Journal officiel
de l'Union européenne

FR
Série L

2023/2854

22.12.2023

RÈGLEMENT (UE) 2023/2854 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 13 décembre 2023

concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (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 de la Banque centrale européenne ([1]),

vu l'avis du Comité économique et social européen ([2]),

vu l'avis du Comité des régions ([3]),

statuant conformément à la procédure législative ordinaire ([4]),

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 prolifération des produits connectés à l'internet, 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. Les mêmes données peuvent être utilisées et réutilisées 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 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, les coûts afférents à la passation de contrats d'interface technique et à la mise en œuvre des interfaces techniques, l'importante fragmentation des informations stockées en silos de données, 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 de nombreuses microentreprises, petites entreprises et moyennes entreprises telles qu'elles sont définies à l'article 2 de l'annexe de la recommandation 2003/361/CE de la Commission ([5]) (PME), on constate souvent un manque de capacités et de compétences numériques pour collecter, analyser et utiliser des données et l'accès à celles-ci est fréquemment restreint soit parce qu'elles sont détenues par un seul acteur au sein du système, soit en raison de l'absence d'interopérabilité entre les données, entre les services de données ou 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 précisant qui dispose du droit d'utiliser les données relatives au produit ou les données relatives au service connexe, dans quelles conditions et sur quel

([1]) JO C 402 du 19.10.2022, p. 5.
([2]) JO C 365 du 23.9.2022, p. 18.
([3]) JO C 375 du 30.9.2022, p. 112.
([4]) Position du Parlement européen du 9 novembre 2023 (non encore parue au Journal officiel) et décision du Conseil du 27 novembre 2023.
([5]) Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

fondement. Par conséquent, les États membres ne devraient pas adopter ou conserver des exigences nationales supplémentaires en ce qui concerne les questions relevant du champ d'application du présent règlement, sauf disposition expresse de ce dernier, car cela porterait atteinte à son application directe et uniforme. De plus, une action au niveau de l'Union devrait être sans préjudice des obligations et des engagements prévus dans les accords commerciaux internationaux conclus par l'Union.

(5) Il est fait en sorte par le présent règlement que les utilisateurs d'un produit connecté ou d'un service connexe dans l'Union puissent avoir accès, en temps utile, aux données générées par l'utilisation de ce produit connecté ou de ce service connexe 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 aux détenteurs de données l'obligation, dans certaines circonstances, de mettre des données à la disposition des utilisateurs et des tiers choisis par un utilisateur. Il prévoit également que les détenteurs de données mettent des données à la disposition des destinataires de données dans l'Union selon des modalités et 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 des déséquilibres contractuels qui entravent l'équité de l'accès aux données et de l'utilisation des données. Le présent règlement prévoit également qu'en cas de besoin exceptionnel, les détenteurs de données mettent à la disposition des organismes du secteur public, de la Commission, de la Banque centrale européenne ou des organes de l'Union les données nécessaires à l'exécution d'une mission spécifique d'intérêt public. Le présent règlement vise en outre à faciliter le changement de services de traitement de données et à améliorer l'interopérabilité des données ainsi que des mécanismes et services de partage de données dans l'Union. Il convient de ne pas interpréter le présent règlement comme reconnaissant ou conférant aux détenteurs de données un droit nouveau d'utiliser les données générées par l'utilisation d'un produit connecté ou d'un service connexe.

(6) Des données sont générées sous l'effet des actions d'au moins deux acteurs, notamment le concepteur ou fabricant d'un produit connecté, qui peut être dans de nombreux cas également un fournisseur de services connexes, et l'utilisateur du produit connecté ou du service connexe. La génération de données soulève des questions d'équité dans l'économie numérique étant donné que les données enregistrées par les produits connectés ou les services connexes constituent un apport important pour les services après-vente, les services auxiliaires et autres. Pour concrétiser les avantages économiques importants que recèlent les données, y compris par le partage de données sur la base d'accords volontaires et le développement de la création de valeur fondée sur les données par les entreprises de l'Union, une approche générale de l'attribution de droits relatifs à l'accès aux données et à l'utilisation de données est préférable à l'octroi de droits exclusifs d'accès et d'utilisation. Le présent règlement prévoit des règles horizontales qui pourraient être suivies par des dispositions du droit de l'Union ou du droit national qui règlent les situations spécifiques des secteurs concernés.

(7) Le droit fondamental à la protection des données à caractère personnel est garanti notamment par les règlements (UE) 2016/679 ([6]) et (UE) 2018/1725 ([7]) du Parlement européen et du Conseil. En outre, la directive 2002/58/CE du Parlement européen et du Conseil ([8]) protège la vie privée et la confidentialité des communications, notamment en prévoyant des conditions régissant tout stockage de données à caractère personnel et à caractère non personnel dans un équipement terminal et tout accès à ces données à partir dudit équipement. Ces actes législatifs de l'Union 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 du droit de l'Union relatives à la protection des données à caractère personnel et à la vie privée, en particulier les règlements (UE) 2016/679 et (UE) 2018/1725, 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. Tout traitement de données à caractère personnel effectué

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

([7]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

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

au titre du présent règlement devrait respecter le droit de l'Union en matière de protection des données, y compris l'exigence d'une base juridique valable pour un traitement relevant de l'article 6 du règlement (UE) 2016/679 et, le cas échéant, les conditions de l'article 9 dudit règlement et de l'article 5, paragraphe 3, de la directive 2002/58/CE. Le présent règlement ne constitue pas une base juridique pour la collecte ou la génération de données à caractère personnel par le détenteur de données. Le présent règlement impose aux détenteurs de données l'obligation de mettre des données personnelles à la disposition des utilisateurs ou de tiers choisis par un utilisateur à la demande dudit utilisateur. Un tel accès devrait être donné aux données à caractère personnel qui sont traitées par le détenteur de données sur le fondement de l'une des bases juridiques mentionnées à l'article 6 du règlement (UE) 2016/679. Lorsque l'utilisateur n'est pas la personne concernée, le présent règlement ne crée pas de base juridique permettant de donner l'accès à des données à caractère personnel ou de mettre des données à caractère personnel à la disposition d'un tiers et il ne devrait pas être interprété comme conférant au détenteur de données un droit nouveau d'utiliser les données à caractère personnel générées par l'utilisation d'un produit connecté ou d'un service connexe. En pareils cas, il pourrait être dans l'intérêt de l'utilisateur de faciliter le respect des exigences de l'article 6 du règlement (UE) 2016/679. Étant donné que le présent règlement ne devrait pas porter atteinte aux droits des personnes concernées en matière de protection des données, le détenteur de données peut donner suite aux demandes en pareils cas, entre autres, en anonymisant les données à caractère personnel ou, lorsque les données facilement accessibles contiennent les données à caractère personnel de plusieurs personnes concernées, en ne transmettant que des données à caractère personnel relatives à l'utilisateur.

(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 le partage de données relevant 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 chiffrement, 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 entre les parties ni copie inutile des données brutes ou des données structurées elles-mêmes.

(9) Sauf disposition contraire de celui-ci, le présent règlement n'affecte pas le droit national des contrats, y compris les règles relatives à la formation, à la validité ou aux effets des contrats, ni les conséquences de la résiliation d'un contrat. Le présent règlement complète, sans y porter atteinte, le droit de l'Union qui vise à promouvoir les intérêts des consommateurs et à assurer un niveau élevé de protection des consommateurs, ainsi qu'à protéger leur santé, leur sécurité et leurs intérêts économiques, en particulier la directive 93/13/CEE du Conseil ([9]) et les directives 2005/29/CE ([10]) et 2011/83/UE ([11]) du Parlement européen et du Conseil.

(10) Le présent règlement est sans préjudice des actes juridiques de l'Union et des actes juridiques nationaux qui prévoient le partage de données, l'accès aux données et l'utilisation de données 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 base juridique prévue par le traité sur le fonctionnement de l'Union européenne sur laquelle ces actes juridiques de l'Union ont été adoptés, et sans préjudice de la coopération internationale dans ce domaine fondée, en particulier, sur la convention du Conseil de l'Europe sur la cybercriminalité, (STE n° 185), signée à Budapest le 23 novembre 2001. Il s'agit notamment des règlements (UE) 2021/784 ([12]), (UE) 2022/2065 ([13]) et (UE) 2023/1543 ([14]) du Parlement européen et du Conseil et de la

([9]) Directive 93/13/CEE du Conseil, du 5 avril 1993, concernant les clauses abusives dans les contrats conclus avec les consommateurs (JO L 95 du 21.4.1993, p. 29).

([10]) 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) n° 2006/2004 du Parlement européen et du Conseil ("directive sur les pratiques commerciales déloyales") (JO L 149 du 11.6.2005, p. 22).

([11]) 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 (JO L 304 du 22.11.2011, p. 64).

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

([13]) Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (JO L 277 du 27.10.2022, p. 1).

([14]) Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation de preuves électroniques, dans les procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale (JO L 191 du 28.7.2023, p. 118).

directive (UE) 2023/1544 du Parlement européen et du Conseil ([15]). Le présent règlement ne s'applique pas à la collecte ou au partage de données, à l'accès aux données ou à l'utilisation de données au titre du règlement (UE) 2015/847 du Parlement européen et du Conseil ([16]) et de la directive (UE) 2015/849 du Parlement européen et du Conseil ([17]). Le présent règlement ne s'applique pas aux domaines qui ne relèvent pas du champ d'application du droit de l'Union et, en tout état de cause, ne porte pas atteinte aux compétences des États membres en ce qui concerne la sécurité publique, la défense ou la sécurité nationale, les douanes et l'administration fiscale ou la santé et la sécurité des citoyens, quel que soit le type d'entité chargée par les États membres d'exécuter des tâches liées à ces compétences.

(11) Sauf disposition expresse spécifique de celui-ci, le présent règlement ne devrait pas avoir d'incidence sur les dispositions du 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 du droit de l'Union qui visent à établir des exigences en matière d'accessibilité applicables à certains produits et services, en particulier la directive (UE) 2019/882 du Parlement européen et du Conseil ([18]).

(13) Le présent règlement n'a pas d'incidence sur les actes juridiques de l'Union et nationaux prévoyant la protection des droits de propriété intellectuelle, notamment les directives 2001/29/CE ([19]), 2004/48/CE ([20]) et (UE) 2019/790 ([21]) du Parlement européen et du Conseil.

(14) Les produits connectés qui, au moyen de leurs composants ou systèmes d'exploitation, obtiennent, génèrent ou collectent 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, d'une connexion physique ou d'un accès sur un appareil, souvent appelés "l'internet des objets", devraient relever du champ d'application du présent règlement, à l'exception des prototypes. Parmi les exemples de tels services de communications électroniques, on peut citer notamment les réseaux téléphoniques terrestres, les réseaux câblés de télévision, les réseaux par satellite et les réseaux de communication en champ proche. Les produits connectés sont présents dans tous les domaines de l'économie et de la société, notamment dans les infrastructures privées, civiles ou commerciales, les véhicules, les équipements de santé et de bien-être, les navires, les avions, les équipements domestiques et les biens de consommation, les dispositifs médicaux et sanitaires, ou encore les machines agricoles et industrielles. Les choix de conception des fabricants et, le cas échéant, les dispositions du droit de l'Union ou du droit national qui répondent aux besoins et aux objectifs propres à un secteur ou les décisions pertinentes des autorités compétentes devraient déterminer les données qu'un produit connecté peut mettre à disposition.

(15) Les données représentent la numérisation des actions de l'utilisateur et des événements et devraient, dès lors, être accessibles à l'utilisateur. Les règles relatives à l'accès aux données provenant de produits connectés et de services connexes et à l'utilisation de ces données au titre du présent règlement concernent à la fois les données relatives au produit et les données relatives au service connexe. Les données relatives au produit désignent les données générées par l'utilisation d'un produit connecté que le fabricant a conçues pour pouvoir être extraites du produit connecté par un utilisateur, un détenteur de données ou un tiers, y compris, le cas échéant, le fabricant. Les données relatives

([15]) Directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de la collecte de preuves électroniques en matière pénale (JO L 191 du 28.7.2023, p. 181).

([16]) Règlement (UE) 2015/847 du Parlement européen et du Conseil du 20 mai 2015 sur les informations accompagnant les transferts de fonds et abrogeant le règlement (CE) n° 1781/2006 (JO L 141 du 5.6.2015, p. 1).

([17]) Directive (UE) 2015/849 du Parlement Européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission (JO L 141 du 5.6.2015, p. 73).

([18]) 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).

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

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

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

au service connexe désignent les données représentant également la numérisation des actions de l'utilisateur ou des événements liés au produit connecté qui sont générées lors de la fourniture d'un service connexe par le fournisseur. Les données générées par l'utilisation d'un produit connecté ou d'un service connexe devraient s'entendre comme comprenant les données enregistrées intentionnellement ou les données qui résultent indirectement de l'action de l'utilisateur, telles que les données relatives à l'environnement ou aux interactions du produit connecté. Cela devrait inclure les données sur l'utilisation d'un produit connecté générées par une interface utilisateur ou par l'intermédiaire d'un service connexe, et ne devraient pas se limiter à l'information indiquant qu'une telle utilisation a eu lieu, mais devraient inclure toutes les données générées par le produit connecté à la suite de cette utilisation, telles que les données générées automatiquement par des capteurs et les données enregistrées par des applications intégrées, y compris les applications indiquant l'état du matériel et les dysfonctionnements. Cela devrait également inclure les données générées par le produit connecté ou le service connexe en période d'inaction de l'utilisateur, par exemple lorsque l'utilisateur choisit de ne pas utiliser un produit connecté pendant une période donnée et de le maintenir en mode veille, voire éteint, étant donné que le statut d'un produit connecté ou de ses composants, par exemple ses batteries, peut varier lorsque le produit connecté est en mode veille ou éteint. Relèvent du champ d'application du présent règlement les données qui ne sont pas substantiellement modifiées, c'est-à-dire les données sous forme brute, également appelées "données sources" ou "données primaires", désignant des points de données qui sont générés automatiquement sans autre forme de traitement, ainsi que les données qui ont été prétraitées dans le but de les rendre compréhensibles et utilisables avant leur traitement et leur analyse ultérieurs. Ces données comprennent les données collectées à partir d'un capteur unique ou d'un groupe de capteurs connecté dans le but de rendre les données collectées compréhensibles pour les cas d'utilisation plus larges en déterminant une grandeur ou une qualité physique ou la modification d'une grandeur physique, telle que la température, la pression, le débit, l'audio, la valeur de pH, le niveau de liquide, la position, l'accélération ou la vitesse. L'expression "données prétraitées" ne devrait pas être interprétée de manière à imposer au détenteur de données l'obligation de réaliser des investissements substantiels dans le nettoyage et la transformation des données. Les données qui doivent être mises à disposition devraient inclure les métadonnées pertinentes, y compris leur contexte de base et leur horodatage, pour rendre les données utilisables, combinées à d'autres données, telles que les données triées et classifiées avec d'autres points de données les concernant, ou reformatées dans un format couramment utilisé. De telles données sont potentiellement précieuses pour l'utilisateur et favorisent l'innovation et le développement de services numériques et d'autres services en faveur de la protection de l'environnement, de la santé et de l'économie circulaire, notamment en facilitant l'entretien et la réparation des produits connectés en question. À l'inverse, les informations dérivées ou déduites de ces données, qui sont le résultat d'investissements supplémentaires dans l'attribution de valeurs ou d'informations tirées des données, en particulier au moyen d'algorithmes complexes et propriétaires, y compris ceux qui font partie d'un logiciel propriétaire, ne devraient pas être considérées comme relevant du champ d'application du présent règlement et ne devraient donc pas être soumises à l'obligation pour un détenteur de données de les mettre à la disposition d'un utilisateur ou d'un destinataire de données, sauf accord contraire entre l'utilisateur et le détenteur de données. Ces données pourraient comprendre en particulier les informations obtenues au moyen de la fusion de capteurs, qui infère ou déduit des données provenant de capteurs multiples, collectées dans le produit connecté, au moyen d'algorithmes complexes et propriétaires, et qui pourraient être soumises à des droits de propriété intellectuelle.

(16) Le présent règlement permet aux utilisateurs de produits connectés de bénéficier de services après-vente, auxiliaires et autres sur la base de données collectées par des capteurs intégrés dans ces produits, la collecte de ces données étant potentiellement utile pour améliorer la performance des produits connectés. Il importe de délimiter, d'une part, les marchés de fourniture de ces produits connectés équipés de capteurs et de fourniture de services connexes et, d'autre part, les marchés de logiciels et de contenus non connexes, tels que les contenus textuels, audio ou audiovisuels, souvent couverts par des droits de propriété intellectuelle. Dès lors, les données que ces produits connectés équipés de capteurs génèrent lorsque l'utilisateur enregistre, transmet, affiche ou lit du contenu, ainsi que le contenu lui-même, qui est souvent couvert par des droits de propriété intellectuelle, entre autres pour une utilisation par un service en ligne, ne devraient pas être couvertes par le présent règlement. Le présent règlement ne devrait pas non plus couvrir les données qui ont été obtenues, générées ou auxquelles il est accédé à partir du produit connecté, ou qui lui ont été transmises, à des fins de stockage ou d'autres opérations de traitement pour le compte d'autres parties, qui ne sont pas l'utilisateur, comme cela peut être le cas pour des serveurs ou des infrastructures en nuage exploités par leurs propriétaires entièrement pour le compte de tiers, entre autres en vue de leur utilisation par un service en ligne.

(17) Il est nécessaire de fixer des règles concernant les produits qui sont connectés à un service connexe au moment de l'achat, de la location ou de la conclusion du crédit-bail d'une manière telle que l'absence de ce service empêcherait le produit connecté de remplir une ou plusieurs de ses fonctions, ou un service connexe qui est ensuite connecté au produit par le fabricant ou un tiers afin de compléter ou d'adapter la fonctionnalité du produit connecté. Ces services connexes impliquent l'échange de données entre le produit connecté et le fournisseur de services et devraient être compris comme étant explicitement liés à l'utilisation des fonctions du produit connecté, tels que des services qui, le cas échéant, transmettent au produit connecté des commandes qui peuvent avoir une incidence sur son action ou son comportement. Les services qui n'ont pas d'incidence sur le fonctionnement du produit connecté et qui n'impliquent pas la transmission de données ou de commandes au produit connecté par le fournisseur de

services ne devraient pas être considérés comme des services connexes. De tels services pourraient inclure, par exemple, des services auxiliaires de conseil, d'analyse ou des services financiers, ou des services réguliers de réparation et d'entretien. Les services connexes peuvent être proposés dans le cadre du contrat d'achat, de location ou de crédit-bail. Des services connexes pourraient aussi être fournis pour des produits du même type et les utilisateurs pourraient raisonnablement s'attendre à ce qu'ils soient fournis en tenant compte de la nature du produit connecté et de toute déclaration publique faite par le vendeur, le loueur, le bailleur ou d'autres personnes situées en amont de la chaîne de transactions, y compris le fabricant, ou pour leur compte. Ces services connexes peuvent eux-mêmes générer des données de valeur pour l'utilisateur indépendamment des capacités de collecte de données du produit connecté avec lequel ils sont interconnectés. Le présent règlement devrait également s'appliquer à un service connexe qui n'est pas fourni par le vendeur, le loueur ou le bailleur lui-même, mais qui est fourni par un tiers. En cas de doute sur la question de savoir si le service est ou non fourni dans le cadre du contrat d'achat, de location ou de crédit-bail, le présent règlement devrait s'appliquer. Ni la fourniture d'énergie ni la fourniture de connectivité ne doivent être interprétées comme étant des services connexes au titre du présent règlement.

(18) Il convient d'entendre par utilisateur d'un produit connecté une personne physique ou morale, telle qu'une entreprise, un consommateur ou un organisme du secteur public, qui est le propriétaire d'un produit connecté, a reçu certains droits temporaires, par exemple en vertu d'un contrat de location ou de crédit-bail, d'accéder aux données obtenues à partir du produit connecté ou de les utiliser, ou reçoit des services connexes pour le produit connecté. Ces droits d'accès ne devraient en aucun cas modifier les droits des personnes concernées qui peuvent interagir avec un produit connecté ou un service connexe en ce qui concerne les données à caractère personnel générées par le produit connecté ou pendant la fourniture du service connexe, ni interférer avec ces droits. L'utilisateur supporte les risques et bénéficie des avantages que présente l'utilisation du produit connecté et devrait également bénéficier de l'accès aux données que ce produit génère. L'utilisateur devrait par conséquent avoir le droit de tirer parti des données générées par ce produit connecté et par tout service connexe. Les propriétaires, les loueurs ou les bailleurs devraient également être considérés comme des utilisateurs, y compris lorsque plusieurs entités peuvent être considérées comme des utilisateurs. Dans le cas d'utilisateurs multiples, chaque utilisateur peut contribuer de manière différente à la production de données et avoir un intérêt dans plusieurs formes d'utilisation, telles que la gestion de flotte pour une entreprise de crédit-bail ou des solutions de mobilité pour les particuliers utilisant un service de partage de véhicule.

(19) L'éducation aux données renvoie aux compétences, aux connaissances et à la compréhension permettant aux utilisateurs, consommateurs et entreprises, en particulier les PME relevant du champ d'application du présent règlement, d'être sensibilisés à la valeur potentielle des données qu'ils génèrent, produisent et partagent et qu'ils sont disposés à offrir et auxquelles ils sont prêts à donner accès, conformément aux règles juridiques applicables. L'éducation aux données devrait aller au-delà de l'apprentissage des outils et technologies et avoir pour objectif de donner aux citoyens et entreprises la capacité et le pouvoir de bénéficier d'un marché des données inclusif et équitable. L'application de mesures en matière d'éducation aux données et l'introduction d'actions de suivi appropriées pourraient contribuer à améliorer les conditions de travail et, en fin de compte, soutenir la consolidation de l'économie des données dans l'Union et son potentiel en matière d'innovation. Les autorités compétentes devraient promouvoir des outils et adopter des mesures visant à faire progresser l'éducation aux données parmi les utilisateurs et les entités relevant du champ d'application du présent règlement, ainsi qu'à les sensibiliser à leurs droits et obligations au titre de celui-ci.

(20) En pratique, les données générées par des produits connectés ou des services connexes ne sont pas toutes facilement accessibles à leurs utilisateurs et les possibilités en ce qui concerne la portabilité des données générées par les produits connectés à l'internet 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, pratiques et plus efficaces. Dans de nombreux secteurs, les fabricants peuvent déterminer, par le contrôle qu'ils exercent sur la conception technique des produits connectés ou des services connexes, les données qui sont 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 connectés soient conçus et fabriqués, et à ce que les services connexes soient conçus et fournis, de telle manière que l'utilisateur dispose toujours d'un accès facile et sécurisé aux données relatives au produit et aux données relatives au service connexe, y compris aux métadonnées correspondantes nécessaires pour interpréter et utiliser ces données, notamment aux fins d'extraction, d'utilisation ou de partage des données, et ce gratuitement, dans un format complet, structuré, couramment utilisé et lisible par machine. On entend par "données facilement accessibles" les données relatives au produit et au service connexe qu'un détenteur de données obtient ou peut obtenir légalement du produit connecté ou du service connexe, par exemple au moyen de la conception du produit connecté, du contrat passé entre le détenteur de données et l'utilisateur pour la fourniture de services connexes et des moyens techniques d'accès aux données dont le détenteur de données dispose, sans effort disproportionné. Les données facilement accessibles ne comprennent pas les données générées par l'utilisation d'un produit connecté lorsque la

conception du produit connecté ne prévoit pas que ces données sont stockées ou transmises en dehors du composant dans lequel elles sont générées ou du produit connecté dans son ensemble. Le présent règlement ne devrait donc pas s'entendre comme imposant une obligation de stocker des données dans l'unité informatique centrale d'un produit connecté. L'absence d'une telle obligation ne devrait pas empêcher le fabricant ou le détenteur de données de convenir volontairement avec l'utilisateur de procéder à de telles adaptations. Les obligations en matière de conception prévues par le présent règlement sont également sans préjudice du principe de minimisation des données énoncé à l'article 5, paragraphe 1, point c), du règlement (UE) 2016/679 et ne devraient pas être interprétées comme imposant une obligation de concevoir des produits connectés et des services connexes de telle manière qu'ils stockent ou traitent d'une autre manière des données à caractère personnel autres que les données à caractère personnel nécessaires en ce qui concerne les finalités pour lesquelles elles sont traitées. Des dispositions du droit de l'Union ou du droit national pourraient être introduites pour définir d'autres spécificités, telles que les données relatives aux produits qui devraient être accessibles à partir de produits connectés ou de services connexes, étant donné que ces données peuvent être essentielles au fonctionnement, à la réparation ou à l'entretien efficaces de ces produits connectés ou services connexes. Lorsque des mises à jour ou des modifications ultérieures d'un produit connecté ou d'un service connexe, par le fabricant ou une autre partie, aboutissent à une augmentation des données accessibles ou à une limitation des données initialement accessibles, ces modifications devraient être communiquées à l'utilisateur dans le cadre de la mise à jour ou de la modification.

(21) Lorsque plusieurs personnes ou entités sont considérées comme étant des utilisateurs, par exemple en cas de copropriété ou lorsqu'un propriétaire, un loueur ou un bailleur partage des droits d'accès aux données ou d'utilisation de données, la conception du produit connecté ou du service connexe, ou l'interface pertinente, devrait permettre à chaque utilisateur d'avoir accès aux données qu'ils génèrent. L'utilisation de produits connectés qui génèrent des données nécessite généralement la création d'un compte d'utilisateur. Un tel compte permet l'identification de l'utilisateur par le détenteur de données, qui peut être le fabricant. Il peut également être utilisé comme moyen de communication et pour introduire et traiter des demandes d'accès aux données. Lorsque plusieurs fabricants ou fournisseurs de services connexes ont vendu ou loué des produits connectés à un même utilisateur ou conclu un crédit-bail ayant pour objet de tels produits avec un même utilisateur, ou fourni des services connexes à un même utilisateur, ces produits et services étant intégrés ensemble, l'utilisateur devrait s'adresser à chacune des parties avec lesquelles il a conclu un contrat. Les fabricants ou concepteurs d'un produit connecté qui est généralement utilisé par plusieurs personnes devraient mettre en place les mécanismes nécessaires permettant la coexistence de comptes d'utilisateur distincts pour différentes personnes, le cas échéant, ou permettant à plusieurs personnes d'utiliser le même compte d'utilisateur. Les solutions de compte devraient permettre aux utilisateurs de supprimer leurs comptes et d'effacer les données qui s'y rapportent et pourraient permettre aux utilisateurs de mettre fin à l'accès aux données, à l'utilisation ou au partage de données, ou de présenter des demandes de résiliation, compte tenu notamment des situations dans lesquelles la propriété ou l'utilisation du produit connecté change. L'accès devrait être accordé à l'utilisateur sur la base d'un mécanisme 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 souhaite effectivement y avoir accès. Lorsqu'il n'est pas possible de procéder à l'exécution automatique de la demande concernant l'accès aux données, par exemple au moyen d'un compte d'utilisateur ou d'une application mobile correspondante fournie avec le produit connecté ou le service connexe, le fabricant devrait informer l'utilisateur des modalités d'accès aux données.

(22) Les produits connectés peuvent être conçus de façon que certaines données soient directement accessibles à partir d'un dispositif de stockage de données intégré à l'appareil ou d'un serveur distant auquel les données sont communiquées. L'accès à ce dispositif de stockage de données intégré à l'appareil 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 du serveur local du fabricant ou de celle d'un tiers ou d'un fournisseur de services d'informatique en nuage. Les sous-traitants tels qu'ils sont définis à l'article 4, point 8), du règlement (UE) 2016/679 ne sont pas considérés comme agissant en qualité de détenteurs de données. Toutefois, ils peuvent être spécifiquement chargés, par le responsable du traitement tel qu'il est défini à l'article 4, point 7), du règlement (UE) 2016/679, de mettre les données à disposition. Les produits connectés peuvent être conçus pour permettre à l'utilisateur ou à un tiers de traiter les données dans le produit connecté, sur une instance informatique du fabricant ou dans un environnement des technologies de l'information et de la communication (TIC) choisi par l'utilisateur ou le tiers.

(23) Les assistants virtuels jouent un rôle croissant dans la dématérialisation de l'environnement des consommateurs et des professionnels, et servent d'interface facile à utiliser pour lire des contenus, obtenir des informations ou activer des produits connectés à l'internet. 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, 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 nouveaux services intelligents. Les assistants virtuels devraient être couverts par les droits d'accès aux données prévus par le présent règlement. Les données générées lorsqu'un utilisateur interagit avec un produit connecté par l'intermédiaire d'un assistant virtuel fourni par une entité autre que le fabricant du produit connecté devraient également être couvertes par les droits d'accès aux données prévus par le présent règlement. Toutefois, seules les données résultant de l'interaction entre l'utilisateur et un produit connecté ou un service connexe par l'intermédiaire de l'assistant virtuel devraient être couvertes par le présent règlement. Les données produites par l'assistant virtuel qui sont sans rapport avec l'utilisation d'un produit connecté ou d'un service connexe ne sont pas couvertes par le présent règlement.

(24) Avant la conclusion d'un contrat d'achat, de location ou de crédit-bail relatif à un produit connecté, le vendeur, le loueur ou le bailleur, qui peut être le fabricant, devrait fournir à l'utilisateur des informations concernant les données relatives au produit qui peuvent être générées par le produit connecté, y compris le type, le format et le volume estimé de ces données, de manière claire et compréhensible. Cela devrait inclure des informations sur les structures de données, les formats de données, les vocabulaires, les systèmes de classification, les taxinomies et les listes de codes, le cas échéant, ainsi que des informations claires et suffisantes utiles pour l'exercice des droits de l'utilisateur sur les modalités de stockage, d'extraction ou d'accès aux données, y compris les conditions d'utilisation et la qualité du service des interfaces de programmation d'applications ou, le cas échéant, la fourniture de kits de développement logiciel. Cette obligation permet de garantir la transparence quant aux données relatives au produit générées et accroît la facilité d'accès pour l'utilisateur. L'obligation d'information pourrait être satisfaite, par exemple, en utilisant un localisateur uniforme de ressources (adresse URL) stable sur l'internet, qui peut être diffusé sous forme de lien internet ou de code QR redirigeant vers les informations pertinentes, que le vendeur, le loueur ou le bailleur, qui peut être le fabricant, peut fournir à l'utilisateur avant la conclusion du contrat d'achat, de location ou de crédit-bail relatif à un produit connecté. Il est en tout cas nécessaire que l'utilisateur ait la possibilité de stocker les informations de manière à pouvoir les retrouver ultérieurement et les reproduire à l'identique. On ne peut attendre du détenteur de données qu'il stocke indéfiniment les données en vue de répondre aux besoins de l'utilisateur du produit connecté, mais il devrait mettre en œuvre une politique raisonnable de conservation des données, le cas échéant, en conformité avec le principe de limitation de la conservation prévu à l'article 5, paragraphe 1, point e), du règlement (UE) 2016/679, qui permet l'application effective des droits d'accès aux données prévus par le présent règlement. L'obligation de fournir des informations 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. L'obligation de fournir des informations avant de conclure un contrat de fourniture d'un service connexe devrait incomber au détenteur de données potentiel, que celui-ci conclue ou non un contrat d'achat, de location ou de crédit-bail relatif à un produit connecté. Lorsque des informations changent au cours de la durée de vie du produit connecté ou de la période contractuelle pour le service connexe, y compris lorsque la finalité pour laquelle ces données doivent être utilisées change par rapport à la finalité initialement spécifiée, elles devraient également être fournies à l'utilisateur.

(25) Le présent règlement ne devrait pas être interprété comme conférant aux détenteurs de données un droit nouveau d'utiliser les données relatives à un produit ou un service connexe. Lorsque le fabricant d'un produit connecté est un détenteur de données, l'utilisation de données à caractère non personnel par le fabricant devrait être fondée sur un contrat entre le fabricant et l'utilisateur. Un tel contrat pourrait faire partie d'un accord pour la fourniture du service connexe, qui pourrait être fourni en même temps que le contrat d'achat, de location ou de crédit-bail relatif au produit connecté. Toute clause contractuelle stipulant que le détenteur de données peut utiliser les données relatives à un produit ou à un service connexe devrait être transparente pour l'utilisateur, y compris en ce qui concerne les finalités pour lesquelles le détenteur de données a l'intention d'utiliser ces données. Ces finalités pourraient inclure l'amélioration du fonctionnement du produit connecté ou des services connexes, le développement de nouveaux produits ou services, ou l'agrégation de données dans le but de mettre les données déduites qui en résultent à la disposition de tiers, pour autant que ces données déduites ne permettent pas d'identifier des données spécifiques transmises au détenteur de données à partir du produit connecté, ou ne permettent pas à un tiers de déduire ces données de l'ensemble de données. Toute modification du contrat devrait dépendre de l'accord éclairé de l'utilisateur. Le présent règlement n'empêche pas les parties de s'accorder sur des clauses contractuelles ayant pour

effet d'exclure ou de limiter l'utilisation de données à caractère non personnel, ou de certaines catégories d'entre elles, par le détenteur de données. Il n'empêche pas non plus les parties de convenir de mettre des données relatives au produit ou des données relatives au service connexe à la disposition de tiers, que ce soit directement ou indirectement, y compris, le cas échéant, par l'intermédiaire d'un autre détenteur de données. De plus, le présent règlement ne fait pas non plus 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 motifs d'ordre public bien définis. Le présent règlement n'empêche pas les utilisateurs, dans le cas de relations entre entreprises, de mettre des données à la disposition de tiers ou de détenteurs de données en vertu de toute disposition contractuelle légale, y compris en acceptant de limiter ou de restreindre le partage ultérieur de ces données, ou d'être indemnisés proportionnellement, par exemple en échange d'une renonciation à leur droit d'utiliser ou de partager ces données. Bien que la notion de "détenteur de données" n'inclue généralement pas les organismes du secteur public, elle peut inclure les entreprises publiques.

(26) Pour favoriser l'émergence de marchés liquides, équitables et efficaces pour les données à caractère non personnel, les utilisateurs de produits connectés devraient avoir la possibilité de partager des données avec d'autres personnes, notamment à des fins commerciales, sans grands efforts juridiques et techniques. À l'heure actuelle, il est souvent difficile pour les entreprises de justifier les frais de personnel ou informatiques qui sont nécessaires pour préparer des ensembles de données à caractère non personnel ou des produits de données et les proposer à des cocontractants potentiels par le biais de services d'intermédiation de données, y compris des places de marché de données. Un obstacle majeur au partage de données à caractère non personnel par les entreprises résulte donc du manque de prévisibilité en ce qui concerne la rentabilité économique des investissements dans la conservation et la mise à disposition d'ensembles de données ou de produits de données. Pour permettre l'émergence de marchés liquides, équitables et efficaces pour les données à caractère non personnel dans l'Union, la partie qui a le droit de proposer ces données sur un marché doit être précisée. Les utilisateurs devraient par conséquent avoir le droit de partager des données à caractère non personnel avec des destinataires de données à des fins commerciales et non commerciales. Un tel partage de données pourrait être assuré directement par l'utilisateur, à la demande de l'utilisateur par l'intermédiaire d'un détenteur de données, ou par le biais de services d'intermédiation de données. Les services d'intermédiation de données, tels qu'ils sont réglementés par le règlement (UE) 2022/868 du Parlement européen et du Conseil ([22]), pourraient favoriser une économie fondée sur les données en établissant des relations commerciales entre les utilisateurs, les destinataires de données et les tiers, et peuvent aider les utilisateurs à exercer leur droit d'utiliser les données, par exemple en garantissant l'anonymisation des données à caractère personnel ou l'agrégation de l'accès aux données de plusieurs utilisateurs individuels. Lorsque l'obligation, pour un détenteur de données, de mettre celles-ci à la disposition d'utilisateurs ou de tiers ne s'applique pas à certaines données, l'éventail des données en question pourrait être défini dans le contrat conclu entre l'utilisateur et le détenteur de données pour la fourniture d'un service connexe de telle manière que les utilisateurs puissent facilement déterminer les données qui leur sont accessibles en vue d'être partagées avec des destinataires de données ou des tiers. Les détenteurs de données ne devraient pas mettre à la disposition de tiers des données à caractère non personnel relatives aux produits à des fins commerciales ou non commerciales autres que l'exécution de leur contrat avec l'utilisateur, sans préjudice des exigences légales en vertu du droit de l'Union ou du droit national imposant à un détenteur de données de mettre des données à disposition. Le cas échéant, les détenteurs de données devraient obliger contractuellement les tiers à ne pas partager les données reçues de leur part.

(27) Dans les secteurs caractérisés par la concentration d'un petit nombre de fabricants qui fournissent des produits connectés aux utilisateurs finaux, les utilisateurs peuvent ne disposer que d'options limitées en matière d'accès aux données et d'utilisation et de partage des données. En pareilles circonstances, il se peut que les contrats ne suffisent pas pour atteindre l'objectif de responsabilisation de l'utilisateur, de sorte qu'il est difficile pour les utilisateurs d'obtenir de la valeur à partir des données générées par le produit connecté qu'ils achètent, qu'ils louent ou qu'ils détiennent en crédit-bail. 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 dans l'Union 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 contrat. Des dispositions du droit de l'Union ou du droit national peuvent être adoptées pour répondre à des besoins et objectifs sectoriels. De surcroît, les détenteurs de données ne pas devraient pas utiliser de données facilement accessibles qui sont des données à caractère non personnel afin d'obtenir des informations sur la situation économique, les actifs

([22]) Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) (JO L 152 du 3.6.2022, p. 1).

ou les méthodes de production de l'utilisateur, ou sur l'utilisation que ce dernier en fait, d'une quelconque autre manière qui puisse porter atteinte à la position commerciale dudit utilisateur sur les marchés où celui-ci exerce ses activités. Cela pourrait inclure l'utilisation 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 l'utilisation de ces informations pour alimenter des bases de données plus vastes relatives à certains marchés dans l'ensemble, 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 convient 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 ces autorisations.

(28) En ce qui concerne les contrats conclus entre un détenteur de données et un consommateur en tant qu'utilisateur d'un produit connecté ou d'un service connexe générant des données, le droit de l'Union en matière de protection des consommateurs, en particulier les directives 93/13/CEE et 2005/29/CE, s'applique afin de garantir que le consommateur ne soit pas soumis à des clauses contractuelles abusives. Aux fins du présent règlement, les clauses contractuelles abusives imposées unilatéralement à une entreprise ne devraient pas lier ladite entreprise.

(29) Les détenteurs de données peuvent 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, les détenteurs de données devraient veiller à ce que la demande d'accès soit reçue et traitée par le sous-traitant.

(30) 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 tout en exerçant ses droits prévus par le présent règlement à un tiers proposant un service après-vente qui peut être en concurrence avec un service fourni par un détenteur de données, ou de donner instruction au détenteur de données de le faire. La demande devrait être présentée par l'utilisateur ou par un tiers autorisé à agir pour le compte d'un utilisateur, y compris un fournisseur d'un service d'intermédiation de données. 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 peut accéder ou a le droit d'accéder du fait de l'utilisation du produit connecté ou du service connexe. Tout 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.

(31) La directive (UE) 2016/943 du Parlement européen et du Conseil ([23]) prévoit que l'obtention, l'utilisation ou la divulgation d'un secret d'affaires est considérée comme licite, entre autres, lorsque cette obtention, cette utilisation ou cette divulgation est requise ou autorisée par le droit de l'Union ou le droit national. Bien que le présent règlement impose aux détenteurs de données de divulguer certaines données aux utilisateurs, ou à des tiers choisis par un utilisateur, même lorsque ces données répondent aux conditions pour être protégées en tant que secrets d'affaires, il devrait être interprété de manière à préserver la protection accordée aux secrets d'affaires au titre de la directive (UE) 2016/943. Dans ce contexte, les détenteurs de données devraient pouvoir exiger des utilisateurs ou des tiers choisis par un utilisateur de préserver la confidentialité des données considérées comme étant des secrets d'affaires. À cette fin, les détenteurs de données devraient identifier les secrets d'affaires avant la divulgation et avoir la possibilité de convenir avec les utilisateurs, ou des tiers choisis par un utilisateur, de mesures nécessaires pour préserver leur confidentialité, y compris par l'utilisation de clauses contractuelles types, d'accords de confidentialité, de protocoles d'accès stricts, de normes techniques et de l'application de codes de conduite. Outre l'utilisation de clauses contractuelles types qui doivent être élaborées et recommandées par la Commission, l'établissement de codes de conduite et de normes techniques relatives à la protection des secrets d'affaires dans le traitement des données pourrait contribuer à la réalisation de l'objectif du présent règlement et devrait être encouragé. En l'absence d'accord sur les mesures nécessaires, ou lorsqu'un utilisateur ou les tiers choisis par un utilisateur ne mettent pas en œuvre les mesures convenues ou compromettent la confidentialité des secrets d'affaires, le détenteur de données devrait pouvoir bloquer ou suspendre le partage de données définies comme secrets d'affaires. En pareils cas, le détenteur de données devrait fournir la décision par écrit à l'utilisateur ou au tiers sans retard injustifié et notifier à l'autorité compétente de l'État membre dans lequel le détenteur de données est établi qu'il a bloqué ou suspendu le

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

partage de données et indiquer les mesures qui n'ont pas été convenues ou mises en œuvre et, le cas échéant, les secrets d'affaires dont la confidentialité a été compromise. Les détenteurs de données ne peuvent pas, en principe, refuser une demande d'accès aux données présentée au titre du présent règlement au seul motif que certaines données sont considérées comme étant des secrets d'affaires, car cela irait à l'encontre des effets attendus du présent règlement. Toutefois, dans des circonstances exceptionnelles, un détenteur de données qui est un détenteur de secrets d'affaires devrait pouvoir, au cas par cas, rejeter une demande portant sur les données spécifiques en question s'il peut démontrer à l'utilisateur ou au tiers que, malgré les mesures techniques et organisationnelles prises par l'utilisateur ou par le tiers, la divulgation de ce secret d'affaires risque fortement de causer un préjudice économique grave. Le préjudice économique grave implique une perte économique grave et irréparable. Le détenteur de données devrait dûment motiver son refus par écrit, sans retard injustifié, à l'utilisateur ou au tiers et en informer l'autorité compétente. Une telle motivation devrait être fondée sur des éléments objectifs, démontrant le risque concret de préjudice économique grave qui devrait résulter d'une divulgation de données spécifiques et les raisons pour lesquelles les mesures prises pour protéger les données demandées ne sont pas considérées comme étant suffisantes. Une éventuelle incidence négative sur la cybersécurité peut être prise en compte dans ce contexte. Sans préjudice du droit de former un recours devant une juridiction d'un État membre, lorsque l'utilisateur ou un tiers souhaite contester la décision du détenteur de données de refuser ou de bloquer ou suspendre le partage de données, l'utilisateur ou le tiers peut introduire une réclamation auprès de l'autorité compétente, laquelle devrait décider, sans retard injustifié, si et dans quelles conditions le partage de données devrait commencer ou reprendre, ou peut convenir avec le détenteur de données de saisir un organe de règlement des litiges. Les exceptions aux droits d'accès aux données prévues par le présent règlement ne devraient en aucun cas limiter le droit d'accès et le droit de portabilité des données des personnes concernées au titre du règlement (UE) 2016/679.

(32) Le présent règlement n'a pas seulement pour objectif de favoriser le développement de nouveaux produits connectés et services connexes innovants et de stimuler l'innovation sur les marchés de l'après-vente, mais aussi de favoriser le développement de services entièrement nouveaux utilisant les données concernées, y compris sur la base de données provenant de divers produits connectés ou services connexes. Le présent règlement vise dans le même temps à éviter que les incitations à l'investissement soient fragilisées pour le type de produit connecté à partir duquel les données sont obtenues, par exemple du fait de l'utilisation des données pour développer un produit connecté concurrent considéré comme interchangeable ou substituable par les utilisateurs, en particulier sur la base des caractéristiques du produit connecté, de son prix et de son usage prévu. Le présent règlement ne prévoit aucune interdiction de développer un service connexe utilisant des données obtenues en vertu du présent règlement, car cela aurait un effet dissuasif indésirable sur l'innovation. L'interdiction d'utiliser les données auxquelles il est accédé au titre du présent règlement pour développer un produit connecté concurrent protège les efforts d'innovation des détenteurs de données. La question de savoir si un produit connecté est en concurrence avec le produit connecté dont proviennent les données dépend de la question de savoir si les deux produits connectés sont en concurrence sur le même marché de produits. Cela doit être déterminé sur la base des principes établis du droit de la concurrence de l'Union pour définir le marché de produits en cause. Cependant, des finalités licites de l'utilisation des données pourraient inclure l'ingénierie inverse, pour autant qu'elle respecte les exigences prévues par le présent règlement ainsi que par le droit de l'Union ou le droit national. Cela peut être le cas aux fins de la réparation ou de la prolongation de la durée de vie d'un produit connecté ou de la fourniture de services après-vente pour des produits connectés.

(33) Lorsque des données sont mises à la disposition d'un tiers, ce tiers peut être une personne physique ou morale, telle qu'un consommateur, une entreprise, un organisme de recherche, un organisme à but non lucratif ou une entité agissant à titre professionnel. 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 facilement accessible pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production du tiers, ou sur l'utilisation que ce dernier en fait, d'une quelconque autre manière qui puisse porter atteinte à la position commerciale du tiers sur les marchés où celui-ci exerce ses activités. L'utilisateur devrait pouvoir partager, à des fins commerciales, des données à caractère non personnel avec des tiers. Avec l'accord de l'utilisateur, et sous réserve des dispositions du présent règlement, des tiers devraient pouvoir transférer à d'autres tiers les droits d'accès aux données accordés par l'utilisateur, y compris en échange d'une compensation. Les intermédiaires de données entre entreprises et les systèmes de gestion des informations personnelles (PIMS), appelés "services d'intermédiation de données" dans le règlement (UE) 2022/868, peuvent aider les utilisateurs ou les tiers à établir des relations commerciales avec un nombre indéterminé de contreparties potentielles à des fins licites relevant du champ d'application du présent règlement. Ils pourraient jouer un rôle essentiel dans l'agrégation de l'accès aux données afin de faciliter les analyses de mégadonnées ou l'apprentissage automatique, pour autant que les utilisateurs gardent totalement le contrôle sur l'opportunité de fournir ou de ne pas fournir leurs données à une telle agrégation et sur les conditions commerciales encadrant l'utilisation de leurs données.

(34) L'utilisation d'un produit connecté ou d'un service connexe peut, en particulier lorsque l'utilisateur est une personne physique, générer des données se rapportant à 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. 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. Au titre du règlement (UE) 2016/679, un utilisateur qui est la personne concernée a le droit, dans certaines circonstances, d'accéder aux données à caractère personnel concernant ledit utilisateur, et le présent règlement ne porte pas atteinte à ce droit. Au titre du présent règlement, l'utilisateur qui est une personne physique a également le droit d'accéder à toutes les données générées par l'utilisation d'un produit connecté, 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, et sauf en cas d'usage domestique partagé du produit connecté, l'utilisateur est considéré comme le responsable du traitement. Dès lors, un tel 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 connecté ou d'un service connexe, est tenu de disposer d'une base juridique pour le traitement des données ainsi que l'exige l'article 6, paragraphe 1, du règlement (UE) 2016/679, comme le consentement de la personne concernée ou l'exécution d'un contrat auquel la personne concernée est partie. Un tel utilisateur devrait veiller à ce que la personne concernée soit dûment informée des finalités déterminées, explicites et légitimes du traitement de ces données et de la manière dont la personne concernée 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 obligations respectives aux fins du respect dudit règlement. Il convient de comprendre qu'un tel utilisateur, une fois que les données ont été mises à disposition, peut à son tour devenir un détenteur de données s'il remplit les critères prévus par le présent règlement et il est alors soumis aux obligations de mise à disposition de données prévues par le présent règlement.

(35) Les données relatives à un produit ou les données relatives à un service connexe ne devraient être mises à la disposition d'un tiers qu'à la demande de l'utilisateur. Le présent règlement complète en conséquence le droit, prévu à l'article 20 du règlement (UE) 2016/679, des personnes concernées de recevoir les données à caractère personnel les concernant dans un format structuré, couramment utilisé et lisible par machine, et de porter ces données vers un autre responsable du traitement, lorsque ces données sont traitées par des procédés automatisés 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), dudit règlement. Les personnes concernées ont également le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, mais uniquement lorsque cela est techniquement possible. L'article 20 du règlement (UE) 2016/679 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 connecté ou un service connexe, par sa conception, observe le comportement d'une personne concernée ou d'autres informations relatives à une personne concernée de manière passive. Les droits prévus par le présent règlement complètent de plusieurs manières le droit de recevoir et de porter des données à caractère personnel prévu à l'article 20 du règlement (UE) 2016/679. Le présent règlement accorde aux utilisateurs le droit d'accéder à toutes données relatives à un produit ou données relatives à un service connexe 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 fournies activement et les données observées passivement, et quelle que soit la base juridique du traitement. À la différence de l'article 20 du règlement (UE) 2016/679, le présent règlement impose 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, garantissant ainsi que les obstacles techniques n'entravent plus ou n'empêchent plus l'accès à ces données. Il permet également aux détenteurs de données de fixer une compensation raisonnable à la charge des tiers, mais pas de l'utilisateur, pour les frais encourus liés à l'octroi d'un accès direct aux données générées par le produit connecté 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 contrat ne permet pas le traitement de catégories particulières de données à caractère personnel par le détenteur de données ou le tiers.

(36) L'accès à toutes les données stockées dans les équipements terminaux et auxquelles il est accédé 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 par l'abonné ou aux seules fins de la transmission d'une communication. La directive 2002/58/CE protège l'intégrité de l'équipement terminal d'un 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 étant des équipements terminaux s'ils sont directement ou indirectement connectés à un réseau de communications public.

(37) Afin d'empêcher l'exploitation des utilisateurs, les tiers au profit desquels des données ont été mises à disposition à la demande de l'utilisateur ne devraient traiter ces données qu'aux fins convenues avec l'utilisateur et ne les partager avec un autre tiers que si l'utilisateur a donné son accord à ce partage de données.

(38) Conformément au principe de minimisation des données, les tiers ne devraient avoir accès qu'aux informations nécessaires à la fourniture du service demandé par l'utilisateur. Après avoir obtenu l'accès aux données, le tiers devrait traiter celles-ci 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. Ni les tiers ni les détenteurs de données ne devraient rendre indûment difficile pour l'utilisateur le fait d'effectuer des choix ou d'exercer des droits, notamment en proposant des choix à l'utilisateur d'une manière qui n'est pas neutre, ou en contraignant, trompant ou manipulant l'utilisateur, ou en réduisant ou en compromettant l'autonomie, la prise de décision ou les choix de l'utilisateur, y compris au moyen d'une interface numérique utilisateur ou d'une partie de celle-ci. Dans ce contexte, les tiers ou les détenteurs de données devraient s'abstenir de recourir à des interfaces trompeuses lors de la conception de leurs interfaces numériques. Les interfaces trompeuses sont des techniques de conception qui poussent les consommateurs à prendre des décisions ayant 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, en particulier les consommateurs vulnérables, d'adopter un comportement non souhaité, de tromper les utilisateurs en les poussant à prendre des décisions relatives à des opérations de divulgation d'informations, ou d'influencer de manière excessive la prise de décision des utilisateurs du service, d'une manière qui sape ou altère leur autonomie, leur prise de 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 étant des interfaces trompeuses. Les tiers et les détenteurs de données devraient respecter les obligations qui leur incombent au titre du droit de l'Union pertinent, en particulier les exigences prévues dans les directives 98/6/CE ([24]) et 2000/31/CE ([25]) du Parlement européen et du Conseil et dans les directives 2005/29/CE et 2011/83/UE.

(39) Les tiers devraient également s'abstenir d'utiliser des données relevant du champ d'application du présent règlement pour effectuer un profilage de personnes, à moins que de telles activités de traitement ne soient strictement nécessaires pour fournir le service demandé par l'utilisateur, y compris dans le contexte d'une prise de décision automatisée. L'obligation d'effacer les données lorsqu'elles ne sont plus nécessaires à la finalité convenue avec l'utilisateur, sauf accord différent en ce qui concerne les données à caractère non personnel, complète le droit à l'effacement conféré à la personne concernée en application de l'article 17 du règlement (UE) 2016/679. Lorsqu'un tiers est un fournisseur d'un service d'intermédiation de données, les garanties pour la personne concernée prévues par le règlement (UE) 2022/868 s'appliquent. Le tiers peut utiliser les données pour développer un produit connecté, ou un service connexe, nouveau et innovant, mais pas pour développer un produit connecté concurrent.

(40) Les start-up, les petites entreprises, les entreprises qui sont qualifiées d'entreprises moyennes au titre de l'article 2 de l'annexe de la recommandation 2003/361/CE 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 soient aussi proportionnées que possible afin d'éviter tout excès. Dans le même temps, un petit nombre de très grandes entreprises ont vu le jour, lesquelles disposent d'une puissance économique considérable dans l'économie numérique grâce à l'accumulation et à l'agrégation de volumes importants de données ainsi qu'à l'infrastructure technologique nécessaire à leur monétisation. Parmi ces très grandes entreprises figurent des entreprises 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 (UE) 2022/1925 du Parlement européen et du Conseil ([26]) vise à remédier à ces manques d'efficacité et déséquilibres en permettant à la Commission de désigner une entreprise en tant que "contrôleur d'accès", et impose à ces contrôleurs d'accès un certain nombre d'obligations, dont l'interdiction de combiner certaines données sans consentement, et l'obligation de garantir des droits effectifs à la portabilité des données en vertu de l'article 20 du règlement (UE) 2016/679. Conformément au règlement (UE) 2022/1925, et compte tenu de la capacité sans égale de ces entreprises en matière d'acquisition de données, il n'est pas nécessaire, pour atteindre

([24]) Directive 98/6/CE du Parlement européen et du Conseil du 16 février 1998 relative à la protection des consommateurs en matière d'indication des prix des produits offerts aux consommateurs (JO L 80 du 18.3.1998, p. 27).

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

([26]) Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques) (JO L 265 du 12.10.2022, p. 1).

l'objectif du présent règlement, et il serait donc disproportionné à l'égard des détenteurs de données soumis à de telles obligations, d'inclure ces contrôleurs d'accès parmi les bénéficiaires du droit d'accès aux données. Il est probable qu'une telle inclusion limiterait également les avantages du présent règlement pour les PME, liés à l'équité de la répartition de la valeur des données entre les acteurs du marché. Cela signifie qu'une entreprise fournissant des services de plateforme essentiels qui a été désignée comme contrôleur d'accès ne peut pas demander ou se voir accorder l'accès aux données des utilisateurs générées par l'utilisation d'un produit connecté ou d'un service connexe ou par un assistant virtuel en vertu du présent règlement. En outre, les tiers au profit desquels 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. Par exemple, le tiers ne peut pas 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. Cela n'empêche pas non plus ces entreprises d'obtenir et d'utiliser les mêmes données par d'autres moyens licites. Les droits d'accès prévus par le présent règlement contribuent à élargir le choix des services offerts aux consommateurs. Étant donné que les accords volontaires entre les contrôleurs d'accès et les détenteurs de données ne sont pas affectés, limiter le droit d'accès pour les contrôleurs d'accès ne les exclurait pas du marché ni ne les empêcherait de proposer leurs services.

(41) Compte tenu de l'état actuel de la technologie, il serait trop lourd d'imposer aux microentreprises et aux petites entreprises d'autres obligations en matière de conception pour les produits connectés fabriqués ou conçus ou les services connexes fournis par elles. Tel n'est toutefois pas le cas lorsqu'une microentreprise ou une petite entreprise a une entreprise partenaire ou une entreprise liée au sens de l'article 3 de l'annexe de la recommandation 2003/361/CE qui n'est pas qualifiée de microentreprise ou de petite entreprise et lorsqu'elle travaille en sous-traitance pour la fabrication ou la conception d'un produit connecté ou pour fournir un service connexe. En pareils cas, l'entreprise qui a sous-traité la fabrication ou la conception à une microentreprise ou à une petite entreprise est en mesure d'accorder au sous-traitant une compensation appropriée. Une microentreprise ou une 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 connecté ou un fournisseur de services connexes. Une période transitoire devrait s'appliquer à une entreprise qui est qualifiée d'entreprise moyenne depuis moins d'un an et aux produits connectés pendant une période d'un an après la date à laquelle ils ont été mis sur le marché par une entreprise moyenne. Cette période d'un an permet à une telle entreprise moyenne de s'adapter et de se préparer avant d'affronter la concurrence sur le marché des services pour les produits connectés qu'elle fabrique sur la base des droits d'accès prévus par le présent règlement. Cette période transitoire ne s'applique pas lorsqu'une telle entreprise moyenne a une entreprise partenaire ou une entreprise liée qui n'est pas qualifiée de microentreprise ou de petite entreprise ou lorsqu'une telle entreprise moyenne a travaillé en sous-traitance pour la fabrication ou la conception du produit connecté ou pour fournir le service connexe.

(42) Compte tenu de la diversité des produits connectés qui génèrent des données de nature, de volume et de fréquence différents, présentent des niveaux différents de risques en matière de données et de cybersécurité et offrent des possibilités économiques de valeur différente, et dans le but d'assurer 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 de données, même dans les domaines où un tel droit d'accès aux données n'est pas prévu, le présent règlement prévoit des règles horizontales sur les modalités d'accès aux données, chaque fois qu'un détenteur de données est tenu, par le droit de l'Union ou la législation nationale adoptée conformément au droit de l'Union, de mettre des données à la disposition d'un destinataire de données. Un tel accès devrait être fondé sur des modalités et conditions équitables, raisonnables, non discriminatoires et transparentes. 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. Les clauses contractuelles types non contraignantes pour le partage de données entre entreprises qui doivent être élaborées et recommandées par la Commission peuvent aider les parties à conclure des contrats qui prévoient des modalités et conditions équitables, raisonnables et non discriminatoires et qui doivent être mis en œuvre de manière transparente. La conclusion de contrats, qui peuvent contenir les clauses contractuelles types non contraignantes, ne devrait pas signifier que le droit de partager des données avec des tiers est, de quelque manière que ce soit, subordonné à l'existence d'un tel accord. Si les parties ne sont pas en mesure de conclure un accord sur le partage des données, y compris avec l'aide d'organes de règlement des litiges, le droit de partager des données avec des tiers est opposable devant les juridictions nationales.

(43) 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. Les clauses de ces contrats pourraient inclure des mesures techniques et organisationnelles, y compris en ce qui concerne la sécurité des données.

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

(45) Aucun accord conclu dans le cadre de relations entre entreprises au sujet d'une mise à disposition de données ne devrait créer de discrimination entre différentes catégories comparables de destinataires de données, que les parties soient de grandes entreprises ou des PME. Afin de compenser le manque d'informations sur les conditions figurant dans les 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 relever de la responsabilité des détenteurs 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 si ces différences sont justifiées par des raisons objectives. Ces obligations sont sans préjudice du règlement (UE) 2016/679.

(46) Afin de promouvoir la poursuite des investissements dans la production et la mise à disposition de données précieuses, y compris dans des outils techniques pertinents, tout en évitant d'alourdir de manière excessive l'accès aux données et l'utilisation de données, ce qui rendrait le partage de données non viable sur le plan commercial, le présent règlement consacre le principe selon lequel, dans les relations entre entreprises, les détenteurs de données peuvent demander une compensation raisonnable lorsqu'ils sont tenus, en vertu du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union, de mettre des données à la disposition d'un destinataire de données. Une telle compensation ne devrait pas être comprise comme constituant un paiement en échange des données proprement dit. Il convient que la Commission adopte des lignes directrices sur le calcul d'une compensation raisonnable dans le cadre de l'économie fondée sur les données.

(47) Premièrement, une compensation raisonnable pour le respect de l'obligation en application du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union de donner suite à une demande de mise à disposition de données peut inclure une compensation pour les coûts occasionnés par la mise à disposition des données. Ces coûts peuvent correspondre à des frais techniques, tels que ceux nécessaires à la reproduction, la diffusion par voie électronique et le stockage des données, mais pas à la collecte ou la production des données. Ces frais techniques peuvent également inclure les frais de traitement nécessaires à la mise à disposition des données, y compris ceux liés au formatage des données. Les coûts associés à la mise à disposition des données peuvent également inclure les frais visant à faciliter les demandes concrètes de partage de données. Ils peuvent aussi varier en fonction du volume des données ainsi que des accords conclus pour la mise à disposition des données. Des accords à long terme entre les détenteurs de données et les destinataires de données, par exemple au moyen d'un modèle d'abonnement ou de l'utilisation de contrats intelligents, peuvent réduire les coûts lors de transactions régulières ou répétitives dans le cadre d'une relation commerciale. Les coûts liés à la mise à disposition des données peuvent être spécifiques à une demande particulière ou partagés avec d'autres demandes. Dans ce dernier cas, un destinataire de données unique ne devrait pas payer l'intégralité des frais relatifs à la mise à disposition des données. Deuxièmement, une compensation raisonnable peut également inclure une marge, sauf en ce qui concerne les PME et les organismes de recherche à but non lucratif. Une marge peut varier en fonction de facteurs liés aux données elles-mêmes, tels que le volume, le format ou la nature des données. Elle peut tenir compte des coûts associés à la collecte des données. Une marge peut donc diminuer lorsque le détenteur de données a collecté les données pour sa propre activité sans investissement important, ou augmenter s'il a beaucoup investi dans la collecte de données pour les besoins de son activité. Elle peut être limitée, voire exclue, dans les situations où l'utilisation des données par le destinataire de données n'a aucune incidence sur les activités propres du détenteur de données. Le fait que les données soient cogénérées par un produit connecté qui appartient à l'utilisateur, qu'il loue ou qu'il utilise en crédit-bail pourrait également réduire le montant de la compensation, comparativement à d'autres situations dans lesquelles les données sont générées par le détenteur de données, par exemple lors de la fourniture d'un service connexe.

(48) Il n'est pas nécessaire d'intervenir en cas de partage de données entre grandes entreprises, ou lorsque le détenteur de données est une petite entreprise ou une entreprise moyenne et que le destinataire de données est une grande entreprise. En pareils cas, les entreprises sont considérées comme capables de négocier la compensation dans les limites de ce qui est raisonnable et non discriminatoire.

(49) Afin de protéger les PME contre des charges économiques excessives qui les pénaliseraient trop sur le plan commercial pour élaborer et appliquer des modèles d'entreprise innovants, la compensation raisonnable à payer par celles-ci pour la mise à disposition de données ne devrait pas dépasser les coûts directement liés à cette mise à disposition. Les coûts directement liés sont ceux qui sont imputables à des demandes individuelles, compte tenu du fait que les interfaces techniques nécessaires ou les logiciels et la connectivité connexes doivent être installés de manière permanente par le détenteur des données. Le même régime devrait s'appliquer aux organismes de recherche à but non lucratif.

(50) Dans des cas dûment justifiés, y compris lorsqu'il faut préserver la participation des consommateurs et la concurrence ou promouvoir l'innovation sur certains marchés, une compensation réglementée pour la mise à disposition de types de données spécifiques peut être prévue par le droit de l'Union ou la législation nationale adoptée conformément au droit de l'Union.

(51) La transparence est un principe important pour garantir que la compensation demandée par un détenteur de données est raisonnable ou, si le destinataire de données est une PME ou un organisme de recherche à but non lucratif, que la compensation n'excède pas les coûts directement liés à la mise à la disposition du destinataire de données, des données et est imputable à la demande individuelle concernée. Afin de mettre les destinataires de données en mesure d'évaluer et de vérifier que la compensation satisfait aux exigences du présent règlement, le détenteur de données devrait fournir au destinataire de données des informations suffisamment détaillées pour le calcul de la compensation.

(52) 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 de données et aux destinataires de données et, partant, renforcer la confiance dans le partage des données. Lorsque les parties ne parviennent pas à s'entendre sur des modalités et conditions équitables, raisonnables et non discriminatoires de mise à disposition des données, des organes de règlement des litiges devraient leur proposer une solution simple, rapide et peu coûteuse. Le présent règlement ne fixant que les conditions devant être remplies par les organes de règlement des litiges pour être certifiés, les États membres sont libres d'adopter toute règle spécifique concernant la procédure de certification, y compris l'expiration ou le retrait de la certification. Les dispositions du présent règlement relatives au règlement des litiges ne devraient pas imposer aux États membres de mettre en place des organes de règlement des litiges.

(53) La procédure de règlement des litiges prévue par le présent règlement est une procédure volontaire qui permet aux utilisateurs, aux détenteurs de données et aux destinataires de données de convenir de porter leurs différends devant des organes de règlement des litiges. Par conséquent, les parties devraient être libres de saisir l'organe de règlement des litiges de leur choix, que celui-ci se trouve à l'intérieur ou à l'extérieur des États membres dans lesquels elles sont établies.

(54) Afin d'éviter des situations dans lesquelles deux ou plusieurs organes de règlement des litiges seraient saisis du même litige, en particulier dans une situation transfrontière, tout organe de règlement des litiges devrait pouvoir refuser de traiter une demande de règlement d'un litige qui a déjà été porté devant un autre organe de règlement des litiges ou devant une juridiction d'un État membre.

(55) Afin d'assurer l'application uniforme du présent règlement, les organes de règlement des litiges devraient tenir compte des clauses contractuelles types non contraignantes qui doivent être élaborées et recommandées par la Commission, ainsi que des dispositions du droit de l'Union ou du droit national précisant les obligations en matière de partage des données ou des lignes directrices publiées par les autorités sectorielles pour l'application de telles dispositions.

(56) 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 un procès équitable. Par conséquent, la décision de saisir un organe de règlement des litiges ne devrait pas priver ces parties de leur droit de demander réparation devant une juridiction d'un État membre. Les organes de règlement des litiges devraient rendre publics des rapports annuels d'activités.

(57) Les détenteurs de données peuvent appliquer des mesures techniques de protection appropriées pour empêcher la divulgation illicite de données ou l'accès illicite à des données. Toutefois, ces mesures ne devraient pas donner lieu à une discrimination entre les destinataires de données ni entraver l'accès aux données ou l'utilisation de celles-ci pour les utilisateurs ou les destinataires de données. En cas de pratiques abusives de la part d'un destinataire de données, comme le fait de duper le détenteur de données en fournissant de fausses informations dans l'intention d'utiliser les données à des fins illicites, notamment la mise au point d'un produit connecté concurrent sur la base des données, le détenteur de données et, le cas échéant et s'il ne s'agit pas de la même personne, le détenteur de secrets d'affaires ou l'utilisateur peut demander au tiers ou au destinataire de données de mettre en œuvre, sans retard injustifié, des mesures correctives ou de remédiation. Toutes les demandes de ce type, et en particulier celles visant à mettre fin à la production, à l'offre ou à la mise sur le marché de biens, de données dérivées ou de services, ainsi que celles visant à mettre fin à l'importation, à l'exportation, au stockage de biens non conformes ou visant à ce que ceux-ci soient détruits, devraient être évaluées à la lumière de leur proportionnalité par rapport aux intérêts du détenteur de données, du détenteur de secrets d'affaires ou de l'utilisateur.

(58) 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 de sorte que l'accès aux données est commercialement moins viable, et parfois prohibitif, sur le plan économique. Ces déséquilibres contractuels portent préjudice à toutes les 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 l'utilisation des données, ou la responsabilité et les voies de recours en cas de violation ou d'extinction des obligations liées aux données, ne devraient pas être contraignantes pour les entreprises lorsque ces clauses ont été imposées unilatéralement à ces entreprises.

(59) Les règles relatives aux clauses contractuelles devraient tenir compte du principe de la liberté contractuelle en tant que concept essentiel dans les relations entre entreprises. Par conséquent, les clauses contractuelles ne devraient pas toutes être soumises à une appréciation du caractère abusif, mais uniquement celles qui sont imposées unilatéralement. Il s'agit des situations du type "à prendre ou à laisser" dans lesquelles une partie prévoit une certaine clause contractuelle et où l'autre entreprise ne peut pas influencer le contenu de cette clause malgré une tentative de négociation. Une clause contractuelle qui est simplement prévue par une partie et acceptée par l'autre entreprise, ou une clause négociée puis convenue sous une forme modifiée entre les parties contractantes, ne devrait pas être considérée comme ayant été imposée unilatéralement.

(60) 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 l'utilisation des données, ainsi que la responsabilité ou les voies de recours en cas de violation et d'extinction 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.

(61) Les critères permettant de déterminer les clauses contractuelles abusives ne devraient s'appliquer qu'aux clauses contractuelles excessives, en cas d'abus d'un 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 entre entreprises, sont une expression normale du principe de la liberté contractuelle et continuent de s'appliquer. Aux fins du présent règlement, un écart flagrant par rapport aux bonnes pratiques commerciales inclurait, entre autres, une atteinte objective à la capacité de la partie à laquelle la clause a été imposée unilatéralement de protéger son intérêt commercial légitime dans les données en question.

(62) Afin de garantir la sécurité juridique, le présent règlement dresse une liste de clauses qui sont toujours considérées comme abusives et une liste de clauses qui sont présumées être abusives. Dans ce dernier cas, l'entreprise qui impose la clause contractuelle devrait pouvoir renverser la présomption de caractère abusif en démontrant que la clause contractuelle mentionnée dans la liste qui figure dans le présent règlement n'est pas abusive dans le cas particulier en question. 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 contractuelles abusives dans le présent règlement devraient servir de critère d'interprétation de la disposition générale relative au caractère abusif. Enfin, des clauses contractuelles types non contraignantes pour les contrats de partage de données entre entreprises que la Commission doit élaborer et recommander peuvent également être utiles aux parties commerciales lorsqu'elles négocient des contrats. Si une clause contractuelle est déclarée abusive, le contrat concerné devrait continuer à s'appliquer sans cette clause, à moins que la clause contractuelle abusive ne soit pas dissociable des autres clauses du contrat.

(63) En cas de besoin exceptionnel, les organismes du secteur public, la Commission, la Banque centrale européenne ou les organes de l'Union peuvent être contraints d'utiliser, dans l'exercice de leurs fonctions statutaires à des fins d'intérêt public, des données existantes, y compris, le cas échéant, les métadonnées qui les accompagnent, pour réagir à des situations d'urgence ou dans d'autres cas exceptionnels. Les besoins exceptionnels correspondent à des circonstances imprévisibles et limitées dans le temps, contrairement à d'autres circonstances qui pourraient être planifiées, programmées, périodiques ou fréquentes. Alors que la notion de "détenteur de données" n'inclut pas, en règle générale, les organismes du secteur public, elle peut inclure des entreprises publiques. 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 ne devraient être tenues de fournir des données aux organismes du secteur public, à la Commission, à la Banque centrale européenne ou aux organes de l'Union qu'en cas de besoin exceptionnel lorsque ces données sont requises pour réagir à une situation d'urgence et que l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union n'est pas en mesure d'obtenir de telles données par d'autres moyens de manière rapide et efficace et dans des conditions équivalentes.

(64) En cas de situations d'urgence, telles que les urgences de santé publique, les urgences résultant de catastrophes naturelles, y compris celles aggravées par le changement climatique et la dégradation de l'environnement, 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, de la Commission, de la Banque centrale européenne ou des organes de l'Union à leur demande. L'existence d'une situation d'urgence devrait être déterminée ou déclarée conformément au droit de l'Union ou au droit national et fondée sur les procédures pertinentes, y compris celles des organisations internationales compétentes. Dans de tels cas, l'organisme du secteur public devrait démontrer que les données faisant l'objet de la demande ne pourraient pas, autrement, être obtenues de manière rapide et efficace et dans des conditions équivalentes, par exemple au moyen de la fourniture volontaire de données par une autre entreprise ou de la consultation d'une base de données publique.

(65) Un besoin exceptionnel peut également résulter de situations non urgentes. Dans de tels cas, un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union devrait être uniquement autorisé à demander des données à caractère non personnel. L'organisme du secteur public devrait démontrer que les données sont nécessaires à l'exécution d'une mission spécifique d'intérêt public explicitement prévue par la loi, telle que la production de statistiques officielles ou l'atténuation d'une situation d'urgence ou le rétablissement à la suite d'une situation d'urgence. En outre, une telle demande ne peut être effectuée que lorsque l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union a déterminé des données spécifiques qui ne pourraient pas, autrement, être obtenues de manière rapide et efficace et dans des conditions équivalentes, et uniquement s'il a épuisé tous les autres moyens à sa disposition pour se procurer ces données, tels que l'obtention des données au moyen d'accords volontaires, notamment en achetant des données à caractère non-personnel sur le marché aux prix du marché, ou le recours aux obligations existantes de mise à disposition des données ou l'adoption de nouvelles mesures législatives susceptibles de garantir la disponibilité des données en temps utile. Les conditions et principes régissant les demandes, tels que ceux liés à la limitation de la finalité, à la proportionnalité, à la transparence et à la limitation dans le temps, devraient également s'appliquer. En cas de demande de données nécessaires à la production de statistiques officielles, l'organisme du secteur public demandeur devrait également démontrer si le droit national l'autorise à acheter des données à caractère non-personnel sur le marché.

(66) Le présent règlement ne devrait pas s'appliquer aux accords volontaires d'échange de données entre entités privées et publiques, y compris la fourniture de données par les PME, ni s'y substituer, et est sans préjudice des actes juridiques de l'Union prévoyant des demandes d'informations obligatoires adressées par des entités publiques à des entités privées. 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, en particulier lorsque l'éventail des données et des détenteurs de données est connu ou 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 dans le but de vérifier le respect des règles applicables, y compris lorsque des organismes du secteur public confient la tâche de vérification du respect des règles à des entités autres que des organismes du secteur public.

(67) Le présent règlement complète, sans y porter atteinte, le droit de l'Union et le droit national prévoyant l'accès aux données et l'utilisation des données à des fins statistiques, en particulier le règlement (CE) nº 223/2009 du Parlement européen et du Conseil ([27]), ainsi que les actes juridiques nationaux relatifs aux statistiques officielles.

(68) Pour l'exercice de leurs missions dans les domaines de la prévention ou de la détection des infractions pénales ou administratives, des enquêtes ou des poursuites en la matière, ou 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, la Commission, la Banque centrale européenne ou les organes de l'Union devraient faire valoir les pouvoirs qui leur sont conférés par le droit de l'Union ou le droit national. Le présent règlement ne porte donc pas atteinte aux actes législatifs relatifs au partage des données, à l'accès aux données et à l'utilisation des données dans ces domaines.

(69) Conformément à l'article 6, paragraphes 1 et 3, du règlement (UE) 2016/679, un cadre proportionné, limité et prévisible au niveau de l'Union est nécessaire lors de l'établissement de la base juridique permettant aux détenteurs de données, en cas de besoins exceptionnels, de mettre des données à la disposition des organismes du secteur public, de la Commission, de la Banque centrale européenne ou des organes 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 émanant d'organismes du secteur public, de la Commission, de la Banque centrale européenne ou d'organes de l'Union adressées aux détenteurs de données devraient être spécifiques, transparentes et proportionnées en ce qui concerne l'étendue de 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'exécuter ses missions spécifiques d'intérêt public. La demande devrait également respecter les intérêts légitimes des détenteurs de données auxquels elle est adressée. La charge pesant sur les détenteurs de données devrait être réduite au minimum en obligeant les entités demandeuses 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 par la Commission, la Banque centrale européenne ou des organes de l'Union. Dans un souci de transparence, les demandes de données formulées par la Commission, la Banque centrale européenne ou des organes de l'Union devraient être rendues publiques sans retard injustifié par l'entité qui demande les données. La Banque centrale européenne et les organes de l'Union devraient informer la Commission de leurs demandes. Si la demande de données a été formulée par un organisme du secteur public, cet organisme devrait également adresser une notification au coordinateur de données de l'État membre dans lequel l'organisme du secteur public est établi. Il convient de veiller à ce que toutes les demandes soient mises à la disposition du public en ligne. Dès réception de la notification d'une demande de données, l'autorité compétente peut décider d'évaluer la légalité de la demande et d'exercer ses fonctions en ce qui concerne l'exécution et l'application du présent règlement. La mise à la disposition du public en ligne de toutes les demandes formulées par des organismes du secteur public devrait être assurée par le coordinateur de données.

(70) L'objectif de l'obligation de fournir les données est de faire en sorte que les organismes du secteur public, la Commission, la Banque centrale européenne ou les organes de l'Union disposent des connaissances nécessaires pour réagir à une situation d'urgence, prévenir une situation d'urgence ou se rétablir à la suite d'une situation d'urgence, 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, ni le règlement (UE) 2022/868 ni la directive (UE) 2019/1024 du Parlement européen et du Conseil ([28]) ne devraient 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. En outre, et pour autant que les conditions énoncées dans le présent règlement soient satisfaites, la possibilité de partager les données à des fins de recherche ou pour le développement, la production et la diffusion de statistiques officielles ne devrait pas être affectée. 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, la Commission, la Banque centrale européenne ou des organes de l'Union afin de répondre aux besoins exceptionnels pour lesquels les données ont été demandées.

([27]) Règlement (CE) nº 223/2009 du Parlement européen et du Conseil du 11 mars 2009 relatif aux statistiques européennes et abrogeant le règlement (CE, Euratom) nº 1101/2008 relatif à la transmission à l'Office statistique des Communautés européennes d'informations statistiques couvertes par le secret, le règlement (CE) nº 322/97 du Conseil relatif à la statistique communautaire et la décision 89/382/CEE, Euratom du Conseil instituant un comité du programme statistique des Communautés européennes (JO L 87 du 31.3.2009, p. 164).

([28]) 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).

(71) Les détenteurs de données devraient avoir la possibilité soit de rejeter une demande présentée par un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union, soit de demander sa modification sans retard injustifié et, en tout état de cause, au plus tard dans un délai de cinq ou trente jours ouvrables, en fonction de la nature du besoin exceptionnel invoqué dans la demande. Le cas échéant, le détenteur de données devrait avoir cette possibilité lorsqu'il n'a aucun contrôle sur les données demandées, c'est-à-dire lorsqu'il n'a pas immédiatement accès aux données et qu'il ne peut pas déterminer leur disponibilité. Un motif valable de ne pas mettre les données à disposition devrait exister s'il peut être démontré que la demande est similaire à une demande présentée précédemment pour la même finalité par un autre organisme du secteur public, ou la Commission, la Banque centrale européenne ou un organe de l'Union et le détenteur de données ne s'est pas vu notifier l'effacement des données en vertu du présent règlement. Un détenteur de données qui rejette la demande ou demande sa modification devrait communiquer à l'organisme du secteur public, à la Commission, à la Banque centrale européenne ou à l'organe de l'Union qui demande les données la justification sous-jacente. Lorsque les droits sui generis liés à la base de données prévus par la directive 96/9/CE du Parlement européen et du Conseil ([29]) s'appliquent aux ensembles de données demandés, les détenteurs de données devraient exercer leur droit d'une manière qui n'empêche pas l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union d'obtenir les données, ou de les partager, conformément au présent règlement.

(72) En cas de besoin exceptionnel lié à une réaction à une situation d'urgence, les organismes du secteur public devraient utiliser des données à caractère non personnel chaque fois que cela est possible. En cas de demande fondée sur un besoin exceptionnel non lié à une situation d'urgence, les données à caractère personnel ne peuvent pas être demandées. Chaque fois que des données à caractère personnel relèvent du champ de la demande, le détenteur de données devrait les anonymiser. Lorsqu'il est strictement nécessaire d'inclure des données à caractère personnel dans les données qui doivent être mises à la disposition d'un organisme du secteur public, de la Commission, de la Banque centrale européenne ou d'un organe de l'Union ou lorsque l'anonymisation s'avère impossible, l'entité qui demande les données devrait démontrer la stricte nécessité et les finalités spécifiques et limitées du traitement. Les règles applicables en matière de protection des données à caractère personnel devraient être respectées. 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.

(73) Les données mises à la disposition des organismes du secteur public, de la Commission, de la Banque centrale européenne ou des organes de l'Union sur le fondement d'un besoin exceptionnel ne devraient être utilisées que pour les finalités 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 effacées dès lors qu'elles ne sont plus nécessaires aux finalités indiquées dans la demande, sauf accord contraire, et le détenteur de données devrait en être informé. Le présent règlement s'appuie sur les règles d'accès en vigueur dans l'Union et dans les États membres et ne modifie pas les dispositions de droit national en matière d'accès du public aux documents dans le contexte des obligations de transparence. Les données devraient être effacées dès qu'elles ne sont plus nécessaires pour se conformer à ces obligations de transparence.

(74) Lors de la réutilisation des données fournies par les détenteurs de données, les organismes du secteur public, la Commission, la Banque centrale européenne ou les organes de l'Union devraient respecter à la fois le droit de l'Union ou le droit national applicables en vigueur et les obligations contractuelles auxquelles le détenteur de données est soumis. Ils devraient s'abstenir de mettre au point ou d'améliorer un produit connecté ou un service connexe concurrençant le produit connecté ou service connexe du détenteur de données, ainsi que de partager les données avec un tiers à ces fins. Ils devraient également accorder une reconnaissance publique aux détenteurs de données à la demande de ces derniers et devraient être responsables du maintien de la sécurité des données reçues. Lorsque la divulgation de secrets d'affaires du détenteur de données à des organismes du secteur public, à la Commission, à la Banque centrale européenne ou à des organes 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 avant la divulgation des données.

(75) Lorsque la sauvegarde d'un bien public important est en jeu, comme lorsqu'il s'agit de réagir à une situation d'urgence, l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union concerné ne devrait pas être tenu d'indemniser les entreprises pour les données obtenues. Les situations d'urgence sont des événements rares et ces urgences ne nécessitent pas toutes l'utilisation de données détenues par des entreprises. Dans le même temps, l'obligation de fournir des données pourrait représenter une charge considérable pour les microentreprises et les petites entreprises. Elles devraient donc être autorisées à réclamer une compensation

([29]) 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).

même dans le cadre d'une réaction à une situation d'urgence. Le fait que les organismes du secteur public, la Commission, la Banque centrale européenne ou les organes de l'Union fassent usage du présent règlement ne devrait donc pas avoir des répercussions négatives sur les activités commerciales des détenteurs de données. Toutefois, étant donné que les cas de besoins exceptionnels autres que les cas de réaction à des situations d'urgence pourraient être plus fréquents, les détenteurs de données devraient, dans de telles situations, avoir droit à une compensation 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, de la Commission, de la Banque centrale européenne ou de l'organe de l'Union. La compensation ne devrait pas être comprise comme constituant le paiement des données proprement dites ou comme étant obligatoire. Les détenteurs de données ne devraient pas pouvoir prétendre à une compensation lorsque le droit national interdit aux instituts nationaux de statistique ou aux autres autorités nationales chargées de la production de statistiques d'indemniser les détenteurs de données pour la mise à disposition de données. L'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union concerné devrait pouvoir contester le niveau de compensation demandé par le détenteur de données en saisissant l'autorité compétente de l'État membre dans lequel le détenteur de données est établi.

(76) Un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union devrait être habilité à 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 des activités d'analyse qu'il ne peut pas réaliser lui-même, à condition que ces activités soient compatibles avec la finalité pour laquelle les données ont été demandées. Il devrait informer le détenteur de données de ce partage en temps utile. Ces données peuvent également être partagées dans les mêmes conditions avec les instituts nationaux de statistique et Eurostat pour le développement, la production et la diffusion 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 exercent une influence notable, permettant à ces entreprises d'exercer un contrôle en raison d'éléments structurels qui pourrait conduire à un accès préférentiel aux résultats des recherches, ne devraient pas être considérés comme étant des organismes de recherche aux fins du présent règlement.

(77) Afin de traiter une situation d'urgence transfrontière ou un autre besoin exceptionnel, des demandes de données peuvent être adressées à des détenteurs de données dans des États membres autres que celui de l'organisme du secteur public demandeur. Dans ce cas, l'organisme du secteur public demandeur devrait adresser une notification à l'autorité compétente de l'État membre dans lequel le détenteur de données est établi afin de lui permettre d'examiner la demande au regard des critères établis dans le présent règlement. Il devrait en aller de même pour les demandes présentées par la Commission, la Banque centrale européenne ou un organe de l'Union. Lorsque des données à caractère personnel sont demandées, l'organisme du secteur public devrait adresser une notification à l'autorité de contrôle chargée de surveiller l'application du règlement (UE) 2016/679 dans l'État membre dans lequel l'organisme du secteur public est établi. L'autorité compétente concernée devrait être habilitée à conseiller l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union en vue de coopérer avec les organismes du secteur public de l'État membre dans lequel le détenteur de données est établi en ce qui concerne la nécessité de réduire au minimum la charge administrative pesant sur le détenteur de données. Lorsque l'autorité compétente soulève des objections dûment étayées en ce qui concerne la conformité de la demande avec le présent règlement, elle devrait rejeter la demande de l'organisme du secteur public, de la Commission, de la Banque centrale européenne ou de l'organe de l'Union, qui devrait tenir compte de ces objections avant de prendre toute nouvelle mesure, y compris soumettre à nouveau la demande.

(78) 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 et sans interruption des services, ou d'utiliser simultanément les services de plusieurs fournisseurs sans obstacles injustifiés ou frais excessifs de transfert de données, est une condition essentielle pour un marché plus concurrentiel, avec des barrières à l'entrée moins élevées pour les nouveaux fournisseurs de services de traitement de données, et pour garantir une plus grande résilience aux utilisateurs de ces services. Les clients bénéficiant d'offres gratuites devraient également bénéficier des dispositions relatives au changement de fournisseur prévues par le présent règlement, de sorte que ces offres n'entraînent pas un effet de verrouillage pour les clients.

(79) Le règlement (UE) 2018/1807 du Parlement européen et du Conseil ([30]) encourage les fournisseurs de services de traitement de données à élaborer et à mettre en œuvre de manière efficace des codes de conduite par autorégulation couvrant les bonnes pratiques pour, entre autres, faciliter le changement de fournisseur de services de traitement de données et le portage des données. Compte tenu de l'adoption 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 précommerciaux, commerciaux, techniques, contractuels et organisationnels, lesquels ne se limitent pas à la réduction de la vitesse de transfert des données lors du désengagement du client, qui freinent le changement effectif de services de traitement de données.

(80) Les services de traitement de données devraient couvrir les services qui permettent un accès universel et à la demande par réseau à un ensemble partagé, configurable, modulable et variable de ressources informatiques distribuées. Ces ressources informatiques comprennent des ressources telles que les réseaux, serveurs ou autres infrastructures virtuelles ou physiques, 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 à s'équiper unilatéralement en ressources informatiques, comme en temps de serveur ou en stockage en réseau, sans aucune intervention humaine de la part du fournisseur de services de traitement de données pourrait être décrite comme exigeant un minimum d'efforts de gestion et d'interaction entre le fournisseur et le client. Le terme "universel" est utilisé pour décrire les capacités de calcul fournies sur le réseau et auxquelles l'accès se fait par des mécanismes encourageant le recours à des plateformes clients légères ou lourdes disparates (des navigateurs internet 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. Le terme "variable" est utilisé 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 "ensemble partagé" sont utilisés pour décrire les ressources informatiques qui sont mises à la 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.

(81) Le concept générique de "services de traitement de données" couvre un nombre important de services ayant un très large éventail de finalités, de fonctionnalités et de configurations techniques différentes. Comme généralement compris par les fournisseurs et les utilisateurs et conformément aux normes largement utilisées, les services de traitement de données relèvent d'un ou de plusieurs des trois modèles de fourniture de services de traitement de données suivants: l'infrastructure à la demande (IaaS), la plateforme à la demande (PaaS) et le logiciel à la demande (SaaS). Ces modèles de fourniture de services représentent une combinaison spécifique de ressources TIC proposées par un fournisseur de services de traitement de données. Ces trois modèles de base de fourniture de services de traitement de données sont complétés par de nouvelles variantes, chacune comprenant une combinaison distincte de ressources TIC, telles que le "stockage à la demande" et la "base de données à la demande". Les services de traitement de données peuvent être classés de manière plus fine et répartis dans une liste non exhaustive d'ensembles de services de traitement de données qui partagent le même objectif principal et les mêmes fonctionnalités principales ainsi que le même type de modèles de traitement de données, qui ne sont pas liés aux caractéristiques opérationnelles du service (même type de services). Les services relevant du même type de service peuvent partager le même modèle de service de traitement de données, toutefois, deux bases de données pourraient sembler partager le même objectif principal, mais après examen de leur modèle de fourniture de traitement de données, de leur modèle de distribution et des cas d'utilisation qu'ils ciblent, ces bases de données pourraient relever d'une sous-catégorie plus fine de services similaires. Des services du même type de service peuvent présenter des caractéristiques différentes et concurrentes, telles que la performance, la sécurité, la résilience et la qualité du service.

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

(82) Des problèmes d'extraction des données exportables appartenant au client chez le fournisseur d'origine de services de traitement de données peuvent entraver le rétablissement des fonctionnalités du service dans l'infrastructure du fournisseur de destination de services de traitement des données. Afin de faciliter la stratégie de sortie du client, d'éviter des tâches inutiles et lourdes et de veiller à ce que le client ne perde aucune de ses données à la suite de la procédure de changement de fournisseur, le fournisseur d'origine de services de traitement de données devrait informer le client à l'avance de l'étendue des données qui peuvent être exportées une fois que ce client décide de passer à un autre service fourni par un fournisseur de services de traitement de données différent ou à une infrastructure TIC sur site. Les données exportables devraient comprendre, au minimum, les données d'entrée et de sortie, y compris les métadonnées directement ou indirectement générées ou cogénérées par l'utilisation du service de traitement de données par le client, à l'exclusion de tous les actifs ou de toutes les données du fournisseur de services de traitement de données ou d'un tiers. Les données exportables devraient exclure les actifs ou les données du fournisseur de services de traitement de données ou des tiers qui sont protégés par des droits de propriété intellectuelle ou qui constituent des secrets d'affaires de ce fournisseur ou de ce tiers, ou les données liées à l'intégrité et à la sécurité du service, dont l'exportation exposera les fournisseurs de services de traitement de données à des vulnérabilités en matière de cybersécurité. Ces exclusions ne devraient pas entraver ou retarder le processus de changement de fournisseur.

(83) Les actifs numériques désignent les éléments en format numérique pour lesquels le client possède un droit d'utilisation, y compris les applications et métadonnées liées à la configuration des paramètres, la sécurité et la gestion des droits d'accès et de contrôle, ainsi que d'autres éléments tels que les réalisations des technologies de virtualisation, y compris les machines virtuelles et la conteneurisation. Les actifs numériques peuvent être transférés lorsque le client est titulaire du droit d'utilisation, quelle que soit la relation contractuelle avec le service de traitement de données qu'il a l'intention de quitter. Ces autres éléments sont essentiels pour une utilisation efficace des données et applications du client dans l'environnement du fournisseur de destination de services de traitement de données.

(84) Le présent règlement vise à faciliter le changement de services de traitement de données, ce qui englobe les conditions et actions qui sont nécessaires pour qu'un client résilie un contrat relatif à un service de traitement de données, conclue un ou plusieurs nouveaux contrats avec différents fournisseurs de services de traitement de données, porte ses données exportables et actifs numériques, et le cas échéant, bénéficie de l'équivalence fonctionnelle.

(85) Le changement de fournisseur est une opération orientée vers le client, qui consiste en plusieurs étapes, notamment l'extraction de données, qui correspond au téléchargement de données à partir de l'écosystème du fournisseur d'origine de services de traitement de données; la transformation, lorsque les données sont structurées d'une manière qui ne correspond pas au schéma de l'emplacement cible; et le téléversement des données dans un nouvel emplacement de destination. Dans une situation particulière décrite dans le présent règlement, le découplage d'un service donné du contrat et son transfert vers un fournisseur différent devraient également être considérés comme un changement de fournisseur. Le processus de changement de fournisseur est parfois géré pour le compte du client par une entité tierce. Par conséquent, tous les droits et obligations du client établis par le présent règlement, y compris l'obligation de coopérer de bonne foi, devraient être compris comme s'appliquant à une telle entité tierce dans ces circonstances. Les fournisseurs de services de traitement de données et les clients ont différents niveaux de responsabilités, selon les étapes du processus visé. Par exemple, le fournisseur d'origine de services de traitement de données est responsable de l'extraction des données dans un format lisible par machine, mais ce sont le client et le fournisseur de destination de services de traitement de données qui doivent téléverser les données dans le nouvel environnement, sauf en cas de recours à un service professionnel spécifique de transition. Un client qui a l'intention d'exercer des droits liés au changement de fournisseur, prévus par le présent règlement, devrait informer le fournisseur d'origine de services de traitement de données de la décision de se tourner vers un fournisseur différent de services de traitement de données, de se tourner vers une infrastructure TIC sur site ou de supprimer les actifs de ce client et d'effacer ses données exportables.

(86) Par équivalence fonctionnelle, on entend le rétablissement, sur la base des données exportables et des actifs numériques du client, d'un niveau minimal de fonctionnalité dans l'environnement d'un nouveau service de traitement de données du même type de service après le changement de fournisseur, lorsque le service de traitement des données de destination donne un résultat sensiblement comparable en réponse au même intrant pour des fonctionnalités partagées fournies au client en vertu du contrat. On peut seulement attendre des fournisseurs de services de traitement de données qu'ils facilitent l'équivalence fonctionnelle pour les fonctionnalités que les services de traitement des données, tant d'origine que de destination, offrent de manière indépendante. Le présent règlement ne constitue pas une obligation de faciliter l'équivalence fonctionnelle pour les fournisseurs de services de traitement de données autres que ceux qui proposent des services du modèle de fourniture IaaS.

(87) Les services de traitement de données sont utilisés dans tous les secteurs et proposent des complexités et types de services différents. Il s'agit d'un élément important à prendre en considération en ce qui concerne le processus de portage et les délais. Néanmoins, une prolongation de la période transitoire en raison de l'impossibilité technique de finaliser le processus de changement de fournisseur dans le délai imparti ne devrait être invoquée que dans des cas dûment justifiés. La charge de la preuve à cet égard devrait incomber entièrement au fournisseur du service de traitement de données concerné. Cela est sans préjudice du droit exclusif du client de prolonger la période transitoire une fois pour une période que le client juge plus adaptée pour ses propres finalités. Le client peut invoquer ce droit à une prolongation avant ou pendant la période transitoire, compte tenu du fait que le contrat reste applicable pendant la période transitoire.

(88) Les frais de changement de fournisseur sont les frais imposés par les fournisseurs de services de traitement de données aux clients pour le processus de changement de fournisseur. En général, ces frais sont destinés à répercuter les coûts que le fournisseur d'origine de services de traitement de données peut encourir en raison du processus de changement de fournisseur, sur le client qui souhaite changer de fournisseur. Les frais de changement de fournisseur courants sont, par exemple, les frais liés au transfert des données d'un fournisseur de services de traitement de données à un autre ou à une infrastructure TIC sur site (les frais de transfert des données) ou les frais encourus pour des actions de soutien spécifiques pendant le processus de changement de fournisseur. Les frais de transfert des données inutilement élevés ou les frais injustifiés non liés à des coûts réels de changement de fournisseur sont un frein au changement de fournisseur pour les clients, restreignent la libre circulation des données, peuvent restreindre la concurrence et provoquent des effets de verrouillage pour les clients en réduisant les incitations à choisir un fournisseur de services différent ou supplémentaire. Les frais de changement de fournisseur devraient dès lors être supprimés après trois ans à compter de la date d'entrée en vigueur du présent règlement. Les fournisseurs de services de traitement de données devraient pouvoir imposer des frais de changement de fournisseur réduits jusqu'à cette date.

(89) Un fournisseur d'origine de services de traitement de données devrait pouvoir externaliser certaines tâches et verser une compensation à des entités tierces afin de se conformer aux obligations prévues par le présent règlement. Un client ne devrait pas supporter les coûts découlant de l'externalisation de services décidée par le fournisseur d'origine de services de traitement de données au cours du processus de changement de fournisseur et ces coûts devraient être considérés comme étant injustifiés, à moins qu'ils ne couvrent des travaux entrepris par le fournisseur de services de traitement de données à la demande du client en vue d'un soutien supplémentaire dans le cadre du processus de changement de fournisseur qui dépassent les obligations en matière de changement de fournisseur expressément prévues par le présent règlement. Aucune disposition du présent règlement n'empêche un client de verser une compensation à des entités tierces pour un soutien dans le cadre du processus de migration, ni des parties de convenir de contrats de services de traitement de données d'une durée déterminée, y compris de pénalités de résiliation anticipée proportionnées pour couvrir la résiliation anticipée de tels contrats, conformément au droit de l'Union ou au droit national. Afin d'encourager la concurrence, la suppression progressive des frais de changement de fournisseur de services de traitement de données devrait porter en particulier sur les frais de transfert des données facturés par un fournisseur de services de traitement de données à un client. En soi, les frais de service standard afférents à la fourniture des services de traitement de données ne constituent pas des frais de changement de fournisseur. Ces frais de service standard ne sont pas susceptibles d'être supprimés et restent applicables jusqu'à ce que le contrat de fourniture des services concernés cesse de s'appliquer. Le présent règlement permet au client de demander la fourniture de services supplémentaires allant au-delà des obligations du fournisseur en matière de changement de fournisseur au titre du présent règlement. Ces services supplémentaires peuvent être fournis et facturés par le fournisseur lorsqu'ils sont fournis à la demande du client et que celui-ci marque à l'avance son accord sur le prix desdits services.

(90) Il est nécessaire d'adopter, en matière d'interopérabilité, une approche réglementaire ambitieuse et propice à l'innovation afin de remédier aux effets de verrouillage, qui nuisent à la concurrence et au développement de nouveaux services. L'interopérabilité des services de traitement de données requiert de multiples interfaces, couches d'infrastructures et couches de logiciels, et se limite rarement à un test binaire visant à en évaluer la faisabilité ou l'impossibilité. Par contre, la mise en œuvre d'une telle interopérabilité est soumise à une analyse coûts/avantages, nécessaire pour déterminer s'il est utile de chercher à obtenir des résultats raisonnablement prévisibles. La norme ISO/CEI 19941:2017 est une norme internationale importante qui constitue une référence pour la réalisation des objectifs du présent règlement, car elle contient des considérations techniques clarifiant la complexité d'un tel processus.

(91) 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 restant liés par les obligations du présent règlement en ce qui concerne leurs propres offres de services.

(92) Les fournisseurs de services de traitement de données devraient être tenus, dans les limites de leurs capacités et proportionnellement à leurs obligations respectives, d'offrir toute l'assistance et le soutien nécessaires pour que le processus de changement de fournisseur de services de traitement de données soit fructueux, efficace et sûr. Le présent règlement n'impose pas aux fournisseurs de services de traitement de données de développer de nouvelles catégories de services de traitement de données, y compris au sein ou sur la base de l'infrastructure TIC de fournisseurs de services de traitement de données différents afin de garantir une équivalence fonctionnelle dans un environnement autre que leurs propres systèmes. Un fournisseur d'origine de services de traitement de données n'a pas accès à l'environnement du fournisseur de destination de services de traitement de données ou n'a pas d'informations sur celui-ci. L'équivalence fonctionnelle ne devrait pas être interprétée comme obligeant le fournisseur d'origine de services de traitement de données à reconstruire le service en question au sein de l'infrastructure du fournisseur de destination de services de traitement de données. Le fournisseur de services de traitement de données d'origine devrait, en revanche, prendre toutes les mesures raisonnables en son pouvoir pour faciliter le processus de réalisation de l'équivalence fonctionnelle en fournissant des capacités, des informations, une documentation, une assistance technique adéquates et, le cas échéant, les outils nécessaires.

(93) Les fournisseurs de services de traitement de données devraient également être tenus de supprimer les obstacles existants et de ne pas en imposer de nouveaux, y compris pour les clients souhaitant passer à une infrastructure TIC sur site. Les obstacles peuvent être notamment de nature précommerciale, commerciale, technique, contractuelle ou organisationnelle. Les fournisseurs de services de traitement de données devraient également être tenus de supprimer les obstacles empêchant de découpler un service individuel spécifique d'autres services de traitement de données fournis dans le cadre d'un contrat et de faire en sorte que le service concerné puisse faire l'objet d'un changement de fournisseur, en l'absence d'obstacles techniques majeurs et avérés empêchant un tel découplage.

(94) Tout au long du processus de changement de fournisseur, un niveau élevé de sécurité devrait être maintenu. Cela signifie que le fournisseur d'origine de services de traitement de données devrait étendre le niveau de sécurité auquel il s'est engagé pour le service à toutes les modalités techniques dont ce fournisseur est responsable au cours du processus de changement de fournisseur, telles que les connexions réseau ou les dispositifs matériels. 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 ([31]). Le présent règlement ne devrait pas être interprété comme empêchant un fournisseur de services de traitement de données de fournir aux clients des services nouveaux ou meilleurs ou des caractéristiques et des fonctionnalités nouvelles ou meilleures, ou de concurrencer d'autres fournisseurs de services de traitement de données sur cette base.

(95) Les informations que les fournisseurs de services de traitement de données doivent donner aux clients pourraient appuyer la stratégie de sortie des clients. Ces informations devraient comprendre les procédures à suivre pour entamer le changement de services de traitement de données; les formats de données lisibles par machine vers lesquels les données de l'utilisateur peuvent être exportées; les outils destinés à exporter les données, dont des interfaces ouvertes, ainsi que les informations sur la compatibilité avec les normes harmonisées ou les spécifications communes fondées sur des spécifications d'interopérabilité ouvertes; des informations sur les restrictions et les limites techniques connues qui pourraient influer sur le processus de changement de fournisseur; et le temps considéré comme nécessaire pour achever ledit processus de changement.

(96) Afin de faciliter l'interopérabilité et le changement de services de traitement de données, les utilisateurs et les fournisseurs de services de traitement de données devraient envisager l'utilisation d'outils de mise en œuvre et de contrôle de la conformité, en particulier ceux publiés par la Commission sous la forme d'un recueil de règles de l'Union européenne sur l'informatique en nuage et d'un guide sur les marchés publics pour les services de traitement

([31]) 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).

des données. Les clauses contractuelles standard, en particulier, sont avantageuses car elles 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 de traitement de données 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 de traitement de données devraient envisager l'utilisation de clauses contractuelles standard ou d'autres outils de contrôle de la conformité par autorégulation, à condition qu'ils soient en totale conformité avec le présent règlement, élaborés par des organes ou groupes d'experts compétents établis en vertu du droit de l'Union.

(97) Afin de faciliter le changement de services de traitement de données, toutes les parties concernées, y compris les fournisseurs d'origine et de destination de services de traitement de données, devraient coopérer de bonne foi en vue de rendre efficace le processus de changement de fournisseur, et de permettre un transfert sécurisé et en temps utile des données nécessaires dans un format couramment utilisé, lisible par machine, et au moyen d'interfaces ouvertes, tout en évitant les perturbations du service et en assurant la continuité des services.

(98) Les services de traitement de données qui portent sur des services dont la majorité des caractéristiques principales ont été conçues sur mesure pour répondre aux demandes spécifiques d'un client donné ou dont tous les composants ont été développés pour les besoins d'un client particulier devraient être exemptés de certaines des obligations applicables au changement de services de traitement de données. Ceci ne devrait pas concerner les services que le fournisseur de services de traitement de données propose sur une large échelle commerciale par l'intermédiaire de son catalogue de services. Le fournisseur de services de traitement de données a notamment l'obligation d'informer dûment les clients potentiels de ces services, avant la conclusion d'un éventuel contrat, des obligations prévues par le présent règlement qui ne s'appliquent pas aux services concernés. Rien n'empêche le fournisseur de services de traitement de données de déployer à terme ces services à grande échelle, auquel cas ce fournisseur devrait se conformer à toutes les obligations en matière de changement de fournisseur prévues par le présent règlement.

(99) Conformément à l'exigence minimale permettant le changement de fournisseur de services de traitement de données, le présent règlement vise également à améliorer l'interopérabilité pour l'utilisation simultanée de services de traitement de données multiples dotés de fonctionnalités complémentaires. Sont visées les situations dans lesquelles les clients ne résilient pas un contrat pour changer de fournisseur de services de traitement de données, mais utilisent simultanément plusieurs services de différents fournisseurs, de manière interopérable, afin de bénéficier des fonctionnalités complémentaires des différents services dans la mise en place du système du client. Toutefois, il est admis que le processus de sortie des données d'un fournisseur de services de traitement de données vers un autre dans le but de faciliter l'utilisation simultanée de services peut constituer une activité continue, contrairement à la sortie ponctuelle requise dans le cadre du processus de changement de fournisseur. Les fournisseurs de services de traitement de données devraient, par conséquent, continuer à pouvoir imposer des frais de transfert des données, ne dépassant pas les coûts encourus, aux fins de l'utilisation simultanée après trois ans à compter de la date d'entrée en vigueur du présent règlement. Cette possibilité est importante, entre autres, pour assurer le succès du déploiement de stratégies multinuages qui permettent aux clients de mettre en œuvre des stratégies TIC à l'épreuve du temps et réduisent la dépendance à l'égard de fournisseurs particuliers de services de traitement de données. Faciliter une approche multinuage pour les clients des services de traitement de données peut également contribuer à accroître leur résilience opérationnelle numérique, ainsi que le prévoit, pour les institutions de services financiers, le règlement (UE) 2022/2554 du Parlement européen et du Conseil ([32]).

(100) Les spécifications et les normes d'interopérabilité ouvertes élaborées conformément à l'annexe II du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil ([33]) dans le domaine de l'interopérabilité et de la portabilité devraient permettre un environnement en nuage multifournisseur, qui est une exigence essentielle pour l'innovation ouverte dans l'économie européenne fondée sur les données. Étant donné que l'adoption par le marché des normes recensées dans le cadre de l'initiative de coordination de la normalisation de l'informatique en nuage (CSC), décidée en 2016, a été limitée, il est également nécessaire que la Commission s'appuie sur les acteurs du marché pour élaborer des spécifications d'interopérabilité ouvertes pertinentes afin de suivre le rythme rapide de l'évolution

([32]) Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 (JO L 333 du 27.12.2022, p. 1).

([33]) Règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

technologique dans ce secteur. Ces spécifications d'interopérabilité ouvertes peuvent ensuite être adoptées par la Commission sous la forme de spécifications communes. En outre, lorsque les processus axés sur le marché n'ont pas démontré une capacité d'établir des spécifications ou des normes communes qui facilitent une interopérabilité effective en nuage au niveau des PaaS et des 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 pour des types de services spécifiques 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. Après avoir consulté les parties prenantes, la Commission devrait pouvoir, par voie d'actes d'exécution, rendre obligatoire l'utilisation de normes harmonisées d'interopérabilité ou de spécifications communes 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 de données. Les fournisseurs de services de traitement de données devraient garantir la compatibilité avec ces normes harmonisées et spécifications communes fondées sur des spécifications d'interopérabilité ouvertes, qui ne devraient pas porter atteinte à la sécurité ou à l'intégrité des données. Les normes harmonisées pour l'interopérabilité des services de traitement de données et les spécifications communes fondées sur des spécifications d'interopérabilité ouvertes ne seront référencées que si elles respectent les critères spécifiés dans le présent règlement, qui ont la même signification que les exigences énoncées à l'annexe II du règlement (UE) nº 1025/2012 et les facettes d'interopérabilité définies dans la norme internationale ISO/CEI 19941:2017. En outre, la normalisation devrait tenir compte des besoins des PME.

(101) 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 à l'extérieur de leurs frontières, 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 des autorités répressives, 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 au titre du droit de l'Union ou au titre du droit national de l'État membre concerné, en particulier en ce qui concerne la protection des 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 nationale ou de défense, 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 de données à caractère non personnel ou l'accès aux données à caractère non personnel 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. Chaque fois que cela est 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, avant d'accorder un accès à ces données, afin de vérifier l'existence d'un conflit potentiel entre cet accès et des dispositions du droit de l'Union ou du droit national, 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 ce qui concerne la confidentialité.

(102) Afin de renforcer encore la confiance placée dans les données, il importe de mettre en œuvre, dans toute la mesure du possible, des garanties pour assurer le contrôle de données qui les concernent par les citoyens, le secteur public et les entreprises de l'Union. En outre, le droit, les valeurs et les normes de l'Union en ce qui concerne, entre autres, la sécurité, la protection des données et le respect de la vie privée, ainsi que la protection des consommateurs devraient être respectés. Afin de prévenir tout accès illicite des pouvoirs publics de pays tiers aux données à caractère non personnel, les fournisseurs de service de traitement de données soumis au présent règlement, 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 chiffrement des données, la sujétion régulière à des audits, le respect vérifié de dispositifs de certification pertinents en matière de réassurance de sécurité et par une modification de leurs politiques d'entreprise.

(103) La normalisation et l'interopérabilité sémantique devraient jouer un rôle essentiel dans l'apport de solutions techniques permettant de garantir l'interopérabilité au sein d'espaces européens communs de données et entre ces espaces, qui sont des cadres interopérables de normes et de pratiques communes spécifiques à chaque finalité ou à chaque secteur ou transsectoriels visant à partager ou à traiter conjointement des données aux fins, entre autres, de la mise au point de nouveaux produits et services, de la recherche scientifique ou d'initiatives de la société civile. Le présent règlement fixe certaines exigences essentielles en matière d'interopérabilité. Les participants aux espaces de données qui proposent des données ou des services de données à d'autres participants, qui sont des entités facilitant le partage de données au sein d'espaces européens communs de données, y compris les détenteurs de données, ou participant à ce partage, devraient respecter ces exigences pour ce qui est des éléments sous leur contrôle. Le respect de ces règles peut être assuré en adhérant aux exigences essentielles établies dans le présent règlement, ou peut être présumé en respectant des normes harmonisées ou des spécifications communes au moyen d'une présomption de conformité. Afin de faciliter la conformité avec les exigences en matière d'interopérabilité, il est nécessaire de prévoir une présomption de conformité des solutions d'interopérabilité qui satisfont à des normes harmonisées ou à des parties de celles-ci conformément au règlement (UE) nº 1025/2012, qui constitue le cadre par défaut pour l'élaboration de normes qui prévoient une telle présomption. La Commission devrait évaluer les obstacles à l'interopérabilité et donner la priorité aux besoins en matière de normalisation, sur la base desquels elle peut demander à une ou plusieurs organisations européennes de normalisation, en vertu du règlement (UE) nº 1025/2012, d'élaborer des normes harmonisées qui satisfont aux exigences essentielles établies dans le présent règlement. Lorsque de telles demandes ne débouchent pas sur des normes harmonisées ou que ces normes harmonisées sont insuffisantes pour garantir le respect des exigences essentielles prévues par le présent règlement, la Commission devrait pouvoir adopter des spécifications communes dans ces domaines, à condition que, ce faisant, elle respecte dûment le rôle et les fonctions des organismes de normalisation. Des spécifications communes ne devraient être adoptées qu'à titre de solution de repli exceptionnelle en vue de faciliter le respect des exigences essentielles prévues par le présent règlement, ou lorsque le processus de normalisation est bloqué, ou lorsque l'établissement de normes harmonisées appropriées accuse du retard. Si un tel retard est dû à la complexité technique de la norme en question, la Commission devrait en tenir compte avant d'envisager l'établissement de spécifications communes. Des spécifications communes devraient être élaborées selon des modalités ouvertes et inclusives et tenir compte, le cas échéant, des conseils formulés par le comité européen de l'innovation dans le domaine des données instauré par le règlement (UE) 2022/868. En outre, des spécifications communes dans différents secteurs pourraient être adoptées, conformément au droit de l'Union ou au droit national, en fonction des besoins spécifiques des secteurs concernés. La Commission devrait par ailleurs être habilitée à demander l'élaboration de normes harmonisées pour l'interopérabilité des services de traitement de données.

(104) Afin de promouvoir l'interopérabilité des outils d'exécution automatique des accords de partage de données, il est nécessaire de définir les exigences essentielles des contrats intelligents que les professionnels créent pour d'autres ou intègrent dans des applications soutenant la mise en œuvre d'accords de partage de données. Afin de faciliter la conformité de ces contrats intelligents avec ces exigences essentielles, il est nécessaire de prévoir une présomption de conformité des contrats intelligents qui satisfont à des normes harmonisées ou à des parties de celles-ci conformément au règlement (UE) nº 1025/2012. La notion de "contrat intelligent" figurant dans le présent règlement est technologiquement neutre. Les contrats intelligents peuvent, par exemple, être connectés à un registre électronique. Les exigences essentielles ne devraient s'appliquer qu'aux vendeurs de contrats intelligents, sauf lorsque ces derniers élaborent des contrats intelligents en interne à des fins exclusivement internes. L'exigence essentielle de faire en sorte que les contrats intelligents puissent être interrompus et résiliés implique le consentement mutuel des parties à l'accord de partage de données. L'utilisation de contrats intelligents pour l'exécution automatique de ces accords reste ou devrait rester sans incidence sur l'applicabilité des règles pertinentes du droit civil, du droit contractuel et du droit de la protection des consommateurs à de tels accords de partage de données.

(105) Afin de démontrer le respect des exigences essentielles du présent règlement, 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 de l'exécution d'un accord ou d'une partie de celui-ci, pour mettre des données à disposition dans le cadre du présent règlement, devrait procéder à une évaluation de la conformité et délivrer une déclaration UE de conformité. Une telle évaluation de la conformité devrait être soumise aux principes généraux établis dans le règlement (CE) nº 765/2008 du Parlement européen et du Conseil ([34]) et dans la décision (CE) nº 768/2008 du Parlement européen et du Conseil ([35]).

([34]) Règlement (CE) nº 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et abrogeant le règlement (CEE) nº 339/93 (JO L 218 du 13.8.2008, p. 30).

([35]) Décision nº 768/2008/CE du Parlement européen et du Conseil du 9 juillet 2008 relative à un cadre commun pour la commercialisation des produits et abrogeant la décision 93/465/CEE du Conseil (JO L 218 du 13.8.2008, p. 82).

(106) Outre l'obligation faite aux développeurs professionnels de contrats intelligents de respecter les exigences essentielles, il est également important d'encourager les participants aux espaces de données qui proposent des données ou des services fondés sur les données à d'autres participants au sein d'espaces européens communs des données et entre ces espaces à soutenir l'interopérabilité des outils de partage de données, y compris les contrats intelligents.

(107) Afin de garantir l'application et l'exécution 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 parmi celles-ci un coordinateur de données. Les autorités compétentes devraient coopérer entre elles. Dans le cadre de l'exercice de leurs pouvoirs d'enquête conformément aux procédures nationales applicables, les autorités compétentes devraient pouvoir rechercher et obtenir des informations, en particulier en ce qui concerne les activités des entités relevant de leur compétence et, y compris dans le cadre d'enquêtes conjointes, en tenant dûment compte du fait que les mesures de surveillance et d'exécution concernant une entité relevant de la compétence d'un autre État membre devraient être adoptées par l'autorité compétente de cet autre État membre, le cas échéant, conformément aux procédures relatives à la coopération transfrontière. Les autorités compétentes devraient se prêter mutuellement assistance en temps utile, en particulier lorsqu'une autorité compétente d'un État membre détient des informations utiles aux fins d'une enquête menée par les autorités compétentes d'autres États membres, ou est en mesure de recueillir de telles informations auxquelles les autorités compétentes de l'État membre dans lequel l'entité est établie n'ont pas accès. Les autorités compétentes et les coordinateurs de données devraient être identifiés dans un registre public tenu par la Commission. Le coordinateur de données pourrait constituer un moyen supplémentaire de faciliter la coopération dans les situations transfrontières, notamment lorsqu'une autorité compétente d'un État membre donné ne sait pas à quelle autorité s'adresser dans l'État membre du coordinateur de données, par exemple lorsque le cas concerne plusieurs autorités compétentes ou secteurs. Le coordinateur de données devrait, entre autres, faire office de point de contact unique pour toutes les questions liées à l'application du présent règlement. Lorsqu'aucun coordinateur de données n'a été désigné, l'autorité compétente devrait assumer les tâches qui sont assignées à ce dernier en vertu du présent règlement. Les autorités chargées de contrôler le respect du droit en matière de protection des données et les autorités compétentes désignées en vertu du droit de l'Union ou du droit national devraient être responsables de l'application du présent règlement dans leurs domaines de compétence. Afin d'éviter des conflits d'intérêts, les autorités compétentes responsables de l'application et de l'exécution du présent règlement pour ce qui est de la mise à disposition de données à la suite d'une demande fondée sur un besoin exceptionnel ne devraient pas bénéficier du droit de présenter une telle demande.

(108) Pour faire valoir leurs droits au titre du présent règlement, les personnes physiques et morales devraient pouvoir demander réparation pour des infractions à ces droits en introduisant une réclamation. Le coordinateur de données devrait, sur demande, fournir aux personnes physiques et morales toutes les informations nécessaires pour introduire leurs réclamations auprès de l'autorité compétente concernée. Les autorités compétentes devraient être tenues de coopérer afin de garantir que la réclamation est gérée et traitée de manière appropriée, efficace et rapide. 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 ([36]) et de la directive (UE) 2020/1828 du Parlement européen et du Conseil ([37]).

(109) Les autorités compétentes devraient veiller à ce que les infractions aux obligations prévues par le présent règlement fassent l'objet de sanctions. Ces sanctions pourraient revêtir la forme, entre autres, de sanctions pécuniaires, d'avertissements, de blâmes ou d'injonctions de mettre des pratiques commerciales en conformité avec les obligations instaurées par le présent règlement. Les sanctions définies par les États membres devraient être effectives, proportionnées et dissuasives et tenir compte des recommandations du comité européen de l'innovation dans le domaine des données, contribuant ainsi à atteindre le plus haut niveau possible de cohérence dans l'instauration et l'application des sanctions. Le cas échéant, les autorités compétentes devraient recourir à des mesures provisoires

([36]) 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) n° 2006/2004 (JO L 345 du 27.12.2017, p. 1).

([37]) 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).

pour limiter les effets d'une infraction présumée tant que l'enquête sur cette infraction est en cours. Ce faisant, elles devraient tenir compte, entre autres, de la nature, de la gravité, de l'ampleur et de la durée de l'infraction 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 de l'infraction. Si l'auteur de l'infraction manque systématiquement ou de façon récurrente aux obligations qui lui incombent au titre du présent règlement, elles devraient également en tenir compte. Afin de garantir le respect du principe ne bis in idem, et d'éviter en particulier que la même infraction aux obligations prévues par le présent règlement ne soit sanctionnée plus d'une fois, un État membre qui entend exercer sa compétence à l'égard de l'auteur d'une infraction qui n'est pas établi dans l'Union et n'a pas désigné de représentant légal dans l'Union devrait, sans retard injustifié, en informer tous les coordinateurs de données ainsi que la Commission.

(110) Le comité européen de l'innovation dans le domaine des données devrait conseiller et assister la Commission dans la coordination des pratiques et politiques nationales sur les sujets couverts par le présent règlement ainsi que dans la réalisation de ses objectifs en matière de normalisation technique en vue de renforcer l'interopérabilité. Le comité devrait également jouer un rôle essentiel pour faciliter des discussions approfondies entre autorités compétentes concernant l'application et l'exécution du présent règlement. Cet échange d'informations vise à améliorer l'accès effectif à la justice ainsi que la coopération en matière répressive et judiciaire dans l'ensemble de l'Union. Entre autres fonctions, les autorités compétentes devraient faire appel au comité européen de l'innovation dans le domaine des données en tant que plateforme pour évaluer, coordonner et adopter des recommandations sur la détermination de sanctions en cas d'infractions au présent règlement. Le comité devrait permettre aux autorités compétentes, avec l'aide de la Commission, de coordonner l'approche optimale pour déterminer et imposer de telles sanctions. Cette approche permet d'éviter la fragmentation tout en laissant une souplesse aux États membres et devrait déboucher sur des recommandations efficaces qui favorisent l'application cohérente du présent règlement. Le comité européen de l'innovation dans le domaine des données devrait également jouer un rôle consultatif dans les processus de normalisation et l'adoption des spécifications communes par voie d'actes d'exécution, dans l'adoption des actes délégués visant à établir un mécanisme de suivi des frais de changement de fournisseur imposés par les fournisseurs de services de traitement de données et à préciser davantage les exigences essentielles pour l'interopérabilité des données, des mécanismes et des services de partage des données, ainsi que pour l'interopérabilité des espaces européens communs des données. Il devrait également conseiller et assister la Commission dans l'adoption des lignes directrices fixant des spécifications d'interopérabilité pour le fonctionnement des espaces européens communs des données.

(111) 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 entre entreprises, 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 particulier les PME à conclure un contrat. Lorsqu'elles seront largement et intégralement utilisées, ces clauses contractuelles types devraient également avoir pour effet bénéfique d'influencer la manière dont sont conçus les contrats en ce qui concerne l'accès aux données et à l'utilisation des données et conduire ainsi plus généralement à des relations contractuelles plus équitables en matière d'accès aux données et de partage des données.

(112) 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 connexe, ou d'autres types de données générées par des machines, invoquent le droit sui generis prévu par l'article 7 de la directive 96/9/CE, et puissent entraver ainsi, en particulier, l'exercice effectif du droit des utilisateurs d'avoir accès aux données et d' utiliser les données ainsi que du droit de partager des données avec des tiers prévus par le présent règlement, il y a lieu de préciser que le droit sui generis ne s'applique pas à ces bases de données. Cela ne porte pas atteinte à la potentielle application du droit *sui generis* prévu par l'article 7 de la directive 96/9/CE aux bases de données contenant des données ne relevant pas du champ d'application du présent règlement, à condition que les conditions de la protection en application du paragraphe 1 dudit article soient remplies.

(113) Afin de tenir compte des aspects techniques des services de traitement de données, il convient 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 dans le but de créer un mécanisme de suivi des frais de changement de fournisseur imposés par les fournisseurs de services de traitement de données sur le marché, et de préciser davantage les exigences essentielles en matière d'interopérabilité imposées aux participants aux espaces de données qui proposent des données ou des services de données aux autres participants. Il importe particulièrement

que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 "Mieux légiférer" ([38]). En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(114) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission en ce qui concerne l'adoption de spécifications communes pour assurer l'interopérabilité des données, des mécanismes et des services de partage des données ainsi que des espaces européens communs de données, de spécifications communes concernant l'interopérabilité des services de traitement de données, et de spécifications communes concernant l'interopérabilité des contrats intelligents. Il convient aussi de conférer des compétences d'exécution à la Commission aux fins de publier les références des normes harmonisées et des spécifications communes pour l'interopérabilité des services de traitement de données dans un répertoire central des normes de l'Union pour l'interopérabilité des services de traitement de données. Ces compétences devraient être exercées conformément au règlement (UE) n° 182/2011 du Parlement européen et du Conseil ([39]).

(115) 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 l'utilisation des données, tels que les aspects liés à la gouvernance ou des exigences en matière de sécurité, y compris de cybersécurité. Le présent règlement devrait également s'entendre sans préjudice de règles plus spécifiques dans le cadre du développement d'espaces européens communs de données ou, sous réserve des exceptions prévues par le présent règlement, sans préjudice du droit de l'Union et du droit national prévoyant l'accès aux données, et autorisant l'utilisation des données, à des fins de recherche scientifique.

(116) Le présent règlement ne devrait pas avoir d'incidence sur l'application des règles relatives à la concurrence, en particulier les articles 101 et 102 du traité sur le fonctionnement de l'Union européenne. Les mesures prévues par le présent règlement ne devraient pas être utilisées pour restreindre la concurrence d'une manière qui soit contraire au traité sur le fonctionnement de l'Union européenne.

(117) Afin de permettre aux acteurs relevant du champ d'application du présent règlement de s'adapter aux nouvelles règles prévues par celui-ci et de mettre en place les aménagements techniques nécessaires, ces règles devraient s'appliquer à partir du 12 septembre 2025.

(118) 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, paragraphes 1 et 2, du règlement (UE) 2018/1725 et ont rendu leur avis le 4 mai 2022.

(119) Étant donné que les objectifs du présent règlement, à savoir garantir l'équité dans l'attribution de valeur issue de données parmi les acteurs de l'économie fondée sur les données et favoriser un accès équitable aux données et une utilisation équitable des données afin de contribuer à la création d'un véritable marché intérieur des données, ne peuvent être atteints de manière suffisante par les États membres mais peuvent, en raison des dimensions ou des effets de l'action et de l'utilisation transfrontière des données, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs,

([38]) JO L 123 du 12.5.2016, p. 1.

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

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

DISPOSITIONS GENERALES

Article premier

Objet et champ d'application

1. Le présent règlement établit des règles harmonisées, entre autres, sur:

a) la mise à disposition de données relatives au produit et de données relatives au service connexe au profit de l'utilisateur du produit connecté ou du service connexe;

b) la mise à disposition de données par les détenteurs de données au profit des destinataires de données;

c) la mise à disposition de données par les détenteurs de données au profit d'organismes du secteur public, de la Commission, de la Banque centrale européenne et d'organes de l'Union, lorsqu'il existe un besoin exceptionnel de disposer de ces données pour exécuter une mission spécifique d'intérêt public;

d) la facilitation du changement de de service de traitement de données;

e) l'introduction de garanties contre l'accès illicite de tiers à des données à caractère non personnel; et

f) le développement de normes d'interopérabilité pour les données auxquelles il doit être accédé, qui doivent être transférées et qui doivent être utilisées.

2. Le présent règlement couvre les données à caractère personnel et non personnel, y compris les types de données ci-après, dans les contextes suivants:

a) le chapitre II s'applique aux données, à l'exception du contenu, relatives à la performance, à l'utilisation et à l'environnement des produits connectés et des services connexes;

b) le chapitre III s'applique aux données du secteur privé qui sont soumises à des obligations légales de partage des données;

c) le chapitre IV s'applique aux données du secteur privé auxquelles il est accédé et qui sont utilisées sur la base d'un contrat entre entreprises;

d) le chapitre V s'applique aux données du secteur privé, en particulier les données à caractère non personnel;

e) le chapitre VI s'applique aux données et aux services traités par des fournisseurs de services de traitement de données;

f) le chapitre VII s'applique aux données à caractère non personnel détenues dans l'Union par des fournisseurs de services de traitement de données.

3. Le présent règlement s'applique:

a) aux fabricants de produits connectés mis sur le marché de l'Union et aux fournisseurs de services connexes, quel que soit le lieu d'établissement de ces fabricants et fournisseurs;

b) aux utilisateurs dans l'Union de produits connectés ou de services connexes tels qu'ils sont visés au point a);

c) aux détenteurs de données, quel que soit leur lieu d'établissement, qui mettent des données à la disposition de destinataires de données dans l'Union;

d) aux destinataires de données dans l'Union au profit desquels des données sont mises à disposition;

e) aux organismes du secteur public, à la Commission, à la Banque centrale européenne et aux organes de l'Union qui demandent aux détenteurs de données de mettre des données à disposition lorsqu'il existe un besoin exceptionnel de disposer de ces données pour exécuter une mission spécifique d'intérêt public, ainsi qu'aux détenteurs de données qui fournissent ces données en réponse à une telle demande;

f) aux fournisseurs de services de traitement de données, quel que soit leur lieu d'établissement, fournissant de tels services à des clients dans l'Union;

g) aux participants à des espaces de données et aux vendeurs d'applications utilisant des contrats intelligents et aux personnes dont l'activité commerciale, l'entreprise ou la profession implique le déploiement de contrats intelligents pour des tiers dans le cadre de l'exécution d'un accord.

4. Lorsque le présent règlement fait référence à des produits connectés ou à des services connexes, ces références s'entendent également comme incluant également les assistants virtuels, dans la mesure où ceux-ci interagissent avec un produit connecté ou un service connexe.

5. Le présent règlement est sans préjudice du droit de l'Union et du droit national en matière de protection des données à caractère personnel, de la vie privée et de la confidentialité des communications et de l'intégrité des équipements terminaux, qui s'appliquent aux données à caractère personnel traitées en lien avec les droits et obligations énoncés dans le présent règlement, en particulier des règlements (UE) 2016/679 et (UE) 2018/1725 et de la directive 2002/58/CE, y compris des pouvoirs et des compétences des autorités de contrôle et des droits des personnes concernées. Dans la mesure où les utilisateurs sont les personnes concernées, les droits fixés au chapitre II du présent règlement complètent les droits d'accès par les personnes concernées et les droits à la portabilité des données prévus aux articles 15 et 20 du règlement (UE) 2016/679. En cas de conflit entre le présent règlement et le droit de l'Union en matière de protection des données à caractère personnel ou de vie privée, ou la législation nationale adoptée conformément audit droit de l'Union, les dispositions pertinentes du droit de l'Union ou du droit national en matière de protection des données à caractère personnel ou de vie privée prévalent.

6. Le présent règlement ne s'applique pas aux accords volontaires d'échange de données entre entités privées et publiques, en particulier aux accords volontaires de partage de données, ni ne les remplace.

Le présent règlement n'affecte pas les actes juridiques de l'Union ou nationaux prévoyant l'accès aux données, le partage et l'utilisation de données 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, en particulier les règlements (UE) 2021/784, (UE) 2022/2065 et (UE) 2023/1543 et la directive (UE) 2023/1544, ou sur la coopération internationale dans ce domaine. Le présent règlement ne s'applique pas à la collecte ou au partage de données, ni à l'accès aux données ou à l'utilisation de données au titre du règlement (UE) 2015/847 et de la directive (UE) 2015/849. Le présent règlement ne s'applique pas aux domaines qui ne relèvent pas du champ d'application du droit de l'Union et, en tout état de cause, ne porte pas atteinte aux compétences des États membres en matière de sécurité publique, de défense ou de sécurité nationale, quel que soit le type d'entité chargée par les États membres d'exécuter des tâches en rapport avec ces compétences, ou leur pouvoir de préserver d'autres fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer l'intégrité territoriale de l'État et de maintenir l'ordre public. Le présent règlement ne porte pas atteinte aux compétences des États membres en matière de douanes et d'administration fiscale, ou de santé et de sécurité des citoyens.

7. Le présent règlement complète l'approche d'autorégulation suivie par le règlement (UE) 2018/1807 en ajoutant des obligations d'application générale en matière de changement de fournisseur de services d'informatique en nuage.

8. Le présent règlement est sans préjudice des actes juridiques de l'Union et nationaux prévoyant la protection des droits de propriété intellectuelle, notamment les directives 2001/29/CE, 2004/48/CE et (UE) 2019/790.

9. Le présent règlement complète le droit de l'Union qui vise à promouvoir les intérêts des consommateurs et à assurer un niveau élevé de protection des consommateurs, et à protéger leur santé, leur sécurité et leurs intérêts économiques, en particulier les directives 93/13/CEE, 2005/29/CE et 2011/83/UE, et il est sans préjudice dudit droit de l'Union.

10. Le présent règlement ne fait pas obstacle à la conclusion de contrats portant sur le partage volontaire et licite de données, y compris de contrats conclus sur une base réciproque, qui respectent les exigences fixées par le présent règlement.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

1) ”données”: toute représentation numérique d’actes, de faits ou d’informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d’enregistrements sonores, visuels ou audiovisuels;

2) ”métadonnées”: une description structurée du contenu ou de l’utilisation des données qui facilite la découverte ou l’utilisation de ces données;

3) ”données à caractère personnel”: les données à caractère personnel au sens de l’article 4, point 1), du règlement (UE) 2016/679;

4) ”données à caractère non personnel”: les données autres que les données à caractère personnel;

5) ”produit connecté”: un objet qui obtient, génère ou recueille des données concernant son utilisation ou son environnement, qui est en mesure de communiquer des données relatives au produit par l’intermédiaire d’un service de communications électroniques, d’une connexion physique ou d’un dispositif d’accès intégré et dont la fonction première n’est pas de stocker, de traiter ou de transmettre des données pour le compte de toute partie autre que l’utilisateur;

6) ”service connexe”: un service numérique, autre qu’un service de communications électroniques, y compris un logiciel, qui est connecté au produit au moment de l’achat, ou de la mise en location ou en crédit-bail, de telle sorte que son absence empêcherait le produit connecté d’exécuter une ou plusieurs de ses fonctions, ou qui est ensuite connecté au produit par le fabricant ou un tiers pour ajouter, mettre à jour ou adapter les fonctions du produit connecté;

7) ”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, telles que la collecte, l’enregistrement, l’organisation, la structuration, la conservation, l’adaptation ou la modification, l’extraction, la consultation, l’utilisation, la communication par transmission, la diffusion ou d’autres moyens de mise à disposition, le rapprochement ou l’interconnexion, la limitation, l’effacement ou la destruction;

8) ”service de traitement de données”: un service numérique qui est fourni à un client et qui permet un accès par réseau en tout lieu et à la demande à un ensemble partagé de ressources informatiques configurables, modulables et variables de nature centralisée, distribuée ou fortement distribuée, qui peuvent être rapidement mobilisées et libérées avec un minimum d’efforts de gestion ou d’interaction avec le fournisseur de services;

9) ”même type de service”: un ensemble de services de traitement de données qui partagent le même objectif principal, le même modèle de service de traitement de données et les principales fonctionnalités;

10) ”service d’intermédiation de données”: le service d’intermédiation de données au sens de l’article 2, point 11), du règlement (UE) 2022/868;

11) ”personne concernée”: la personne concernée telle qu’elle est visée à l’article 4, point 1), du règlement (UE) 2016/679;

12) ”utilisateur”: une personne physique ou morale à laquelle appartient un produit connecté ou à laquelle des droits temporaires d’utilisation de ce produit connecté ont été cédés contractuellement, ou qui reçoit des services connexes;

13) ”détenteur de données”: une personne physique ou morale qui, conformément au présent règlement, aux dispositions applicables du droit de l’Union ou à la législation nationale adoptée conformément au droit de l’Union, a le droit ou l’obligation d’utiliser et de mettre à disposition des données, y compris, lorsqu’il en a été convenu par contrat, des données relatives au produit ou des données relatives au service connexe qu’elle a extraites ou générées au cours de la fourniture d’un service connexe;

14) ”destinataire de données”: une personne physique ou morale, autre que l'utilisateur d'un produit connecté ou d'un service connexe, agissant à des fins qui sont liées à son activité commerciale, industrielle, artisanale ou libérale, à la disposition duquel 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 adoptée conformément au droit de l'Union;

15) ”données relatives au produit”: les données générées par l'utilisation d'un produit connecté que le fabricant a conçu pour qu'elles puissent être extraites, au moyen d'un service de communications électroniques, d'une connexion physique ou d'un dispositif d'accès intégré, par un utilisateur, un détenteur de données ou un tiers, y compris, le cas échéant, le fabricant;

16) ”données relatives au service connexe”: les données représentant la numérisation des actions de l'utilisateur ou des événements liés au produit connecté, enregistrées intentionnellement par l'utilisateur ou générées en tant que produit annexe de l'action de l'utilisateur lors de la fourniture d'un service connexe par le fournisseur;

17) ”données facilement accessibles”: les données relatives à un produit et les données relatives à un service connexe qu'un détenteur de données obtient légalement ou peut obtenir légalement à partir du produit connecté ou du service connexe, sans effort disproportionné allant au-delà d'une simple opération;

18) ”secret d'affaires”: un secret d'affaires au sens de l'article 2, point 1), de la directive (UE) 2016/943;

19) ”détenteur de secrets d'affaires”: un détenteur de secrets d'affaires au sens de l'article 2, point 2), de la directive (UE) 2016/943;

20) ”profilage”: le profilage au sens de l'article 4, point 4), du règlement (UE) 2016/679;

21) ”mise à disposition sur le marché”: toute fourniture d'un produit connecté destiné à être distribué, consommé ou utilisé sur le marché de l'Union dans le cadre d'une activité commerciale, à titre onéreux ou gratuit;

22) ”mise sur le marché”: la première mise à disposition d'un produit connecté sur le marché de l'Union;

23) ”consommateur”: toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale;

24) ”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;

25) ”petite entreprise”: une petite entreprise telle qu'elle est définie à l'article 2, paragraphe 2, de l'annexe de la recommandation 2003/361/CE;

26) ”microentreprise”: une microentreprise telle qu'elle est définie à l'article 2, paragraphe 3, de l'annexe de la recommandation 2003/361/CE;

27) ”organes de l'Union”: les organes et organismes de l'Union mis en place par ou en vertu des actes adoptés sur la base du traité sur l'Union européenne, du traité sur le fonctionnement de l'Union européenne ou du traité instituant la Communauté européenne de l'énergie atomique;

28) ”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;

29) ” situation d'urgence”: une situation exceptionnelle, d'une durée limitée, telle qu'une urgence de santé publique, une urgence résultant d'une catastrophe naturelle ou d'une catastrophe majeure d'origine humaine, y compris un incident majeur de cybersécurité, ayant une incidence négative sur la population de l'Union ou sur l'ensemble ou une partie d'un État membre, entraînant un risque de répercussions graves et durables sur les conditions de vie ou la stabilité économique, la stabilité financière, ou la détérioration substantielle et immédiate d'actifs économiques dans l'Union ou l'État membre concerné, et qui est déterminée ou officiellement déclarée conformément aux procédures pertinentes prévues par le droit de l'Union ou le droit national;

30) ”client”: une personne physique ou morale qui a noué une relation contractuelle avec un fournisseur de services de traitement de données dans le but d'utiliser un ou plusieurs services de traitement de données;

31) ”assistants virtuels”: des logiciels capables de traiter des demandes, des tâches ou des questions, notamment celles fondées sur des données d'entrée sonores ou écrites, ou des gestes ou des mouvements, et qui, sur la base de ces demandes, tâches ou questions, donnent accès à d'autres services ou contrôlent les fonctions des produits connectés;

32) ”actifs numériques”: des éléments en format numérique, y compris des applications, pour lesquels le client est titulaire du droit d'utilisation, indépendamment de la relation contractuelle que le client a avec le service de traitement de données qu'il a l'intention de quitter;

33) ”infrastructure TIC sur site”: une infrastructure TIC et des ressources informatiques qui appartiennent au client, qu'il loue ou qu'il utilise en crédit-bail, situées dans le centre de données du client lui-même et exploitées par le client ou par un tiers;

34) ”changement de fournisseur”: le processus impliquant un fournisseur d'origine de services de traitement de données, un client d'un service de traitement de données et, le cas échéant, un fournisseur de destination de services de traitement de données, par lequel le client d'un service de traitement de données passe de l'utilisation d'un service de traitement de données à l'utilisation d'un autre service de traitement de données du même type de service, ou un autre service, proposé par un fournisseur de services de traitement de données différent, ou à une infrastructure TIC sur site, y compris par l'extraction, la transformation et le téléversement des données;

35) ”frais de transfert des données”: les frais de transfert de données facturés aux clients pour l'extraction de leurs données au moyen du réseau depuis l'infrastructure TIC d'un fournisseur de services de traitement de données vers le système d'un fournisseur différent ou vers une infrastructure TIC sur site;

36) ”frais de changement de fournisseur”: les frais, autres que les frais de service standard ou les pénalités de résiliation anticipée, imposés par un fournisseur de services de traitement de données à un client pour les actions requises par le présent règlement pour changer de fournisseur en passant au système d'un fournisseur différent ou à une infrastructure TIC sur site, y compris les frais de transfert des données;

37) ”équivalence fonctionnelle”: le rétablissement, sur la base des données exportables et des actifs numériques du client, d'un niveau minimal de fonctionnalité dans l'environnement d'un nouveau service de traitement de données du même type de service après le processus de changement de fournisseur, lorsque le service de traitement de données de destination donne un résultat sensiblement comparable en réponse à la même entrée pour les fonctionnalités partagées fournies au client en vertu du contrat;

38) ”données exportables”: aux fins des articles 23 à 31 et de l'article 35, les données d'entrée et de sortie, y compris les métadonnées, générées directement ou indirectement, ou cogénérées, par l'utilisation par le client du service de traitement de données, à l'exclusion des actifs ou des données protégés par des droits de propriété intellectuelle, ou constituant un secret d'affaires, des fournisseurs de services de traitement de données ou des tiers;

39) ”contrat intelligent”: un programme informatique utilisé pour l'exécution automatique d'un accord ou d'une partie de celui-ci, utilisant une séquence d'enregistrements de données électroniques et garantissant leur intégrité et l'exactitude de leur ordre chronologique;

40) ”interopérabilité”: la capacité d'au moins deux espaces de données ou réseaux de communication, systèmes, produits connectés, applications, services de traitement de données ou composants d'échanger et d'utiliser des données afin de remplir leurs fonctions;

41) ”spécification d'interopérabilité ouverte”: une spécification technique dans le domaine des technologies de l'information et de la communication qui est orientée vers les performances et la réalisation de l'interopérabilité entre les services de traitement de données;

42) "spécifications communes": un document, autre qu'une norme, contenant des solutions techniques qui permettent de satisfaire à certaines exigences et obligations établies au titre du présent règlement;

43) "norme harmonisée": une norme harmonisée au sens de l'article 2, point 1), c), du règlement (UE) nº 1025/2012.

CHAPITRE II

PARTAGE DE DONNEES ENTRE ENTREPRISES ET CONSOMMATEURS ET ENTRE ENTREPRISES

Article 3

Obligation de rendre les données relatives aux produits et les données relatives aux services connexes accessibles à l'utilisateur

1. Les produits connectés sont conçus et fabriqués, et les services connexes conçus et fournis, de telle sorte que les données relatives auxdits produits et les données relatives aux services connexes, y compris les métadonnées pertinentes nécessaires à l'interprétation et à l'utilisation de ces données, sont, par défaut, accessibles à l'utilisateur, de manière aisée, sécurisée, sans frais, dans un format complet, structuré, couramment utilisé et lisible par machine, et sont, lorsque cela est pertinent et techniquement possible, directement accessibles à l'utilisateur.

2. Avant la conclusion d'un contrat d'achat, de location ou de crédit-bail relatif à un produit connecté, le vendeur, le loueur ou le bailleur, qui peut être le fabricant, communique à l'utilisateur, de manière claire et compréhensible, au moins les informations suivantes:

a) le type, le format et le volume estimé des données relatives au produit que le produit connecté est capable de générer;

b) si le produit connecté est capable de générer des données en continu et en temps réel;

c) si le produit connecté est capable de stocker des données sur un dispositif intégré ou sur un serveur distant, y compris, le cas échéant, la durée de conservation prévue;

d) la manière dont l'utilisateur peut accéder aux données, extraire les données ou, le cas échéant, les effacer, y compris les moyens techniques nécessaires pour ce faire, ainsi que leurs conditions d'utilisation et leur qualité de service.

3. Avant la conclusion d'un contrat relatif à la fourniture d'un service connexe, le fournisseur d'un tel service connexe communique à l'utilisateur, de manière claire et compréhensible, au moins les informations suivantes:

a) la nature, le volume estimé et la fréquence de collecte des données relatives au produit que le détenteur de données potentiel devrait obtenir et, le cas échéant, les modalités selon lesquelles l'utilisateur peut accéder à ces données ou les extraire, y compris les modalités de stockage des données du détenteur de données potentiel et la durée de conservation;

b) la nature et le volume estimé des données relatives aux services connexes à générer, ainsi que les modalités selon lesquelles l'utilisateur peut avoir accès à ces données ou les extraire, y compris les modalités de stockage des données du détenteur de données potentiel et la durée de conservation;

c) si le détenteur de données potentiel a l'intention d'utiliser lui-même des données facilement accessibles et les finalités pour lesquelles ces données sont utilisées, et s'il a l'intention d'autoriser un ou plusieurs tiers à utiliser les données pour des finalités convenues avec l'utilisateur;

d) l'identité du détenteur de données potentiel, telle que sa raison sociale et l'adresse géographique à laquelle il est établi et, le cas échéant, des autres parties au traitement de données;

e) les moyens de communication qui permettent de contacter rapidement le détenteur de données potentiel et de communiquer efficacement avec lui;

f) la manière dont l'utilisateur peut demander à ce que les données soient partagées avec un tiers et, le cas échéant, mettre un terme au partage des données;

g) le droit de l'utilisateur d'introduire une réclamation pour infraction aux dispositions du présent chapitre auprès de l'autorité compétente désignée en vertu de l'article 37;

h) si un détenteur de données potentiel est le détenteur de secrets d'affaires contenus dans les données qui sont accessibles à partir du produit connecté ou générées au cours de la fourniture d'un service connexe, et, lorsque le détenteur de données potentiel n'est pas le détenteur de secrets d'affaires, l'identité du détenteur de secrets d'affaires;

i) la durée du contrat entre l'utilisateur et le détenteur de données potentiel, ainsi que les modalités de résiliation de ce contrat.

Article 4

Droits et obligations des utilisateurs et des détenteurs de données concernant l'accès aux données relatives au produit et aux données relatives au service connexe, leur utilisation et leur mise à disposition

1. Lorsque l'utilisateur ne peut pas accéder directement à des données à partir du produit connecté ou du service connexe, les détenteurs de données rendent les données facilement accessibles, ainsi que les métadonnées pertinentes nécessaires à l'interprétation et à l'utilisation de ces données, accessibles à l'utilisateur sans retard injustifié, à un niveau de qualité identique à celui dont bénéficie le détenteur de données, de manière aisée, sécurisée, sans frais, dans un format complet, structuré, couramment utilisé et lisible par machine et, lorsque cela est pertinent et techniquement possible, en continu et en temps réel. À cet effet, une simple demande est envoyée par voie électronique lorsque cela est techniquement possible.

2. Les utilisateurs et les détenteurs de données peuvent contractuellement restreindre ou interdire l'accès aux données, leur utilisation ou leur partage ultérieur, si un tel traitement est susceptible de porter atteinte aux exigences de sécurité du produit connecté, telles qu'elles sont prévues par le droit de l'Union ou le droit national, entraînant de graves effets indésirables pour la santé, la sûreté ou la sécurité des personnes physiques. Les autorités sectorielles peuvent fournir aux utilisateurs et aux détenteurs de données une expertise technique dans ce contexte. Lorsque le détenteur de données refuse de partager des données en vertu du présent article, il adresse une notification à l'autorité compétente désignée conformément à l'article 37.

3. Sans préjudice du droit de l'utilisateur de demander réparation à tout moment devant une juridiction d'un État membre, l'utilisateur, dans le cadre de tout litige avec le détenteur de données concernant les restrictions ou interdictions contractuelles visées au paragraphe 2, peut:

a) introduire une réclamation auprès de l'autorité compétente conformément à l'article 37, paragraphe 5, point b); ou

b) convenir avec le détenteur de données de porter la question devant un organe de règlement des litiges conformément à l'article 10, paragraphe 1.

4. Les détenteurs de données ne rendent pas indûment difficile pour les utilisateurs le fait d'effectuer des choix ou d'exercer des droits prévus au présent article, y compris en offrant des choix à l'utilisateur d'une manière qui n'est pas neutre ou en réduisant ou en compromettant l'autonomie, la prise de décision ou le choix des utilisateurs au moyen de la structure, de la conception, de la fonction ou du mode de fonctionnement d'une interface numérique utilisateur ou d'une partie de celle-ci.

5. Afin de vérifier si une personne physique ou morale peut être considérée comme un utilisateur aux fins du paragraphe 1, un détenteur de données n'exige pas de ladite personne qu'elle fournisse d'autres informations que celles qui sont nécessaires. Les détenteurs de données ne conservent aucune autre information, en particulier aucune donnée de connexion, 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.

6. Les secrets d'affaires sont préservés et ne sont divulgués que lorsque le détenteur de données et l'utilisateur prennent toutes les mesures nécessaires avant la divulgation pour préserver leur confidentialité, en particulier en ce qui concerne les tiers. Le détenteur de données ou, s'il ne s'agit pas de la même personne, le détenteur de secrets d'affaires recense les données protégées en tant que secrets d'affaires, y compris dans les métadonnées pertinentes, et convient avec l'utilisateur de mesures techniques et organisationnelles proportionnées nécessaires afin de préserver la confidentialité des données partagées, en particulier en ce qui concerne les tiers, telles que des clauses contractuelles types, des accords de confidentialité, des protocoles d'accès stricts, des normes techniques et l'application de codes de conduite.

7. En l'absence d'accord sur les mesures nécessaires visées au paragraphe 6, ou si l'utilisateur ne met pas en œuvre les mesures convenues en vertu du paragraphe 6 ou compromet la confidentialité des secrets d'affaires, le détenteur de données peut bloquer ou, selon le cas, suspendre le partage des données définies comme secrets d'affaires. La décision du détenteur de données est dûment motivée et communiquée par écrit à l'utilisateur sans retard injustifié. Dans de tels cas, le détenteur de données notifie à l'autorité compétente désignée en vertu de l'article 37 qu'il a retenu ou suspendu le partage de données et indique les mesures qui n'ont pas été convenues ou mises en œuvre et, le cas échéant, les secrets d'affaires dont la confidentialité a été compromise.

8. Dans des circonstances exceptionnelles, lorsque le détenteur de données qui est un détenteur de secret d'affaires peut démontrer qu'il est très probable qu'il subisse un préjudice économique grave du fait de la divulgation de secrets d'affaires, malgré les mesures techniques et organisationnelles prises par l'utilisateur en vertu du paragraphe 6 du présent article, ce détenteur de données peut refuser au cas par cas une demande d'accès aux données spécifiques en question. Cette démonstration est dûment étayée sur la base d'éléments objectifs, en particulier l'opposabilité de la protection des secrets d'affaires dans les pays tiers, la nature et le niveau de confidentialité des données demandées, ainsi que le caractère unique et neuf du produit connecté, et est fournie par écrit à l'utilisateur sans retard injustifié. Lorsque le détenteur de données refuse de partager des données en vertu du présent paragraphe, il adresse une notification à l'autorité compétente désignée en vertu de l'article 37.

9. Sans préjudice du droit d'un utilisateur de demander réparation à tout moment devant une juridiction d'un État membre, un utilisateur souhaitant contester la décision d'un détenteur de données de refuser ou de bloquer ou suspendre le partage de données en vertu des paragraphes 7 et 8 peut:

a) introduire une réclamation auprès de l'autorité compétente conformément à l'article 37, paragraphe 5, point b), qui décide, sans retard injustifié, si et dans quelles conditions le partage des données doit commencer ou reprendre; ou

b) convenir avec le détenteur de données de porter la question devant un organe de règlement des litiges conformément à l'article 10, paragraphe 1.

10. L'utilisateur ne se sert pas des données obtenues en réponse à une demande visée au paragraphe 1 pour mettre au point un produit connecté concurrençant le produit connecté dont proviennent les données, ni ne partage les données avec un tiers dans cette intention, et il n'utilise pas ces données pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production du fabricant ou, le cas échéant, du détenteur de données.

11. L'utilisateur s'abstient d'avoir recours à des moyens coercitifs ou de tirer avantage de lacunes dans l'infrastructure technique du détenteur de données qui est destinée à protéger les données pour obtenir l'accès aux données.

12. Lorsque l'utilisateur n'est pas la personne concernée dont les données à caractère personnel font l'objet de la demande, les données à caractère personnel générées par l'utilisation d'un produit connecté ou d'un service connexe ne sont mises à la disposition de l'utilisateur par le détenteur de données que s'il existe un fondement juridique valable pour le traitement au titre de l'article 6 du règlement (UE) 2016/679 et, le cas échéant, si les conditions énoncées à l'article 9 dudit règlement et à l'article 5, paragraphe 3, de la directive 2002/58/CE sont remplies.

13. Un détenteur de données n'utilise les données facilement accessibles qui sont des données à caractère non personnel que sur la base d'un contrat avec l'utilisateur. Un détenteur de données n'utilise pas ces données pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production de l'utilisateur, ou sur l'utilisation qu'en fait ce dernier, d'une quelconque autre manière susceptible de porter atteinte à la position commerciale dudit utilisateur sur les marchés où celui-ci est actif.

14. Les détenteurs de données ne mettent pas à la disposition de tiers les données à caractère non personnel relatives aux produits à des fins commerciales ou non commerciales autres que l'exécution de leur contrat avec l'utilisateur. Le cas échéant, les détenteurs de données obligent contractuellement les tiers à ne pas partager les données reçues de leur part.

Article 5

Droit de l'utilisateur de partager des données avec des tiers

1. Lorsqu'un utilisateur ou une partie agissant pour le compte d'un utilisateur en fait la demande, le détenteur de données met les données facilement accessibles, ainsi que les métadonnées pertinentes nécessaires à l'interprétation et à l'utilisation de ces données, à la disposition d'un tiers sans retard injustifié, à un niveau de qualité identique à celui dont bénéficie le détenteur de données, de manière aisée, sécurisée, sans frais pour l'utilisateur, dans un format complet, structuré, couramment utilisé et lisible par machine et, lorsque cela est pertinent et techniquement possible, en continu et en temps réel. Les données sont mises à la disposition du tiers par le détenteur de données conformément aux articles 8 et 9.

2. Le paragraphe 1 ne s'applique pas aux données facilement accessibles dans le cadre de l'essai de nouveaux produits connectés, substances ou procédés qui ne sont pas encore mis sur le marché, à moins que leur utilisation par un tiers ne soit contractuellement autorisée.

3. Toute entreprise désignée comme contrôleur d'accès, conformément à l'article 3 du règlement (UE) 2022/1925, 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.

4. Afin de vérifier si une personne physique ou morale peut être considérée comme un utilisateur ou un tiers aux fins du paragraphe 1, l'utilisateur ou le tiers n'est pas tenu de fournir d'autres informations que celles qui sont nécessaires. Les détenteurs de données ne conservent 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.

5. Le tiers s'abstient d'avoir recours à des moyens coercitifs ou de tirer avantage de lacunes dans l'infrastructure technique d'un détenteur de données qui est destinée à protéger les données pour obtenir l'accès aux données.

6. Un détenteur de données n'utilise aucune donnée facilement accessible pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production du tiers, ou sur l'utilisation qu'en fait ce dernier, d'une quelconque autre manière susceptible 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 facilement cette autorisation à tout moment.

7. Lorsque l'utilisateur n'est pas la personne concernée dont les données à caractère personnel font l'objet de la demande, les données à caractère personnel générées par l'utilisation d'un produit connecté ou d'un service connexe, ne sont mises à la disposition du tiers par le détenteur de données que s'il existe un fondement juridique valable pour le traitement au titre de l'article 6 du règlement (UE) 2016/679 et, le cas échéant, si les conditions énoncées à l'article 9 dudit règlement et à l'article 5, paragraphe 3, de la directive 2002/58/CE sont remplies.

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

9. Les secrets d'affaires sont préservés et ne sont divulgués à des tiers que dans la mesure où cette divulgation est strictement nécessaire pour atteindre la finalité convenue entre l'utilisateur et le tiers. Le détenteur de données ou, s'il ne s'agit pas de la même personne, le détenteur de secrets d'affaires, recense les données protégées en tant que secrets d'affaires, y compris dans les métadonnées pertinentes, et convient avec le tiers de toutes les mesures techniques et organisationnelles proportionnées nécessaires afin de préserver la confidentialité des données partagées, telles que des clauses contractuelles types, des accords de confidentialité, des protocoles d'accès stricts, des normes techniques et l'application de codes de conduite.

10. En l'absence d'accord sur les mesures nécessaires visées au paragraphe 9 du présent article, ou si le tiers ne met pas en œuvre les mesures convenues en vertu du paragraphe 9 du présent article ou compromet la confidentialité des secrets d'affaires, le détenteur de données peut bloquer ou, selon le cas, suspendre le partage des données définies comme constituant des secrets d'affaires. La décision du détenteur de données est dûment motivée et communiquée par écrit au tiers, sans retard injustifié. Dans de tels cas, le détenteur de données notifie à l'autorité compétente désignée en vertu de l'article 37 qu'il a retenu ou suspendu le partage de données et indique les mesures qui n'ont pas été convenues ou mises en œuvre et, le cas échéant, les secrets d'affaires dont la confidentialité a été compromise.

11. Dans des circonstances exceptionnelles, lorsque le détenteur de données qui est un détenteur de secret d'affaires peut démontrer qu'il est très probable qu'il subisse un préjudice économique grave du fait de la divulgation de secrets d'affaires, malgré les mesures techniques et organisationnelles prises par le tiers en vertu du paragraphe 9 du présent article, ce détenteur de données peut refuser au cas par cas une demande d'accès aux données spécifiques en question. Cette démonstration est dûment étayée sur la base d'éléments objectifs, en particulier l'opposabilité de la protection des secrets d'affaires dans les pays tiers, la nature et le niveau de confidentialité des données demandées, ainsi que le caractère unique et neuf du produit connecté, et est fournie par écrit au tiers sans retard injustifié. Lorsque le détenteur de données refuse de partager des données en vertu du présent paragraphe, il adresse une notification à l'autorité compétente désignée en vertu de l'article 37.

12. Sans préjudice du droit du tiers de demander réparation à tout moment devant une juridiction d'un État membre, un tiers souhaitant contester la décision du détenteur de données de refuser ou de bloquer ou suspendre le partage de données en vertu des paragraphes 10 et 11 peut:

a) introduire une réclamation auprès de l'autorité compétente conformément à l'article 37, paragraphe 5, point b), qui décide, sans retard injustifié, si et dans quelles conditions le partage des données doit commencer ou reprendre; ou

b) convenir avec le détenteur de données de porter la question devant un organe de règlement des litiges conformément à l'article 10, paragraphe 1.

13. Le droit visé au paragraphe 1 ne porte pas atteinte aux droits des personnes concernées conformément au droit de l'Union et au droit national applicables en matière de protection des données à caractère personnel.

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 du droit de l'Union et du droit national en matière de protection des données à caractère personnel, y compris les droits de la personne concernée dans la mesure où les données à caractère personnel sont concernées. Le tiers efface les données lorsqu'elles ne sont plus nécessaires à la finalité convenue, sauf accord contraire avec l'utilisateur en ce qui concerne les données à caractère non personnel.

2. Le tiers ne peut pas:

a) rendre l'exercice des choix ou des droits de l'utilisateur, au titre de l'article 5 et du présent article, indûment difficile, y compris en proposant des choix à l'utilisateur d'une manière qui n'est pas neutre, ou en contraignant, en trompant ou en manipulant l'utilisateur, ou en réduisant ou en compromettant l'autonomie, la prise de décision ou les choix de l'utilisateur, y compris au moyen d'une interface numérique utilisateur ou d'une partie de celle-ci;

b) nonobstant l'article 22, paragraphe 2, points a) et c), du règlement (UE) 2016/679, utiliser les données qu'il reçoit à des fins de profilage, à moins que cela ne soit nécessaire pour fournir le service demandé par l'utilisateur;

c) mettre les données qu'il reçoit à la disposition d'un autre tiers, à moins que les données ne soient mises à disposition sur le fondement d'un contrat avec l'utilisateur, et à condition que l'autre tiers prenne toutes les mesures nécessaires convenues entre le détenteur de données et le tiers pour préserver la confidentialité des secrets d'affaires;

d) mettre les données qu'il reçoit à la disposition d'une entreprise désignée comme contrôleur d'accès, conformément à l'article 3 du règlement (UE) 2022/1925;

e) utiliser les données qu'il reçoit pour développer un produit concurrençant le produit connecté dont proviennent les données auxquelles il a accès ou de partager les données avec un autre tiers à cette fin; les tiers n'utilisent pas non plus de données à caractère non personnel relatives au produit ou relatives au service connexe mises à leur disposition pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production du détenteur de données ou sur l'utilisation que ce dernier en fait;

f) utiliser les données qu'il reçoit d'une manière qui nuit à la sécurité du produit connecté ou du service connexe;

g) méconnaître les mesures spécifiques convenues avec le détenteur de données ou le détenteur de secrets d'affaires conformément à l'article 5, paragraphe 9, et compromettre la confidentialité des secrets d'affaires;

h) empêcher l'utilisateur qui est un consommateur, y compris sur le fondement 'd'un contrat, 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 consommateurs et entreprises et entre entreprises

1. Les obligations définies dans le présent chapitre ne s'appliquent pas aux données générées par l'utilisation de produits connectés fabriqués ou conçus ou de services connexes fournis par une microentreprise ou une petite entreprise, à condition que cette entreprise n'ait pas une entreprise partenaire ou une entreprise liée au sens de l'article 3 de l'annexe de la recommandation 2003/361/CE qui n'est pas qualifiée de microentreprise ou de petite entreprise et lorsque la microentreprise et petite entreprise ne travaille pas en sous-traitance pour fabriquer ou concevoir un produit connecté ou pour fournir un service connexe.

Il en va de même pour les données générées par l'utilisation de produits connectés fabriqués ou de services connexes fournis par une entreprise qui est qualifiée d'entreprise moyenne au titre de l'article 2 de l'annexe de la recommandation 2003/361/CE depuis moins d'un an et pour les produits connectés pendant une période d'un an après la date à laquelle ils ont été mis sur le marché par une entreprise moyenne.

2. Toute clause contractuelle qui, au détriment de l'utilisateur, exclut l'application des droits de l'utilisateur au titre du présent chapitre, y déroge ou en modifie les effets, n'est pas contraignante pour l'utilisateur.

CHAPITRE III

OBLIGATIONS APPLICABLES AUX DETENTEURS DE DONNEES TENUS DE METTRE DES DONNEES A DISPOSITION EN VERTU DU DROIT DE L'UNION

Article 8

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

1. Lorsque, dans le cadre de relations entre entreprises, un détenteur de données est tenu de mettre des données à la disposition d'un destinataire de données au titre de l'article 5 ou au titre d'autres dispositions applicables du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union, il convient des modalités de cette mise à disposition des données avec un destinataire de données, et ce selon des modalités et conditions équitables, raisonnables et non discriminatoires et de manière transparente, conformément au présent chapitre et au chapitre IV.

2. Une clause contractuelle concernant l'accès aux données et l'utilisation des données, ou la responsabilité et les voies de recours en cas de violation ou d'extinction des obligations relatives aux données, n'est pas contraignante si elle constitue une clause contractuelle abusive au sens de l'article 13 ou si, au détriment de l'utilisateur, 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 en ce qui concerne les modalités de mise à disposition des données entre des catégories comparables de destinataires de données, y compris les entreprises partenaires ou les entreprises liées du destinataire de données. Lorsqu'un destinataire de données considère que les conditions dans lesquelles des données ont été mises à sa disposition sont discriminatoires, le détenteur de données fournit, sans retard injustifié, au destinataire de données, sur demande motivée de celui-ci, des informations attestant l'absence de discrimination.

4. Un détenteur de données ne met pas de données à la disposition d'un destinataire de données, y compris sur une base d'exclusivité, sauf si l'utilisateur le demande au titre 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 clauses contractuelles convenues pour la mise à disposition des données ou des obligations qui leur incombent au titre du présent règlement ou d'autres dispositions applicables du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union.

6. Sauf disposition contraire du droit de l'Union, y compris l'article 4, paragraphe 6, et l'article 5, paragraphe 9, du présent règlement, ou de la législation nationale adoptée conformément au 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.

Article 9

Compensation pour la mise à disposition de données

1. Toute compensation convenue, dans le cadre de relations entre entreprises, entre un détenteur de données et un destinataire de données pour la mise à disposition des données est non discriminatoire et raisonnable et peut inclure une marge.

2. Lorsqu'ils s'accordent sur une compensation, le détenteur de données et le destinataire de données tiennent compte en particulier:

a) des coûts occasionnés par la mise à disposition des données, dont, notamment, les coûts encourus pour le formatage des données, leur diffusion par voie électronique et leur stockage;

b) des investissements dans la collecte et la production de données, le cas échéant, en prenant en compte le fait que d'autres parties ont contribué ou non à l'obtention, à la production ou à la collecte des données en question.

3. La compensation visée au paragraphe 1 peut également dépendre du volume, du format et de la nature des données.

4. Lorsque le destinataire de données est une PME ou un organisme de recherche à but non lucratif et que ce destinataire de données n'a pas d'entreprises partenaires ou d'entreprises liées qui ne sont pas considérées comme des PME, toute compensation convenue n'excède pas les coûts visés au paragraphe 2, point a).

5. La Commission adopte des lignes directrices sur le calcul de la compensation raisonnable, en tenant compte de l'avis du comité européen de l'innovation dans le domaine des données visé à l'article 42.

6. Le présent article ne fait pas obstacle à ce que d'autres dispositions du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union excluent une éventuelle compensation pour la mise à disposition de données ou prévoient une compensation moins élevée.

7. 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 d'évaluer si les exigences des paragraphes 1 à 4 sont respectées.

Article 10

Règlement des litiges

1. Les utilisateurs, les détenteurs de données et les destinataires de données ont accès à un organe de règlement des litiges, certifié conformément au paragraphe 5 du présent article, pour régler les litiges en vertu de l'article 4, paragraphes 3 et 9, et de l'article 5, paragraphe 12, ainsi que les litiges portant sur les modalités et conditions équitables, raisonnables et non discriminatoires applicables à la mise à disposition de données et à la façon de mettre ces données à disposition en toute transparence conformément au présent chapitre et au chapitre IV.

2. Les organes de règlement des litiges informent les parties concernées des frais, ou des mécanismes utilisés pour les déterminer, avant que ces parties ne demandent une décision.

3. Pour les litiges portés devant un organe de règlement des litiges en vertu de l'article 4, paragraphes 3 et 9, et de l'article 5, paragraphe 12, lorsque l'organe de règlement des litiges se prononce sur un litige en faveur de l'utilisateur ou du destinataire de données, le détenteur de données supporte tous les frais facturés par l'organe de règlement des litiges et rembourse à cet utilisateur ou à ce destinataire de données toute autre dépense raisonnable qu'il a supportée en lien avec le règlement du litige. Lorsque l'organe de règlement des litiges se prononce sur un litige en faveur du détenteur de données, l'utilisateur ou le destinataire de données n'est pas tenu de rembourser les frais ou autres dépenses que le détenteur de données a engagés ou dont il est redevable en lien avec le règlement du litige, à moins que l'organe de règlement des litiges ne constate que l'utilisateur ou le destinataire de données a manifestement agi de mauvaise foi.

4. Les clients et les fournisseurs de services de traitement de données ont accès à un organe de règlement des litiges, certifié conformément au paragraphe 5 du présent article, pour régler les litiges relatifs aux violations des droits des clients et aux obligations des fournisseurs de services de traitement de données conformément aux articles 23 à 31.

5. L'État membre dans lequel l'organe de règlement des litiges est établi certifie cet organe à sa demande, lorsqu'il a démontré qu'il remplit toutes les conditions suivantes:

a) il est impartial et indépendant et doit rendre ses décisions conformément à des règles de procédure claires, non discriminatoires et équitables;

b) il dispose de l'expertise nécessaire, en particulier en ce qui concerne les modalités et conditions équitables, raisonnables et non discriminatoires, y compris en matière de compensation, et en ce qui concerne la mise à disposition de données en toute transparence, ce qui permet à l'organisme de déterminer efficacement ces modalités et conditions;

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

d) il est en mesure d'adopter ses décisions de manière rapide, efficace et économiquement avantageuse, dans au moins une langue officielle de l'Union.

6. Les États membres notifient à la Commission la liste des organes de règlement des litiges certifiés conformément au paragraphe 5. La Commission publie une liste de ces organes sur un site internet spécifique et la tient à jour.

7. Un organe de règlement des litiges refuse de traiter une demande de règlement d'un litige qui a déjà été porté devant un autre organe de règlement des litiges ou devant une juridiction d'un État membre.

8. Un organe de règlement des litiges donne aux parties la possibilité, dans un délai raisonnable, d'exprimer leur point de vue sur les questions qu'elles ont soumises à cet organe. Dans ce contexte, chaque partie à un litige se voit communiquer les observations de l'autre partie au litige et toute déclaration faite par des experts. Les parties ont la possibilité de formuler des observations sur ces observations et déclarations.

9. Un organe de règlement des litiges prend sa décision sur toute question qui lui est soumise dans un délai de 90 jours à compter de la réception d'une demande présentée en vertu des paragraphes 1 et 4. Cette décision est formulée par écrit ou sur un support durable et est étayée par un exposé des motifs.

10. Les organes de règlement des litiges rédigent et rendent publics des rapports annuels d'activité. Ces rapports annuels incluent en particulier les informations générales suivantes:

a) une agrégation des résultats des litiges;

b) le laps de temps moyen nécessaire à la résolution des litiges;

c) les causes les plus courantes de litiges.

11. Afin de faciliter l'échange d'informations et de bonnes pratiques, un organe de règlement des litiges peut décider d'inclure des recommandations dans le rapport visé au paragraphe 10 sur la manière dont les problèmes peuvent être évités ou résolus.

12. La décision d'un organe de règlement des litiges n'est contraignante pour les parties que si celles-ci ont expressément consenti à son caractère contraignant avant le début de la procédure de règlement du litige.

13. 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 relatives à l'utilisation ou à la divulgation non autorisées de données

1. Un détenteur de données peut appliquer des mesures techniques appropriées de protection, y compris des contrats intelligents et le chiffrement, afin d'empêcher l'accès non autorisé aux données, y compris les métadonnées, et de garantir le respect des articles 4, 5, 6, 8 et 9, ainsi que des clauses contractuelles convenues pour la mise à disposition des données. Ces mesures techniques de protection ne doivent pas donner lieu à une discrimination entre les destinataires de données ni porter atteinte au droit de l'utilisateur d'obtenir une copie des données, de les récupérer, de les utiliser ou d'y accéder, de fournir des données à des tiers conformément à l'article 5 ou aux droits des tiers au titre du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union. Les utilisateurs, les tiers et les destinataires de données ne modifient pas ni ne suppriment de telles mesures techniques de protection, sauf accord du détenteur de données.

2. Dans les circonstances visées au paragraphe 3, le tiers ou le destinataire de données donne suite, sans retard injustifié, aux demandes du détenteur de données et, le cas échéant et s'il ne s'agit pas de la même personne, du détenteur de secrets d'affaires ou de l'utilisateur:

a) d'effacer les données mises à disposition par le détenteur de données et les éventuelles copies de celles-ci;

b) de mettre fin à la production, à l'offre ou à la mise sur le marché ou à l'utilisation de biens, de données dérivées ou de services 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 de détruire tout bien non conforme, lorsqu'il existe un risque grave que l'utilisation illicite de ces données cause un préjudice important au détenteur de données, au détenteur de secrets d'affaires ou à l'utilisateur ou lorsqu'une telle mesure ne serait pas disproportionnée au regard des intérêts du détenteur de données, du détenteur de secrets d'affaires ou de l'utilisateur;

c) d'informer l'utilisateur de l'utilisation ou de la divulgation non autorisées des données et des mesures prises pour mettre fin à l'utilisation ou à la divulgation non autorisée des données;

d) d'indemniser la partie lésée par l'utilisation abusive ou la divulgation de ces données auxquelles il a été accédé illégalement ou qui ont été utilisées illégalement.

3. Le paragraphe 2 s'applique lorsqu'un tiers ou un destinataire de données:

a) aux fins de l'obtention de données, a fourni de fausses informations à un détenteur de données, a eu recours à des moyens trompeurs ou coercitifs ou a tiré avantage de lacunes dans l'infrastructure technique du détenteur de données destinée à protéger les données;

b) a utilisé les données mises à disposition à des fins non autorisées, y compris le développement d'un produit connecté concurrent au sens de l'article 6, paragraphe 2, point e);

c) a divulgué illégalement des données à une autre partie;

d) n'a pas maintenu les mesures techniques et organisationnelles convenues en vertu de l'article 5, paragraphe 9; ou

e) a modifié ou supprimé des mesures techniques de protection appliquées par le détenteur de données en vertu du paragraphe 1 du présent article sans l'accord du détenteur de données.

4. Le paragraphe 2 s'applique également lorsqu'un utilisateur ou un destinataire de données modifie ou retire des mesures techniques de protection appliquées par le détenteur de données ou ne maintient pas des mesures techniques et organisationnelles prises par l'utilisateur en accord avec le détenteur de données ou, s'il ne s'agit pas de la même personne, le détenteur de secrets d'affaires, afin de préserver les secrets d'affaires, ainsi qu'à l'égard de toute autre partie qui reçoit les données de l'utilisateur à la suite d'une infraction au présent règlement.

5. Lorsque le destinataire de données enfreint l'article 6, paragraphe 2, point a) ou b), les utilisateurs disposent des mêmes droits que les détenteurs de données au titre du paragraphe 2 du présent article.

Article 12

Champ d'application des obligations applicables aux détenteurs de données tenus au titre du droit de l'Union de mettre des données à disposition

1. Le présent chapitre s'applique lorsque, dans le cadre de relations entre entreprises, un détenteur de données est tenu, au titre de l'article 5 ou des dispositions applicables du droit de l'Union ou de la législation nationale adoptée conformément au 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.

CHAPITRE IV

CLAUSES CONTRACTUELLES ABUSIVES RELATIVES A L'ACCES AUX DONNEES ET A L'UTILISATION DES DONNEES ENTRE ENTREPRISES

Article 13

Clauses contractuelles abusives imposées unilatéralement à une autre entreprise

1. Une clause contractuelle concernant l'accès aux données et l'utilisation des données ou la responsabilité et les voies de recours en cas de violation ou d'extinction d'obligations liées aux données qu'une entreprise a imposée unilatéralement à une autre entreprise ne lie pas cette dernière entreprise si elle est abusive.

2. Une clause contractuelle qui reflète des dispositions impératives du droit de l'Union ou des dispositions du droit de l'Union qui s'appliqueraient si les clauses contractuelles ne réglaient pas la question n'est pas considérée comme étant abusive.

3. Une clause contractuelle est abusive si elle est d'une nature telle que son utilisation s'écarte manifestement des bonnes pratiques commerciales en matière d'accès aux données et d'utilisation des données, contrairement à la bonne foi et à un usage loyal.

4. En particulier, aux fins du paragraphe 3, 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 a unilatéralement imposé la clause 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 contractuelle.

5. Aux fins du paragraphe 3, une clause contractuelle est présumée être 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, ou d'étendre la responsabilité de l'entreprise à laquelle la clause a été imposée unilatéralement;

b) de permettre à la partie qui a imposé unilatéralement la clause d'avoir accès 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, en particulier lorsque ces données contiennent des données commercialement sensibles ou sont protégées par des secrets d'affaires ou des droits de propriété intellectuelle;

c) d'empêcher la partie à laquelle la clause a été imposée unilatéralement 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 ou à enregistrer ces données, à y accéder ou à les contrôler ou à en exploiter la valeur de manière adéquate;

d) d'empêcher la partie à laquelle la clause a été imposée unilatéralement de résilier l'accord dans un délai raisonnable;

e) d'empêcher la partie à laquelle la clause a été imposée unilatéralement 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;

f) de permettre à la partie qui a imposé unilatéralement la clause de résilier le contrat dans un délai excessivement court, compte tenu des possibilités dont l'autre partie contractante dispose raisonnablement pour 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;

g) de permettre à la partie qui a imposé unilatéralement la clause de modifier substantiellement le prix indiqué dans le contrat ou toute autre condition de fond liée à la nature, au format, à la qualité ou à la quantité des données à partager, lorsqu'aucun motif valable ou aucun droit pour l'autre partie de résilier le contrat dans le cas d'une telle modification n'est stipulé dans le contrat.

Le premier alinéa, point g), n'affecte pas les clauses par lesquelles la partie qui a imposé unilatéralement la clause en question se réserve le droit de modifier unilatéralement les clauses d'un contrat à durée indéterminée, pour autant que le contrat ait prévu une raison valable pour effectuer de telles modifications unilatéralement, que la partie qui a imposé unilatéralement la clause soit tenue d'informer l'autre partie contractante moyennant un préavis raisonnable de son intention d'effectuer une telle modification, et que l'autre partie contractante soit libre de résilier le contrat sans frais dans le cas d'une telle modification.

6. Une clause contractuelle est considérée comme étant 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 la clause contractuelle de prouver que cette clause n'a pas été imposée unilatéralement. La partie contractante qui a fourni la clause contractuelle faisant l'objet d'une contestation ne peut pas invoquer le caractère abusif de la clause contractuelle.

7. Lorsque la clause abusive est dissociable des autres clauses du contrat, ces dernières sont contraignantes.

8. Le présent article ne s'applique pas aux clauses contractuelles définissant l'objet principal du contrat ni à l'adéquation entre le prix et les données fournies en contrepartie.

9. Les parties à un contrat relevant du paragraphe 1 n'excluent pas l'application du présent article, n'y dérogent pas ou n'en modifient pas les effets.

CHAPITRE V

MISE A LA DISPOSITION D'ORGANISMES DU SECTEUR PUBLIC, DE LA COMMISSION, DE LA BANQUE CENTRALE EUROPEENNE ET D'ORGANES DE L'UNION DE DONNEES SUR LE FONDEMENT D'UN BESOIN EXCEPTIONNEL

Article 14

Obligation de mettre des données à disposition sur le fondement d'un besoin exceptionnel

Lorsqu'un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union démontre l'existence d'un besoin exceptionnel, tel qu'il est décrit à l'article 15, d'utiliser certaines données, y compris les métadonnées pertinentes nécessaires à l'interprétation et à l'utilisation de ces données, pour exercer ses fonctions statutaires à des fins d'intérêt public, les détenteurs de données qui sont des personnes morales, autres que des organismes du secteur public, qui détiennent ces données les mettent à disposition sur demande dûment motivée.

Article 15

Besoin exceptionnel d'utiliser des données

1. Un besoin exceptionnel d'utiliser certaines données au sens du présent chapitre a une durée et une portée limitées et est réputé exister uniquement dans les cas suivants:

a) lorsque les données demandées sont nécessaires pour réagir à une situation d'urgence et que l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union n'est pas en mesure d'obtenir ces données par d'autres moyens en temps utile et de manière efficace et dans des conditions équivalentes;

b) dans des circonstances non couvertes par le point a) et uniquement en ce qui concerne les données à caractère non personnel, lorsque:

   i) un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union agit sur la base du droit de l'Union ou du droit national et a déterminé des données spécifiques, dont l'absence l'empêche d'exécuter une mission spécifique d'intérêt public, qui a été explicitement prévue par la loi, telle que la production de statistiques officielles, l'atténuation d'une situation d'urgence ou le rétablissement à la suite d'une situation d'urgence; et

   ii) l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union a épuisé tous les autres moyens à sa disposition pour obtenir ces données, y compris l'achat de données à caractère non personnel sur le marché aux prix du marché ou le recours aux obligations existantes de mise à disposition des données ou l'adoption de nouvelles mesures législatives pouvant garantir la disponibilité des données en temps utile.

2. Le paragraphe 1, point b), ne s'applique pas aux microentreprises ni aux petites entreprises.

3. L'obligation de démontrer que l'organisme du secteur public n'a pas été en mesure d'obtenir des données à caractère non personnel en les achetant sur le marché ne s'applique pas lorsque la mission spécifique exécutée dans l'intérêt public consiste en la production de statistiques officielles et que l'achat de ces données n'est pas autorisé par le droit national.

Article 16

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

1. Le présent chapitre n'affecte pas les 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'accès aux informations ou de la démonstration ou de la vérification du respect des obligations légales.

2. Le présent chapitre ne s'applique pas aux organismes du secteur public, à la Commission, à la Banque centrale européenne ou aux organes de l'Union lorsqu'ils exercent des activités de prévention et de détection des infractions pénales ou administratives, d'enquêtes ou de poursuites en la matière, ou d'exécution de sanctions pénales, ni à l'administration douanière ou fiscale. Le présent chapitre n'affecte pas les dispositions applicables du droit de l'Union et du droit national relatives à la prévention et à la détection des infractions pénales ou administratives, aux enquêtes et aux poursuites en la matière, à l'exécution de sanctions pénales ou administratives, ou relatives à l'administration douanière ou fiscale.

Article 17

Demandes de mise à disposition de données

1. Lorsqu'un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union demande des données en vertu de l'article 14, il ou elle:

a) précise les données qui sont demandées, y compris les métadonnées nécessaires à l'interprétation et à l'utilisation de ces données;

b) démontre que les conditions nécessaires à l'existence d'un besoin exceptionnel conformément à l'article 15 pour lequel les données sont demandées sont remplies;

c) explique la finalité de la demande, l'utilisation qu'il est prévu de faire des données demandées, y compris, le cas échéant, par un tiers conformément au paragraphe 4 du présent article, la durée de cette utilisation et, le cas échéant, la manière dont le traitement de données à caractère personnel doit répondre au besoin exceptionnel;

d) précise, si possible, la date à laquelle les données sont censées être effacées par toutes les parties qui y ont accès;

e) justifie le choix du détenteur de données auquel la demande est adressée;

f) précise avec qui, parmi les autres organismes du secteur public, la Commission, la Banque centrale européenne ou les organes de l'Union ou les tiers, il est prévu de partager les données demandées;

g) lorsque des données à caractère personnel sont demandées, précise les éventuelles mesures techniques et organisationnelles proportionnées et nécessaires pour mettre en œuvre les principes de protection des données et les garanties nécessaires, telles que la pseudonymisation, et si l'anonymisation peut être appliquée par le détenteur de données avant de mettre les données à disposition;

h) indique la disposition juridique confiant à l'organisme du secteur public demandeur, à la Commission, à la Banque centrale européenne ou à l'organe de l'Union la mission spécifique exécutée dans l'intérêt public qui justifie la demande de données;

i) précise le délai dans lequel les données doivent être mises à disposition et le délai visé à l'article 18, paragraphe 2, dans lequel le détenteur de données peut rejeter la demande ou demander sa modification;

j) met tout en œuvre pour éviter qu'en donnant suite à la demande de données, les détenteurs de données n'engagent leur responsabilité pour infraction au droit de l'Union ou au droit national.

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

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

b) est spécifique quant au type de données demandées et correspond aux données sur lesquelles le détenteur de données exerce un contrôle au moment de la demande;

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

d) respecte les objectifs légitimes du détenteur de données, en s'engageant à garantir la protection des secrets d'affaires conformément à l'article 19, paragraphe 3, ainsi qu'en tenant compte des coûts et des efforts nécessaires pour mettre les données à disposition;

e) concerne des données à caractère non personnel et, uniquement s'il est démontré que cela est insuffisant pour répondre au besoin exceptionnel d'utiliser des données, conformément à l'article 15, paragraphe 1, point a), des données à caractère personnel sous une forme pseudonymisée et établit les mesures techniques et organisationnelles qui doivent être prises pour protéger les données;

f) informe le détenteur de données des sanctions qui doivent être imposées au titre de l'article 40 par l'autorité compétente désignée en vertu de l'article 37 s'il n'est pas donné suite à la demande;

g) lorsqu'elle est présentée par un organisme du secteur public, est transmise au coordinateur de données visé à l'article 37 de l'État membre dans lequel est établi l'organisme du secteur public demandeur, qui publie la demande en ligne sans retard injustifié, à moins que le coordinateur de données ne considère qu'une telle publication présenterait un risque pour la sécurité publique;

h) lorsqu'elle est présentée par la Commission, la Banque centrale européenne ou un organe de l'Union, est mise à disposition en ligne sans retard injustifié;

i) lorsque des données à caractère personnel sont demandées, est notifiée sans retard injustifié à l'autorité de contrôle chargée de surveiller l'application du règlement (UE) 2016/679 dans l'État membre dans lequel l'organisme du secteur public est établi.

La Banque centrale européenne et les organes de l'Union informent la Commission de leurs demandes.

3. Un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union ne met pas les données obtenues au titre du présent chapitre à disposition en vue de leur réutilisation au sens de l'article 2, point 2), du règlement (UE) 2022/868 ou de l'article 2, point 11), de la directive (UE) 2019/1024. Le règlement (UE) 2022/868 et la directive (UE) 2019/1024 ne s'appliquent pas aux données détenues par des organismes du secteur public obtenues au titre du présent chapitre.

4. Le paragraphe 3 du présent article n'empêche pas un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union d'échanger des données obtenues en vertu du présent chapitre avec un autre organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union en vue de l'accomplissement des tâches prévues à l'article 15, comme indiqué dans la demande conformément au paragraphe 1, point f), du présent article, ni de mettre les données à la disposition d'un tiers lorsqu'il ou elle a délégué, 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 conformément à l'article 19, en particulier les garanties visant à préserver la confidentialité des secrets d'affaires, s'appliquent également à ces tiers. Lorsqu'un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union transmet ou met des données à disposition en vertu du présent paragraphe, il ou elle adresse une notification, sans retard injustifié, au détenteur de données auprès duquel les données ont été obtenues.

5. Lorsque le détenteur de données estime que ses droits au titre du présent chapitre ont été enfreints par la transmission ou la mise à disposition de données, il peut introduire une réclamation auprès de l'autorité compétente désignée en vertu de l'article 37 de l'État membre dans lequel le détenteur de données est établi.

6. La Commission élabore un modèle de demande conformément au présent article.

Article 18

Suivi des demandes de données

1. Le détenteur de données qui reçoit une demande de mise à disposition de données au titre du présent chapitre met ces données à la disposition de l'organisme du secteur public demandeur, de la Commission, de la Banque centrale européenne ou d'un organe de l'Union sans retard injustifié, en tenant compte des mesures techniques, organisationnelles et juridiques nécessaires.

2. Sans préjudice des besoins spécifiques concernant la disponibilité des données définis dans le droit de l'Union ou le droit national, un détenteur de données peut rejeter la demande de mise à disposition de données ou demander sa modification dans le cadre du présent chapitre, sans retard injustifié et, en tout état de cause, dans un délai maximal de cinq jours ouvrables suivant la réception d'une demande de données nécessaires pour réagir à une situation d'urgence, sans retard injustifié et, en tout état de cause, dans un délai maximal de trente jours ouvrables suivant la réception d'une telle demande dans les autres cas de besoin exceptionnel, pour l'un quelconque des motifs suivants:

a) le détenteur de données n'exerce pas de contrôle sur les données demandées;

b) une demande similaire a été présentée précédemment pour la même finalité par un autre organisme du secteur public ou la Commission, la Banque centrale européenne ou un organe de l'Union, et le détenteur de données ne s'est pas vu notifier l'effacement des données conformément à l'article 19, paragraphe 1, point c);

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

3. Si le détenteur de données décide de rejeter la demande ou de demander sa modification conformément au paragraphe 2, point b), il indique l'identité de l'organisme du secteur public ou de la Commission, de la Banque centrale européenne ou de l'organe de l'Union qui a présenté précédemment une demande pour la même finalité.

4. Lorsque les données demandées comprennent des données à caractère personnel, le détenteur de données anonymise correctement les données, à moins que le suivi de la demande de mettre des données à la disposition d'un organisme du secteur public, de la Commission, de la Banque centrale européenne ou d'un organe de l'Union n'exige la divulgation de données à caractère personnel. En pareils cas, le détenteur de données pseudonymise les données.

5. Lorsque l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union souhaite contester le refus d'un détenteur de données de fournir les données demandées, ou lorsque le détenteur de données souhaite contester la demande et que la question ne peut pas être résolue par une modification appropriée de la demande, la question est portée devant l'autorité compétente désignée en vertu de l'article 37 de l'État membre dans lequel le détenteur de données est établi.

Article 19

Obligations des organismes du secteur public, de la Commission, de la Banque centrale européenne et des organes de l'Union

1. Un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union qui reçoit 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) a mis en œuvre des mesures techniques et organisationnelles qui préservent la confidentialité et l'intégrité des données demandées et la sécurité des transferts de données, en particulier en ce qui concerne les données à caractère personnel, et garantissent les droits et libertés des personnes concernées;

c) efface les données dès qu'elles ne sont plus nécessaires à la finalité indiquée et informe, sans retard injustifié, le détenteur de données ainsi que les personnes ou organisations qui ont reçu les données conformément à l'article 21, paragraphe 1, que les données ont été effacées, à moins que l'archivage des données ne soit requis conformément au droit de l'Union ou au droit national en matière d'accès du public aux documents dans le cadre des obligations de transparence.

2. Un organisme du secteur public, la Commission, la Banque centrale européenne, un organe de l'Union ou un tiers qui reçoit des données en vertu du présent chapitre ne peut pas:

a) utiliser les données ou les informations sur la situation économique, les actifs et les méthodes de production ou d'exploitation du détenteur de données pour développer ou améliorer un produit connecté ou un service connexe concurrençant le produit connecté ou le service connexe du détenteur de données;

b) partager les données avec un autre tiers pour l'une quelconque des finalités visées au point a).

3. La divulgation de secrets d'affaires à un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union n'est exigée que dans la mesure où elle est strictement nécessaire pour atteindre la finalité d'une demande présentée au titre de l'article 15. Dans ce cas, le détenteur de données ou, s'il ne s'agit pas de la même personne, le détenteur de secrets d'affaires détermine les données qui sont protégées en tant que secrets d'affaires, y compris dans les métadonnées pertinentes. L'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union prend, avant la divulgation de secrets d'affaires, toutes les mesures techniques et organisationnelles nécessaires et appropriées pour préserver la confidentialité des secrets d'affaires, y compris, le cas échéant, l'utilisation de clauses contractuelles types et de normes techniques et l'application de codes de conduite.

4. Un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union est responsable de la sécurité des données qu'il ou elle reçoit.

Article 20

Compensation en cas de besoin exceptionnel

1. Les détenteurs de données autres que les microentreprises et les petites entreprises mettent gratuitement à disposition les données nécessaires pour réagir à une situation d'urgence conformément à l'article 15, paragraphe 1, point a). L'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union qui a reçu des données accorde une reconnaissance publique au détenteur de données si celui-ci lui en fait la demande.

2. Le détenteur de données dispose d'un droit à une juste compensation pour la mise à disposition de données à la suite d'une demande présentée au titre de l'article 15, paragraphe 1, point b). Une telle compensation couvre les coûts techniques et organisationnels encourus pour donner suite à la demande, y compris, le cas échéant, les coûts d'anonymisation, de pseudonymisation, d'agrégation et d'adaptation technique, et une marge raisonnable. À la demande de l'organisme du secteur public, de la Commission, de la Banque centrale européenne ou de l'organe de l'Union, le détenteur de données fournit des informations sur la base du calcul des coûts et de la marge raisonnable.

3. Le paragraphe 2 s'applique également lorsqu'une microentreprise ou une petite entreprise demande une compensation pour la mise à disposition de données.

4. Les détenteurs de données ne sont pas habilités à recevoir une compensation pour la mise à disposition de données à la suite d'une demande présentée au titre de l'article 15, paragraphe 1, point b), lorsque la mission spécifique effectuée dans l'intérêt public consiste en la production de statistiques officielles et que l'achat de données n'est pas autorisé par le droit national. Les États membres adressent une notification à la Commission lorsque le droit national n'autorise pas l'achat de données en vue de la production de statistiques officielles.

5. Lorsque l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union conteste le niveau de compensation demandé par le détenteur de données, il ou elle peut introduire une réclamation auprès de l'autorité compétente désignée en vertu de l'article 37 de l'État membre dans lequel le détenteur de données est établi.

Article 21

Partage de données obtenues dans le cadre d'un besoin exceptionnel avec des organismes de recherche ou des organismes statistiques

1. Un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union a le droit de partager les données reçues au titre du présent chapitre:

a) 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

b) avec des instituts nationaux de statistique et Eurostat en vue de la production de 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 national. Sont exclus les organismes sur lesquels des entreprises commerciales ont une influence significative, ce qui est susceptible de conduire à un accès préférentiel aux résultats des recherches.

3. Les particuliers ou les organismes qui reçoivent les données en vertu du paragraphe 1 du présent article se conforment aux mêmes obligations que celles qui sont applicables aux organismes du secteur public, à la Commission, à la Banque centrale européenne ou aux organes de l'Union au titre de l'article 17, paragraphe 3, et de l'article 19.

4. Nonobstant l'article 19, paragraphe 1, point c), les personnes ou organismes qui reçoivent les données en vertu du paragraphe 1 du présent article peuvent conserver les données reçues pour la finalité pour laquelle elles ont été demandées pendant une période maximale de six mois après leur effacement par les organismes du secteur public, la Commission, la Banque centrale européenne et les organes de l'Union.

5. Lorsqu'un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union a l'intention de transmettre ou de mettre à disposition des données au titre du paragraphe 1 du présent article, il ou elle adresse une notification sans retard injustifié au détenteur de données dont émanent les données reçues, en précisant l'identité et les coordonnées de l'organisme ou du particulier destinataire des données, la finalité de la transmission ou de la mise à disposition des données, la période pendant laquelle les données doivent être utilisées et les mesures de protection techniques et organisationnelles prises, y compris lorsque des données à caractère personnel ou des secrets d'affaires sont concernés. Lorsque le détenteur de données conteste la transmission ou la mise à disposition de données, il peut introduire une réclamation auprès de l'autorité compétente désignée en vertu de l'article 37 de l'État membre dans lequel le détenteur de données est établi.

Article 22

Assistance mutuelle et coopération transfrontière

1. Les organismes du secteur public, la Commission, la Banque centrale européenne et les organes 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 désignée en vertu de l'article 37 dans ledit État membre. Cette exigence s'applique également aux demandes adressées par la Commission, la Banque centrale européenne et les organes de l'Union. La demande est examinée par l'autorité compétente de l'État membre dans lequel le détenteur de données est établi.

4. Après avoir examiné la demande à la lumière des exigences prévues à l'article 17, l'autorité compétente concernée prend, sans retard injustifié, l'une des mesures suivantes:

a) transmettre la demande au détenteur de données et, le cas échéant, informer l'organisme du secteur public demandeur, la Commission, la Banque centrale européenne ou l'organe de l'Union 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 pesant sur le détenteur de données qui donne suite à la demande;

b) rejeter la demande pour des motifs dûment étayés, conformément au présent chapitre.

L'organisme du secteur public demandeur, la Commission, la Banque centrale européenne et l'organe de l'Union tiennent compte de l'avis de l'autorité compétente concernée et des motifs avancés par l'autorité compétente concernée en vertu du premier alinéa avant de prendre une quelconque mesure, comme soumettre à nouveau la demande, le cas échéant.

CHAPITRE VI

CHANGEMENT DE SERVICES DE TRAITEMENT DE DONNEES

Article 23

Suppression des obstacles à un changement de fournisseur effectif

Les fournisseurs de services de traitement de données prennent les mesures prévues aux articles 25, 26, 27, 29 et 30 afin de permettre aux clients de changer de fournisseur pour passer à un service de traitement de données, couvrant le même type de service, qui est fourni par un fournisseur de services de traitement de données différent, ou passer à une infrastructure TIC sur site, ou, le cas échéant, recourir simultanément à plusieurs fournisseurs de services de traitement de données. En particulier, les fournisseurs de services de traitement de données n'imposent pas d'obstacles et suppriment les obstacles précommerciaux, commerciaux, techniques, contractuels et organisationnels, qui freinent les clients dans les démarches suivantes:

a) la résiliation, après le préavis maximal et l'achèvement avec succès du processus de changement de fournisseur, conformément à l'article 25, du contrat portant sur le service de traitement de données;

b) la conclusion de nouveaux contrats avec un fournisseur de services de traitement de données différent couvrant le même type de service;

c) le portage des données exportables et des actifs numériques du client vers un fournisseur de services de traitement de données différent ou vers une infrastructure TIC sur site, y compris après avoir bénéficié d'une offre gratuite;

d) conformément à l'article 24, la réalisation de l'équivalence fonctionnelle lors de l'utilisation du nouveau service de traitement de données dans l'environnement TIC d'un fournisseur de services de traitement de données différent couvrant le même type de service;

e) le découplage, lorsqu'il est techniquement possible, des services de traitement de données visés à l'article 30, paragraphe 1, des autres services de traitement de données fournis par le fournisseur de services de traitement de données.

Article 24

Champ d'application des obligations techniques

Les responsabilités des fournisseurs de services de traitement de données définies aux articles 23, 25, 29, 30 et 34 ne s'appliquent qu'aux services, contrats ou pratiques commerciales du fournisseur d'origine de services de traitement de données.

Article 25

Clauses contractuelles concernant le changement de fournisseur

1. Les droits du client et les obligations du fournisseur de services de traitement de données dans le cadre d'un changement de fournisseur entre des fournisseurs de ces services ou, le cas échéant, le passage à une infrastructure TIC sur site sont clairement énoncés dans un contrat écrit. Le fournisseur de services de traitement de données met le contrat à la disposition du client avant la signature du contrat d'une manière qui permet à ce dernier de le stocker et de le reproduire.

2. Sans préjudice de la directive (UE) 2019/770, le contrat visé au paragraphe 1 du présent article comporte au moins les éléments suivants:

a) des clauses permettant au client, sur demande, de passer à un service de traitement de données proposé par un fournisseur de services de traitement de données différent ou de porter toutes les données exportables et tous les actifs numériques vers une infrastructure TIC sur site, sans retard injustifié et, en tout état de cause, pas après la période transitoire maximale obligatoire de trente jours calendaires prenant effet au terme du délai de préavis maximal visé au point d), période pendant laquelle le contrat de fourniture de service reste applicable et durant laquelle le fournisseur de services de traitement de données:

   i) fournit une assistance raisonnable au client et aux tiers autorisés par le client dans le cadre du processus de changement de fournisseur;

ii) agit avec la diligence requise pour maintenir la continuité des activités et poursuivre la fourniture des fonctions ou services au titre du contrat;

iii) fournit des informations claires sur les risques connus, qui relèvent du fournisseur d'origine de services de traitement de données, pour la continuité de la fourniture des fonctions ou services;

iv) veille à ce qu'un niveau élevé de sécurité soit maintenu tout au long du processus de changement de fournisseur, en particulier en ce qui concerne la sécurité des données pendant leur transfert et le maintien de la sécurité des données pendant la période de récupération indiquée au point g), conformément au droit de l'Union ou au droit national applicables;

b) une obligation pour le fournisseur de services de traitement de données de concourir à la stratégie de sortie du client concernant les services couverts par le contrat, y compris en communiquant toutes les informations pertinentes;

c) une clause précisant que le contrat est considéré comme étant résilié et que la résiliation est notifiée au client dans l'un des cas suivants:

i) le cas échéant, lorsque le processus de changement de fournisseur est achevé avec succès;

ii) au terme du délai de préavis maximal visé au point d), lorsque le client ne souhaite pas changer de fournisseur mais souhaite effacer ses données exportables et actifs numériques lors de la résiliation du service;

d) un délai de préavis maximal pour le lancement du processus de changement de fournisseur, qui ne dépasse pas deux mois;

e) une spécification exhaustive de toutes les catégories de données et d'actifs numériques qui peuvent être portées pendant le processus de changement de fournisseur, y compris, au minimum, toutes les données exportables;

f) une spécification exhaustive des catégories de données spécifiques au fonctionnement interne du service de traitement de données du fournisseur qui doivent être exclues des données exportables au titre du point e) du présent paragraphe lorsqu'il existe un risque de violation des secrets d'affaires du fournisseur, à condition que ces exclusions n'entravent ni ne retardent le processus de changement de fournisseur prévu à l'article 23;

g) une période minimale d'au moins trente jours calendaires pour la récupération des données, débutant après la fin de la période transitoire convenue entre le client et le fournisseur de services de traitement de données, conformément au point a) du présent paragraphe et au paragraphe 4;

h) une clause garantissant l'effacement intégral de toutes les données exportables et de tous les actifs numériques générés directement par le client, ou se rapportant directement au client, après l'expiration de la période de récupération visée au point g) ou après l'expiration d'une autre période convenue à une date postérieure à la date d'expiration de la période de récupération visée au point g), à condition que le processus de changement de fournisseur soit achevé avec succès;

i) les frais de changement de fournisseur pouvant être facturés par les fournisseurs de services de traitement de données conformément à l'article 29.

3. Le contrat visé au paragraphe 1 comprend notamment des clauses prévoyant que le client peut notifier au fournisseur de services de traitement de données sa décision de prendre une ou plusieurs des mesures suivantes à la fin du délai de préavis maximal visé au paragraphe 2, point d):

a) passer à un fournisseur de services de traitement de données différent, auquel cas le client fournit les renseignements nécessaires concernant ce fournisseur;

b) passer à une infrastructure TIC sur site;

c) effacer ses données exportables et ses actifs numériques.

4. Lorsqu'il est techniquement impossible de respecter la période transitoire maximale obligatoire prévue au paragraphe 2, point a), le fournisseur de services de traitement de données en informe le client dans un délai de quatorze jours ouvrables à compter de la présentation de la demande de changement de fournisseur, motive dûment l'impossibilité technique et indique une autre période transitoire, qui ne peut excéder sept mois. Conformément au paragraphe 1, la continuité du service est assurée tout au long de l'autre période transitoire.

5. Sans préjudice du paragraphe 4, le contrat visé au paragraphe 1 contient des clauses accordant au client le droit de prolonger la période transitoire une fois pour une durée que le client juge plus appropriée à ses propres fins.

Article 26

Obligation d'information incombant aux fournisseurs de services de traitement de données

Le fournisseur de services de traitement de données fournit au client:

a) des informations sur les procédures disponibles pour le changement de fournisseur et le portage vers le service de traitement de données, y compris des informations sur les méthodes et formats de changement de fournisseur et de portage disponibles, ainsi que sur les restrictions et les limitations techniques connues du fournisseur de services de traitement de données;

b) une référence à un registre en ligne à jour et hébergé par le fournisseur de services de traitement de données, avec des informations détaillées sur toutes les structures de données et tous les formats de données ainsi que les normes pertinentes et les spécifications d'interopérabilité ouvertes, dans lequel les données exportables visées à l'article 25, paragraphe 2, point e), sont disponibles.

Article 27

Obligation de bonne foi

Toutes les parties impliquées, y compris les fournisseurs de destination de services de traitement de données, coopèrent de bonne foi pour rendre le processus de changement de fournisseur effectif, permettre le transfert en temps utile des données et maintenir la continuité du service de traitement de données.

Article 28

Obligations contractuelles en matière de transparence concernant l'accès et le transfert internationaux

1. Les fournisseurs de services de traitement de données mettent à disposition et tiennent à jour sur leur site internet les informations suivantes:

a) les juridictions dont dépend l'infrastructure TIC déployée pour le traitement des données de leurs différents services;

b) une description générale des mesures techniques, organisationnelles et contractuelles adoptées par le fournisseur de services de traitement de données afin d'empêcher l'accès international des autorités publiques aux données à caractère non personnel détenues dans l'Union ou le transfert international de ces données lorsque cet accès ou ce transfert risque d'être en conflit avec le droit de l'Union ou le droit de l'État membre concerné.

2. Les sites internet visés au paragraphe 1 sont énumérés dans les contrats concernant tous les services de traitement de données proposés par les fournisseurs de services de traitement de données.

Article 29

Suppression progressive des frais de changement de fournisseur

1. À compter du 12 janvier 2027, les fournisseurs de services de traitement de données ne peuvent imposer aucun frais de changement de fournisseur au client pour le processus de changement de fournisseur.

2. À compter du 11 janvier 2024 et jusqu'au 12 janvier 2027, les fournisseurs de services de traitement de données peuvent imposer des frais de changement de fournisseur réduits au client, pour le processus de changement de fournisseur.

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

4. Avant de conclure un contrat avec un client, les fournisseurs de services de traitement de données fournissent au client potentiel des informations claires sur les frais de service standard et les pénalités liées à la résiliation anticipée qui pourraient lui être facturés, ainsi que sur les frais de changement de fournisseur réduits qui pourraient lui être facturés pendant le délai visé au paragraphe 2.

5. Le cas échéant, les fournisseurs de services de traitement de données communiquent à un client des informations sur les services de traitement de données pour lesquels un changement de fournisseur est très complexe ou coûteux ou pour lesquels il est impossible de changer de fournisseur sans qu'il y ait une interférence significative portant sur les données, les actifs numériques ou l'architecture des services.

6. Le cas échéant, les fournisseurs de services de traitement de données mettent les informations visées aux paragraphes 4 et 5 à la disposition des clients publiquement au travers d'une section spécifique de leur site internet ou par tout autre moyen facilement accessible.

7. La Commission est habilitée à adopter des actes délégués conformément à l'article 45 pour compléter le présent règlement en mettant en place un mécanisme de suivi permettant à la Commission de suivre les frais de changement de fournisseur imposés par les fournisseurs de services de traitement de données sur le marché afin de garantir que la suppression et la réduction des frais de changement de fournisseur en vertu des paragraphes 1 et 2 du présent article sont réalisées dans les délais prévus aux mêmes paragraphes.

Article 30

Aspects techniques du changement de fournisseur

1. Les fournisseurs de services de traitement de données qui concernent 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, sans donner accès aux services, logiciels et applications d'exploitation qui sont stockés, autrement traités ou déployés sur ces éléments d'infrastructure, prennent, conformément à l'article 27, toutes les mesures raisonnables en leur pouvoir afin de faciliter une équivalence fonctionnelle pour le client dans l'utilisation du service de traitement de données de destination, après qu'il soit passé à un service couvrant le même type de service. Le fournisseur d'origine de services de traitement de données facilite le processus de changement de fournisseur en fournissant des capacités, les informations adéquates, de la documentation, une assistance technique et, le cas échéant, les outils nécessaires.

2. Les fournisseurs de services de traitement de données, autres que ceux visés au paragraphe 1, mettent gratuitement et dans la même mesure à la disposition de tous leurs clients et des fournisseurs de destination de services de traitement de données concernés des interfaces ouvertes afin de faciliter le processus de changement de fournisseur. Ces interfaces contiennent des informations suffisantes sur le service concerné pour permettre le développement de logiciels capables de communiquer avec les services, aux fins de la portabilité et de l'interopérabilité des données.

3. Pour les services de traitement de données autres que ceux visés au paragraphe 1 du présent article, les fournisseurs de services de traitement de données assurent la compatibilité avec les spécifications communes fondées sur des spécifications d'interopérabilité ouvertes ou les normes harmonisées d'interopérabilité au moins douze mois après que les références à ces spécifications communes ou à ces normes harmonisées pour l'interopérabilité des services de traitement des données ont été publiées dans le répertoire central des normes de l'Union pour l'interopérabilité des services de traitement de données à la suite de la publication des actes d'exécution sous-jacents au *Journal officiel de l'Union européenne* conformément à l'article 35, paragraphe 8.

4. Les fournisseurs de services de traitement de données autres que ceux visés au paragraphe 1 du présent article mettent à jour le registre en ligne visé à l'article 26, point b), conformément aux obligations qui leur incombent au titre du paragraphe 3 du présent article.

5. En cas de changement de services du même type de service, pour lequel des spécifications communes ou des normes harmonisées pour l'interopérabilité visées au paragraphe 3 du présent article n'ont pas été publiées dans le répertoire central des normes de l'Union pour l'interopérabilité des services de traitement de données conformément à l'article 35, paragraphe 8, le fournisseur des services de traitement de données exporte, à la demande du client, toutes les données exportables, dans un format structuré, couramment utilisé et lisible par machine.

6. Les fournisseurs de services de traitement de données ne sont pas tenus de développer de nouvelles technologies ou de nouveaux services, ou de divulguer ou transférer des actifs numériques qui sont protégés par des droits de propriété intellectuelle ou qui constituent un secret d'affaires, à un client ou à un fournisseur de services de traitement de données différent ou de compromettre la sécurité et l'intégrité du service du client ou du fournisseur.

Article 31

Régime spécifique applicable à certains services de traitement de données

1. Les obligations prévues à l'article 23, point d), à l'article 29 et à l'article 30, paragraphes 1 et 3, ne s'appliquent pas aux services de traitement de données dont la majorité des caractéristiques principales ont été conçues sur mesure pour répondre aux besoins spécifiques d'un client particulier ou dont tous les composants ont été développés pour les besoins d'un client particulier, et lorsque ces services de traitement de données ne sont pas proposés à grande échelle sur le plan commercial par l'intermédiaire du catalogue de services du fournisseur de services de traitement de données.

2. Les obligations prévues dans le présent chapitre ne s'appliquent pas aux services de traitement de données fournis en tant que version non destinée à la production à des fins d'essai et d'évaluation et pour une durée limitée.

3. Avant la conclusion d'un contrat pour la fourniture de services de traitement de données visés au présent article, le fournisseur de services de traitement de données informe le client potentiel des obligations énoncées au présent chapitre qui ne s'appliquent pas.

CHAPITRE VII

ACCES INTERNATIONAL ILLICITE AUX DONNEES A CARACTERE NON PERSONNEL ET TRANSFERT INTERNATIONAL ILLICITE DE CES DONNEES PAR LES AUTORITES PUBLIQUES

Article 32

Accès et transfert internationaux par les autorités publiques

1. Les fournisseurs de services de traitement de données prennent toutes les mesures techniques, organisationnelles et juridiques adéquates, y compris des contrats, afin d'empêcher l'accès international des autorités publiques et l'accès des autorités publiques des pays tiers aux données à caractère non personnel détenues dans l'Union et le transfert de ces données lorsque ce transfert ou cet accès risque d'être en conflit avec le droit de l'Union ou le droit national de l'État membre concerné, sans préjudice du paragraphe 2 ou 3.

2. Toute décision ou tout jugement d'une juridiction d'un pays tiers et toute décision d'une autorité administrative d'un pays tiers exigeant d'un fournisseur de services de traitement de données qu'il transfère des données à caractère non personnel relevant du champ d'application du présent règlement et détenues dans l'Union ou qu'il donne accès à ces données ne sont reconnus ou rendus exécutoires de quelque manière que ce soit que s'ils sont fondés sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union, ou tout accord de ce type entre le pays tiers demandeur et un État membre.

3. En l'absence d'un accord international tel qu'il est visé au paragraphe 2, lorsqu'un fournisseur de services de traitement de données est destinataire d'une décision ou d'un jugement d'une juridiction d'un pays tiers ou d'une décision d'une autorité administrative d'un pays tiers imposant de transférer 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 conflit avec le droit de l'Union ou avec le droit national 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 d'une telle décision ou d'un tel jugement soient exposés et que cette décision ou ce jugement 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 du pays tiers; et

c) la juridiction compétente d'un pays tiers 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 ou du jugement peut solliciter l'avis de l'autorité nationale ou de l'organisme national concernés compétents pour la coopération internationale en matière juridique, afin de déterminer si les conditions prévues au premier alinéa sont remplies, notamment lorsqu'il estime que la décision peut concerner des secrets d'affaires et d'autres données commercialement sensibles ainsi que du contenu protégé par des droits de propriété intellectuelle, ou que le transfert peut donner lieu à une réidentification. L'autorité nationale ou l'organisme national concernés peut consulter la Commission. Si le destinataire estime que la décision ou le jugement est susceptible de porter atteinte aux intérêts de l'Union ou de ses États membres en matière de sécurité nationale ou de défense, il demande l'avis de l'autorité nationale ou de l'organisme national concernés afin de déterminer si les données demandées concernent les intérêts de l'Union ou de ses États membres en matière de sécurité nationale ou de défense. Si le destinataire n'a pas reçu de réponse dans un délai d'un mois, ou si cette autorité ou cet organisme conclut dans son avis que les conditions prévues au premier alinéa ne sont pas remplies, le destinataire peut, pour ces motifs, rejeter la demande de transfert de données à caractère non personnel ou d'accès à de telles données.

Le comité européen de l'innovation dans le domaine des données visé à l'article 42 conseille et assiste la Commission dans l'élaboration de lignes directrices relatives à l'évaluation du respect des conditions prévues au premier alinéa du présent paragraphe.

4. Si les conditions énoncées au paragraphe 2 ou 3 sont remplies, le fournisseur de services de traitement de données fournit le volume minimal de données admissible en réponse à une demande, sur la base de l'interprétation que peut raisonnablement donner de cette demande le fournisseur ou l'autorité nationale ou l'organisme national concernés visés au paragraphe 3, deuxième alinéa.

5. Le fournisseur de services de traitement de données informe le client de l'existence d'une demande d'accès à des données le concernant qui émane d'une autorité d'un pays tiers avant de donner suite à cette demande, sauf lorsque cette demande sert des fins répressives et aussi longtemps que cela est nécessaire pour préserver l'efficacité de l'action répressive.

CHAPITRE VIII

INTEROPERABILITE

Article 33

Exigences essentielles concernant l'interopérabilité des données, des mécanismes et des services de partage des données ainsi que des espaces européens communs de données

1. Les participants aux espaces de données qui proposent des données ou des services de données à d'autres participants respectent les exigences essentielles suivantes en vue de faciliter l'interopérabilité des données, des mécanismes et des services de partage de données, ainsi que des espaces européens communs des données qui sont des cadres interopérables de normes et de pratiques communes transsectoriels ou spécifiques à chaque finalité ou à chaque secteur visant à partager ou à traiter conjointement des données pour, entre autres, la mise au point de nouveaux produits et services, la recherche scientifique ou des initiatives de la société civile:

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, le cas échéant, dans un format lisible par machine, 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, le cas échéant, 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, en téléchargement de masse ou en temps réel dans un format lisible par machine, lorsque cela est techniquement possible et n'entrave pas le bon fonctionnement du produit connecté;

d) le cas échéant, les moyens permettant l'interopérabilité des outils d'exécution automatique des accords de partage de données, tels que les contrats intelligents, 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 dispositions du droit de l'Union ou du droit national.

2. La Commission est habilitée à adopter des actes délégués conformément à l'article 45 du présent règlement afin de compléter le présent règlement en précisant davantage les exigences essentielles prévues au paragraphe 1 du présent article, en ce qui concerne les exigences qui, par leur nature, ne peuvent produire l'effet escompté que si elles sont précisées davantage dans des actes juridiques contraignants de l'Union, et afin de refléter correctement l'évolution des technologies et du marché.

Lorsqu'elle adopte des actes délégués, la Commission tient compte des avis du comité européen de l'innovation dans le domaine des données conformément à l'article 42, point c), iii).

3. Les participants aux espaces de données qui proposent des données ou des services de données à d'autres participants aux espaces de données qui satisfont aux normes harmonisées ou à des parties de normes harmonisées, dont les références sont publiées au *Journal officiel de l'Union européenne*, sont présumés être en conformité avec les exigences essentielles prévues au paragraphe 1, dans la mesure où ces exigences sont couvertes par de telles normes harmonisées ou des parties de ces normes.

4. En application de l'article 10 du règlement (UE) n° 1025/2012, la Commission demande à une ou plusieurs organisations européennes de normalisation d'élaborer des normes harmonisées qui satisfont aux exigences essentielles prévues au paragraphe 1 du présent article.

5. La Commission peut, par voie d'actes d'exécution, adopter des spécifications communes couvrant l'une ou l'ensemble des exigences essentielles prévues au paragraphe 1 lorsque les conditions suivantes sont remplies:

a) la Commission a demandé, conformément à l'article 10, paragraphe 1, du règlement (UE) n° 1025/2012, à une ou plusieurs organisations européennes de normalisation d'élaborer une norme harmonisée qui satisfait aux exigences essentielles prévues au paragraphe 1 du présent article et:

   i) la demande n'a pas été acceptée;

   ii) les normes harmonisées répondant à cette demande ne sont pas fournies dans le délai déterminé conformément à l'article 10, paragraphe 1, du règlement (UE) n° 1025/2012; ou

   iii) les normes harmonisées ne répondent pas à la demande; et

b) aucune référence à des normes harmonisées couvrant les exigences essentielles pertinentes prévues au paragraphe 1 du présent article n'est publiée au *Journal officiel de l'Union européenne* conformément au règlement (UE) n° 1025/2012 et aucune référence de ce type ne devrait être publiée dans un délai raisonnable.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 46, paragraphe 2.

6. Avant de préparer un projet d'acte d'exécution visé au paragraphe 5 du présent article, la Commission informe le comité visé à l'article 22 du règlement (UE) n° 1025/2012 qu'elle estime que les conditions énoncées au paragraphe 5 du présent article ont été remplies.

7. Lorsqu'elle prépare le projet d'acte d'exécution visé au paragraphe 5, la Commission tient compte de l'avis du comité européen de l'innovation dans le domaine des données et du point de vue d'autres organismes ou groupes d'experts compétents et consulte dûment toutes les parties prenantes concernées.

8. Les participants aux espaces de données qui proposent des données ou des services de données aux autres participants aux espaces de données qui satisfont aux spécifications communes établies par des actes d'exécution visés au paragraphe 5 ou à des parties de celles-ci sont présumés être en conformité avec les exigences essentielles prévues au paragraphe 1 dans la mesure où ces exigences sont couvertes par de telles spécifications communes ou des parties de celles-ci.

9. Lorsqu'une norme harmonisée est adoptée par une organisation européenne de normalisation et proposée à la Commission en vue de la publication de sa référence au *Journal officiel de l'Union européenne*, la Commission évalue la norme harmonisée conformément au règlement (UE) n° 1025/2012. Lorsque la référence d'une norme harmonisée est publiée au *Journal officiel de l'Union européenne*, la Commission abroge les actes d'exécution visés au paragraphe 5 du présent article, ou les parties de ces actes qui couvrent les mêmes exigences essentielles que celles couvertes par ladite norme harmonisée.

10. Lorsqu'un État membre estime qu'une spécification commune ne satisfait pas entièrement aux exigences essentielles prévues au paragraphe 1, il en informe la Commission en lui fournissant une explication détaillée. La Commission évalue cette explication détaillée et peut, le cas échéant, modifier l'acte d'exécution établissant la spécification commune en question.

11. La Commission peut adopter des lignes directrices en tenant compte de la proposition du comité européen de l'innovation dans le domaine des données conformément à l'article 30, point h), du règlement (UE) 2022/868 établissant des cadres interopérables pour les normes et pratiques communes pour le fonctionnement des espaces européens communs des données.

Article 34

Interopérabilité aux fins de l'utilisation simultanée de services de traitement de données

1. Les exigences prévues à l'article 23, à l'article 24, à l'article 25, paragraphe 2, points a) ii), a) iv), e) et f), et à l'article 30, paragraphes 2 à 5, s'appliquent également mutatis mutandis aux fournisseurs de services de traitement de données pour faciliter l'interopérabilité aux fins de l'utilisation simultanée de services de traitement de données.

2. Lorsqu'un service de traitement de données et un autre service de traitement de données sont utilisés simultanément, les fournisseurs de services de traitement de données peuvent imposer des frais de transfert des données, mais seulement aux fins de répercuter les coûts de sortie occasionnés, sans dépasser de tels coûts.

Article 35

Interopérabilité des services de traitement de données

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

a) réalisent, lorsque cela est techniquement possible, l'interopérabilité entre différents services de traitement de données couvrant le même type de service;

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

c) facilitent, lorsque cela est techniquement possible, l'équivalence fonctionnelle entre différents services de traitement de données visés à l'article 30, paragraphe 1, couvrant le même type de service;

d) ne portent pas atteinte à la sécurité et à l'intégrité des services de traitement des données et des données;

e) sont conçues de manière à permettre des avancées techniques et l'inclusion de nouvelles fonctions et innovations dans les services de traitement de données.

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

a) les aspects de l'interopérabilité de l'informatique en nuage qui concernent l'interopérabilité du transport, l'interopérabilité syntactique, l'interopérabilité sémantique des données, l'interopérabilité comportementale et l'interopérabilité du cadre normatif;

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 applicatifs de l'informatique en nuage qui concernent 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 à l'annexe II du règlement (UE) n° 1025/2012.

4. Après avoir tenu compte des normes internationales et européennes pertinentes ainsi que des initiatives d'autorégulation, la Commission peut, conformément à l'article 10, paragraphe 1, du règlement (UE) n° 1025/2012, demander à une ou plusieurs organisations européennes de normalisation d'élaborer des normes harmonisées qui satisfont aux exigences essentielles prévues aux paragraphes 1 et 2 du présent article.

5. La Commission peut, par voie d'actes d'exécution, adopter des spécifications communes fondées sur des spécifications d'interopérabilité ouvertes couvrant toutes les exigences essentielles prévues aux paragraphes 1 et 2.

6. Lorsqu'elle prépare le projet d'acte d'exécution visé au paragraphe 5 du présent article, la Commission tient compte du point de vue des autorités compétentes visées à l'article 37, paragraphe 5, point h), et d'autres organismes ou groupes d'experts compétents et consulte dûment toutes les parties prenantes concernées.

7. Lorsqu'un État membre estime qu'une spécification commune ne satisfait pas entièrement aux exigences essentielles prévues aux paragraphes 1 et 2, il en informe la Commission en lui fournissant une explication détaillée. La Commission évalue cette explication détaillée et peut, le cas échéant, modifier l'acte d'exécution établissant la spécification commune en question.

8. Aux fins de l'article 30, paragraphe 3, la Commission publie, par voie d'actes d'exécution, les références des normes harmonisées et des spécifications communes pour l'interopérabilité des services de traitement de données dans un répertoire central des normes de l'Union pour l'interopérabilité des services de traitement de données.

9. Les actes d'exécution visés au présent article sont adoptés en conformité avec la procédure d'examen visée à l'article 46, paragraphe 2.

Article 36

Exigences essentielles concernant les contrats intelligents pour l'exécution des accords de 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 de l'exécution d'un accord ou d'une partie d'un accord de mise à disposition des données, veille à ce que ces contrats intelligents respectent les exigences essentielles suivantes:

a) robustesse et contrôle de l'accès, pour veiller à ce que le contrat intelligent ait été conçu de manière à offrir des mécanismes de contrôle d'accès et un degré très élevé de robustesse afin d'éviter des erreurs fonctionnelles et de résister aux tentatives de manipulation par des tiers;

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

c) archivage et continuité des données, pour garantir, dans les circonstances dans lesquelles un contrat intelligent doit être résilié ou désactivé, qu'il y a 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);

d) contrôle de l'accès, pour garantir qu'un contrat intelligent est protégé par des mécanismes rigoureux de contrôle d'accès au niveau de la gouvernance et des contrats intelligents; et

e) cohérence, pour assurer la cohérence avec les dispositions de l'accord de partage de données que le contrat intelligent exécute.

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 de l'exécution d'un accord ou d'une partie d'un accord de mise à disposition des données, procède à une évaluation de la conformité en vue de satisfaire aux exigences essentielles prévues au paragraphe 1 et, en ce qui concerne le respect de ces 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 de l'exécution d'un accord ou d'une partie d'un accord de mise à disposition des données est responsable du respect des exigences essentielles prévues au paragraphe 1.

4. Un contrat intelligent qui satisfait aux normes harmonisées ou aux parties concernées de celles-ci et dont les références sont publiées au *Journal officiel de l'Union européenne* est présumé être en conformité avec les exigences essentielles prévues au paragraphe 1, dans la mesure où ces exigences sont couvertes par de telles normes harmonisées ou des parties de celles-ci.

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

6. La Commission peut, par voie d'actes d'exécution, adopter des spécifications communes couvrant l'une ou l'ensemble des exigences essentielles prévues au paragraphe 1 lorsque les conditions suivantes sont remplies:

a) la Commission a demandé, conformément à l'article 10, paragraphe 1, du règlement (UE) nº 1025/2012, à une ou plusieurs organisations européennes de normalisation d'élaborer une norme harmonisée qui satisfait aux exigences essentielles prévues au paragraphe 1 du présent article et:

   i) la demande n'a pas été acceptée;

   ii) les normes harmonisées répondant à cette demande n'ont pas été fournies dans le délai déterminé conformément à l'article 10, paragraphe 1, du règlement (UE) nº 1025/2012; ou

   iii) les normes harmonisées ne répondent pas à la demande; et

b) aucune référence à des normes harmonisées couvrant les exigences essentielles pertinentes prévues au paragraphe 1 du présent article n'est publiée au *Journal officiel de l'Union européenne* conformément au règlement (UE) nº 1025/2012 et aucune référence de ce type ne devrait être publiée dans un délai raisonnable.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 46, paragraphe 2.

7. Avant de préparer un projet d'acte d'exécution visé au paragraphe 6 du présent article, la Commission informe le comité visé à l'article 22 du règlement (UE) nº 1025/2012 qu'elle estime que les conditions prévues au paragraphe 6 du présent article ont été remplies.

8. Lorsqu'elle prépare le projet d'acte d'exécution visé au paragraphe 6, la Commission tient compte de l'avis du comité européen de l'innovation dans le domaine des données et du point de vue d'autres organismes ou groupes d'experts compétents et consulte dûment toutes les parties prenantes concernées.

9. 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 de l'exécution d'un accord ou d'une partie d'un accord de mise à disposition des données qui sont conformes aux spécifications communes établies par des actes d'exécution visés au paragraphe 6, ou à des parties de celles-ci, est présumé respecter les exigences essentielles prévues au paragraphe 1 dans la mesure où ces exigences sont couvertes par de telles spécifications communes ou par des parties de celles-ci.

10. Lorsqu'une norme harmonisée est adoptée par une organisation européenne de normalisation et proposée à la Commission en vue de la publication de sa référence au *Journal officiel de l'Union européenne*, la Commission évalue la norme harmonisée conformément au règlement (UE) nº 1025/2012. Lorsque la référence d'une norme harmonisée est publiée au *Journal officiel de l'Union européenne*, la Commission abroge les actes d'exécution visés au paragraphe 6 du présent article, ou des parties de ces actes qui couvrent les mêmes exigences essentielles que celles qui sont couvertes par ladite norme harmonisée.

11. Lorsqu'un État membre estime qu'une spécification commune ne satisfait pas entièrement aux exigences essentielles prévues au paragraphe 1, il en informe la Commission en lui fournissant une explication détaillée. La Commission évalue ladite explication détaillée et peut, le cas échéant, modifier l'acte d'exécution établissant la spécification commune en question.

CHAPITRE IX

MISE EN ŒUVRE ET EXECUTION

Article 37

Autorités compétentes et coordinateurs de données

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

2. Lorsqu'un État membre désigne plus d'une autorité compétente, il désigne un coordinateur de données parmi celles-ci afin de faciliter la coopération entre les autorités compétentes et afin d'aider les entités relevant du champ d'application du présent règlement sur toutes les questions liées à son application et à son exécution. Les autorités compétentes coopèrent entre elles dans l'exercice des missions et pouvoirs qui leur sont conférés au titre du paragraphe 5.

3. Les autorités de contrôle chargées de surveiller l'application du règlement (UE) 2016/679 sont chargées de surveiller 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 mutatis mutandis.

Le Contrôleur européen de la protection des données est chargé de surveiller l'application du présent règlement dans la mesure où il concerne la Commission, la Banque centrale européenne ou des organes de l'Union. Le cas échéant, l'article 62 du règlement (UE) 2018/1725 s'applique mutatis mutandis.

Les autorités de contrôle visées au présent paragraphe exercent leurs missions et leurs pouvoirs à l'égard du traitement des données à caractère personnel.

4. Sans préjudice du paragraphe 1 du présent article:

a) pour les questions spécifiques sur l'accès aux données sectorielles et leur utilisation en lien avec l'application du présent règlement, la compétence des autorités sectorielles est respectée;

b) l'autorité compétente chargée de l'application et de l'exécution des articles 23 à 31 et des articles 34 et 35 dispose d'une expérience dans le domaine des données et des services de communications électroniques.

5. Les États membres veillent à ce que les missions et pouvoirs des autorités compétentes soient clairement définis et incluent:

a) la promotion de l'éducation aux données et 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 des infractions alléguées au présent règlement, y compris en lien avec des secrets d'affaires, l'examen de l'objet de la réclamation, dans la mesure nécessaire, et l'information à intervalles réguliers de l'auteur de la réclamation, le cas échéant conformément au droit national, sur l'état d'avancement et 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 de sanctions financières effectives, proportionnées et 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 et commerciales pertinentes pour la mise à disposition et l'utilisation des données;

f) la coopération avec les autorités compétentes d'autres États membres, et, le cas échéant, avec la Commission ou le comité européen de l'innovation dans le domaine des données, pour garantir l'application cohérente et efficace du présent règlement, y compris l'échange de toutes les informations pertinentes par voie électronique, sans retard injustifié, y compris en ce qui concerne le paragraphe 10 du présent article;

g) la coopération avec les autorités compétentes concernées chargées de la mise en œuvre d'autres actes juridiques de l'Union ou nationaux, y compris avec les autorités compétentes dans le domaine des données et des services de communications électroniques, avec l'autorité de contrôle chargée de surveiller l'application du règlement (UE) 2016/679 ou avec les autorités sectorielles afin de veiller à ce que le présent règlement soit appliqué de manière cohérente par rapport aux autres dispositions du droit de l'Union et du droit national;

h) la coopération avec les autorités compétentes concernées afin de veiller à ce que les articles 23 à 31 et les articles 34 et 35 soient exécutées de manière cohérente par rapport au droit de l'Union et aux mesures d'autoréglementation applicables aux fournisseurs de services de traitement de données;

i) l'assurance que les frais de changement de fournisseur sont supprimés conformément à l'article 29;

j) l'examen des demandes de données introduites en application du chapitre V.

Lorsqu'un coordinateur de données a été désigné, il facilite la coopération visée aux points f), g) et h) du premier alinéa et assiste les autorités compétentes à leur demande.

6. Lorsqu'une telle autorité compétente a été désignée, le coordinateur de données:

a) fait office de point de contact unique pour toutes les questions liées à l'application du présent règlement;

b) veille à ce que soient mises à la disposition du public en ligne les demandes de mise à disposition des données présentées par des organismes du secteur public en cas de besoin exceptionnel au titre du chapitre V et encourage les accords de partage volontaire de données entre les organismes du secteur public et les détenteurs de données;

c) informe annuellement la Commission des refus notifiés au titre de l'article 4, paragraphes 2 et 8, et de l'article 5, paragraphe 11.

7. Les États membres communiquent à la Commission le nom des autorités compétentes ainsi que leurs missions et pouvoirs et, le cas échéant, le nom du coordinateur de données. La Commission tient un registre public de ces autorités.

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

9. Les États membres veillent à ce que les autorités compétentes disposent de ressources humaines et techniques suffisantes et de l'expertise adéquate pour s'acquitter efficacement de leurs missions conformément au présent règlement.

10. Les entités relevant du champ d'application du présent règlement sont soumises à la compétence de l'État membre dans lequel elles sont établies. Lorsque l'entité est établie dans plus d'un État membre, elle est considérée comme relevant de la compétence de l'État membre dans lequel se trouve son établissement principal, c'est-à-dire là où l'entité a son siège social ou son siège statutaire d'où sont exercés les principales fonctions financières et le contrôle opérationnel.

11. Toute entité relevant du champ d'application du présent règlement qui met des produits connectés à disposition ou propose des services connexes dans l'Union et qui n'est pas établie dans l'Union désigne un représentant légal dans l'un des États membres.

12. Aux fins de garantir le respect du présent règlement, un représentant légal est mandaté par une entité relevant du champ d'application du présent règlement qui met des produits connectés à disposition ou propose des services connexes dans l'Union pour être contacté, en plus de ladite entité ou à sa place, par les autorités compétentes en ce qui concerne toutes les questions liées à cette entité. Ce représentant légal coopère avec les autorités compétentes et leur démontre de manière exhaustive, sur demande, les mesures prises et les dispositions mises en place par l'entité relevant du champ d'application du présent règlement qui met des produits connectés à disposition ou propose des services connexes dans l'Union pour garantir le respect du présent règlement.

13. Une entité relevant du champ d'application du présent règlement qui met à disposition des produits connectés ou propose des services dans l'Union est considérée comme relevant de la compétence de l'État membre dans lequel se trouve son représentant légal. La désignation d'un représentant légal par une telle entité est sans préjudice de la responsabilité de cette entité et des actions en justice qui pourraient être intentées contre elle. Jusqu'à ce qu'une entité désigne un représentant légal conformément au présent article, elle relève de la compétence de tous les États membres, le cas échéant, aux fins de garantir l'application et l'exécution du présent règlement. Toute autorité compétente peut exercer sa compétence, y compris en imposant des sanctions effectives, proportionnées et dissuasives, pour autant que l'entité ne fasse pas l'objet d'une procédure d'exécution au titre du présent règlement portant sur les mêmes faits par une autre autorité compétente.

14. Les autorités compétentes sont habilitées à demander aux utilisateurs, aux détenteurs de données ou aux destinataires de données, ou à leurs représentants légaux, qui relèvent de la compétence de leur État membre toutes les informations nécessaires pour vérifier le respect du présent règlement. Toute demande d'information est proportionnée à l'accomplissement de la mission sous-jacente et est motivée.

15. Lorsqu'une autorité compétente dans un État membre sollicite l'assistance d'une autorité compétente d'un autre État membre ou l'application de mesures d'exécution par celle-ci, elle présente une demande motivée. Lorsqu'elle reçoit une telle demande, une autorité compétente fournit, sans retard injustifié, une réponse détaillant les mesures qui ont été prises ou qu'il est prévu de prendre.

16. Les autorités compétentes respectent les principes de confidentialité et de secret professionnel et commercial et protègent les données à caractère personnel conformément au droit de l'Union ou au droit national. Toutes les informations échangées dans le cadre d'une demande d'assistance et fournies en vertu du présent article ne sont utilisées qu'aux fins pour lesquelles elles ont été demandées.

Article 38

Droit d'introduire une réclamation

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. Le coordinateur de données fournit, sur demande, aux personnes physiques et morales toutes les informations nécessaires à l'introduction de leur réclamation auprès de l'autorité compétente concernée.

2. L'autorité compétente auprès de laquelle la réclamation a été introduite informe l'auteur de la réclamation, conformément au droit national, de l'état d'avancement de la procédure et de la décision prise.

3. Les autorités compétentes coopèrent pour gérer et traiter les réclamations de manière efficace et rapide, y compris en échangeant toutes les informations pertinentes par voie électronique, sans retard injustifié. Cette coopération n'affecte pas les mécanismes de coopération prévus aux chapitres VI et VII du règlement (UE) 2016/679 et ceux prévus par le règlement (UE) 2017/2394.

Article 39

Droit à un recours juridictionnel effectif

1. Nonobstant tout recours administratif ou tout autre recours non juridictionnel, toute personne physique ou morale lésée dispose du droit à un recours juridictionnel effectif en ce qui concerne les décisions juridiquement contraignantes prises par les autorités compétentes.

2. Lorsqu'une autorité compétente ne donne pas suite à une réclamation, toute personne physique ou morale lésée a, conformément au droit national, soit droit à un recours juridictionnel effectif, soit accès à un réexamen réalisé par un organe impartial doté des compétences appropriées.

3. Les actions intentées en vertu du présent article sont portées devant les juridictions de l'État membre de l'autorité compétente contre laquelle le recours juridictionnel a été formé individuellement ou, le cas échéant, collectivement par les représentants d'une ou de plusieurs personnes physiques ou morales.

Article 40

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. Ces sanctions doivent être effectives, proportionnées et dissuasives.

2. Les États membres informent la Commission, au plus tard le 12 septembre 2025, 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. La Commission tient et met à jour régulièrement un registre public facilement accessible de ces mesures.

3. Les États membres tiennent compte des recommandations du comité européen de l'innovation dans le domaine des données et des critères non exhaustifs suivants pour l'imposition de sanctions en cas de violation du présent règlement:

a) la nature, la gravité, l'ampleur et la durée de l'infraction;

b) toute mesure prise par l'auteur de l'infraction pour atténuer ou réparer le préjudice causé par l'infraction;

c) toute infraction antérieure commise par l'auteur de l'infraction;

d) les avantages financiers obtenus ou les pertes évitées par l'auteur de l'infraction en raison de l'infraction, si ces avantages ou pertes peuvent être établis de manière fiable;

e) toute autre circonstance aggravante ou atténuante applicable au cas concerné;

f) le chiffre d'affaires annuel réalisé par l'auteur de l'infraction au cours de l'exercice précédent dans l'Union.

4. En ce qui concerne les infractions aux obligations prévues aux chapitres II, III et V du présent règlement, les autorités de contrôle chargées de surveiller l'application du règlement (UE) 2016/679 peuvent, dans les limites de leur compétence, imposer 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.

5. En ce qui concerne les infractions aux obligations prévues au chapitre V du présent règlement, le Contrôleur européen de la protection des données peut, dans les limites de sa compétence, imposer 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 41

Clauses contractuelles types et clauses contractuelles standard

Avant le 12 septembre 2025, la Commission élabore et recommande des clauses contractuelles types non contraignantes concernant l'accès aux données et l'utilisation des données, y compris des clauses relatives à une compensation raisonnable et à la protection des secrets d'affaires, ainsi que des clauses contractuelles standard non contraignantes pour les contrats d'informatique en nuage, afin d'aider les parties à rédiger et à négocier des contrats garantissant des droits et obligations contractuels équitables, raisonnables et non discriminatoires.

Article 42

Rôle du comité européen de l'innovation dans le domaine des données

Le comité européen de l'innovation dans le domaine des données, institué par la Commission en tant que groupe d'experts en vertu de l'article 29 du règlement (UE) 2022/868, au sein duquel les autorités compétentes sont représentées, favorise l'application cohérente du présent règlement:

a) en conseillant et en assistant la Commission en ce qui concerne l'élaboration d'une pratique cohérente des autorités compétentes pour l'exécution des chapitres II, III, V et VII;

b) en facilitant la coopération entre les autorités compétentes par le renforcement des capacités et l'échange d'informations, notamment en établissant des méthodes pour l'échange efficace d'informations relatives à l'application des droits et obligations prévus aux chapitres II, III et V dans les affaires transfrontières, y compris la coordination en ce qui concerne l'instauration de sanctions;

c) en conseillant et en assistant la Commission en ce qui concerne:

   i) l'opportunité de demander l'élaboration de normes harmonisées visées à l'article 33, paragraphe 4, à l'article 35, paragraphe 4, et à l'article 36, paragraphe 5;

   ii) la préparation des actes d'exécution visés à l'article 33, paragraphe 5, à l'article 35, paragraphes 5 et 8, et à l'article 36, paragraphe 6;

   iii) la préparation des actes délégués visés à l'article 29, paragraphe 7, et à l'article 33, paragraphe 2; et

   iv) l'adoption de lignes directrices établissant des cadres interopérables de normes et de pratiques communes pour le fonctionnement d'espaces européens communs des données visées à l'article 33, paragraphe 11.

CHAPITRE X

DROIT SUI GENERIS PREVU PAR LA DIRECTIVE 96/9/CE

Article 43

Bases de données contenant certaines données

Le droit sui generis prévu par l'article 7 de la directive 96/9/CE ne s'applique pas lorsque des données sont obtenues à partir d'un produit connecté ou d'un service connexe relevant du champ d'application du présent règlement ou générées par un tel produit ou service, en particulier en ce qui concerne ses articles 4 et 5.

CHAPITRE XI

DISPOSITIONS FINALES

Article 44

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 en vigueur au 11 janvier 2024 ou avant cette date et dans les actes délégués ou d'exécution adoptés en vertu de ces actes, restent inchangées.

2. Le présent règlement est sans préjudice du droit de l'Union précisant, 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'avoir accès à certaines données fournies par les utilisateurs ou de les utiliser;

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

3. Le présent règlement, à l'exception du chapitre V, est sans préjudice du droit de l'Union et du droit national prévoyant l'accès aux données et autorisant l'utilisation de données à des fins de recherche scientifique.

Article 45

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 29, paragraphe 7, et à l'article 33, paragraphe 2, est conféré à la Commission pour une durée indéterminée à compter du 11 janvier 2024.

3. La délégation de pouvoir visée à l'article 29, paragraphe 7, et à l'article 33, paragraphe 2, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 "Mieux légiférer".

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 29, paragraphe 7, ou de l'article 33, paragraphe 2, 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 46

Comité

1. La Commission est assistée par le comité institué par le règlement (UE) 2022/868. 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 47

Modification du règlement (UE) 2017/2394

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

"29. Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données) (JO L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).".

Article 48

Modification de la directive (UE) 2020/1828

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

"68. Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données) (JO L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).".

Article 49

Évaluation et réexamen

1. Au plus tard le 12 septembre 2028, 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 situations qui doivent être considérées comme des situations de besoin exceptionnel aux fins de l'article 15 du présent règlement et de l'application du chapitre V du présent règlement, en particulier l'expérience acquise dans l'application du chapitre V du présent règlement par les organismes du secteur public, la Commission, la Banque centrale européenne et les organes de l'Union; le nombre de procédures engagées auprès de l'autorité compétente au titre de l'article 18, paragraphe 5, concernant l'application du chapitre V du présent règlement et leur issue, telles que déclarées par les autorités compétentes; l'incidence d'autres obligations prévues par le droit de l'Union ou le droit national aux fins de donner suite aux demandes d'accès aux informations; l'incidence des mécanismes de partage volontaire des données, tels que ceux mis en place par des organisations altruistes en matière de données reconnues en vertu du règlement (UE) 2022/868, sur la réalisation des objectifs du chapitre V du présent règlement, et le rôle des données à caractère personnel dans le contexte de l'article 15 du présent règlement, y compris l'évolution des technologies renforçant la protection de la vie privée;

b) l'incidence du présent règlement sur l'utilisation des données dans l'économie, y compris sur l'innovation dans le domaine des données, les pratiques de monétisation des données et les services d'intermédiation de données, ainsi que sur le partage de données au sein des espaces européens communs des données;

c) l'accessibilité et l'utilisation des différentes catégories et des différents types de données;

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

e) l'absence de toute incidence sur les droits de propriété intellectuelle;

f) l'incidence sur les secrets d'affaires, y compris sur la protection contre leur obtention, leur utilisation et leur divulgation illicites, ainsi que l'incidence du mécanisme permettant au détenteur de données de refuser la demande de l'utilisateur au titre de l'article 4, paragraphe 8, et de l'article 5, paragraphe 11, en tenant compte, dans la mesure du possible, de toute révision de la directive (UE) 2016/943;

g) la question de savoir si la liste des clauses contractuelles abusives visée à l'article 13 est à jour à la lumière des nouvelles pratiques commerciales et du rythme rapide de l'innovation sur le marché;

h) les changements dans les pratiques contractuelles des fournisseurs de services de traitement de données et la question de savoir si cela se traduit par un respect suffisant de l'article 25;

i) la réduction des frais imposés par les fournisseurs de services de traitement de données pour le processus de changement de fournisseur, en conformité avec la suppression progressive des frais de changement de fournisseur en vertu de l'article 29;

j) l'interaction du présent règlement avec d'autres actes juridiques de l'Union présentant un intérêt pour l'économie fondée sur les données;

k) la prévention de tout accès illicite des pouvoirs publics aux données à caractère non personnel;

l) l'efficacité du système de contrôle d'application requis au titre de l'article 37;

m) les effets du présent règlement sur les PME en ce qui concerne leur capacité d'innovation, la disponibilité des services de traitement des données pour les utilisateurs dans l'Union et la charge que représente le respect de nouvelles obligations.

2. Au plus tard le 12 septembre 2028, la Commission procède à une évaluation du présent règlement et présente au Parlement européen et au Conseil, ainsi qu'au Comité économique et social européen, un rapport reprenant ses principales conclusions. Cette évaluation porte sur les effets des articles 23 à 31 et des articles 34 et 35, en particulier en ce qui concerne la tarification et la diversité des services de traitement de données offerts au sein de l'Union, en accordant une attention particulière aux PME en tant que fournisseurs.

3. Les États membres fournissent à la Commission les informations nécessaires à l'établissement des rapports visés aux paragraphes 1 et 2.

4. Sur la base des rapports visés aux paragraphes 1 et 2, la Commission peut, le cas échéant, présenter au Parlement européen et au Conseil une proposition législative de modification du présent règlement.

Article 50

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 septembre 2025.

L'obligation découlant de l'article 3, paragraphe 1, s'applique aux produits connectés et aux services connexes mis sur le marché après le 12 septembre 2026.

Le chapitre III s'applique en ce qui concerne les obligations de mise à disposition de données au titre du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union, qui entre en vigueur après le 12 septembre 2025.

Le chapitre IV s'applique aux contrats conclus après le 12 septembre 2025.

Le chapitre IV s'applique à partir du 12 septembre 2027 aux contrats conclus le 12 septembre 2025 ou avant cette date, à condition:

a) qu'ils soient à durée indéterminée; ou

b) qu'ils viennent à échéance au moins dix ans à compter du 11 janvier 2024.

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

Fait à Strasbourg, le 13 décembre 2023.

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président*
R. METSOLA	P. NAVARRO RÍOS