a mis les données à disposition n'ait expressément consenti à ce que les données soient utilisées à d'autres fins. Les données devraient être détruites dès lors qu'elles ne sont plus nécessaires à la finalité indiquée dans la demande, sauf accord contraire, et le détenteur des données devrait en être informé.

(66) Lors de la réutilisation des données fournies par les détenteurs de données, les organismes du secteur public et les institutions, organes ou organismes de l'Union devraient respecter à la fois la législation applicable en vigueur et les obligations contractuelles auxquelles le détenteur de données est soumis. Lorsque la divulgation de secrets d'affaires du détenteur de données à des organismes du secteur public ou à des institutions, organes ou organismes de l'Union est strictement nécessaire pour atteindre la finalité pour laquelle les données ont été demandées, la confidentialité de cette divulgation devrait être garantie au détenteur des données.

(67) Lorsque la sauvegarde d'un bien public important est en jeu, comme dans le cas d'une réponse apportée à une urgence publique, l'organisme du secteur public ou l'institution, l'organe ou l'organisme de l'Union ne devrait pas être tenu d'indemniser les entreprises pour les données obtenues. Les urgences publiques sont des événements rares et toutes ces urgences ne nécessitent pas l'utilisation de données détenues par des entreprises. Le fait que les organismes du secteur public ou les institutions, organes ou organismes de l'Union font usage du présent règlement ne devrait donc pas avoir des répercussions négatives sur les activités commerciales des détenteurs de données. Toutefois, étant donné que des besoins exceptionnels autres que la réponse à une urgence publique pourraient être plus fréquents, y compris les cas de prévention d'une urgence publique ou de rétablissement à la suite d'une urgence publique, les détenteurs de données devraient, dans de telles situations, avoir droit à une indemnisation raisonnable qui ne devrait pas dépasser les coûts techniques et organisationnels encourus pour se conformer à la demande et la marge raisonnable nécessaire pour mettre les données à la disposition de l'organisme du secteur public ou de l'institution, l'organe ou l'organisme de l'Union. L'indemnisation ne doit pas être comprise comme constituant le paiement des données proprement dites et comme étant obligatoire.

(68) L'organisme du secteur public ou l'institution, l'organe ou l'organisme de l'Union peut partager les données qu'il a obtenues à la suite de la demande avec d'autres entités ou personnes lorsque cela est nécessaire pour mener des activités de recherche

scientifique ou d'analyse qu'il ne peut pas réaliser lui-même. Ces données peuvent également être partagées dans les mêmes conditions avec les instituts nationaux de statistique et Eurostat pour l'établissement de statistiques officielles. Ces activités de recherche devraient toutefois être compatibles avec la finalité pour laquelle les données ont été demandées et le détenteur des données devrait être informé du partage ultérieur des données qu'il a fournies. Les personnes menant des activités de recherche ou les organismes de recherche avec lesquels ces données peuvent être partagées devraient agir soit dans un but non lucratif, soit dans le cadre d'une mission d'intérêt public reconnue par l'État. Les organismes sur lesquels des entreprises commerciales ont une influence déterminante leur permettant d'exercer un contrôle en raison d'éléments structurels, ce qui pourrait conduire à un accès préférentiel aux résultats des recherches, ne devraient pas être considérés comme des organismes de recherche aux fins du présent règlement.

(69) La capacité des clients de services de traitement de données, y compris de services en nuage et de services à la périphérie, de passer d'un service de traitement de données à un autre, tout en maintenant une fonctionnalité minimale du service, est une condition essentielle pour un marché plus concurrentiel, avec des barrières à l'entrée moins élevées pour les nouveaux fournisseurs de services.

(70) Le règlement (UE) 2018/1807 du Parlement européen et du Conseil encourage les fournisseurs de services à élaborer et à mettre en œuvre de manière efficace des codes de conduite par autorégulation couvrant les meilleures pratiques pour faciliter, entre autres, le changement de fournisseur de services de traitement de données et le portage des données. Compte tenu de l'efficacité limitée des cadres d'autorégulation mis au point à cette fin et de l'indisponibilité générale de normes et d'interfaces ouvertes, il est nécessaire d'adopter un ensemble d'obligations réglementaires minimales pour les fournisseurs de services de traitement de données afin d'éliminer les obstacles contractuels, économiques et techniques au passage effectif d'un service de traitement de données à un autre.

(71) Les services de traitement de données devraient couvrir les services qui permettent l'accès sur demande et l'accès large à distance à un ensemble modulable et variable de ressources informatiques distribuées et pouvant être partagées. Ces ressources informatiques comprennent des ressources telles que les réseaux, serveurs ou autres infrastructures virtuelles ou physiques, les systèmes d'exploitation, les logiciels, y compris les outils de développement de logiciels, le stockage, les applications et les services. La capacité du client du service de traitement de données de s'autofournir unilatéralement des capacités informatiques, comme du temps de serveur ou du stockage en réseau, sans aucune intervention humaine de la part du fournisseur de service pourrait être décrite comme une gestion sur demande. Le terme «accès large à distance» est utilisé pour décrire le fait que les capacités de calcul sont fournies sur le réseau et que l'accès à celles-ci se fait par des mécanismes encourageant le recours à des plateformes clients légères ou lourdes disparates (des navigateurs web aux appareils mobiles et aux postes de travail). Le terme «modulable» renvoie aux ressources informatiques qui sont attribuées d'une manière souple par le fournisseur de services de traitement de données, indépendamment de la localisation géographique de ces ressources, pour gérer les fluctuations de la demande. Les termes «ensemble variable» sont utilisés pour décrire les ressources informatiques qui sont mobilisées et libérées en fonction de la demande pour pouvoir augmenter ou réduire rapidement les ressources disponibles en fonction de la charge de travail. Les termes «pouvant être partagées» sont utilisés pour décrire les ressources informatiques qui sont mises à

disposition de nombreux utilisateurs qui partagent un accès commun au service, le traitement étant effectué séparément pour chaque utilisateur bien que le service soit fourni à partir du même équipement électronique. Le terme «distribué» est utilisé pour décrire les ressources informatiques qui se trouvent sur des ordinateurs ou des appareils en réseau différents, qui communiquent et se coordonnent par transmission de messages. Le terme «fortement distribué» est utilisé pour décrire les services de traitement de données qui impliquent un traitement de données plus proche du lieu où les données sont générées ou collectées, par exemple dans un dispositif de traitement de données connecté. Le traitement de données à la périphérie, qui est une forme de traitement de données fortement distribué, devrait générer de nouveaux modèles d'entreprise et de fourniture de services en nuage, qui devraient être ouverts et interopérables dès le départ

(72) Le présent règlement vise à faciliter le passage d'un service de traitement de données à un autre, ce qui englobe toutes les conditions et actions qui sont nécessaires pour qu'un client résilie un accord contractuel relatif à un service de traitement de données, conclue un ou plusieurs nouveaux contrats avec différents fournisseurs de services de traitement de données, transmette tous ses actifs numériques, y compris les données, aux autres fournisseurs concernés et continue à les utiliser dans le nouvel environnement tout en bénéficiant de l'équivalence fonctionnelle. Les actifs numériques désignent les éléments en format numérique pour lesquels le client a le droit d'utilisation, y compris les données, les applications, les machines virtuelles et d'autres réalisations des technologies de virtualisation, telles que la conteneurisation. L'équivalence fonctionnelle désigne le maintien d'un niveau minimal de fonctionnalité d'un service après le changement de fournisseur et devrait être considérée comme techniquement réalisable chaque fois que les services de traitement de données, aussi bien à l'origine qu'à destination couvrent (en tout ou en partie) le même type de service. Les métadonnées générées par l'utilisation d'un service par le client devraient également être portables conformément aux dispositions du présent règlement relatives au changement de fournisseur.

(73) Lorsque les fournisseurs de services de traitement de données sont à leur tour clients de services de traitement de données fournis par un prestataire tiers, ils bénéficieront eux-mêmes d'un changement de fournisseur plus efficace, tout en étant immanquablement liés par les obligations du présent règlement en ce qui concerne leurs propres offres de services.

(74) Les fournisseurs de services de traitement de données devraient être tenus d'offrir toute l'assistance et le soutien nécessaires pour que le processus de changement de fournisseur soit fructueux et efficace, sans exiger de ces fournisseurs de services de traitement de données qu'ils développent de nouvelles catégories de services au sein ou sur la base de l'infrastructure informatique de différents fournisseurs de services de traitement de données pour garantir une équivalence fonctionnelle dans un environnement autre que leurs propres systèmes. Néanmoins, les fournisseurs de services sont tenus d'offrir toute l'assistance et le soutien nécessaires pour que la procédure de changement de fournisseur soit efficace. Cela ne devrait pas porter atteinte aux droits existants en matière de résiliation des contrats, y compris ceux

introduits par le règlement (UE) 2016/679 et la directive (UE) 2019/770 du Parlement européen et du Conseil[67].

(75) Afin de faciliter le passage d'un service de traitement de données à l'autre, les fournisseurs de services de traitement de données devraient envisager l'utilisation d'outils de mise en œuvre et/ou de contrôle de la conformité, notamment ceux publiés par la Commission sous la forme d'un corpus réglementaire relatif aux services en nuage. Les clauses contractuelles types, en particulier, contribuent à accroître la confiance dans les services de traitement de données, à créer une relation plus équilibrée entre les utilisateurs et les fournisseurs de services et à améliorer la sécurité juridique quant aux conditions applicables au passage à d'autres services de traitement de données. Dans ce contexte, les utilisateurs et les fournisseurs de services devraient envisager l'utilisation de clauses contractuelles types élaborées par des organismes ou groupes d'experts compétents établis en vertu du droit de l'Union.

(76) Les spécifications et les normes d'interopérabilité ouvertes élaborées conformément à l'annexe II, paragraphes 3 et 4, du règlement (UE) nº 1025/2021 dans le domaine de l'interopérabilité et de la portabilité permettent un environnement en nuage multifournisseur continu, qui est une exigence essentielle pour l'innovation ouverte dans l'économie européenne fondée sur les données. Étant donné que les processus axés sur le marché n'ont pas démontré la capacité d'établir des spécifications techniques ou des normes qui facilitent une interopérabilité effective en nuage au niveau des plateformes à la demande (PaaS) et des logiciels à la demande (SaaS), la Commission devrait pouvoir, sur la base du présent règlement et conformément au règlement (UE) nº 1025/2012, demander aux organismes européens de normalisation de définir de telles normes, en particulier pour les types de services pour lesquels ces normes n'existent pas encore. La Commission encouragera en outre les acteurs du marché à élaborer des spécifications d'interopérabilité ouvertes pertinentes. La Commission peut, au moyen d'actes délégués, rendre obligatoire l'utilisation de normes européennes d'interopérabilité ou de spécifications d'interopérabilité ouvertes pour des types de services spécifiques par une référence dans un répertoire central des normes de l'Union pour l'interopérabilité des services de traitement des données. Les normes européennes et les spécifications d'interopérabilité ouvertes ne seront référencées que si elles sont conformes aux critères spécifiés dans le présent règlement, qui ont la même signification que les exigences énoncées aux paragraphes 3 et 4 de l'annexe II du règlement (UE) nº 1025/2021 et les facettes d'interopérabilité définies dans la norme ISO/CEI 19941: 2017.

(77) Les pays tiers peuvent adopter des lois, des règlements et d'autres actes législatifs visant à obtenir un transfert direct de données à caractère non personnel situées en dehors de leur territoire, y compris dans l'Union, ou à donner à leurs pouvoirs publics un accès direct à ces données. Les décisions de juridictions ou d'autres autorités judiciaires ou administratives, y compris de services répressifs, 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 d'autres cas, il peut arriver qu'une demande de transfert de données à caractère non personnel ou d'accès à de telles données fondée sur le droit d'un pays tiers soit incompatible avec l'obligation de protéger ces données en vertu du

[67] Directive (UE) 2019/770 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques (JO L 136 du 22.5.2019, p. 1).

droit de l'Union ou du droit national, en particulier lorsqu'il s'agit de protéger les droits fondamentaux de la personne, tels que le droit à la sécurité et le droit à un recours effectif, ou les intérêts fondamentaux d'un État membre en matière de sécurité ou de défense nationale, ainsi que des données commercialement sensibles, notamment des secrets d'affaires, ou des droits de propriété intellectuelle, y compris les engagements contractuels 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 s'il a été vérifié qu'en vertu du système juridique du pays tiers, les motifs et la proportionnalité de la décision doivent être exposés, la décision judiciaire ou administrative doit avoir un caractère spécifique, et l'objection motivée du destinataire doit faire l'objet d'un contrôle par une juridiction compétente du pays tiers habilitée à tenir dûment compte des intérêts juridiques pertinents du fournisseur des données. Dans la mesure du possible selon les termes de la demande d'accès aux données de l'autorité du pays tiers, le fournisseur de services de traitement de données devrait être en mesure d'informer le client dont les données sont demandées afin de vérifier l'existence d'un conflit potentiel entre cet accès et les règles de l'Union ou nationales, telles que celles relatives à la protection des données commercialement sensibles, y compris la protection des secrets d'affaires et des droits de propriété intellectuelle et les engagements contractuels en matière de confidentialité.

(78) Afin de renforcer encore la confiance placée dans les données, il importe de mettre en œuvre des garanties, pour les citoyens, le secteur public et les entreprises de l'Union, qui leur permettent dans toute la mesure du possible de contrôler leurs données. En outre, le droit, les valeurs et les normes de l'Union devraient être respectés en termes de sécurité, de protection des données et de respect de la vie privée, ainsi que de protection des consommateurs (mais pas exclusivement). Afin de prévenir tout accès illicite aux données à caractère non personnel, les fournisseurs de service de traitement des données soumis à cet instrument, tels que les services d'informatique en nuage et en périphérie, devraient prendre toute mesure raisonnable pour empêcher l'accès aux systèmes dans lesquels sont stockées des données à caractère non personnel, y compris, s'il y a lieu, par le cryptage des données, la sujétion régulière à des audits, le respect vérifié de dispositifs de certification pertinents en matière de réassurance de sécurité et une modification de leurs politiques d'entreprise.

(79) La normalisation et l'interopérabilité sémantique devraient jouer un rôle essentiel dans l'apport de solutions techniques permettant de garantir l'interopérabilité. Afin de faciliter la conformité avec les exigences en matière d'interopérabilité, il est nécessaire de prévoir une présomption de conformité pour les solutions d'interopérabilité qui satisfont à des normes harmonisées ou à des parties de celles-ci conformément au règlement (UE) nº 1025/2012 du Parlement européen et du Conseil. Il conviendrait que la Commission adopte des spécifications communes dans les domaines dans lesquels il n'existe pas de normes harmonisées, ou dans lesquels les normes existantes sont insuffisantes pour renforcer encore l'interopérabilité des espaces européens communs de données, des interfaces de programmation, du changement de fournisseur de services en nuage et des contrats intelligents. En outre, il restera peut-être à adopter, conformément au droit sectoriel de l'Union ou national, des spécifications communes dans les différents secteurs, en fonction des besoins spécifiques de ces derniers. Il conviendrait que fassent également partie des spécifications techniques de l'interopérabilité sémantique des structures et modèles de données réutilisables (sous la forme de vocabulaires de base), des ontologies, un profil d'application des métadonnées, des données de référence sous la forme d'un vocabulaire de base, des

taxinomies, des listes de codes, des tables d'autorité et des thésaurus. La Commission devrait par ailleurs être habilitée à demander l'élaboration de normes harmonisées pour l'interopérabilité des services de traitement des données.

(80) Afin de promouvoir l'interopérabilité des contrats intelligents dans les applications de partage de données, il est nécessaire de définir les exigences essentielles des contrats intelligents à l'intention des professionnels qui en créent pour d'autres ou qui en intègrent dans des applications soutenant la mise en œuvre d'accords de partage de données. Afin de faciliter la conformité des contrats intelligents avec ces exigences essentielles, il est nécessaire de prévoir une présomption de conformité pour les contrats intelligents qui satisfont à des normes harmonisées ou à des parties de celles-ci conformément au règlement (UE) nº 1025/2012 du Parlement européen et du Conseil.

(81) Afin de garantir une mise en œuvre efficace du présent règlement, les États membres devraient désigner une ou plusieurs autorités compétentes. Si un État membre désigne plusieurs autorités compétentes, il devrait également désigner une autorité compétente coordonnatrice. Les autorités compétentes devraient coopérer entre elles. Les autorités chargées de contrôler le respect de la protection des données et les autorités compétentes désignées en vertu de la législation sectorielle devraient être responsables de l'application du présent règlement dans leurs domaines de compétence.

(82) Pour faire valoir leurs droits au titre du présent règlement, les personnes physiques et morales devraient pouvoir demander réparation des violations desdits droits en déposant plainte auprès des autorités compétentes. Les autorités compétentes devraient être tenues de coopérer de manière à garantir un traitement et un règlement appropriés de la plainte. Afin de recourir au mécanisme du réseau de coopération en matière de protection des consommateurs et de permettre des actions représentatives, le présent règlement modifie les annexes du règlement (UE) 2017/2394 du Parlement européen et du Conseil[68] et de la directive (UE) 2020/1828 du Parlement européen et du Conseil[69].

(83) Les autorités compétentes des États membres devraient veiller à ce que les manquements aux obligations prévues par le présent règlement soient frappés de sanctions. Ce faisant, elles devraient tenir compte de la nature, de la gravité, de l'éventuelle récurrence et de la durée du manquement au regard de l'intérêt public en jeu, de la portée et du type d'activités exercées, ainsi que de la capacité économique de l'auteur du manquement. Si l'auteur du manquement manque systématiquement ou de façon récurrente aux obligations qui lui incombent en vertu du présent règlement, elles devraient en tenir compte. Afin d'aider les entreprises à rédiger et à négocier des contrats, la Commission devrait élaborer et recommander des clauses contractuelles types non contraignantes pour les contrats de partage de données interentreprises, en tenant compte, si nécessaire, des conditions prévalant dans certains secteurs et des pratiques existantes en matière de mécanismes de partage volontaire de données. Ces clauses contractuelles types devraient avant tout constituer un outil pratique aidant en

---

68 Règlement (UE) 2017/2394 du Parlement européen et du Conseil du 12 décembre 2017 sur la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs et abrogeant le règlement (CE) nº 2006/2004 (JO L 345 du 27.12.2017, p. 1).

69 Directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE (JO L 409 du 4.12.2020, p. 1).

particulier les petites entreprises à conclure un contrat. Lorsqu'elles seront largement et intégralement utilisées, elles devraient également avoir pour effet bénéfique d'influencer la manière dont sont conçus les contrats relatifs à l'accès aux données et à l'utilisation des données et conduire ainsi plus généralement à des relations contractuelles plus équitables en termes d'accès aux données et de partage des données.

(84) Afin d'éliminer le risque que les détenteurs de données contenues dans des bases de données obtenues ou générées au moyen de composants physiques tels que des capteurs, d'un produit connecté ou d'un service lié invoquent le droit «sui generis» prévu par l'article 7 de la directive 96/9/CE, alors que ces bases de données ne remplissent pas les conditions attachées à ce droit «sui generis», et puissent entraver ainsi l'exercice effectif du droit des utilisateurs d'accéder aux données et de les utiliser ainsi que le droit de partager des données avec des tiers prévus par le présent règlement, celui-ci devrait préciser que le droit «sui generis» ne s'applique pas à ces bases de données, parce que les conditions de la protection ne seraient pas remplies.

(85) Afin de tenir compte des aspects techniques des services de traitement de données, il conviendrait de déléguer à la Commission le pouvoir d'adopter des actes, conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne en vue de compléter le présent règlement, par l'introduction d'un mécanisme de suivi des frais de changement de fournisseur imposés par les fournisseurs de services de traitement de données sur le marché, de préciser davantage les exigences essentielles en matière d'interopérabilité imposées aux exploitants d'espaces de données et aux fournisseurs de services de traitement des données et de publier la référence des spécifications d'interopérabilité ouvertes et des normes européennes pour l'interopérabilité des services de traitement des données. Il importe particulièrement que la Commission procède aux consultations appropriées durant ses travaux préparatoires, 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»[70]. En particulier, aux fins de 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 associés à la préparation des actes délégués.

(86) Afin de garantir des conditions uniformes de mise en œuvre du présent règlement, il conviendrait de conférer des compétences d'exécution à la Commission en vue de compléter le présent règlement par l'adoption de spécifications communes pour l'interopérabilité des espaces européens communs de données et du partage des données, le changement de fournisseur de services de traitement des données, les contrats intelligents et l'interopérabilité des contrats intelligents ainsi que de moyens techniques tels que les interfaces de programmation, la transmission de données entre parties, y compris en continu ou en temps réel, et les vocabulaires de base de l'interopérabilité sémantique. Ces compétences devraient être exercées conformément au règlement (UE) nº 182/2011 du Parlement européen et du Conseil[71].

---

70 JO L 123 du 12.5.2016, p. 1.

71 Règlement (UE) nº 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).

(87) Le présent règlement ne devrait pas porter atteinte aux dispositions spécifiques des actes de l'Union qui ont été adoptés avant sa propre date d'adoption dans le domaine du partage de données entre entreprises, entre entreprises et consommateurs et entre entreprises et organismes du secteur public. Afin de garantir la cohérence et le bon fonctionnement du marché intérieur, la Commission devrait, s'il y a lieu, évaluer l'articulation du présent règlement et des actes réglementant le partage des données qui ont été adoptés avant la date d'adoption du présent règlement, afin d'apprécier la nécessité d'aligner les dispositions spécifiques de ces actes sur le présent règlement. Le présent règlement devrait s'entendre sans préjudice des règles répondant à des besoins spécifiques à certains secteurs ou domaines d'intérêt public. Ces règles peuvent comprendre des exigences supplémentaires concernant les aspects techniques de l'accès aux données, tels que les interfaces d'accès aux données, ou la manière dont l'accès aux données pourrait être fourni, par exemple directement à partir du produit ou par l'intermédiaire de services d'intermédiation de données. Ces règles peuvent également inclure des limites aux droits des détenteurs de données d'accéder aux données des utilisateurs ou de les utiliser, ou d'autres aspects allant au-delà de l'accès aux données et de leur utilisation, tels que les aspects liés à la gouvernance. Le présent règlement devrait également s'entendre sans préjudice de règles plus spécifiques dans le cadre du développement d'espaces européens communs de données.

(88) Le présent règlement ne devrait pas avoir d'incidence sur l'application des règles de concurrence, en particulier les articles 101 et 102 du traité. Les mesures prévues dans le présent règlement ne devraient pas servir à restreindre la concurrence d'une manière contraire au traité.

(89) Afin de permettre aux acteurs économiques de s'adapter aux nouvelles règles énoncées dans le présent règlement, celles-ci devraient s'appliquer un an après son entrée en vigueur.

(90) 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 et ont rendu leur avis le [XX XX 2022],

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I
DISPOSITIONS GÉNÉRALES

Article premier
Objet et champ d'application

1. Le présent règlement établit des règles harmonisées relatives au fait de mettre des données, générées par l'utilisation d'un produit ou d'un service lié, à la disposition de l'utilisateur de ce produit ou service et, en ce qui concerne les détenteurs de données, au fait de mettre des données à la disposition de destinataires de données ainsi que, en cas de besoin exceptionnel, pour l'exécution d'une mission d'intérêt public, à la disposition d'organismes du secteur public ou d'institutions, organes ou organismes de l'Union.

2. Le présent règlement s'applique:

   (a) aux fabricants de produits et aux fournisseurs de services liés mis sur le marché de l'Union et aux utilisateurs de ces produits ou services;

(b) aux détenteurs de données qui mettent des données à la disposition de destinataires de données dans l'Union;

(c) aux destinataires de données dans l'Union à la disposition desquels sont mises des données;

(d) aux organismes du secteur public et aux institutions, organes et organismes de l'Union qui demandent aux détenteurs de données de rendre des données disponibles lorsqu'il existe un besoin exceptionnel de disposer de ces données pour exécuter une mission d'intérêt public, ainsi qu'aux détenteurs de données qui fournissent ces données en réponse à une telle demande;

(e) aux prestataires de services de traitement de données offrant de tels services à des clients dans l'Union.

3. Le droit de l'Union relatif à la protection des données à caractère personnel, de la vie privée et de la confidentialité des communications et de l'intégrité des équipements terminaux s'applique aux données à caractère personnel traitées en lien avec les droits et obligations énoncés dans le présent règlement. Le présent règlement est sans préjudice de l'applicabilité du droit de l'Union sur la protection des données à caractère personnel, en particulier le règlement (UE) 2016/679 et la directive 2002/58/CE, y compris en ce qui concerne les pouvoirs et compétences des autorités de contrôle. En ce qui concerne les droits énoncés au chapitre II du présent règlement, et lorsque les utilisateurs sont les personnes concernées par des données à caractère personnel soumises aux droits et obligations énoncées dans ledit chapitre, les dispositions du présent règlement complètent le droit à la portabilité des données prévu à l'article 20 du règlement (UE) 2016/679.

4. Le présent règlement n'a pas d'incidence sur les actes juridiques de l'Union et nationaux prévoyant l'accès aux données, leur partage et leur utilisation 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, y compris le règlement (UE) 2021/784 du Parlement européen et du Conseil[72] et les [propositions sur les preuves électroniques COM (2018) 225 et 226] une fois adoptées, ni sur la coopération internationale dans ce domaine. Le présent règlement n'affecte ni la collecte et le partage de données, ni l'accès à ces dernières et leur utilisation au titre de la directive (UE) 2015/849 du Parlement européen et du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme et du règlement (UE) 2015/847 du Parlement européen et du Conseil sur les informations accompagnant le transfert de fonds. Le présent règlement ne porte pas atteinte aux compétences des États membres en ce qui concerne les activités relatives à la sécurité publique, à la défense, à la sécurité nationale, aux douanes et à l'administration fiscale, ainsi qu'à la santé et à la sécurité des citoyens conformément au droit de l'Union.

Article 2
Définitions

Aux fins du présent règlement, on entend par:

[72] Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion de contenus à caractère terroriste en ligne (JO L 172 du 17.5.2021, p. 79).

(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) «produit»: un objet mobilier corporel, y compris lorsqu'il est incorporé dans un bien immeuble, qui obtient, génère ou recueille des données concernant son utilisation ou son environnement, qui est en mesure de communiquer des données par l'intermédiaire d'un service de communications électroniques accessible au public et dont la fonction première n'est pas le stockage et le traitement de données;

(3) «service lié»: un service numérique, y compris un logiciel, intégré dans un produit ou interconnecté avec celui-ci de telle sorte que son absence empêcherait le produit de remplir l'une de ses fonctions;

(4) «assistants virtuels»: des logiciels capables de traiter des demandes, des tâches ou des questions, notamment à partir de données d'entrée sonores ou écrites, ou de gestes ou de mouvements, et qui, sur la base de ces demandes, tâches ou questions, permettent d'accéder à leurs propres services et à des services tiers, ou contrôlent leurs appareils et des appareils tiers;

(5) «utilisateur»: une personne physique ou morale qui possède ou loue un produit ou reçoit un service;

(6) «détenteur de données», une personne morale ou une personne physique qui, conformément au présent règlement, aux dispositions législatives applicables de l'Union ou à la législation nationale mettant en œuvre le droit de l'Union, a le droit ou l'obligation ou, dans le cas de données à caractère non personnel et par le contrôle de la conception du produit et des services liés, a la possibilité, de rendre disponibles certaines données à caractère personnel;

(7) «destinataire de données», une personne physique ou morale, autre que l'utilisateur d'un produit ou d'un service lié, agissant à des fins qui sont liées à son activité commerciale, industrielle, artisanale ou libérale, à la disposition de laquelle le détenteur de données met des données, y compris un tiers lorsque l'utilisateur a adressé une demande au détenteur de données ou conformément à une obligation légale découlant du droit de l'Union ou de la législation nationale mettant en œuvre le droit de l'Union;

(8) «entreprise»: une personne physique ou morale qui, en ce qui concerne les contrats et pratiques relevant du présent règlement, agit à des fins liées à son activité commerciale, industrielle, artisanale ou libérale;

(9) «organismes du secteur public»: les autorités nationales, régionales ou locales des États membres et les organismes de droit public des États membres ou les associations formées par une ou plusieurs de ces autorités ou un ou plusieurs de ces organismes;

(10) «urgence publique»: une situation exceptionnelle ayant une incidence négative sur la population de l'Union, d'un État membre ou d'une partie de celui-ci, entraînant un risque de répercussions graves et durables sur les conditions de vie ou la stabilité économique, ou la détérioration substantielle d'actifs économiques dans l'Union ou les États membres concernés;

(11) «traitement»: toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou à des ensembles de données sous forme électronique, telles que la collecte, l'enregistrement, l'organisation, la

structuration, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

(12) «service de traitement des données»: un service numérique autre qu'un service de contenu en ligne au sens de l'article 2, point 5, du règlement (UE) 2017/1128, fourni à un client, qui permet la gestion à la demande et un large accès à distance à un ensemble modulable et variable de ressources informatiques pouvant être partagées de nature centralisée, distribuée ou fortement distribuée;

(13) «type de service»: un ensemble de services de traitement de données qui partagent le même objectif principal et le même modèle fondamental de service de traitement des données;

(14) «équivalence fonctionnelle»: le maintien d'un niveau minimal de fonctionnalité dans l'environnement d'un nouveau service de traitement de données après le changement de fournisseur, de sorte que, lorsque l'utilisateur effectue une action d'entrée sur des éléments essentiels du service, le service de destination fournit le même résultat, aux mêmes niveaux de performance, de sécurité, de résilience opérationnelle et de qualité de service que le service d'origine au moment de la résiliation du contrat;

(15) «spécifications d'interopérabilité ouvertes», les spécifications techniques des TIC, telles que définies dans le règlement (UE) nº 1025/2012, qui sont orientées vers les performances et la réalisation de l'interopérabilité entre les services de traitement de données;

(16) «contrat intelligent»: un programme informatique stocké dans un système de registre électronique, le résultat de l'exécution du programme étant enregistré dans le registre électronique;

(17) «registre électronique»: un registre électronique au sens de l'article 3, point 53), du règlement (UE) nº 910/2014;

(18) «spécifications communes»: un document, autre qu'une norme, contenant des solutions techniques qui permettent de satisfaire à certaines exigences et obligations établies en vertu du présent règlement;

(19) «interopérabilité», la capacité d'au moins deux espaces de données ou réseaux de communication, systèmes, produits, applications ou composants d'échanger et d'utiliser des données afin de remplir leurs fonctions;

(20) «norme harmonisée»: une norme harmonisée au sens de l'article 2, point 1 c), du règlement (UE) n° 1025/2012;

CHAPITRE II
PARTAGE DE DONNÉES ENTRE ENTREPRISES ET CONSOMMATEURS ET INTERENTREPRISES

Article 3
Obligation de rendre accessibles les données générées par l'utilisation de produits ou de services liés

1. La conception et la fabrication des produits, et la fourniture des services liés, sont telles que les données générées par leur utilisation sont, par défaut, facilement, de

manière sécurisée et, lorsque cela est pertinent et approprié, directement accessibles à l'utilisateur.

2. Avant la conclusion d'un contrat relatif à l'achat ou à la location d'un produit ou d'un service lié, l'utilisateur reçoit sous une forme claire et compréhensible, des informations concernant au moins les aspects suivants:

   (a) la nature et le volume des données susceptibles d'être générées par l'utilisation du produit ou du service lié;

   (b) si les données sont susceptibles d'être générées en continu et en temps réel;

   (c) la manière dont l'utilisateur peut accéder à ces données;

   (d) si le fabricant qui fournit le produit ou le fournisseur qui fournit le service lié a l'intention d'utiliser lui-même les données ou d'autoriser un tiers à les utiliser et, dans l'affirmative, les finalités pour lesquelles ces données seront utilisées;

   (e) si le vendeur ou le loueur est le détenteur de données et, dans la négative, l'identité du détenteur de données, telle que sa raison sociale et l'adresse géographique à laquelle il est établi;

   (f) les moyens de communication qui permettent à l'utilisateur de contacter rapidement le détenteur de données et de communiquer efficacement avec lui;

   (g) la manière dont l'utilisateur peut demander que les données soient partagées avec un tiers;

   (h) le droit de l'utilisateur d'introduire une plainte pour violation des dispositions du présent chapitre auprès de l'autorité compétente visée à l'article 31.

Article 4

Droits des utilisateurs à accéder aux données générées par l'utilisation de produits ou de services liés et à les utiliser

1. Lorsque l'utilisateur ne peut pas accéder directement à des données à partir du produit, le détenteur de données met à sa disposition dans les meilleurs délais, gratuitement et, le cas échéant, en continu et en temps réel, les données générées par l'utilisation que cet utilisateur fait d'un produit ou d'un service lié. À cet effet, une simple demande est envoyée par voie électronique lorsque cela est techniquement possible.

2. Le détenteur de données n'exige pas de l'utilisateur qu'il fournisse d'autres informations que celles qui sont nécessaires pour vérifier sa qualité d'utilisateur en application du paragraphe 1. Le détenteur de données ne conserve aucune autre information sur l'accès de l'utilisateur aux données demandées que celles qui sont nécessaires à la bonne exécution de la demande d'accès de l'utilisateur et à la sécurité et à la maintenance de l'infrastructure de données.

3. Les secrets d'affaires ne sont divulgués qu'à condition que toutes les mesures spécifiques nécessaires soient prises pour préserver leur confidentialité, en particulier en ce qui concerne les tiers. Le détenteur de données et l'utilisateur peuvent convenir de mesures visant à préserver la confidentialité des données partagées, en particulier en ce qui concerne les tiers.

4. L'utilisateur ne se sert pas des données obtenues en réponse à une demande visée au paragraphe 1 pour mettre au point un produit concurrençant le produit dont proviennent les données.

5. Lorsque l'utilisateur n'est pas une personne concernée, les éventuelles données à caractère personnel générées par l'utilisation d'un produit ou d'un service lié ne sont rendues disponibles par le détenteur de données que s'il existe une base juridique valable en vertu de l'article 6, paragraphe 1, du règlement (UE) 2016/679 et, le cas échéant, si les conditions énoncées à l'article 9 dudit règlement sont remplies.

6. Le détenteur de données n'utilise les données à caractère non personnel générées par l'utilisation d'un produit ou d'un service lié que dans le cadre d'un accord contractuel avec l'utilisateur. Le détenteur de données n'utilise pas les données générées par l'utilisation du produit ou du service lié pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production de l'utilisateur, ou sur l'utilisation que ce dernier fait du produit ou du service lié, qui sont susceptibles de porter atteinte à la position commerciale de l'utilisateur sur les marchés où celui-ci est actif.

Article 5
Droit de partager des données avec des tiers

1. Lorsqu'un utilisateur ou une partie agissant au nom de ce dernier en fait la demande, le détenteur de données met à la disposition d'un tiers, dans les meilleurs délais, sans frais pour l'utilisateur et, le cas échéant, en continu et en temps réel, les données générées par l'utilisation d'un produit ou d'un service lié, à un niveau de qualité identique à celui dont lui-même bénéficie.

2. Toute entreprise fournissant des services de plateforme essentiels dont un ou plusieurs ont été désignés comme contrôleur d'accès, conformément à l'article [...] du [règlement XXX relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques)[73]], n'est pas un tiers éligible au titre du présent article et ne peut par conséquent pas:

   (a) inviter un utilisateur, par une sollicitation ou par une incitation commerciale, quelles qu'elles soient, y compris en fournissant une compensation pécuniaire ou de toute autre nature, à mettre à la disposition de l'un de ses services des données que l'utilisateur a obtenues à la suite d'une demande introduite au titre de l'article 4, paragraphe 1;

   (b) inviter un utilisateur, par une sollicitation ou par une incitation commerciale, à demander au détenteur de données de mettre des données à la disposition de l'un de ses services conformément au paragraphe 1 du présent article;

   (c) recevoir d'un utilisateur des données que ce dernier a obtenues à la suite d'une demande introduite au titre de l'article 4, paragraphe 1.

3. L'utilisateur ou le tiers n'est pas tenu de fournir d'autres informations que celles qui sont nécessaires pour vérifier sa qualité d'utilisateur ou de tiers en application du paragraphe 1. Le détenteur de données ne conserve aucune autre information sur l'accès du tiers aux données demandées que celles qui sont nécessaires à la bonne exécution de la demande d'accès du tiers et à la sécurité et à la maintenance de l'infrastructure de données.

4. Le tiers s'abstient d'avoir recours à des moyens coercitifs ou de tirer avantage de lacunes manifestes de l'infrastructure technique du détenteur de données destinée à protéger les données pour obtenir l'accès aux données.

---

[73] JO [...].

5. Le détenteur de données n'utilise aucune donnée à caractère non personnel générée par l'utilisation du produit ou du service lié pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production du tiers ou sur l'utilisation que ce dernier fait du produit ou du service lié, qui sont susceptibles de porter atteinte à la position commerciale du tiers sur les marchés sur lesquels il exerce ses activités, à moins que le tiers n'ait autorisé cette utilisation et ne dispose de la possibilité technique de retirer cette autorisation à tout moment.

6. Lorsque l'utilisateur n'est pas une personne concernée, les éventuelles données à caractère personnel générées par l'utilisation d'un produit ou d'un service lié ne sont rendues disponibles que s'il existe une base juridique valable en vertu de l'article 6, paragraphe 1, du règlement (UE) 2016/679 et, le cas échéant, si les conditions énoncées à l'article 9 dudit règlement sont remplies.

7. L'éventuelle absence d'accord entre le détenteur de données et le tiers concernant les modalités de transmission des données ne doit pas entraver ou empêcher l'exercice des droits de la personne concernée en vertu du règlement (UE) 2016/679 et, en particulier, du droit à la portabilité des données prévu à l'article 20 dudit règlement.

8. Les secrets d'affaires ne sont divulgués à des tiers que dans la mesure où ils sont strictement nécessaires pour atteindre la finalité convenue entre l'utilisateur et le tiers et où le tiers prend toutes les mesures spécifiques nécessaires qu'il a arrêtées avec le détenteur de données pour préserver la confidentialité du secret d'affaires. Dans ce cas, la qualité de secret d'affaires des données et les mesures visant à préserver la confidentialité sont précisées dans l'accord conclu entre le détenteur de données et le tiers.

9. Le droit visé au paragraphe 1 ne porte pas atteinte aux droits d'autres parties en matière de protection des données.

Article 6

Obligations des tiers recevant des données à la demande de l'utilisateur

1. Un tiers traite les données mises à sa disposition en application de l'article 5 uniquement aux fins et dans les conditions convenues avec l'utilisateur, et sous réserve des droits de la personne concernée eu égard aux données à caractère personnel, et supprime les données lorsqu'elles ne sont plus nécessaires à la finalité convenue.

2. Le tiers s'abstient:

   (a) de contraindre, tromper ou manipuler l'utilisateur de quelque manière que ce soit, en nuisant ou en portant atteinte à l'autonomie, à la prise de décision ou aux choix de l'utilisateur, y compris au moyen d'une interface numérique avec l'utilisateur;

   (b) d'utiliser les données qu'il reçoit à des fins de profilage de personnes physiques au sens de l'article 4, point 4, du règlement (UE) 2016/679, à moins que cela ne soit nécessaire pour fournir le service demandé par l'utilisateur;

   (c) de mettre les données qu'il reçoit à la disposition d'un autre tiers, sous forme brute, agrégée ou dérivée, à moins que cela ne soit nécessaire pour fournir le service demandé par l'utilisateur;

   (d) de mettre les données qu'il reçoit à la disposition d'une entreprise fournissant des services de plateforme essentiels dont un ou plusieurs ont été désignés

comme contrôleur d'accès, conformément à l'article [...] du [règlement XXX relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques);

(e) d'utiliser les données qu'il reçoit pour mettre au point un produit concurrençant le produit dont proviennent les données auxquelles il a accès ou de partager les données avec un autre tiers à cette fin;

(f) d'empêcher l'utilisateur, y compris au moyen d'engagements contractuels, de mettre à la disposition d'autres parties les données qu'il reçoit.

Article 7

Champ d'application des obligations en matière de partage de données entre entreprises et consommateurs et interentreprises

1. Les obligations du présent chapitre ne s'appliquent pas aux données générées par l'utilisation de produits manufacturés ou de services liés fournis par des entreprises qui sont considérées comme des micro ou petites entreprises au sens de l'article 2 de l'annexe de la recommandation 2003/361/CE, à condition que ces entreprises n'aient pas d'entreprises partenaires ou d'entreprises liées qui, au sens de l'article 3 de l'annexe de la recommandation 2003/361/CE, ne sont pas considérées comme des micro ou petites entreprises.

2. Lorsque le présent règlement fait référence à des produits ou à des services liés, cette référence s'entend également comme incluant les assistants virtuels, dans la mesure où ceux-ci sont utilisés pour accéder à un produit ou un service lié ou pour le contrôler.

CHAPITRE III
OBLIGATIONS APPLICABLES AUX DÉTENTEURS DE DONNÉES LÉGALEMENT TENUS DE RENDRE DES DONNÉES DISPONIBLES

Article 8

Conditions dans lesquelles les détenteurs de données mettent des données à la disposition de destinataires de données

1. Lorsqu'un détenteur de données est tenu de mettre des données à la disposition d'un destinataire de données en application de l'article 5 ou d'autres dispositions du droit de l'Union ou de la législation nationale mettant en œuvre le droit de l'Union, il le fait dans des conditions équitables, raisonnables et non discriminatoires et de manière transparente, conformément aux dispositions du présent chapitre et du chapitre IV.

2. Le détenteur de données convient avec le destinataire de données des conditions de mise à disposition des données. Une clause contractuelle concernant l'accès aux données et leur utilisation ou la responsabilité et les voies de recours en cas de violation ou de résiliation des obligations relatives aux données n'est pas contraignante si elle satisfait aux conditions de l'article 13 ou si elle exclut l'application des droits de l'utilisateur au titre du chapitre II, y déroge ou en modifie les effets.

3. Lorsqu'il met des données à disposition, un détenteur de données s'abstient de toute discrimination entre des catégories comparables de destinataires de données, y compris les entreprises partenaires ou les entreprises liées du destinataire de données, telles que définies à l'article 3 de l'annexe de la recommandation 2003/361/CE. Lorsqu'un destinataire de données considère que les conditions dans lesquelles des données ont été mises à sa disposition sont discriminatoires, il incombe au détenteur de données de démontrer l'absence de discrimination.

4. Un détenteur de données ne met pas de données à la disposition d'un destinataire de données sur une base d'exclusivité, sauf si l'utilisateur le demande en vertu du chapitre II.

5. Les détenteurs de données et les destinataires de données ne sont pas tenus de fournir des informations autres que celles qui sont nécessaires pour vérifier le respect des conditions contractuelles convenues pour la mise à disposition des données ou des obligations qui leur incombent au titre du présent règlement ou d'autres dispositions législatives applicables de l'Union ou de la législation nationale mettant en œuvre le droit de l'Union.

6. Sauf disposition contraire du droit de l'Union, y compris de l'article 6 du présent règlement, ou de la législation nationale mettant en œuvre le droit de l'Union, l'obligation de mettre des données à la disposition d'un destinataire de données n'impose pas la divulgation de secrets d'affaires au sens de la directive (UE) 2016/943.

Article 9
Compensation pour la mise à disposition de données

1. Toute compensation convenue entre un détenteur de données et un destinataire de données pour la mise à disposition des données est raisonnable.

2. Lorsque le destinataire de données est une micro, petite ou moyenne entreprise, au sens de l'article 2 de l'annexe de la recommandation 2003/361/CE, toute compensation convenue n'excède pas les coûts qui sont directement liés à la mise à la disposition des données au destinataire de données et qui sont imputables à la demande. L'article 8, paragraphe 3, s'applique en conséquence.

3. Le présent article ne fait pas obstacle à ce que d'autres dispositions du droit de l'Union ou de la législation nationale mettant en œuvre le droit de l'Union excluent une éventuelle compensation pour la mise à disposition de données ou prévoient une compensation moins élevée.

4. Le détenteur de données fournit au destinataire de données des informations exposant la base de calcul de la compensation de manière suffisamment détaillée pour lui permettre de vérifier que les exigences du paragraphe 1 et, le cas échéant, du paragraphe 2 sont respectées.

Article 10
Règlement des litiges

1. Les détenteurs de données et les destinataires de données ont accès à des organismes de règlement des litiges, certifiés conformément au paragraphe 2 du présent article, pour régler les litiges concernant la détermination de conditions équitables, raisonnables et non discriminatoires applicables à la mise à disposition de données et

la façon de rendre ces données disponibles en toute transparence, conformément aux articles 8 et 9.

2. L'État membre dans lequel l'organisme de règlement des litiges est établi certifie l'organisme à la demande de celui-ci, lorsque cet organisme a démontré qu'il remplit toutes les conditions suivantes:

   (a) il est impartial et indépendant et rendra ses décisions conformément à des règles de procédure claires et équitables;

   (b) il dispose de l'expertise nécessaire en ce qui concerne la détermination de conditions équitables, raisonnables et non discriminatoires applicables à la mise à disposition de données et la façon de rendre ces données disponibles en toute transparence, ce qui permet à l'organisme de déterminer efficacement ces conditions;

   (c) il est facilement accessible au moyen de technologies de communication électronique;

   (d) il est en mesure de rendre ses décisions de manière rapide, efficace et économiquement avantageuse, et dans au minimum une langue officielle de l'Union;

   Si aucun organisme de règlement des litiges n'est certifié dans un État membre au plus tard le [date d'application du règlement], cet État membre crée et certifie un organisme de règlement des litiges qui remplit les conditions énoncées aux points a) à d) du présent paragraphe.

3. Les États membres notifient à la Commission les organismes de règlement des litiges certifiés conformément au paragraphe 2. La Commission publie une liste de ces organismes sur un site web spécifique et la tient à jour.

4. Les organismes de règlement des litiges informent les parties concernées des redevances, ou des mécanismes utilisés pour les déterminer, avant que ces parties ne demandent une décision.

5. Les organismes de règlement des litiges refusent de traiter une demande de règlement relative à un litige qui a déjà été porté devant un autre organisme de règlement des litiges ou devant une juridiction d'un État membre.

6. Les organismes de règlement des litiges donnent aux parties la possibilité, dans un délai raisonnable, d'exprimer leur point de vue sur les questions qu'elles ont soumises à ces organismes. Dans ce contexte, les organismes de règlement des litiges communiquent à ces parties les observations de l'autre partie et toute déclaration faite par des experts. Ces organismes donnent aux parties la possibilité de formuler des observations sur ces observations et déclarations.

7. Les organismes de règlement des litiges prennent leur décision sur les questions qui leur sont soumises au plus tard 90 jours après le dépôt de la demande de décision. Ces décisions sont présentées par écrit ou sur un support durable et sont étayées par un exposé des motifs à l'appui de la décision.

8. La décision de l'organisme de règlement des litiges n'est contraignante pour les parties que si celles-ci ont expressément accepté son caractère contraignant avant le début de la procédure de règlement du litige.

9. Le présent article ne porte pas atteinte au droit des parties de former un recours effectif devant une juridiction d'un État membre.

Article 11

Mesures techniques de protection et dispositions relatives à l'utilisation ou à la divulgation non autorisées de données

1. Le détenteur de données peut appliquer des mesures techniques appropriées de protection, y compris des contrats intelligents, afin d'empêcher l'accès non autorisé aux données et de garantir le respect des articles 5, 6, 9 et 10 ainsi que des conditions contractuelles convenues pour la mise à disposition des données. Ces mesures techniques de protection ne sont pas utilisées pour porter atteinte au droit de l'utilisateur de fournir effectivement des données à des tiers conformément à l'article 5 ou à tout droit dont bénéficie un tiers en vertu des dispositions du droit de l'Union ou de la législation nationale mettant en œuvre le droit de l'Union visées à l'article 8, paragraphe 1.

2. À moins que le détenteur de données ou l'utilisateur n'ait donné une instruction contraire, un destinataire de données qui, aux fins de l'obtention de données, a fourni des informations inexactes ou fausses au détenteur de données, a eu recours à des moyens trompeurs ou coercitifs ou a tiré avantage de lacunes manifestes dans l'infrastructure technique du détenteur de données destinée à protéger les données, a utilisé les données rendues disponibles à des fins non autorisées ou a divulgué ces données à une autre partie sans l'autorisation du détenteur de données:

   (a) détruit, dans les meilleurs délais, les données rendues disponibles par le détenteur de données et les éventuelles copies de celles-ci;

   (b) met fin, dans les meilleurs délais, à la production, à l'offre, à la mise sur le marché ou à l'utilisation de biens, de données ou de services dérivés produits sur la base des connaissances obtenues au moyen de ces données, ou à l'importation, à l'exportation ou au stockage de biens non conformes destinés aux fins précitées, et détruit tout bien non conforme.

3. Le paragraphe 2, point b), ne s'applique pas dans les cas suivants:

   (a) l'utilisation des données n'a pas causé de préjudice important au détenteur de données;

   (b) l'application des dispositions qu'il prévoit serait disproportionnée au regard des intérêts du détenteur de données.

Article 12

CHAMP D'APPLICATION DES OBLIGATIONS CONCERNANT LES DÉTENTEURS DE DONNÉES LÉGALEMENT TENUS DE RENDRE DES DONNÉES DISPONIBLES

1. Le présent chapitre s'applique lorsqu'un détenteur de données est tenu, en application de l'article 5, du droit de l'Union ou de la législation nationale mettant en œuvre le droit de l'Union, de mettre des données à la disposition d'un destinataire de données.

2. Toute clause contractuelle figurant dans un accord de partage de données qui, au détriment d'une partie ou, le cas échéant, au détriment de l'utilisateur, exclut l'application du présent chapitre, y déroge ou en modifie les effets, n'est pas contraignante pour cette partie.

3. Le présent chapitre ne s'applique qu'en ce qui concerne les obligations de mise à disposition de données en vertu du droit de l'Union ou de la législation nationale

mettant en œuvre le droit de l'Union, qui entrent en vigueur après le [date d'application du règlement].

CHAPITRE IV
CLAUSES ABUSIVES RELATIVES À L'ACCÈS AUX DONNÉES ET À L'UTILISATION DES DONNÉES INTERENTREPRISES

Article 13
Clauses contractuelles abusives imposées unilatéralement à une micro, petite ou moyenne entreprise

1. Une clause contractuelle concernant l'accès aux données et leur utilisation ou la responsabilité et les voies de recours en cas de violation ou de résiliation d'obligations relatives aux données qu'une entreprise a imposée unilatéralement à une micro, petite ou moyenne entreprise au sens de l'article 2 de l'annexe de la recommandation 2003/361/CE ne lie pas cette dernière entreprise si elle est abusive.

2. Une clause contractuelle est abusive si elle est d'une nature telle que son utilisation s'écarte fortement des bonnes pratiques commerciales en matière d'accès aux données et d'utilisation de celles-ci, et qu'elle est contraire à la bonne foi et à la loyauté.

3. Aux fins du présent article, une clause contractuelle est abusive si elle a pour objet ou pour effet:

   (a) d'exclure ou de limiter la responsabilité de la partie qui a unilatéralement imposé la clause en cas d'actes intentionnels ou de négligence grave;

   (b) d'exclure les voies de recours dont dispose la partie à laquelle la clause a été unilatéralement imposée en cas d'inexécution d'obligations contractuelles ou la responsabilité de la partie qui l'a imposée unilatéralement en cas de manquement à ces obligations;

   (c) de donner à la partie qui a unilatéralement imposé la clause le droit exclusif de déterminer si les données fournies sont conformes au contrat ou d'interpréter toute clause du contrat.

4. Aux fins du présent article, une clause contractuelle est réputée abusive si elle a pour objet ou pour effet:

   (a) de limiter de manière inappropriée les voies de recours en cas d'inexécution des obligations contractuelles ou la responsabilité en cas de manquement à ces obligations;

   (b) de permettre à la partie qui a unilatéralement imposé la clause d'accéder aux données de l'autre partie contractante et de les utiliser d'une manière qui porte gravement atteinte aux intérêts légitimes de l'autre partie contractante;

   (c) d'empêcher la partie à laquelle la clause a été unilatéralement imposée d'utiliser les données qu'elle a fournies ou générées pendant la durée du contrat, ou de limiter l'utilisation de ces données dans la mesure où cette partie n'est pas autorisée à utiliser, à capturer, à consulter ou à contrôler ces données ou à en exploiter la valeur de manière proportionnée;

(d) d’empêcher la partie à laquelle la clause a été unilatéralement imposée d’obtenir une copie des données qu’elle a fournies ou générées pendant la durée du contrat ou dans un délai raisonnable après la résiliation de celui-ci;

(e) de permettre à la partie qui a unilatéralement imposé la clause de résilier le contrat dans un délai excessivement court, compte tenu des possibilités raisonnables de l’autre partie contractante de se tourner vers un service alternatif et comparable et du préjudice financier causé par cette résiliation, sauf s’il existe des motifs sérieux de le faire.

5. Une clause contractuelle est considérée comme imposée unilatéralement au sens du présent article si elle a été fournie par une partie contractante et si l’autre partie contractante n’a pas été en mesure d’influencer son contenu malgré une tentative de négociation. Il appartient à la partie contractante qui a fourni une clause contractuelle de prouver que cette clause n’a pas été imposée unilatéralement.

6. Lorsque la clause contractuelle abusive est dissociable des autres clauses du contrat, ces dernières restent contraignantes.

7. Le présent article ne s’applique pas aux clauses contractuelles définissant l’objet principal du contrat ni aux conditions contractuelles déterminant le prix à payer.

8. Les parties à un contrat visé au paragraphe 1 ne peuvent exclure l’application du présent article, y déroger ou en modifier les effets.

CHAPITRE V
METTRE DES DONNÉES À LA DISPOSITION DES ORGANISMES DU SECTEUR PUBLIC ET DES INSTITUTIONS, ORGANES OU ORGANISMES DE L’UNION EN RAISON D'UN BESOIN EXCEPTIONNEL

Article 14

Obligation de mettre les données à disposition en raison d'un besoin exceptionnel

1. Sur demande, un détenteur de données met des données à la disposition d’un organisme du secteur public ou d’une institution, d’un organe ou d'un organisme de l’Union démontrant l’existence d’un besoin exceptionnel d’utiliser les données demandées.

2. Le présent chapitre ne s’applique pas aux petites et microentreprises telles que définies à l’article 2 de l’annexe de la recommandation 2003/361/CE.

Article 15

Besoin exceptionnel d’utiliser des données

Un besoin exceptionnel d’utiliser des données au sens du présent chapitre est réputé exister dans les cas suivants:

(a) lorsque les données demandées sont nécessaires pour réagir à une urgence publique;

(b) lorsque la demande de données a une durée et une portée limitées et est nécessaire pour prévenir une urgence publique ou pour contribuer au rétablissement à la suite d’une urgence publique;

(c) lorsque l'absence de données disponibles empêche l'organisme du secteur public ou l'institution, l'organe ou l'organisme de l'Union de s'acquitter d'une mission spécifique d'intérêt public explicitement prévue par la loi; et que

(1) l'organisme du secteur public ou l'institution, l'organe ou l'organisme de l'Union n'a pas été en mesure d'obtenir ces données par d'autres moyens, notamment en achetant les données sur le marché aux prix du marché ou en invoquant les obligations existantes de mise à disposition des données, et que l'adoption de nouvelles mesures législatives ne peut garantir la disponibilité des données en temps utile; ou

(2) l'obtention des données selon la procédure établie dans le présent chapitre réduirait substantiellement la charge administrative pesant sur les détenteurs de données ou sur d'autres entreprises.

Article 16

Relation avec d'autres obligations de mettre des données à la disposition d'organismes du secteur public et d'institutions, organes et organismes de l'Union

1. Le présent chapitre ne porte pas atteinte aux obligations prévues par le droit de l'Union ou par le droit national aux fins de l'établissement de rapports, du respect des demandes d'information ou de la démonstration ou de la vérification du respect des obligations légales.

2. Les organismes du secteur public et les institutions, les organes et les organismes de l'Union n'exercent pas les droits découlant du présent chapitre en vue de mener des activités à des fins de prévention et de détection des infractions pénales ou administratives, d'enquêtes et de poursuites en la matière, d'exécution de sanctions pénales, ou d'administration douanière ou fiscale. Le présent chapitre n'affecte pas le droit de l'Union et le droit national applicables en matière de prévention et de détection des infractions pénales ou administratives, d'enquêtes et de poursuites en la matière, d'exécution de sanctions pénales ou administratives, ou d'administration douanière ou fiscale.

Article 17

Demandes de mise à disposition de données

1. Lorsqu'un organisme du secteur public ou une institution, un organe ou un organisme de l'Union qui demande des données en vertu de l'article 14, paragraphe 1, il ou elle:

(a) précise quelles sont les données demandées;

(b) démontre le besoin exceptionnel pour lequel les données sont demandées;

(c) explique la finalité de la demande, l'utilisation prévue des données demandées et la durée de cette utilisation;

(d) indique la base juridique de la demande de données;

(e) précise le délai dans lequel les données doivent être mises à disposition ou dans lequel le détenteur de données peut demander à l'organisme du secteur public, à l'institution, à l'organe ou à l'organisme de l'Union de modifier ou de retirer la demande.

2. Une demande de données présentée en vertu du paragraphe 1 du présent article:

(a) est exprimée en termes clairs, concis et simples, compréhensibles pour le détenteur de données;

(b) est proportionnée au besoin exceptionnel, en ce qui concerne la granularité et le volume des données demandées, ainsi que la fréquence d'accès aux données demandées;

(c) respecte les objectifs légitimes du détenteur de données, compte tenu de la protection des secrets d'affaires ainsi que des coûts et des efforts nécessaires pour mettre les données à disposition;

(d) concerne, dans la mesure du possible, les données à caractère non personnel;

(e) informe le détenteur de données des sanctions qui sont imposées en vertu de l'article 33 par une autorité compétente visée à l'article 31 en cas de non-respect de la demande;

(f) est rendue publiquement accessible en ligne dans les meilleurs délais.

3. Un organisme du secteur public ou une institution, un organe ou un organisme de l'Union ne met pas les données obtenues en vertu du présent chapitre à disposition en vue de leur réutilisation au sens de la directive (UE) 2019/1024. La directive (UE) 2019/1024 ne s'applique pas aux données détenues par des organismes du secteur public obtenues au titre du présent chapitre.

4. Le paragraphe 3 n'empêche pas un organisme du secteur public ou une institution, un organe ou un organisme de l'Union d'échanger des données obtenues en vertu du présent chapitre avec un autre organisme du secteur public, une autre institution, un autre organe ou un autre organisme de l'Union en vue de l'accomplissement des tâches prévues à l'article 15, ni de mettre les données à la disposition d'un tiers dans les cas où il ou elle a externalisé, au moyen d'un accord accessible au public, des inspections techniques ou d'autres fonctions auprès de ce tiers. Les obligations incombant aux organismes du secteur public, aux institutions, aux organes ou aux organismes de l'Union en vertu de l'article 19 s'appliquent.

Lorsqu'un organisme du secteur public ou une institution, un organe ou un organisme de l'Union transmet ou met des données à disposition en vertu du présent paragraphe, il ou elle en informe le détenteur de données auprès duquel les données ont été obtenues.

Article 18
Respect des demandes de données

1. Le détenteur de données qui reçoit une demande d'accès à des données au titre du présent chapitre met ces données à la disposition de l'organisme du secteur public qui les demande ou d'une institution, d'un organe ou d'un organisme de l'Union dans les meilleurs délais.

2. Sans préjudice des besoins spécifiques concernant la disponibilité des données définis dans la législation sectorielle, le détenteur de données peut rejeter la demande ou demander sa modification dans un délai de cinq jours ouvrables à compter de la réception d'une demande de données nécessaires pour réagir à une situation d'urgence publique, et dans un délai de quinze jours ouvrables dans les autres cas de besoin exceptionnel, pour l'un des motifs suivants:

(a) les données ne sont pas disponibles;

(b) la demande ne satisfait pas aux conditions énoncées à l'article 17, paragraphes 1 et 2).

3. En cas de demande de données nécessaires pour réagir à une urgence publique, le détenteur de données peut également rejeter la demande ou demander sa modification s'il a déjà fourni les données demandées en réponse à une demande présentée précédemment pour la même finalité par un autre organisme du secteur public ou par une autre institution, un autre organe ou un autre organisme de l'Union et qu'il n'a pas été informé de la destruction des données conformément à l'article 19, paragraphe 1, point c).

4. Si le détenteur de données décide de rejeter la demande ou de demander sa modification conformément au paragraphe 3, il indique l'identité de l'organisme du secteur public ou de l'institution, de l'organe ou de l'organisme de l'Union qui a présenté précédemment une demande pour la même finalité.

5. Lorsque le respect de la demande de mise à disposition de données adressée à un organisme du secteur public ou à une institution, un organe ou un organisme de l'Union requiert la divulgation de données à caractère personnel, le détenteur de données s'efforce de les pseudonymiser, dans la mesure où la demande peut être satisfaite au moyen de données pseudonymisées.

6. Lorsque l'organisme du secteur public ou l'institution, l'organe ou l'organisme de l'Union souhaite contester le refus d'un détenteur de données de fournir les données demandées, ou sa demande de modification de la demande, ou lorsque le détenteur de données souhaite contester la demande, l'affaire est portée devant l'autorité compétente visée à l'article 31.

Article 19

Obligations des organismes du secteur public et des institutions, organes et organismes de l'Union

1. Un organisme du secteur public ou une institution, un organe ou un organisme de l'Union ayant reçu des données à la suite d'une demande présentée en vertu de l'article 14:

   (a) n'utilise pas les données d'une manière incompatible avec la finalité pour laquelle elles ont été demandées;

   (b) met en œuvre, dans la mesure où le traitement des données à caractère personnel est nécessaire, des mesures techniques et organisationnelles garantissant les droits et libertés des personnes concernées;

   (c) détruit les données dès qu'elles ne sont plus nécessaires à la finalité indiquée et informe le détenteur de données que les données ont été détruites.

2. La divulgation de secrets d'affaires ou de secrets d'affaires présumés à un organisme du secteur public ou à une institution, un organe ou un organisme de l'Union n'est exigée que dans la mesure où elle est strictement nécessaire pour atteindre la finalité de la demande. Dans ce cas, l'organisme du secteur public ou l'institution, l'organe ou l'organisme de l'Union prend les mesures appropriées pour préserver la confidentialité de ces secrets d'affaires.

Article 20
Compensation en cas de besoin exceptionnel

1. Les données mises à disposition pour réagir à une urgence publique conformément à l'article 15, point a), sont fournies gratuitement.

2. Lorsque le détenteur de données réclame une compensation pour la mise à disposition de données conformément à une demande présentée au titre de l'article 15, points b) ou c), cette compensation ne dépasse pas les coûts techniques et organisationnels encourus pour se conformer à la demande, y compris, le cas échéant, les coûts d'anonymisation et d'adaptation technique, augmentés d'une marge raisonnable. À la demande de l'organisme du secteur public ou de l'institution, de l'organe ou de l'organisme de l'Union demandant les données, le détenteur de données fournit des informations sur la base du calcul des coûts et de la marge raisonnable.

Article 21
Contribution des organismes de recherche ou des instituts de statistique dans le cadre de besoins exceptionnels

1. Un organisme du secteur public ou une institution, un organe ou un organisme de l'Union a le droit de partager les données reçues au titre du présent chapitre avec des particuliers ou des organismes en vue de mener des travaux de recherche scientifique ou des analyses compatibles avec la finalité pour laquelle les données ont été demandées, ou avec des instituts nationaux de statistique et Eurostat en vue d'établir des statistiques officielles.

2. Les particuliers ou les organismes qui reçoivent les données en vertu du paragraphe 1 agissent dans un but non lucratif ou dans le cadre d'une mission d'intérêt public reconnue par le droit de l'Union ou le droit d'un État membre. Sont exclus les organismes sur lesquels des entreprises commerciales ont une influence déterminante, ce qui pourrait conduire à un accès préférentiel aux résultats des recherches.

3. Les particuliers ou les organismes qui reçoivent les données en vertu du paragraphe 1 se conforment aux dispositions de l'article 17, paragraphe 3, et de l'article 19.

4. Lorsqu'un organisme du secteur public ou une institution, un organe ou un organisme de l'Union transmet ou met des données à disposition en vertu du paragraphe 1, il ou elle en informe le détenteur de données de qui émanent les données reçues.

Article 22
Assistance mutuelle et coopération transfrontière

1. Les organismes du secteur public et les institutions, organes et organismes de l'Union coopèrent et se prêtent mutuellement assistance afin de mettre en œuvre le présent chapitre de manière cohérente.

2. Les données échangées dans le cadre de la demande d'assistance et fournies en vertu du paragraphe 1 ne sont pas utilisées d'une manière incompatible avec la finalité pour laquelle elles ont été demandées.

3. Lorsqu'un organisme du secteur public a l'intention de demander des données à un détenteur de données établi dans un autre État membre, il notifie d'abord cette

intention à l'autorité compétente de cet État membre comme le prévoit l'article 31. Cette exigence s'applique également aux demandes adressées par les institutions, organes et organismes de l'Union.

4. Après avoir été avisée conformément au paragraphe 3, l'autorité compétente concernée informe l'organisme du secteur public demandeur de la nécessité, le cas échéant, de coopérer avec les organismes du secteur public de l'État membre dans lequel le détenteur de données est établi, dans le but de réduire la charge administrative qui pèse sur le détenteur de données pour se conformer à la demande. L'organisme du secteur public demandeur tient compte de l'avis de l'autorité compétente concernée.

CHAPITRE VI

CHANGEMENT DE SERVICES DE TRAITEMENT DES DONNÉES

Article 23

Suppression des obstacles au changement efficace de fournisseur de services de traitement des données

1. Les fournisseurs d'un service de traitement des données prennent les mesures prévues aux articles 24, 25 et 26 pour veiller à ce que les clients de leur service puissent passer à un autre service de traitement des données, couvrant le même type de service, qui est proposé par un autre fournisseur de services. En particulier, les fournisseurs de services de traitement des données suppriment les obstacles commerciaux, techniques, contractuels et organisationnels, qui freinent les clients dans les démarches suivantes:

   (a) la résiliation, après un préavis maximal de 30 jours calendaires, de l'accord contractuel couvrant le service;

   (b) la conclusion de nouveaux accords contractuels avec un autre fournisseur de services de traitement des données couvrant le même type de service;

   (c) le portage de leurs données, applications et autres actifs numériques vers un autre fournisseur de services de traitement des données;

   (d) le maintien de l'équivalence fonctionnelle du service dans l'environnement informatique du ou des différents fournisseurs de services de traitement des données couvrant le même type de service, conformément à l'article 26.

2. Le paragraphe 1 ne s'applique qu'aux obstacles liés aux services, accords contractuels ou pratiques commerciales du fournisseur initial.

Article 24

Clauses contractuelles concernant le changement de fournisseur de services de traitement des données

1. Les droits du client et les obligations du fournisseur d'un service de traitement des données en ce qui concerne le changement de fournisseur de ces services sont clairement énoncés dans un contrat écrit. Sans préjudice de la directive (UE) 2019/770, ce contrat comporte au moins les éléments suivants:

(a) des clauses permettant au client, sur demande, de passer à un service de traitement des données proposé par un autre fournisseur de services de traitement des données ou de transférer toutes les données, applications et actifs numériques générés directement ou indirectement par le client vers un système sur place, en particulier la mise en place d'une période transitoire obligatoire maximale de 30 jours calendaires pendant laquelle le fournisseur de services de traitement des données:

(1) apporte son aide dans le processus de changement de fournisseur et, lorsque cela est techniquement possible, achève ledit processus;

(2) assure la pleine continuité dans la fourniture des fonctions ou services respectifs;

(b) une spécification exhaustive de toutes les catégories de données et d'applications exportables pendant le processus de changement de fournisseur, y compris, au minimum, toutes les données importées par le client au début de l'accord de service et toutes les données et métadonnées créées par le client et par l'utilisation du service pendant la période de fourniture du service, y compris, mais sans s'y limiter, les paramètres de configuration, les paramètres de sécurité, les droits d'accès et les historiques d'accès au service;

(c) une période minimale pour l'extraction des données d'au moins 30 jours calendaires à compter de la fin de la période transitoire convenue entre le client et le fournisseur de services, conformément au paragraphe 1, point a), et au paragraphe 2.

2. Lorsqu'il est techniquement impossible de respecter la période transitoire obligatoire définie au paragraphe 1, points a) et c), du présent article, le fournisseur de services de traitement des données en informe le client dans un délai de 7 jours ouvrables à compter de la présentation de la demande de changement de fournisseur, en motivant dûment l'impossibilité technique par un rapport détaillé et en indiquant une autre période transitoire, qui ne peut excéder 6 mois. Conformément au paragraphe 1 du présent article, la pleine continuité du service est assurée tout au long de l'autre période transitoire avec une réduction des frais, visée à l'article 25, paragraphe 2.

Article 25

Suppression progressive des frais de changement de fournisseur

1. À compter du [date X + 3 ans], les fournisseurs de services de traitement des données n'imposent aucun frais au client pour le changement de fournisseur.

2. À compter du [date X, la date d'entrée en vigueur du règlement sur les données] et jusqu'au [date X + 3 ans], les fournisseurs de services de traitement des données peuvent imposer des frais réduits au client pour le changement de fournisseur.

3. Les frais visés au paragraphe 2 ne dépassent pas les coûts supportés par le fournisseur de services de traitement des données qui sont directement liés au changement concerné.

4. La Commission est habilitée à adopter des actes délégués conformément à l'article 38 pour compléter le présent règlement afin d'introduire un mécanisme de suivi permettant à la Commission de suivre les frais de changement de fournisseur appliqués sur le marché par les fournisseurs de services de traitement des données

afin de garantir que la suppression des frais de changement de fournisseur visée au paragraphe 1 du présent article est réalisée dans le délai prévu au même paragraphe.

Article 26
Aspects techniques du changement de fournisseur

1. Les fournisseurs de services de traitement des données qui sont liés à des ressources informatiques modulables et variables limitées à des éléments d'infrastructure tels que les serveurs, les réseaux et les ressources virtuelles nécessaires à l'exploitation de l'infrastructure, mais qui ne donnent pas accès aux services, logiciels et applications d'exploitation qui sont stockés, traités ou déployés sur ces éléments d'infrastructure, veillent à ce que le client, après être passé à un service couvrant le même type de service proposé par un autre fournisseur de services de traitement des données, bénéficie d'une équivalence fonctionnelle dans l'utilisation du nouveau service.
2. Pour les services de traitement des données autres que ceux visés au paragraphe 1, les fournisseurs de services de traitement des données mettent gratuitement à la disposition du public des interfaces ouvertes.
3. Pour les services de traitement des données autres que ceux visés au paragraphe 1, les fournisseurs de services de traitement des données assurent la compatibilité avec les spécifications d'interopérabilité ouvertes ou les normes européennes d'interopérabilité qui sont définies conformément à l'article 29, paragraphe 5, du présent règlement.
4. Lorsque les spécifications d'interopérabilité ouvertes ou les normes européennes visées au paragraphe 3 n'existent pas pour le type de service concerné, le fournisseur de services de traitement des données exporte, à la demande du client, toutes les données générées ou cogénérées, y compris les formats de données et structures de données pertinents, dans un format structuré, couramment utilisé et lisible par machine.

CHAPITRE VII
GARANTIES EN MATIÈRE DE DONNÉES À CARACTÈRE NON PERSONNEL DANS UN CONTEXTE INTERNATIONAL

Article 27
Accès et transfert à l'échelle internationale

1. Les fournisseurs de services de traitement des données prennent toutes les mesures techniques, juridiques et organisationnelles raisonnables, y compris les accords contractuels, afin d'empêcher le transfert à l'échelle internationale de données à caractère non personnel détenues dans l'Union ou l'accès des gouvernements tiers 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, sans préjudice des paragraphes 2 ou 3.
2. Toute décision ou tout jugement d'une juridiction et toute décision d'une autorité administrative d'un pays tiers exigeant d'un fournisseur de services de traitement des données qu'il transfère ou donne accès à des données à caractère non personnel relevant du champ d'application du présent règlement et détenues dans l'Union ne peuvent être reconnus ou rendus exécutoires de quelque manière que ce soit qu'à la condition qu'ils soient fondés 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.

3. En l'absence d'un tel accord international, lorsqu'un fournisseur de services de traitement des données est destinataire d'une décision d'une juridiction ou d'une autorité administrative d'un pays tiers de transférer depuis l'Union des données à caractère non personnel relevant du champ d'application du présent règlement et détenues dans l'Union ou d'y donner accès, 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 ou du jugement soient exposés et que cette décision ou ce jugement, 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) la juridiction compétente qui rend la décision ou le jugement ou qui contrôle la décision d'une autorité administrative est habilitée, en vertu du droit de ce pays tiers, à prendre dûment en compte les intérêts juridiques concernés du fournisseur des données protégées par le droit de l'Union ou par le droit national de l'État membre concerné.

Le destinataire de la décision peut solliciter l'avis des autorités ou organismes compétents concernés, en application du présent règlement, afin de déterminer s'il est satisfait à ces conditions, notamment lorsqu'il estime que la décision peut concerner des données commercialement sensibles ou porter atteinte aux intérêts de l'Union ou de ses États membres en matière de sécurité nationale ou de défense.

Le comité européen de l'innovation dans le domaine des données mis en place en vertu du règlement [xxx - règlement sur la gouvernance des données] conseille et assiste la Commission dans l'élaboration de lignes directrices relatives à l'appréciation de la question de savoir si ces conditions sont remplies.

4. Si les conditions énoncées au paragraphe 2 ou au paragraphe 3 sont remplies, le fournisseur de services de traitement des données fournit le volume minimal de données admissible en réponse à une demande, en partant d'une interprétation raisonnable de la demande.

5. Le fournisseur de services de traitement des 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 avant de donner suite à la demande, 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.

CHAPITRE VIII
INTEROPÉRABILITÉ

Article 28
Exigences essentielles concernant l'interopérabilité

1. Les exploitants d'espaces des données respectent les exigences essentielles suivantes en vue de faciliter l'interopérabilité des données, des mécanismes de partage de données et des services en la matière:

   (a) le contenu de l'ensemble de données, les restrictions d'utilisation, les licences, la méthode de collecte des données, la qualité des données et l'incertitude sur les données sont suffisamment décrits pour permettre au destinataire de trouver les données, d'y accéder et de les utiliser;

   (b) les structures de données, les formats de données, les vocabulaires, les systèmes de classification, les taxinomies et les listes de codes sont décrits de manière publiquement accessible et cohérente;

   (c) les moyens techniques d'accès aux données, tels que les interfaces de programmation d'applications, ainsi que leurs conditions d'utilisation et leur qualité de service sont suffisamment décrits pour permettre l'accès automatique aux données et leur transmission automatique entre les parties, y compris en continu ou en temps réel dans un format lisible par machine;

   (d) les moyens permettant l'interopérabilité des contrats intelligents dans le cadre de leurs services et activités sont prévus.

Ces exigences peuvent être de nature générique ou concerner des secteurs spécifiques, tout en tenant pleinement compte de l'interdépendance avec les exigences découlant d'autres législations sectorielles nationales ou de l'Union.

2. La Commission est habilitée à adopter des actes délégués conformément à l'article 38 afin de compléter le présent règlement en précisant davantage les exigences essentielles visées au paragraphe 1.

3. Les exploitants d'espaces des données qui satisfont aux normes harmonisées ou à des parties de normes harmonisées dont les références ont été publiées au Journal officiel de l'Union européenne sont présumés respecter les exigences essentielles visées au paragraphe 1 du présent article, dans la mesure où ces normes couvrent ces exigences.

4. Conformément à l'article 10 du règlement (UE) nº 1025/2012, la Commission peut demander à une ou plusieurs organisations européennes de normalisation d'élaborer des normes harmonisées qui satisfont aux exigences essentielles visées au paragraphe 1 du présent article.

5. La Commission, par voie d'actes d'exécution, adopte des spécifications communes lorsque les normes harmonisées visées au paragraphe 4 du présent article n'existent pas ou lorsqu'elle estime que les normes harmonisées pertinentes sont insuffisantes pour garantir la conformité aux exigences essentielles visées au paragraphe 1 du présent article, le cas échéant, en ce qui concerne l'une ou l'ensemble des exigences énoncées au paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 39, paragraphe 2.

6. La Commission peut adopter des lignes directrices établissant des spécifications d'interopérabilité pour le fonctionnement des espaces européens communs des données, telles que des règles et accords juridiques d'exécution entre parties pour les modèles architecturaux et les normes techniques qui favorisent le partage de données, par exemple en ce qui concerne les droits d'accès et la traduction technique du consentement ou de l'autorisation.

Article 29
Interopérabilité des services de traitement des données

1. Les spécifications d'interopérabilité ouvertes et les normes européennes pour l'interopérabilité des services de traitement des données:

   (a) sont orientées vers les performances et la réalisation de l'interopérabilité entre différents services de traitement des données couvrant le même type de service;

   (b) améliorent la portabilité des actifs numériques entre différents services de traitement des données couvrant le même type de service;

   (c) garantissent, lorsque cela est techniquement possible, l'équivalence fonctionnelle entre différents services de traitement des données couvrant le même type de service.

2. Les spécifications d'interopérabilité ouvertes et les normes européennes pour l'interopérabilité des services de traitement des données couvrent:

   (a) les aspects de l'interopérabilité de l'informatique en nuage pour l'interopérabilité du transport de données, l'interopérabilité syntactique, l'interopérabilité sémantique des données, l'interopérabilité comportementale et l'interopérabilité stratégique;

   (b) les aspects de la portabilité des données en nuage pour la portabilité syntactique des données, la portabilité sémantique des données et la portabilité stratégique des données;

   (c) les aspects des applications en nuage pour la portabilité syntactique des applications, la portabilité des instructions des applications, la portabilité des métadonnées des applications, la portabilité comportementale des applications et la portabilité stratégique des applications.

3. Les spécifications d'interopérabilité ouvertes sont conformes aux paragraphes 3 et 4 de l'annexe II du règlement (UE) nº 1025/2012.

4. Conformément à l'article 10 du règlement (UE) nº 1025/2012, la Commission peut demander à une ou plusieurs organisations européennes de normalisation d'élaborer des normes européennes applicables à des types spécifiques de services de traitement des données.

5. Aux fins de l'article 26, paragraphe 3, du présent règlement, la Commission est habilitée à adopter des actes délégués, conformément à l'article 38, pour publier la référence des spécifications d'interopérabilité ouvertes et des normes européennes pour l'interopérabilité des services de traitement des données dans le répertoire central des normes de l'Union pour l'interopérabilité des services de traitement des données, lorsque celles-ci satisfont aux critères énoncés aux paragraphes 1 et 2 du présent article.

Article 30

Exigences essentielles concernant les contrats intelligents pour le partage de données

1. Le vendeur d'une application utilisant des contrats intelligents ou, à défaut, la personne dont l'activité commerciale, l'entreprise ou la profession nécessite le déploiement de contrats intelligents pour des tiers dans le cadre d'un accord de mise à disposition des données, respecte les exigences essentielles suivantes:

   (a) robustesse: veiller à ce que le contrat intelligent ait été conçu de manière à offrir un degré très élevé de robustesse afin d'éviter les erreurs fonctionnelles et de résister aux tentatives de manipulation par des tiers;

   (b) résiliation et interruption en toute sécurité: veiller à ce qu'il existe un mécanisme permettant de mettre fin à l'exécution continue des transactions: le contrat intelligent intègre des fonctions internes qui peuvent réinitialiser le contrat ou lui donner instruction de cesser ou d'interrompre l'opération afin d'éviter de futures exécutions (accidentelles);

   (c) archivage et continuité des données: prévoir, si un contrat intelligent doit être résilié ou désactivé, la possibilité d'archiver les données relatives aux transactions, la logique et le code du contrat intelligent afin de conserver l'enregistrement des opérations effectuées sur les données dans le passé (vérifiabilité); et

   (d) contrôle de l'accès: un contrat intelligent est protégé par des mécanismes rigoureux de contrôle d'accès au niveau de la gouvernance et des contrats intelligents.

2. Le vendeur d'un contrat intelligent ou, à défaut, la personne dont l'activité commerciale, l'entreprise ou la profession nécessite le déploiement de contrats intelligents pour des tiers dans le cadre d'un accord de mise à disposition des données, procède à une évaluation de la conformité en vue de satisfaire aux exigences essentielles visées au paragraphe 1 et, en ce qui concerne le respect des exigences, délivre une déclaration UE de conformité.

3. Lorsqu'il établit la déclaration UE de conformité, le vendeur d'une application utilisant des contrats intelligents ou, à défaut, la personne dont l'activité commerciale, l'entreprise ou la profession nécessite le déploiement de contrats intelligents pour des tiers dans le cadre d'un accord de mise à disposition des données, est responsable du respect des exigences prévues au paragraphe 1.

4. Un contrat intelligent qui satisfait aux normes harmonisées ou aux parties concernées des normes harmonisées établies et publiées au Journal officiel de l'Union européenne est présumé conforme aux exigences essentielles visées au paragraphe 1 du présent article, dans la mesure où ces normes couvrent ces exigences.

5. Conformément à l'article 10 du règlement (UE) nº 1025/2012, la Commission peut demander à une ou plusieurs organisations européennes de normalisation d'élaborer des normes harmonisées qui satisfont aux exigences essentielles visées au paragraphe 1 du présent article.

6. Lorsque les normes harmonisées visées au paragraphe 4 du présent article n'existent pas ou lorsque la Commission estime que les normes harmonisées pertinentes sont insuffisantes pour garantir la conformité aux exigences essentielles visées au paragraphe 1 du présent article dans un contexte transfrontière, la Commission peut, par voie d'actes d'exécution, adopter des spécifications communes en ce qui

concerne les exigences essentielles énoncées au paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 39, paragraphe 2.

CHAPITRE IX
MISE EN ŒUVRE ET EXÉCUTION

Article 31
Autorités compétentes

1. Chaque État membre désigne une ou plusieurs autorités compétentes chargées de l'application et de l'exécution du présent règlement. Les États membres peuvent mettre en place une ou plusieurs nouvelles autorités ou s'appuyer sur des autorités existantes.

2. Sans préjudice des dispositions du paragraphe 1 du présent article:

   (a) les autorités de contrôle indépendantes chargées de contrôler l'application du règlement (UE) 2016/679 sont responsables du contrôle de l'application du présent règlement en ce qui concerne la protection des données à caractère personnel. Les chapitres VI et VII du règlement (UE) 2016/679 s'appliquent par analogie. Les missions et pouvoirs des autorités de contrôle sont exercés à l'égard du traitement des données à caractère personnel;

   (b) pour les questions spécifiques sur l'échange de données sectorielles en lien avec la mise en œuvre du présent règlement, la compétence des autorités sectorielles est respectée;

   (c) l'autorité nationale compétente chargée de l'application et de l'exécution du chapitre VI du présent règlement dispose d'une expérience dans le domaine des données et des services de communications électroniques.

3. Les États membres veillent à ce que les missions et pouvoirs respectifs des autorités compétentes désignées en vertu du paragraphe 1 du présent article soient clairement définis et incluent:

   (a) la sensibilisation des utilisateurs et des entités relevant du champ d'application du présent règlement aux droits et obligations découlant du présent règlement;

   (b) le traitement des réclamations découlant de prétendues violations du présent règlement, l'examen de l'objet de la réclamation, dans la mesure nécessaire, et l'information de l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité compétente est nécessaire;

   (c) la réalisation d'enquêtes sur des questions concernant l'application du présent règlement, y compris sur la base d'informations reçues d'une autre autorité compétente ou d'une autre autorité publique;

   (d) l'imposition, par des procédures administratives, de sanctions financières dissuasives, pouvant comporter des astreintes et des sanctions avec effet rétroactif, ou l'engagement de procédures judiciaires en vue d'infliger des amendes;

   (e) le suivi des évolutions technologiques pertinentes pour la mise à disposition et l'utilisation des données;

(f) la coopération avec les autorités compétentes d'autres États membres pour garantir l'application cohérente du présent règlement, y compris l'échange de toutes les informations pertinentes par voie électronique, dans les meilleurs délais;

(g) l'assurance que les demandes d'accès aux données présentées par des organismes du secteur public en cas d'urgences publiques au titre du chapitre V sont mises à la disposition du public en ligne;

(h) la coopération avec toutes les autorités compétentes concernées afin de veiller à ce que les obligations du chapitre VI soient exécutées de manière cohérente avec les autres actes législatifs de l'Union et mesures d'autoréglementation applicables aux fournisseurs de services de traitement des données;

(i) l'assurance que les frais facturés pour le changement de fournisseur de services de traitement des données sont supprimés conformément à l'article 25.

4. Lorsqu'un État membre désigne plusieurs autorités compétentes, celles-ci coopèrent entre elles, dans l'exercice des missions et pouvoirs qui leur sont conférés en vertu du paragraphe 3 du présent article, y compris, le cas échéant, avec l'autorité de contrôle chargée de contrôler l'application du règlement (UE) 2016/679, afin d'assurer l'application cohérente du présent règlement. En pareil cas, les États membres concernés désignent une autorité compétente coordonnatrice.

5. Les États membres communiquent à la Commission le nom des autorités compétentes désignées ainsi que leurs missions et pouvoirs respectifs et, le cas échéant, le nom de l'autorité compétente coordonnatrice. La Commission tient un registre public de ces autorités.

6. Lorsqu'elles accomplissent leurs missions et exercent leurs pouvoirs conformément au présent règlement, les autorités compétentes restent libres de toute influence extérieure, qu'elle soit directe ou indirecte, et ne sollicitent ni n'acceptent d'instructions d'aucune autre autorité publique ni d'aucune entité privée.

7. Les États membres veillent à ce que les autorités compétentes désignées disposent des ressources nécessaires pour s'acquitter correctement de leurs tâches conformément au présent règlement.

Article 32

Droit d'introduire une réclamation auprès d'une autorité compétente

1. Sans préjudice de tout autre recours administratif ou juridictionnel, les personnes physiques et morales ont le droit d'introduire une réclamation, individuellement ou, le cas échéant, collectivement, auprès de l'autorité compétente concernée dans l'État membre dans lequel se trouve leur résidence habituelle, leur lieu de travail ou leur lieu d'établissement, si elles considèrent qu'il a été porté atteinte aux droits que leur confère le présent règlement.

2. L'autorité compétente 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.

3. Les autorités compétentes coopèrent pour traiter et résoudre les réclamations, y compris en échangeant toutes les informations pertinentes par voie électronique, dans les meilleurs délais. Cette coopération est sans effet sur le mécanisme de coopération spécifique prévu aux chapitres VI et VII du règlement (UE) 2016/679.

Article 33
Sanctions

1. Les États membres déterminent le régime des sanctions applicables aux violations du présent règlement et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Les sanctions ainsi prévues sont effectives, proportionnées et dissuasives.

2. 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, de même que, sans retard, de toute modification apportée ultérieurement à ce régime ou à ces mesures.

3. En ce qui concerne les manquements aux obligations prévues aux chapitres II, III et V du présent règlement, les autorités de contrôle visées à l'article 51 du règlement (UE) 2016/679 peuvent, dans les limites de leur compétence, infliger des amendes administratives conformément à l'article 83 du règlement (UE) 2016/679, jusqu'à concurrence du montant visé à l'article 83, paragraphe 5, dudit règlement.

4. En ce qui concerne les manquements aux obligations prévues au chapitre V du présent règlement, l'autorité de contrôle visée à l'article 52 du règlement (UE) 2018/1725 peut, dans les limites de sa compétence, infliger des amendes administratives conformément à l'article 66 du règlement (UE) 2018/1725, à concurrence du montant visé à l'article 66, paragraphe 3, dudit règlement.

Article 34
Clauses contractuelles types

La Commission élabore et recommande des clauses contractuelles types non contraignantes concernant l'accès aux données et leur utilisation afin d'aider les parties à rédiger et à négocier des contrats garantissant l'équilibre des droits et obligations contractuels.

CHAPITRE X
DROIT «SUI GENERIS» PRÉVU PAR LA DIRECTIVE 96/9/CE

Article 35
Bases de données contenant certaines données

Afin de ne pas entraver l'exercice du droit des utilisateurs d'accéder aux données et de les utiliser conformément à l'article 4 du présent règlement ou du droit de partager ces données avec des tiers conformément à l'article 5 du présent règlement, le droit «sui generis» prévu par l'article 7 de la directive 96/9/CE ne s'applique pas aux bases de données contenant des données obtenues ou générées par l'utilisation d'un produit ou d'un service lié.

CHAPITRE XI
DISPOSITIONS FINALES

Article 36
Modification du règlement (UE) 2017/2394

À l'annexe du règlement (UE) 2017/2394, le point suivant est ajouté:

«29. [Règlement (UE) XXX du Parlement européen et du Conseil (règlement sur les

données)].».

Article 37
Modification de la directive (UE) 2020/1828

À l'annexe I de la directive (UE) 2020/1828, le point suivant est ajouté:

«67) [Règlement (UE) XXX du Parlement européen et du Conseil (règlement sur les données)].».

Article 38
Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées dans le présent article.
2. Le pouvoir d'adopter des actes délégués visé à l'article 25, paragraphe 4, à l'article 28, paragraphe 2, et à l'article 29, paragraphe 5, est conféré à la Commission pour une durée indéterminée à compter du [...].
3. La délégation de pouvoir visée à l'article 25, paragraphe 4, à l'article 28, paragraphe 2, et à l'article 29, paragraphe 5, 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 d'adopter un acte délégué, la Commission consulte des experts désignés par chaque État membre conformément aux principes énoncés dans l'accord interinstitutionnel «Mieux légiférer» du 13 avril 2016.
5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie simultanément au Parlement européen et au Conseil.
6. Un acte délégué adopté en vertu de l'article 25, paragraphe 4, de l'article 28, paragraphe 2, et de l'article 29, paragraphe 5, 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 39
Procédure de comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) nº 182/2011.
2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

Article 40

Autres actes juridiques de l'Union régissant les droits et obligations relatifs à l'accès aux données et à leur utilisation

1. Les obligations spécifiques relatives à la mise à disposition de données entre entreprises, entre entreprises et consommateurs, et, à titre exceptionnel, entre entreprises et organismes du secteur public, définies dans les actes juridiques de l'Union entrés en vigueur le [xx XXX xxx] ou avant cette date et dans les actes délégués ou d'exécution fondés sur ces actes, restent inchangées.

2. Le présent règlement est sans préjudice de la législation de l'Union spécifiant, à la lumière des besoins d'un secteur, d'un espace européen commun des données ou d'un domaine d'intérêt public, d'autres exigences, en particulier en ce qui concerne:

   (a) les aspects techniques de l'accès aux données;

   (b) les limitations des droits des détenteurs de données d'accéder à certaines données fournies par les utilisateurs ou de les utiliser;

   (c) les aspects allant au-delà de l'accès aux données et de leur utilisation.

Article 41

Évaluation et réexamen

Au plus tard le [*deux 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. Cette évaluation porte, en particulier, sur les aspects suivants:

(a) les autres catégories ou types de données devant être rendus accessibles;

(b) l'exclusion de certaines catégories d'entreprises en tant que bénéficiaires au titre de l'article 5;

(c) les autres situations devant être considérées comme des besoins exceptionnels aux fins de l'article 15;

(d) les changements dans les pratiques contractuelles des fournisseurs de services de traitement des données et la question de savoir si cela se traduit par un respect suffisant de l'article 24;

(e) la réduction des frais imposés par les fournisseurs de services de traitement des données pour le processus de changement, en concordance avec la suppression progressive des frais de changement de fournisseur en vertu de l'article 25.

Article 42

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 la date d'entrée en vigueur du présent règlement].

Fait à Bruxelles, le

Par le Parlement européen
La présidente

Par le Conseil
Le président