I

(Actes législatifs)

RÈGLEMENTS

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)

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

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen ([1]),

après consultation du Comité des régions,

statuant conformément à la procédure législative ordinaire ([2]),

considérant ce qui suit:

(1) Le traité sur le fonctionnement de l'Union européenne prévoit l'établissement d'un marché intérieur ainsi que l'instauration d'un régime garantissant que la concurrence sur le marché intérieur n'est pas faussée. La mise en place de règles et pratiques communes dans les États membres en ce qui concerne l'élaboration d'un cadre de gouvernance des données devrait contribuer à la réalisation de ces objectifs, dans le plein respect des droits fondamentaux. Elle devrait également garantir le renforcement de l'autonomie stratégique ouverte de l'Union tout en facilitant la libre circulation des données à l'échelle internationale.

(2) Au cours de la dernière décennie, les technologies numériques ont transformé l'économie et la société, touchant tous les secteurs d'activité et la vie quotidienne. Les données sont au cœur de cette transformation: l'innovation fondée sur les données apportera des avantages considérables aussi bien aux citoyens de l'Union qu'à l'économie, par exemple en améliorant et en personnalisant la médecine, en offrant une mobilité nouvelle et en contribuant à la communication de la Commission du 11 décembre 2019 sur le pacte vert pour l'Europe. Afin que l'économie fondée sur les données soit inclusive à l'égard de tous les citoyens de l'Union, il faut veiller tout particulièrement à réduire la fracture numérique, à encourager la participation des femmes à l'économie des données et à promouvoir une expertise européenne de pointe dans le secteur des technologies. L'économie des données doit être construite de manière à permettre aux entreprises, en particulier aux micro, petites et moyennes entreprises (PME), telles qu'elles sont définies à l'annexe de la recommandation 2003/361/CE de la Commission ([3]), et aux jeunes pousses de prospérer, en garantissant la neutralité de l'accès aux données ainsi que la portabilité et l'interopérabilité des données, et en évitant les effets de verrouillage. Dans sa communication du 19 février 2020 sur une stratégie européenne pour les données (ci-après dénommée «stratégie européenne pour les données»), la Commission a décrit la vision qu'elle a d'un espace européen unique des données, à savoir un marché intérieur des données dans lequel les données pourraient être utilisées quel que soit leur lieu de stockage physique dans l'Union, conformément au droit applicable, et qui soit susceptible, entre autres, de jouer un rôle déterminant dans le développement rapide des technologies de l'intelligence artificielle.

([1]) JO C 286 du 16.7.2021, p. 38.

([2]) Position du Parlement européen du 6 avril 2022 (non encore parue au Journal officiel) et décision du Conseil du 16 mai 2022.

([3]) 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).

La Commission a également plaidé en faveur de la libre circulation sécurisée des données avec les pays tiers, sous réserve des exceptions et des restrictions en matière de sécurité publique, d'ordre public et d'autres objectifs légitimes de politique publique de l'Union, conformément aux obligations internationales, y compris en ce qui concerne les droits fondamentaux. Afin que cette vision devienne réalité, la Commission a proposé de mettre en place des espaces européens communs de données spécifiques à certains domaines en vue du partage de données et de la mise en commun de données. Ainsi que le propose la stratégie européenne pour les données, ces espaces européens communs de données pourraient couvrir des domaines tels que la santé, la mobilité, l'industrie manufacturière, les services financiers, l'énergie ou l'agriculture, ou une combinaison de ces domaines, par exemple l'énergie et le climat, ainsi que des domaines thématiques tels que le pacte vert pour l'Europe, l'administration publique ou les compétences. Les espaces européens communs de données devraient rendre les données traçables, accessibles, interopérables et réutilisables (ci-après dénommé «principes FAIR pour les données»), tout en garantissant un niveau élevé de cybersécurité. Lorsqu'il existe des conditions de concurrence équitables dans l'économie des données, les entreprises se font concurrence sur la qualité des services, et non sur la quantité de données qu'elles contrôlent. Aux fins de la conception, de la création et du maintien de conditions de concurrence équitables dans l'économie des données, une gouvernance solide est nécessaire, à laquelle les parties prenantes concernées d'un espace européen commun de données doivent participer et dans laquelle elles doivent être représentées.

(3) Il est nécessaire d'améliorer les conditions du partage des données dans le marché intérieur, en créant un cadre harmonisé pour les échanges de données et en définissant un certain nombre d'exigences de base pour la gouvernance des données, en veillant tout particulièrement à faciliter la coopération entre les États membres. Le présent règlement devrait viser à développer davantage le marché intérieur numérique sans frontières ainsi qu'une société et une économie des données centrées sur l'humain, dignes de confiance et sûres. Le droit sectoriel de l'Union peut élaborer, adapter et proposer des éléments nouveaux et complémentaires, en fonction des spécificités du secteur, telles que les dispositions du droit de l'Union envisagées en ce qui concerne l'espace européen des données relatives à la santé et en ce qui concerne l'accès aux données relatives aux véhicules. En outre, certains secteurs de l'économie sont déjà réglementés par le droit sectoriel de l'Union, qui comprend des règles relatives au partage de données ou à l'accès aux données au niveau transfrontalier ou à l'échelle de l'Union, par exemple la directive 2011/24/UE du Parlement européen et du Conseil ([4]) dans le cadre de l'espace européen des données relatives à la santé, et les actes législatifs pertinents dans le domaine des transports, tels que les règlements (UE) 2019/1239 ([5]) et (UE) 2020/1056 ([6]) et la directive 2010/40/UE ([7]) du Parlement européen et du Conseil dans le cadre de l'espace européen des données relatives à la mobilité.

([4]) Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (JO L 88 du 4.4.2011, p. 45).

([5]) Règlement (UE) 2019/1239 du Parlement européen et du Conseil du 20 juin 2019 établissant un système de guichet unique maritime européen et abrogeant la directive 2010/65/UE (JO L 198 du 25.7.2019, p. 64).

([6]) Règlement (UE) 2020/1056 du Parlement européen et du Conseil du 15 juillet 2020 concernant les informations électroniques relatives au transport de marchandises (JO L 249 du 31.7.2020, p. 33).

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

Le présent règlement devrait par conséquent être sans préjudice des règlements (CE) nº 223/2009 ([8]), (UE) 2018/858 ([9]) et (UE) 2018/1807 ([10]) ainsi que des directives 2000/31/CE ([11]), 2001/29/CE ([12]), 2004/48/CE ([13]), 2007/2/CE ([14]), 2010/40/UE, (UE) 2015/849 ([15]), (UE) 2016/943 ([16]), (UE) 2017/1132 ([17]), (UE) 2019/790 ([18]) et (UE) 2019/1024 ([19]) du Parlement européen et du Conseil et de toute autre disposition du droit sectoriel de l'Union qui régit l'accès aux données et la réutilisation des données. Le présent règlement devrait s'entendre sans préjudice du droit de l'Union et du droit national concernant l'accès aux données et l'utilisation des 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, ainsi qu'aux fins de la coopération internationale dans ce cadre.

Le présent règlement devrait s'entendre sans préjudice des compétences des États membres en ce qui concerne leurs activités relatives à la sécurité publique, à la défense et à la sécurité nationale. La réutilisation des données protégées à de telles fins et détenues par des organismes du secteur public, y compris les données issues des procédures de passation de marchés relevant du champ d'application de la directive 2009/81/CE du Parlement européen et du Conseil ([20]), ne devrait pas être couverte par le présent règlement. Il convient d'instaurer un régime horizontal pour la réutilisation de certaines catégories de données protégées détenues par des organismes du secteur public et pour la fourniture de services d'intermédiation de données et de services fondée sur l'altruisme en matière de données dans l'Union. Les caractéristiques spécifiques des différents secteurs peuvent rendre nécessaire la conception de systèmes sectoriels fondés sur les données, tout en s'appuyant sur les exigences posées par le présent règlement. Les prestataires de services d'intermédiation de données qui satisfont aux exigences fixées dans le présent règlement devraient pouvoir utiliser le label «prestataire de services d'intermédiation de données reconnu dans l'Union». Les personnes morales qui cherchent à promouvoir des objectifs d'intérêt général en mettant à disposition des données pertinentes sur le fondement de l'altruisme en matière de données à la bonne échelle et qui satisfont aux exigences fixées dans le présent règlement devraient pouvoir s'enregistrer en tant que «organisation altruiste en matière de données reconnue dans l'Union» et utiliser ce label. Lorsque le droit sectoriel de l'Union ou le droit sectoriel national impose aux organismes du secteur public, à de tels prestataires de services d'intermédiation de données ou à de telles personnes morales (organisations altruistes en matière de données reconnues) de respecter des exigences techniques, administratives ou organisationnelles particulières supplémentaires, y compris au moyen d'un régime d'autorisation ou de certification, les dispositions du droit sectoriel de l'Union ou du droit sectoriel national devraient également s'appliquer.

([8]) 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).

([9]) Règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) nº 715/2007 et (CE) nº 595/2009 et abrogeant la directive 2007/46/CE (JO L 151 du 14.6.2018, p. 1).

([10]) 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).

([11]) 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).

([12]) 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).

([13]) 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).

([14]) Directive 2007/2/CE du Parlement européen et du Conseil du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE) (JO L 108 du 25.4.2007, p. 1).

([15]) 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) no 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).

([16]) 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).

([17]) Directive (UE) 2017/1132 du Parlement européen et du Conseil du 14 juin 2017 relative à certains aspects du droit des sociétés (JO L 169 du 30.6.2017, p. 46).

([18]) 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).

([19]) 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).

([20]) Directive 2009/81/CE du Parlement européen et du Conseil du 13 juillet 2009 relative à la coordination des procédures de passation de certains marchés de travaux, de fournitures et de services par des pouvoirs adjudicateurs ou entités adjudicatrices dans les domaines de la défense et de la sécurité, et modifiant les directives 2004/17/CE et 2004/18/CE (JO L 216 du 20.8.2009, p. 76).

(4) Le présent règlement devrait s'entendre sans préjudice des règlements (UE) 2016/679 ([21]) et (UE) 2018/1725 ([22]) du Parlement européen et du Conseil et des directives 2002/58/CE ([23]) et (UE) 2016/680 ([24]) du Parlement européen et du Conseil et des dispositions correspondantes du droit national, y compris lorsque les données à caractère personnel et non personnel d'un ensemble de données sont inextricablement liées. En particulier, le présent règlement ne devrait pas être lu comme créant une nouvelle base juridique pour le traitement des données à caractère personnel dans le cadre de l'une des activités réglementées, ni comme modifiant les exigences en matière d'information prévues par le règlement (UE) 2016/679. La mise en œuvre du présent règlement ne devrait pas empêcher les transferts transfrontaliers de données conformément au chapitre V 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 le droit national adopté conformément audit droit de l'Union, le droit de l'Union ou le droit national applicable relatif à la protection des données à caractère personnel devrait prévaloir. Il devrait être possible de considérer les autorités chargées de la protection des données comme des autorités compétentes au titre du présent règlement. Lorsque d'autres autorités agissent comme autorités compétentes au titre du présent règlement, elles devraient agir sans préjudice des pouvoirs de surveillance et des compétences conférés aux autorités chargées de la protection des données au titre du règlement (UE) 2016/679.

(5) Une action au niveau de l'Union est nécessaire pour accroître la confiance dans le partage des données en établissant des mécanismes appropriés permettant aux personnes concernées et aux détenteurs de données d'exercer un contrôle sur les données les concernant, et pour lever les autres obstacles au bon fonctionnement d'une économie fondée sur les données qui soit compétitive. Cette action devrait être sans préjudice des obligations et des engagements prévus dans les accords commerciaux internationaux conclus par l'Union. Un cadre de gouvernance à l'échelle de l'Union devrait avoir pour objectif d'instaurer la confiance entre les personnes physiques et les entreprises en ce qui concerne l'accès aux données, leur contrôle, leur partage, leur utilisation et leur réutilisation, en particulier en concevant des mécanismes appropriés permettant aux personnes concernées de connaître et d'exercer utilement leurs droits, ainsi qu'en ce qui concerne la réutilisation de certains types de données détenues par des organismes du secteur public, la fourniture de services aux personnes concernées, aux détenteurs de données et aux utilisateurs de données par les prestataires de services d'intermédiation de données, ainsi qu'en ce qui concerne la collecte et le traitement des données mises à disposition à des fins altruistes par des personnes physiques et morales. En particulier, une plus grande transparence en ce qui concerne la finalité de l'utilisation des données et les conditions dans lesquelles les données sont stockées par les entreprises peut contribuer à renforcer la confiance.

(6) L'idée selon laquelle les données produites ou collectées par des organismes du secteur public ou d'autres entités aux frais des budgets publics devraient profiter à la société est depuis longtemps présente dans la politique de l'Union. La directive (UE) 2019/1024 et le droit sectoriel de l'Union garantissent que les organismes du secteur public rendent facilement accessibles un volume accru des données qu'ils produisent, à des fins d'utilisation et de réutilisation. Toutefois, il arrive souvent que certaines catégories de données, telles que les données commerciales confidentielles, les données couvertes par le secret statistique et les données protégées par des droits de propriété intellectuelle détenus par des tiers, y compris les secrets d'affaires et les données à caractère personnel, figurant dans des bases de données publiques ne soient pas rendues accessibles, même pour des activités de recherche ou d'innovation relevant de l'intérêt public, bien que cette disponibilité soit possible en vertu du droit de l'Union en vigueur, notamment le règlement (UE) 2016/679 et les directives 2002/58/CE et (UE) 2016/680. En raison du caractère sensible de ces données, certaines exigences procédurales de nature technique et juridique doivent être satisfaites avant leur mise à disposition, en particulier afin de garantir le respect des droits que d'autres personnes détiennent sur ces données ou de limiter les répercussions négatives sur les droits fondamentaux, le principe de non-discrimination et la protection des données. Satisfaire à ces exigences nécessite généralement beaucoup de temps et des connaissances pointues. Cela a conduit à une utilisation insuffisante de ces données. Si certains États membres mettent en place des structures, des processus ou des législations pour faciliter ce type de réutilisation, ce n'est pas le cas dans l'ensemble de l'Union. Afin de faciliter l'utilisation des données par les entités privées et publiques dans le cadre de la recherche et de l'innovation en Europe, il est nécessaire de fixer des conditions claires pour l'accès à ces données et leur utilisation dans l'ensemble de l'Union.

([21]) 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).

([22]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

([23]) 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).

([24]) Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

(7) Il existe des techniques permettant d'effectuer des analyses dans les bases de données contenant des données à caractère personnel, notamment l'anonymisation, la confidentialité différentielle, la généralisation, la suppression et la randomisation, l'utilisation de données synthétiques ou des méthodes similaires, et d'autres méthodes de préservation de la vie privée à la pointe de la technologie, qui pourraient contribuer à un traitement des données plus respectueux de la vie privée. Les États membres devraient aider les organismes du secteur public à exploiter au mieux ces techniques et à mettre ainsi à disposition un maximum de données à partager. L'application de ces techniques, ainsi que d'analyses d'impact globales en matière de protection des données et d'autres garanties, peut contribuer à une plus grande sécurité dans l'utilisation et la réutilisation des données à caractère personnel et devrait garantir la réutilisation sûre des données commerciales confidentielles à des fins de recherche, d'innovation et de statistiques. Dans de nombreux cas, l'application de ces techniques, analyses d'impact et autres garanties suppose que les données ne peuvent être utilisées et réutilisées que dans un environnement de traitement sécurisé qui est fourni ou contrôlé par l'organisme du secteur public. Il existe, au niveau de l'Union, une certaine expérience de tels environnements de traitement sécurisés, qui sont utilisés pour la recherche sur les microdonnées statistiques sur le fondement du règlement (UE) nº 557/2013 de la Commission ([25]). D'une manière générale, dans la mesure où des données à caractère personnel sont concernées, le traitement de telles données devrait se fonder sur une ou plusieurs des bases légales relatives au traitement prévues aux articles 6 et 9 du règlement (UE) 2016/679.

(8) Conformément au règlement (UE) 2016/679, il n'y a pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. La réidentification des personnes concernées à partir d'ensembles de données anonymisées devrait être interdite. Cette interdiction ne devrait pas porter atteinte à la possibilité de mener des recherches sur des techniques d'anonymisation, en particulier en vue de garantir la sécurité des informations, de renforcer les techniques d'anonymisation existantes et de contribuer à la fiabilité générale de l'anonymisation, en conformité avec le règlement (UE) 2016/679.

(9) Afin de faciliter la protection des données à caractère personnel et des données confidentielles et d'accélérer le processus de mise à disposition de ces données en vue de leur réutilisation au titre du présent règlement, les États membres devraient encourager les organismes du secteur public à créer et à mettre à disposition des données conformément au principe d'«ouverture dès la conception et par défaut» visé à l'article 5, paragraphe 2, de la directive (UE) 2019/1024, ainsi qu'à promouvoir la création et l'acquisition de données selon des formats et des structures qui facilitent l'anonymisation à cet égard.

(10) Les catégories de données détenues par des organismes du secteur public qui devraient faire l'objet d'une réutilisation en vertu du présent règlement ne relèvent pas du champ d'application de la directive (UE) 2019/1024, qui exclut les données qui ne sont pas accessibles pour des raisons de confidentialité commerciale ou de secret statistique et les données contenues dans des œuvres ou autres objets pour lesquels des tiers détiennent les droits de propriété intellectuelle. Les données commerciales confidentielles comprennent les données protégées par le secret d'affaires, le savoir-faire protégé et toute autre information dont la divulgation abusive aurait une incidence sur la position sur le marché ou la santé financière de l'entreprise. Le présent règlement devrait s'appliquer aux données à caractère personnel qui ne relèvent pas du champ d'application de la directive (UE) 2019/1024 dans la mesure où les règles d'accès excluent ou limitent l'accès à ces données pour des motifs de protection des données, de protection de la vie privée et d'intégrité de la personne physique, en particulier au regard des règles relatives à la protection des données. La réutilisation de données susceptibles de contenir des secrets d'affaires devrait se faire sans préjudice de la directive (UE) 2016/943, qui fixe le cadre pour l'obtention, l'utilisation ou la divulgation licites des secrets d'affaires.

(11) Le présent règlement ne devrait pas créer une obligation d'autoriser la réutilisation des données détenues par les organismes du secteur public. En particulier, chaque État membre devrait par conséquent pouvoir décider si les données sont rendues accessibles à des fins de réutilisation, y compris en ce qui concerne les finalités et la portée de cet accès. Le présent règlement devrait compléter les obligations plus spécifiques que le droit sectoriel de l'Union ou le droit sectoriel national impose aux organismes du secteur public pour autoriser la réutilisation de données, et il devrait être sans préjudice de ces obligations. L'accès du public aux documents officiels peut être considéré comme étant dans l'intérêt public. Compte tenu du rôle joué par l'accès du public aux documents officiels et par la transparence dans une société démocratique, le présent règlement devrait également être sans préjudice du droit de l'Union ou du droit national relatif à l'octroi de l'accès aux documents officiels et à leur divulgation. L'accès aux documents officiels peut notamment être octroyé conformément au droit national sans imposer de conditions spécifiques ou en imposant des conditions spécifiques qui ne sont pas prévues par le présent règlement.

([25]) Règlement (UE) nº 557/2013 de la Commission du 17 juin 2013 mettant en œuvre le règlement (CE) nº 223/2009 du Parlement européen et du Conseil relatif aux statistiques européennes en ce qui concerne l'accès aux données confidentielles à des fins scientifiques et abrogeant le règlement (CE) nº 831/2002 de la Commission (JO L 164 du 18.6.2013, p. 16).

(12) Le régime de réutilisation prévu par le présent règlement devrait s'appliquer aux données dont la fourniture est une activité qui relève des missions de service public dévolues aux organismes du secteur public concernés en vertu de la loi ou d'autres règles contraignantes en vigueur dans les États membres. En l'absence de telles règles, les missions de service public devraient être définies conformément aux pratiques administratives courantes dans les États membres, sous réserve que l'objet de ces missions soit transparent et soumis à réexamen. Les missions de service public pourraient être définies à titre général ou au cas par cas pour les différents organismes du secteur public. Étant donné que les entreprises publiques ne sont pas couvertes par la définition d'organisme du secteur public, les données que détiennent les entreprises publiques ne devraient pas être couvertes par le présent règlement. Les données détenues par des établissements culturels, tels que les bibliothèques, les archives et les musées ainsi que les orchestres, les opéras, les ballets et les théâtres, et par des établissements d'enseignement ne devraient pas être couvertes par le présent règlement puisque les œuvres et autres documents que détiennent ces établissements sont principalement couverts par des droits de propriété intellectuelle détenus par des tiers. 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.

Le présent règlement devrait s'appliquer à ces organismes hybrides uniquement en leur qualité d'organismes exerçant une activité de recherche. Si un organisme exerçant une activité de recherche détient des données dans le cadre d'une association public-privé spécifique avec des organismes du secteur privé ou d'autres organismes du secteur public, des organismes de droit public ou des organismes hybrides exerçant une activité de recherche, c'est-à-dire organisés soit en tant qu'organismes du secteur public soit en tant qu'entreprises publiques, dans le but principal d'effectuer des recherches, ces données ne devraient pas non plus être couvertes par le présent règlement. Le cas échéant, les États membres devraient pouvoir appliquer le présent règlement aux entreprises publiques ou aux entreprises privées qui exercent des fonctions du secteur public ou fournissent des services d'intérêt général. L'échange de données, effectué exclusivement dans le cadre de leurs missions de service public, entre des organismes du secteur public dans l'Union ou entre des organismes du secteur public dans l'Union et des organismes du secteur public dans des pays tiers ou des organisations internationales, ainsi que l'échange de données entre chercheurs à des fins de recherche scientifique non commerciale, ne devraient pas être soumis aux dispositions du présent règlement concernant la réutilisation de certaines catégories de données protégées détenues par des organismes du secteur public.

(13) Les organismes du secteur public devraient respecter le droit de la concurrence lorsqu'ils établissent les principes régissant la réutilisation des données qu'ils détiennent, en évitant la conclusion d'accords qui pourraient avoir pour objet ou pour effet de créer des droits d'exclusivité pour la réutilisation de certaines données. De tels accords ne devraient être possibles que lorsque cela est justifié et nécessaire en vue de la fourniture d'un service ou d'un produit dans l'intérêt général. Tel peut être le cas lorsque l'utilisation exclusive des données est le seul moyen de maximiser les avantages sociétaux des données en question, par exemple lorsqu'il n'existe qu'une seule entité (spécialisée dans le traitement d'un ensemble de données particulier) capable de fournir le service ou le produit permettant à l'organisme du secteur public de fournir un service ou un produit dans l'intérêt général. De tels accords devraient toutefois être conclus conformément au droit de l'Union ou au droit national applicable et pouvoir faire l'objet d'un réexamen régulier sur la base d'une analyse de marché, afin de déterminer si cette exclusivité reste nécessaire. En outre, ces accords devraient respecter les règles applicables en matière d'aides d'État, le cas échéant, et être conclus pour une durée limitée qui ne devrait pas dépasser douze mois. Dans un souci de transparence, ces accords d'exclusivité devraient être publiés en ligne, sous une forme conforme au droit de l'Union applicable en matière de marchés publics. Lorsqu'un droit d'exclusivité pour la réutilisation des données ne respecte pas le présent règlement, il ne devrait pas être valide.

(14) Lorsqu'ils ont été conclus ou étaient déjà en place avant la date d'entrée en vigueur du présent règlement, les accords d'exclusivité interdits et les autres pratiques ou arrangements portant sur la réutilisation des données détenues par des organismes du secteur public qui ne confèrent pas expressément de droits d'exclusivité mais dont on peut raisonnablement s'attendre à ce qu'ils restreignent la disponibilité des données à des fins de réutilisation ne devraient pas être renouvelés à leur terme. Dans le cas d'accords à durée indéterminée ou à long terme, la résiliation devrait intervenir dans un délai de trente mois à compter de la date d'entrée en vigueur du présent règlement.

(15) Il convient que le présent règlement fixe les conditions de réutilisation des données protégées qui s'appliquent aux organismes du secteur public désignés comme compétents en vertu du droit national pour octroyer ou refuser l'accès à des fins de réutilisation, et qui s'entendent sans préjudice des droits ou obligations concernant l'accès à ces données. Ces conditions devraient être non discriminatoires, transparentes, proportionnées et objectivement justifiées, sans restreindre la concurrence, l'accent étant mis sur la promotion de l'accès à ces données par les PME et les jeunes pousses. Les conditions de réutilisation devraient être conçues de manière à promouvoir la recherche scientifique afin que, par exemple, le fait de privilégier la recherche scientifique puisse en principe être considéré comme non discriminatoire. Les organismes du secteur public autorisant la réutilisation devraient disposer des moyens techniques nécessaires pour assurer la protection des droits et intérêts des tiers et être habilités à demander les informations nécessaires au réutilisateur. Les conditions liées à la réutilisation des données devraient être limitées à ce qui est nécessaire pour préserver les droits et intérêts des tiers à l'égard des données, ainsi que l'intégrité des

systèmes d'information et de communication des organismes du secteur public. Ces derniers devraient appliquer des conditions qui servent au mieux les intérêts du réutilisateur sans entraîner de charge disproportionnée pour les organismes du secteur public. Les conditions liées à la réutilisation des données devraient être conçues de manière à offrir des garanties efficaces en matière de protection des données à caractère personnel. Avant leur transmission, les données à caractère personnel devraient être anonymisées, afin d'empêcher l'identification des personnes concernées, et les données contenant des informations commerciales confidentielles devraient être modifiées de telle sorte qu'aucune information confidentielle ne soit divulguée. Dans le cas où la fourniture de données anonymisées ou modifiées ne permettrait pas de répondre aux besoins du réutilisateur, sous réserve de satisfaire à toutes les exigences découlant des articles 35 et 36 du règlement (UE) 2016/679 qui imposent d'effectuer une analyse d'impact relative à la protection des données et de consulter l'autorité de contrôle, et lorsqu'il a été constaté que les risques pour les droits et les intérêts des personnes concernées sont minimes, la réutilisation des données dans un environnement de traitement sécurisé, sur place ou à distance, pourrait être autorisée.

Il pourrait s'agir d'un arrangement approprié pour la réutilisation des données pseudonymisées. Les analyses de données dans ces environnements de traitement sécurisés devraient être supervisées par l'organisme du secteur public, afin de protéger les droits et intérêts des tiers. En particulier, des données à caractère personnel ne devraient être transmises à un tiers à des fins de réutilisation que lorsqu'une base juridique au titre du droit sur la protection des données autorise une telle transmission. Les données à caractère non personnel ne devraient être transmises que lorsqu'il n'y a aucune raison de penser que la combinaison d'ensembles de données à caractère non personnel conduirait à l'identification des personnes concernées. Cela devrait également s'appliquer aux données pseudonymisées qui conservent leur statut de données à caractère personnel. En cas de réidentification de personnes concernées, une obligation de notifier une telle violation de données à l'organisme du secteur public devrait s'appliquer en plus d'une obligation de notifier cette violation de données à une autorité de contrôle et à la personne concernée conformément au règlement (UE) 2016/679. Le cas échéant, les organismes du secteur public devraient faciliter la réutilisation des données fondée sur le consentement des personnes concernées ou l'autorisation des détenteurs de données quant à la réutilisation des données les concernant, par des moyens techniques appropriés. À cet égard, l'organisme du secteur public devrait tout mettre en oeuvre pour aider les réutilisateurs potentiels à solliciter un tel consentement ou une telle autorisation, en mettant en place des mécanismes techniques permettant la transmission des demandes de consentement ou d'autorisation émanant des réutilisateurs, lorsque cela est réalisable en pratique. Les coordonnées permettant aux utilisateurs de prendre directement contact avec les personnes concernées ou les détenteurs de données ne devraient pas être communiquées. Lorsque l'organisme du secteur public transmet une demande de consentement ou d'autorisation, il devrait veiller à ce que la personne concernée ou le détenteur de données soit clairement informé de la possibilité de refuser de donner son consentement ou son autorisation.

(16) Afin de faciliter et d'encourager l'utilisation des données détenues par des organismes du secteur public à des fins de recherche scientifique, ces organismes sont encouragés à élaborer une approche harmonisée et des procédures harmonisées pour rendre ces données facilement accessibles aux fins de la recherche scientifique dans l'intérêt public. Il pourrait s'agir, entre autres, de mettre en place des procédures administratives rationalisées, des formats de données normalisés, des métadonnées informatives sur les choix méthodologiques et les choix en matière de collecte de données, ainsi que des champs de données normalisés qui permettent de chainer aisément des ensembles de données provenant de différentes sources de données du secteur public, lorsque cela est pertinent à des fins d'analyse. L'objectif de ces pratiques devrait être de promouvoir des données financées et produites par les pouvoirs publics à des fins de recherche scientifique, conformément au principe «aussi ouvert que possible, aussi fermé que nécessaire».

(17) Le présent règlement ne devrait pas porter atteinte aux droits de propriété intellectuelle détenus par des tiers. Le présent règlement ne devrait pas non plus porter atteinte à l'existence des droits de propriété intellectuelle des organismes du secteur public ou à la qualité de titulaires de droits de propriété intellectuelle de ces organismes, de même qu'il ne devrait restreindre en aucune manière l'exercice de ces droits. Les obligations imposées conformément au présent règlement ne devraient s'appliquer que dans la mesure où elles sont compatibles avec les accords internationaux sur la protection des droits de propriété intellectuelle, notamment la convention de Berne pour la protection des œuvres littéraires et artistiques (convention de Berne), l'accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (accord sur les ADPIC) et le traité de l'Organisation mondiale de la propriété intellectuelle sur le droit d'auteur (WCT), ainsi qu'avec le droit de la propriété intellectuelle de l'Union ou national. Les organismes du secteur public devraient, toutefois, exercer leurs droits d'auteur d'une manière qui facilite la réutilisation des données.

(18) Les données faisant l'objet de droits de propriété intellectuelle ainsi que les secrets d'affaires ne devraient être transmis à un tiers que si cette transmission est licite en vertu du droit de l'Union ou du droit national ou avec l'accord du titulaire des droits. Lorsque les organismes du secteur public sont titulaires du droit du fabricant d'une base de données prévu à l'article 7, paragraphe 1, de la directive 96/9/CE du Parlement européen et du Conseil ([26]), ils ne devraient pas exercer ce droit dans le but de prévenir la réutilisation de données ou de restreindre la réutilisation au-delà des limites fixées par le présent règlement.

([26]) 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).

(19) Les entreprises et les personnes concernées devraient pouvoir avoir la certitude que la réutilisation de certaines catégories de données protégées qui sont détenues par les organismes du secteur public se fera dans le respect de leurs droits et intérêts. Des garanties supplémentaires devraient dès lors être mises en place pour les situations dans lesquelles la réutilisation de telles données du secteur public a lieu sur la base d'un traitement des données en dehors du secteur public, comme l'obligation pour les organismes du secteur public de veiller à ce que les droits et intérêts des personnes physiques et morales soient pleinement protégés, en particulier en ce qui concerne les données à caractère personnel, les données commercialement sensibles et les droits de propriété intellectuelle, dans tous les cas, y compris lorsque ces données sont transférées vers des pays tiers. Les organismes du secteur public ne devraient pas autoriser la réutilisation des informations stockées dans les applications de santé en ligne par des entreprises d'assurance ou tout autre prestataire de services à des fins de discrimination dans la fixation des prix, car cela irait à l'encontre du droit fondamental d'accès aux soins de santé.

(20) En outre, afin de préserver une concurrence loyale et une économie de marché ouverte, il est de la plus haute importance de préserver les données protégées à caractère non personnel, en particulier les secrets d'affaires, mais aussi les données à caractère non personnel représentant des contenus protégés par des droits de propriété intellectuelle, contre tout accès illicite susceptible de conduire à un vol de propriété intellectuelle ou à de l'espionnage industriel. Afin de garantir la protection des droits ou des intérêts des détenteurs de données, il devrait être possible de transférer les données à caractère non personnel qui doivent être protégées contre un accès illicite ou non autorisé conformément au droit de l'Union ou au droit national et qui sont détenues par des organismes du secteur public vers des pays tiers, mais uniquement lorsque des garanties appropriées sont prévues pour l'utilisation des données. Parmi ces garanties appropriées devrait figurer l'obligation pour l'organisme du secteur public de ne transmettre des données protégées à un réutilisateur que si ledit réutilisateur prend des engagements contractuels dans l'intérêt de la protection des données. Un réutilisateur ayant l'intention de transférer les données protégées vers un pays tiers devrait respecter les obligations prévues dans le présent règlement, même après le transfert des données vers le pays tiers. Afin de garantir la bonne exécution de ces obligations, le réutilisateur devrait également admettre, pour le règlement judiciaire des litiges, la compétence de l'État membre de l'organisme du secteur public qui a autorisé la réutilisation.

(21) La mise en place de garanties appropriées devrait également être envisagée lorsque, dans le pays tiers vers lequel des données à caractère non personnel sont transférées, il existe des mesures équivalentes garantissant que les données bénéficient d'un niveau de protection similaire à celui qui est applicable en vertu du droit de l'Union, notamment en ce qui concerne la protection des secrets d'affaires et les droits de propriété intellectuelle. À cette fin, la Commission devrait pouvoir déclarer, par voie d'actes d'exécution, lorsque cela est justifié en raison d'un grand nombre de demandes dans l'ensemble de l'Union concernant la réutilisation de données à caractère non personnel dans des pays tiers déterminés, qu'un pays tiers offre un niveau de protection essentiellement équivalent à celui prévu par le droit de l'Union. La Commission devrait évaluer la nécessité de tels actes d'exécution sur la base des informations fournies par les États membres par l'intermédiaire du comité européen de l'innovation dans le domaine des données. De tels actes d'exécution permettraient de garantir aux organismes du secteur public que la réutilisation, dans le pays tiers concerné, de données détenues par les organismes du secteur public ne risque pas de compromettre la nature protégée de ces données. Pour évaluer le niveau de protection offert dans le pays tiers concerné, il convient en particulier de prendre en considération le droit général et sectoriel applicable, y compris en matière de sécurité publique, de défense, de sécurité nationale et de droit pénal, en ce qui concerne l'accès aux données à caractère non personnel et à leur protection, tout accès par les organismes du secteur public de ce pays tiers aux données transférées, l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes qui sont chargées dans le pays tiers de veiller au respect du régime juridique garantissant l'accès à ces données et de le faire appliquer, les engagements internationaux pris par le pays tiers concerné en ce qui concerne la protection des données, ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants ainsi que de la participation à des systèmes multilatéraux ou régionaux.

L'existence de voies de droit effectives pour les détenteurs de données, les organismes du secteur public ou les prestataires de services d'intermédiation de données dans le pays tiers concerné revêt une importance particulière dans le contexte du transfert de données à caractère non personnel vers ce pays tiers. Ces garanties devraient donc inclure l'existence de droits opposables et de voies de droit effectives. Ces actes d'exécution devraient être sans préjudice de toute obligation juridique déjà contractée ou de tout arrangement contractuel déjà pris par un réutilisateur dans l'intérêt de la protection des données à caractère non personnel, en particulier des données industrielles, et du droit des organismes du secteur public d'obliger les réutilisateurs à respecter les conditions de réutilisation, conformément au présent règlement.

(22) Certains pays tiers adoptent des lois, des règlements et d'autres actes juridiques qui visent à transférer directement des données à caractère non personnel dans l'Union, ou à donner aux pouvoirs publics l'accès à de telles données, sous le contrôle de personnes physiques et morales relevant de la juridiction des États membres. Les décisions de juridictions de pays tiers ou les décisions d'autorités administratives de pays tiers qui exigent un tel transfert de données à caractère non personnel ou un accès à de telles données devraient être exécutoires lorsqu'elles sont fondées sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre. Dans certains cas, il peut arriver que l'obligation, découlant du droit d'un pays tiers, de transférer des données à caractère non personnel ou de donner accès à de telles données soit incompatible avec une obligation

concurrente de protéger ces données en vertu du droit de l'Union ou du droit national, en particulier en ce qui concerne la protection des droits fondamentaux des personnes physiques ou des intérêts fondamentaux d'un État membre en matière de sécurité nationale ou de défense, ainsi que la protection des données commercialement sensibles et la protection des droits de propriété intellectuelle, y compris les engagements contractuels pris en matière de confidentialité conformément à ce droit. En l'absence d'accords internationaux régissant ces questions, il convient de n'autoriser le transfert de données à caractère non personnel ou l'accès à de telles données que si, en particulier, il a été vérifié que le système juridique du pays tiers exige que les motifs et la proportionnalité de la décision judiciaire ou administrative soient exposés, que la décision judiciaire ou administrative a un caractère spécifique et que l'objection motivée du destinataire peut faire l'objet d'un réexamen dans le pays tiers par une juridiction compétente habilitée à tenir dûment compte des intérêts juridiques pertinents du fournisseur de ces données.

En outre, les organismes du secteur public, les personnes physiques ou morales auxquelles le droit de réutilisation des données a été accordé, les prestataires de services d'intermédiation de données et les organisations altruistes en matière de données reconnues devraient veiller, lorsqu'ils signent des accords contractuels avec d'autres parties privées, à ce que les données à caractère non personnel détenues dans l'Union ne soient accessibles dans des pays tiers ou transférées vers des pays tiers que conformément au droit de l'Union ou au droit national de l'État membre concerné.

(23) Pour renforcer la confiance dans l'économie des données de l'Union, il est essentiel de veiller à ce que les garanties permettant aux citoyens, au secteur public et aux entreprises de l'Union d'exercer un contrôle sur leurs données stratégiques et sensibles soient appliquées, et à ce que le droit, les valeurs et les normes de l'Union en matière, entre autres, de sécurité, de protection des données et de protection des consommateurs, soient respectés. Afin d'empêcher un accès illicite à des données à caractère non personnel, les organismes du secteur public, les personnes physiques ou morales auxquelles le droit de réutilisation des données a été accordé, les prestataires de services d'intermédiation de données et les organisations altruistes en matière de données reconnues devraient prendre toutes les mesures raisonnables pour empêcher l'accès aux systèmes dans lesquels des données à caractère non personnel sont stockées, y compris le cryptage des données ou des politiques internes. À cette fin, il convient de veiller à ce que les organismes du secteur public, les personnes physiques ou morales auxquelles le droit de réutilisation des données a été accordé, les prestataires de services d'intermédiation de données et les organisations altruistes en matière de données reconnues respectent l'ensemble des normes techniques, codes de conduite et certifications pertinents au niveau de l'Union.

(24) Afin de développer la confiance dans les mécanismes de réutilisation, il peut être nécessaire d'assortir de conditions plus strictes certains types de données à caractère non personnel dont le caractère hautement sensible peut être reconnu dans des actes législatifs spécifiques futurs de l'Union, en ce qui concerne le transfert vers des pays tiers, si un tel transfert risque de compromettre des objectifs de politique publique de l'Union, conformément aux engagements internationaux. Par exemple, dans le domaine de la santé, certains ensembles de données détenus par des acteurs du système de santé publique, tels que les hôpitaux publics, pourraient être reconnus comme des données relatives à la santé hautement sensibles. Parmi les autres secteurs concernés figurent les transports, l'énergie, l'environnement et la finance. Afin de garantir l'harmonisation des pratiques dans l'ensemble de l'Union, ces types de données publiques à caractère non personnel hautement sensibles devraient être définis par le droit de l'Union, par exemple dans le cadre de l'espace européen des données relatives à la santé ou d'autres dispositions du droit sectoriel. Ces conditions liées au transfert de telles données vers des pays tiers devraient être fixées dans des actes délégués. Elles devraient être proportionnées, non discriminatoires et nécessaires pour protéger des objectifs légitimes de politique publique de l'Union déterminés, tels que la protection de la santé publique, la sécurité, l'environnement, la moralité publique, la protection des consommateurs, la protection de la vie privée et la protection des données à caractère personnel. Les conditions devraient correspondre aux risques mis en évidence en ce qui concerne la sensibilité de ces données, y compris le risque de réidentification des personnes physiques. Ces conditions pourraient comprendre des conditions applicables au transfert ou des arrangements techniques, tels que l'obligation d'utiliser un environnement de traitement sécurisé, des limitations en ce qui concerne la réutilisation des données dans des pays tiers ou les catégories de personnes habilitées à transférer ces données vers des pays tiers ou pouvant y avoir accès dans des pays tiers. Dans des cas exceptionnels, ces conditions pourraient également inclure des restrictions au transfert des données vers des pays tiers afin de protéger l'intérêt public.

(25) Les organismes du secteur public devraient avoir la possibilité de percevoir des redevances pour la réutilisation des données, mais aussi d'autoriser la réutilisation de ces données moyennant le paiement d'une redevance réduite ou gratuitement, par exemple pour certaines catégories de réutilisation telles que la réutilisation à des fins non commerciales ou à des fins de recherche scientifique, ou la réutilisation par les PME et les jeunes pousses, la société civile et les établissements d'enseignement, de manière à inciter à cette réutilisation pour stimuler la recherche et l'innovation et soutenir des entreprises qui représentent une source importante d'innovation et ont généralement plus de difficultés à collecter elles-mêmes des données pertinentes, conformément aux règles en matière d'aides d'État. Dans ce contexte spécifique, les finalités liées à la recherche scientifique devraient s'entendre comme incluant

tout type d'objectif en rapport avec la recherche, quelle que soit la structure organisationnelle ou financière de l'organisme de recherche concerné, à l'exception de la recherche menée par une entreprise ayant pour but la mise au point, l'amélioration ou l'optimisation de produits ou de services. Ces redevances devraient être transparentes, non discriminatoires et limitées aux coûts nécessaires supportés et ne devraient pas restreindre la concurrence. Il convient de rendre publique une liste des catégories de réutilisateurs pour lesquels des redevances réduites ou nulles s'appliquent, assortie des critères utilisés pour établir cette liste.

(26) Afin d'inciter à la réutilisation de ces catégories de données spécifiques détenues par des organismes du secteur public, les États membres devraient créer un point d'information unique servant d'interface pour les réutilisateurs qui souhaitent réutiliser ces données. Ses attributions devraient s'étendre à plusieurs secteurs et compléter, si nécessaire, les dispositions prises au niveau sectoriel. Le point d'information unique devrait pouvoir s'appuyer sur des moyens automatisés lorsqu'il transmet des demandes d'information ou des demandes de réutilisation. Un contrôle humain suffisant devrait être assuré pendant le processus de transmission. À cette fin, les modalités pratiques existantes, telles que les portails des données ouvertes, pourraient être utilisées. Le point d'information unique devrait disposer d'une liste de ressources comprenant un aperçu de toutes les ressources en données disponibles, y compris, le cas échéant, les ressources en données qui sont disponibles dans les points d'information sectoriels, régionaux ou locaux, ainsi que les informations pertinentes décrivant les données disponibles. En outre, les États membres devraient désigner, établir ou contribuer à établir des organismes compétents pour soutenir les activités des organismes du secteur public autorisant la réutilisation de certaines catégories de données protégées. L'une des tâches qui leur sont confiées peut être d'octroyer l'accès aux données, lorsque le droit sectoriel de l'Union ou le droit sectoriel national l'exige. Ces organismes compétents devraient fournir une assistance aux organismes du secteur public en recourant à des techniques de pointe, notamment en ce qui concerne la meilleure manière de structurer et de stocker les données en vue de les rendre facilement accessibles, en particulier au moyen d'interfaces de programmation d'applications, et de rendre les données interopérables, transférables et interrogeables, en tenant compte des meilleures pratiques en matière de traitement des données et de toutes les normes réglementaires et techniques existantes ainsi que des environnements sécurisés pour le traitement des données, qui permettent l'analyse des données d'une manière qui préserve le caractère privé des informations.

Les organismes compétents devraient agir conformément aux instructions reçues de l'organisme du secteur public. Une telle structure d'assistance pourrait aider les personnes concernées et les détenteurs de données dans la gestion du consentement ou de l'autorisation de réutilisation, y compris en ce qui concerne le consentement et l'autorisation relatifs à certains domaines de la recherche scientifique, dans le respect des normes éthiques reconnues en matière de recherche scientifique. Les organismes compétents ne devraient pas avoir de fonction de contrôle, celle-ci étant réservée aux autorités de contrôle au titre du règlement (UE) 2016/679. Sans préjudice des pouvoirs de contrôle conférés aux autorités chargées de la protection des données, le traitement des données devrait être réalisé sous la responsabilité de l'organisme du secteur public responsable du registre contenant les données, qui reste un responsable du traitement des données tel qu'il est défini dans le règlement (UE) 2016/679 en ce qui concerne les données à caractère personnel. Les États membres devraient pouvoir se doter d'un ou de plusieurs organismes compétents, qui pourraient agir dans différents secteurs. Les services internes des organismes du secteur public pourraient également faire office d'organismes compétents. Un organisme compétent pourrait être un organisme du secteur public qui aide d'autres organismes du secteur public à autoriser la réutilisation de données, le cas échéant, ou un organisme du secteur public autorisant lui-même la réutilisation. L'assistance apportée à d'autres organismes du secteur public devrait impliquer de les informer, sur demande, des meilleures pratiques concernant la manière de satisfaire aux exigences prévues par le présent règlement, par exemple en ce qui concerne les moyens techniques permettant de mettre à disposition un environnement de traitement sécurisé ou de garantir le respect de la vie privée et la confidentialité lorsqu'un accès est donné pour la réutilisation des données relevant du champ d'application du présent règlement.

(27) Les services d'intermédiation de données sont appelés à jouer un rôle essentiel dans l'économie des données, notamment en soutenant et en promouvant les pratiques volontaires de partage de données entre les entreprises, ou en facilitant le partage de données dans le cadre des obligations fixées par le droit de l'Union ou le droit national. Ils pourraient devenir un outil facilitant l'échange de quantités substantielles de données pertinentes. Les prestataires de services d'intermédiation de données, lesquels peuvent comprendre des organismes du secteur public, qui proposent des services mettant en relation les différents acteurs contribuent potentiellement à la mise en commun efficace des données ainsi qu'à la facilitation du partage bilatéral des données. Les services d'intermédiation de données spécialisés qui sont indépendants des personnes concernées, des détenteurs de données et des utilisateurs de données pourraient jouer un rôle de facilitation dans l'émergence de nouveaux écosystèmes fondés sur les données qui soient indépendants de tout acteur jouissant d'une puissance significative sur le marché, tout en permettant un accès non discriminatoire à l'économie des données pour les entreprises de toutes tailles, notamment les PME et les jeunes pousses disposant de moyens financiers, juridiques ou administratifs limités. Cela revêtira une importance particulière dans la perspective de la création d'espaces européens communs de données, c'est-à-dire de cadres interopérables spécifiques à chaque finalité ou à chaque secteur ou transsectoriels de normes et de pratiques communes 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. Les services d'intermédiation de données pourraient inclure le partage bilatéral ou multilatéral de données ou la création de plateformes ou de bases de données permettant l'échange ou l'exploitation conjointe de données, ainsi que la mise en place d'une infrastructure spécifique pour l'interconnexion des personnes concernées et des détenteurs de données avec les utilisateurs de données.

(28) Le présent règlement devrait concerner les services qui visent à établir, par des moyens techniques, juridiques ou autres, des relations commerciales à des fins de partage de données entre un nombre indéterminé de personnes concernées et de détenteurs de données, d'une part, et des utilisateurs de données, d'autre part, y compris aux fins de l'exercice des droits des personnes concernées à l'égard des données à caractère personnel. Lorsque des entreprises ou autres entités proposent de multiples services liés aux données, seules les activités qui concernent directement la fourniture de services d'intermédiation de données devraient être couvertes par le présent règlement. La fourniture de services de stockage en nuage, d'analyse, de logiciels de partage de données, de navigateurs internet, de modules d'extension de navigateurs ou de services de messagerie électronique ne devrait pas être considérée comme une fourniture de services d'intermédiation de données au sens du présent règlement, à condition que ces services ne fournissent que des outils techniques permettant aux personnes concernées ou aux détenteurs de données de partager des données avec d'autres personnes, mais que la fourniture de tels outils ne vise ni à établir une relation commerciale entre les détenteurs de données et les utilisateurs de données, ni à permettre au prestataire de services d'intermédiation de données d'obtenir des informations sur l'établissement de relations commerciales à des fins de partage de données. Parmi les exemples de services d'intermédiation de données figurent les places de marché de données sur lesquelles les entreprises pourraient mettre des données à la disposition de tiers, les maîtres d'œuvre d'écosystèmes de partage de données ouverts à toutes les parties intéressées, par exemple dans le cadre d'espaces européens communs de données, ainsi que les réserves de données mises en place conjointement par plusieurs personnes morales ou physiques dans le but de concéder à toutes les parties intéressées des licences d'utilisation de ces réserves de données, de façon à ce que tous les participants qui contribuent aux réserves de données reçoivent une contrepartie pour leur contribution.

En seraient exclus les services qui obtiennent des données auprès des détenteurs de données et les agrègent, les enrichissent ou les transforment afin d'en accroître substantiellement la valeur et concèdent une licence d'utilisation des données résultantes aux utilisateurs de données, sans établir de relation commerciale entre les détenteurs de données et les utilisateurs de données. Seraient également exclus les services qui sont à l'usage exclusif d'un seul détenteur de données pour lui permettre d'utiliser les données qu'il détient, ou qui sont utilisés par des personnes morales multiples au sein d'un groupe fermé, y compris dans le cadre de relations de fournisseur ou de client ou de collaborations établies par contrat, en particulier ceux qui ont pour principal objectif de garantir les fonctionnalités d'objets et de dispositifs connectés à l'internet des objets.

(29) Les services axés sur l'intermédiation de contenus protégés par le droit d'auteur, tels que les fournisseurs de services de partage de contenus en ligne au sens de l'article 2, point 6), de la directive (UE) 2019/790, ne devraient pas être couverts par le présent règlement. Les fournisseurs de système consolidé de publication, définis à l'article 2, paragraphe 1, point 35), du règlement (UE) nº 600/2014 du Parlement européen et du Conseil ([27]) et les prestataires de services d'information sur les comptes définis à l'article 4, point 19), de la directive (UE) 2015/2366 du Parlement européen et du Conseil ([28]), ne devraient pas être considérés comme des prestataires de services d'intermédiation de données aux fins du présent règlement. Le présent règlement ne devrait pas s'appliquer aux services proposés par des organismes du secteur public afin de faciliter soit la réutilisation de données protégées détenues par les organismes du secteur public conformément au présent règlement, soit l'utilisation de toute autre donnée, dans la mesure où ces services ne visent pas à établir de relations commerciales. Les organisations altruistes en matière de données qui sont régies par le présent règlement ne devraient pas être considérées comme proposant des services d'intermédiation de données, pour autant que ces services n'établissent pas de relation commerciale entre les utilisateurs potentiels des données, d'une part, et les personnes concernées et les détenteurs de données qui mettent des données à disposition à des fins altruistes, d'autre part. D'autres services qui ne visent pas à établir des relations commerciales, tels que les référentiels visant à permettre la réutilisation des données de la recherche scientifique conformément aux principes du libre accès, ne devraient pas être considérés comme des services d'intermédiation de données au sens du présent règlement.

(30) Les prestataires de services qui proposent leurs services à des personnes concernées constituent une catégorie spécifique de prestataires de services d'intermédiation de données. Ces prestataires de services d'intermédiation de données cherchent à renforcer la capacité d'action des personnes concernées, et plus particulièrement le contrôle qu'exercent les personnes physiques sur les données les concernant. Ces prestataires devraient aider les personnes physiques à exercer leurs droits au titre du règlement (UE) 2016/679, notamment l'octroi et le retrait de leur consentement au traitement des données, le droit d'accès à leurs propres données, le droit de rectification des données à caractère personnel inexactes, le droit à l'effacement ou droit «à l'oubli», le droit à la limitation du traitement, et le droit à la portabilité des données qui permet aux personnes concernées de transférer leurs données à caractère personnel d'un responsable du traitement des données à un autre. Dans ce contexte, il importe que le modèle commercial de ces prestataires garantisse qu'il n'existe pas d'incitations inadaptées poussant les personnes physiques à recourir à de tels services pour mettre à disposition, en vue d'un traitement, davantage de données les concernant qu'elles ne devraient le faire dans leur intérêt. Les prestataires pourraient notamment conseiller les personnes physiques sur les utilisations potentielles de leurs données et pratiquer des contrôles de diligence raisonnable à l'égard des utilisateurs de données avant de les autoriser à contacter les personnes concernées, afin d'éviter des pratiques frauduleuses. Dans certaines circonstances, il pourrait être souhaitable de compiler des données réelles dans un espace de données à caractère personnel, de telle sorte que le traitement puisse avoir lieu dans cet espace sans que les données à caractère personnel soient transmises à des tiers, afin d'assurer une protection maximale des données à caractère personnel et de la vie privée. Ces espaces de données à caractère

([27]) Règlement (UE) nº 600/2014 du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant le règlement (UE) nº 648/2012 (JO L 173 du 12.6.2014, p. 84).

([28]) Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) nº 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35).

personnel pourraient contenir des données à caractère personnel statiques, telles que le nom, l'adresse ou la date de naissance, ainsi que des données dynamiques qu'une personne physique génère, par exemple, lorsqu'elle recourt à un service en ligne ou à un objet connecté à l'internet des objets. Ils pourraient aussi être utilisés pour stocker des données d'identification vérifiées telles que le numéro de passeport ou les informations relatives à la sécurité sociale, ainsi que des justificatifs tels que permis de conduire, diplômes ou coordonnées de compte bancaire.

(31) Les coopératives de données visent à atteindre un certain nombre d'objectifs, et notamment à renforcer la position des personnes physiques en leur permettant de faire des choix en connaissance de cause avant de donner leur consentement à l'utilisation des données, en influant sur les conditions et modalités appliquées par les organisations d'utilisateurs de données à l'utilisation des données d'une manière qui offre de meilleurs choix aux membres individuels du groupe ou en trouvant, le cas échéant, des solutions aux conflits de positions des membres individuels d'un groupe sur la manière d'utiliser les données lorsque celles-ci portent sur plusieurs personnes concernées au sein de ce groupe. Dans ce contexte, il importe de tenir compte du fait que les droits consacrés par le règlement (UE) 2016/679 sont des droits personnels de la personne concernée et que les personnes concernées ne peuvent y renoncer. Les coopératives de données pourraient également constituer un outil utile pour les entreprises unipersonnelles et les PME, qui sont souvent comparables à des personnes physiques en termes de connaissance du partage des données.

(32) Afin d'accroître la confiance dans ces services d'intermédiation de données, notamment en ce qui concerne l'utilisation des données et le respect des conditions imposées par les personnes concernées et les détenteurs de données, il est nécessaire de créer un cadre réglementaire à l'échelle de l'Union qui fixe des exigences largement harmonisées concernant la prestation fiable de ces services d'intermédiation de données et qui soit mis en œuvre par les autorités compétentes. Ce cadre contribuera à renforcer le contrôle que les personnes concernées et les détenteurs de données ainsi que les utilisateurs de données exercent sur l'accès à leurs données et sur l'utilisation de celles-ci, conformément au droit de l'Union. La Commission pourrait également encourager et faciliter l'élaboration de codes de conduite au niveau de l'Union, en associant les parties prenantes concernées, en particulier en ce qui concerne l'interopérabilité. Tant dans les situations où le partage de données intervient entre entreprises que dans celles où il intervient entre entreprises et consommateurs, les prestataires de services d'intermédiation de données devraient proposer une nouvelle gouvernance des données «à l'européenne», en prévoyant une séparation, dans l'économie des données, entre fourniture, intermédiation et utilisation des données. Les prestataires de services d'intermédiation de données pourraient également mettre à disposition une infrastructure technique spécifique pour l'interconnexion des personnes concernées et des détenteurs de données avec les utilisateurs de données. À cet égard, il est particulièrement important de façonner cette infrastructure de telle sorte que les PME et les jeunes pousses ne rencontrent aucune barrière technique ni d'autres barrières à leur participation à l'économie des données.

Les prestataires de services d'intermédiation de données devraient être autorisés à fournir, aux détenteurs de données ou aux personnes concernées, des outils et services spécifiques supplémentaires visant spécifiquement à faciliter l'échange de données, tels que le stockage temporaire, l'organisation, la conversion, l'anonymisation et la pseudonymisation. Ces outils et services ne devraient être utilisés qu'à la demande expresse ou que moyennant l'approbation expresse du détenteur de données ou de la personne concernée et les outils de tiers proposés dans ce contexte ne devraient pas utiliser les données à d'autres fins. Parallèlement, les prestataires de services d'intermédiation de données devraient être autorisés à apporter des adaptations aux données échangées afin d'améliorer la facilité d'utilisation des données par l'utilisateur de données, si ce dernier le souhaite, ou d'améliorer l'interopérabilité, par exemple en convertissant les données dans des formats spécifiques.

(33) Il est important de favoriser un environnement compétitif pour le partage des données. La neutralité des prestataires de services d'intermédiation de données à l'égard des données échangées entre les détenteurs de données ou les personnes concernées et les utilisateurs de données est fondamentale pour renforcer la confiance et accroître le contrôle des détenteurs de données, des personnes concernées et des utilisateurs de données à l'égard des services d'intermédiation de données. Il est donc nécessaire que les prestataires de services d'intermédiation de données agissent uniquement en tant qu'intermédiaires dans les transactions, et qu'ils n'utilisent les données échangées à aucune autre fin. Les conditions commerciales, y compris la tarification, pour la fourniture de services d'intermédiation de données ne devraient pas dépendre du fait qu'un détenteur ou un utilisateur potentiel de données utilise d'autres services fournis par le même prestataire de services d'intermédiation de données ou par une entité liée à lui, notamment le stockage, l'analyse, l'intelligence artificielle ou d'autres applications fondées sur les données, ni, le cas échéant, de la mesure dans laquelle le détenteur de données ou l'utilisateur de données utilise ces autres services. Cela nécessitera également une séparation structurelle entre le service d'intermédiation de données et tout autre service fourni, afin d'éviter des conflits d'intérêts. Cela signifie que le service d'intermédiation de données devrait être fourni par une personne morale distincte des autres activités dudit prestataire de services d'intermédiation de données. Toutefois, les prestataires de services d'intermédiation de données devraient pouvoir utiliser les données fournies par le détenteur de données pour améliorer leurs services d'intermédiation de données.

Les prestataires de services d'intermédiation de données ne devraient être en mesure de mettre à la disposition des détenteurs de données, des personnes concernées ou des utilisateurs de données leurs propres outils ou les outils de tiers aux fins de faciliter l'échange de données, tels que des outils de conversion ou d'organisation de données, qu'à la demande expresse ou que moyennant l'approbation expresse de la personne concernée ou du détenteur de données. Les outils de tiers proposés dans ce contexte ne devraient pas utiliser les données à des fins autres que celles liées aux

services d'intermédiation de données. Les prestataires de services d'intermédiation de données agissant en tant qu'intermédiaires dans l'échange de données entre des personnes physiques qui sont des personnes concernées et des personnes morales qui sont des utilisateurs de données devraient, en outre, assumer un devoir de loyauté à l'égard des personnes physiques, pour garantir qu'ils agissent au mieux des intérêts des personnes concernées. Les questions de responsabilité pour tous les dommages et préjudices matériels et immatériels résultant d'un comportement du prestataire de services d'intermédiation de données pourraient être traitées dans le contrat concerné, sur la base des régimes nationaux en matière de responsabilité.

(34) Les prestataires de services d'intermédiation de données devraient prendre des mesures raisonnables pour assurer l'interopérabilité au sein d'un secteur et entre les différents secteurs afin d'assurer le bon fonctionnement du marché intérieur. Parmi les mesures raisonnables pourrait figurer le respect des normes en vigueur et couramment mises en œuvre dans le secteur dans lequel les prestataires de services d'intermédiation de données exercent leurs activités. Le comité européen de l'innovation dans le domaine des données devrait faciliter l'émergence de normes industrielles supplémentaires, si nécessaire. Les prestataires de services d'intermédiation de données devraient, en temps utile, mettre en œuvre les mesures d'interopérabilité entre les services d'intermédiation de données adoptées par le comité européen de l'innovation dans le domaine des données.

(35) Le présent règlement est sans préjudice de l'obligation qui est faite aux prestataires de services d'intermédiation de données de respecter le règlement (UE) 2016/679 et de la responsabilité qui incombe aux autorités de contrôle de veiller au respect dudit règlement. Lorsque les prestataires de services d'intermédiation de données traitent des données à caractère personnel, le présent règlement ne devrait pas avoir d'incidence sur la protection de ces données. Lorsque les prestataires de services d'intermédiation de données sont des responsables du traitement ou des sous-traitants au sens du règlement (UE) 2016/679, ils sont liés par les règles prévues dans ledit règlement.

(36) Les prestataires de services d'intermédiation de données devraient avoir mis en place des procédures et des mesures pour sanctionner les pratiques frauduleuses ou abusives en lien avec des parties qui cherchent à obtenir un accès par le biais des services d'intermédiation de données qu'ils proposent, y compris des mesures telles que l'exclusion des utilisateurs de données qui enfreignent les conditions de service ou le droit en vigueur.

(37) Les prestataires de services d'intermédiation de données devraient également prendre des mesures pour veiller au respect du droit de la concurrence et avoir mis en place des procédures à cette fin. Cela vaut en particulier dans les situations où le partage de données permet aux entreprises de prendre connaissance des stratégies de marché de leurs concurrents réels ou potentiels. Parmi ces informations sensibles sous l'angle de la concurrence, on trouve généralement des informations sur les données relatives aux clients, les prix futurs, les coûts de production, les quantités, les chiffres d'affaires, les ventes ou les capacités.

(38) Une procédure de notification pour les services d'intermédiation de données devrait être mise en place afin de garantir que la gouvernance des données au sein de l'Union est fondée sur un échange de données digne de confiance. Le meilleur moyen de tirer avantage d'un environnement digne de confiance serait d'imposer un certain nombre d'exigences pour la fourniture de services d'intermédiation de données sans pour autant qu'une décision expresse ou un acte administratif ne soient exigés de l'autorité compétente en matière de services d'intermédiation de données pour la fourniture de tels services. La procédure de notification ne devrait pas créer d'obstacles injustifiés pour les PME, les jeunes pousses et les organisations de la société civile et elle devrait respecter le principe de non-discrimination.

(39) Afin de favoriser l'efficacité de la prestation transfrontalière de services, le prestataire de services d'intermédiation de données devrait être invité à envoyer une notification uniquement à l'autorité compétente en matière de services d'intermédiation de données de l'État membre dans lequel est situé son établissement principal ou dans lequel se trouve son représentant légal. Une telle notification ne devrait nécessiter qu'une simple déclaration de l'intention de proposer de tels services, assortie uniquement de la mise à disposition des informations énoncées dans le présent règlement. Après la notification concernée, le prestataire de services d'intermédiation de données devrait être en mesure de commencer ses activités dans tout État membre sans autre obligation de notification.

(40) La procédure de notification prévue par le présent règlement devrait s'entendre sans préjudice des règles spécifiques complémentaires applicables à la fourniture de services d'intermédiation de données en vertu du droit sectoriel.

(41) L'établissement principal d'un prestataire de services d'intermédiation de données dans l'Union devrait être le lieu de son administration centrale dans l'Union. L'établissement principal d'un prestataire de services d'intermédiation de données dans l'Union devrait être déterminé conformément à des critères objectifs et impliquer l'exercice effectif et réel d'activités de gestion. Les activités d'un prestataire de services d'intermédiation de données devraient respecter le droit national de l'État membre dans lequel il a son établissement principal.

(42) Afin de garantir le respect par les prestataires de services d'intermédiation de données du présent règlement, il convient qu'ils aient leur établissement principal dans l'Union. Lorsqu'un prestataire de services d'intermédiation de données qui n'est pas établi dans l'Union propose des services à l'intérieur de l'Union, il devrait désigner un représentant légal. La désignation d'un représentant légal est nécessaire dans de telles situations, étant donné que ces prestataires de services d'intermédiation de données traitent des données à caractère personnel ainsi que des données commerciales confidentielles, ce qui nécessite un contrôle étroit du respect, par ces prestataires de services d'intermédiation de données, du présent règlement. Afin de déterminer si un tel prestataire de services d'intermédiation de données propose des services dans l'Union, il convient de vérifier s'il est clair qu'il envisage d'offrir des services à des personnes dans un ou plusieurs États membres. La seule accessibilité, dans l'Union, du site internet ou d'une adresse électronique et d'autres coordonnées du prestataire de services d'intermédiation de données, ou encore l'utilisation d'une langue généralement utilisée dans le pays tiers où le prestataire de services d'intermédiation de données est établi, devraient être considérées comme insuffisantes aux fins de vérifier si telle est son intention. Cependant, des facteurs tels que l'utilisation d'une langue ou d'une monnaie généralement utilisées dans un ou plusieurs États membres avec la possibilité de commander des services dans cette langue ou la mention d'utilisateurs qui se trouvent dans l'Union pourraient indiquer clairement que le prestataire de services d'intermédiation de données envisage d'offrir des services dans l'Union.

Un représentant légal désigné devrait agir pour le compte du prestataire de services d'intermédiation de données et les autorités compétentes en matière de services d'intermédiation de données devraient pouvoir contacter le représentant légal, en plus du prestataire de services d'intermédiation de données ou à la place de celui-ci, y compris en cas d'infraction, aux fins de lancer une procédure d'exécution à l'encontre d'un prestataire de services d'intermédiation de données non établi dans l'Union qui ne respecterait pas ses obligations. Le représentant légal devrait être désigné par un mandat écrit du prestataire de services d'intermédiation de données le chargeant d'agir pour son compte afin de remplir les obligations qui incombent à ce dernier au titre du présent règlement.

(43) Afin d'aider les personnes concernées et les détenteurs de données à identifier facilement les prestataires de services d'intermédiation de données reconnus dans l'Union et, partant, de renforcer leur confiance en ces derniers, il convient de créer un logo commun reconnaissable dans toute l'Union, outre le label «prestataire de services d'intermédiation de données reconnu dans l'Union».

(44) Les autorités compétentes en matière de services d'intermédiation de données désignées pour contrôler le respect des exigences du présent règlement par les prestataires de services d'intermédiation de données devraient être choisies sur la base de leurs capacités et de leur expertise en matière de partage de données horizontal ou sectoriel. Elles devraient être indépendantes de tout prestataire de services d'intermédiation de données, transparentes et impartiales dans l'exercice de leurs tâches. Les États membres devraient notifier à la Commission l'identité de ces autorités compétentes en matière de services d'intermédiation de données. Les pouvoirs et compétences des autorités compétentes en matière de services d'intermédiation de données devraient être sans préjudice des pouvoirs des autorités chargées de la protection des données. En particulier, pour toute question nécessitant une évaluation du respect du règlement (UE) 2016/679, l'autorité compétente en matière services d'intermédiation de données devrait solliciter, s'il y a lieu, un avis ou une décision de l'autorité de contrôle compétente instituée en vertu dudit règlement.

(45) Pour atteindre des objectifs d'intérêt général, nombreuses sont les possibilités offertes par l'utilisation de données mises à disposition volontairement par les personnes concernées sur le fondement de leur consentement éclairé ou, lorsqu'il s'agit de données à caractère non personnel, mises à disposition par des détenteurs de données. Ces objectifs auraient trait notamment aux soins de santé, à la lutte contre le changement climatique, à l'amélioration de la mobilité, à la facilitation du développement, de la production et de la diffusion de statistiques officielles, à l'amélioration de la prestation de services publics ou à l'élaboration des politiques publiques. Le soutien à la recherche scientifique devrait également être considéré comme un objectif d'intérêt général. Le présent règlement devrait viser à contribuer à l'émergence de réserves de données d'une taille suffisante mises à disposition sur le fondement de l'altruisme en matière de données pour permettre l'analyse des données et l'apprentissage automatique, y compris dans l'ensemble de l'Union. Pour atteindre cet objectif, les États membres devraient pouvoir mettre en place des arrangements organisationnels ou techniques, ou les deux, qui faciliteraient l'altruisme en matière de données. Ces arrangements pourraient comprendre la disponibilité d'outils facilement utilisables permettant aux personnes concernées ou aux détenteurs de données de donner leur consentement ou leur autorisation à l'utilisation altruiste de leurs données, l'organisation de campagnes de sensibilisation ou un échange structuré entre les autorités compétentes sur la manière dont les politiques publiques, telles que l'amélioration du trafic, la santé publique et la lutte contre le changement climatique, tirent profit de l'altruisme en matière de données. À cette fin, les États membres devraient pouvoir élaborer des politiques nationales concernant l'altruisme en matière de données. Les personnes concernées ne devraient pouvoir recevoir de compensation que pour les coûts qu'elles supportent lorsqu'elles mettent leurs données à disposition pour des objectifs d'intérêt général.

(46) L'enregistrement d'organisations altruistes en matière de données reconnues et l'utilisation du label «organisation altruiste en matière de données reconnue dans l'Union» devraient aboutir à la mise en place de référentiels de données. L'enregistrement dans un État membre serait valable dans toute l'Union et devrait faciliter l'utilisation transfrontalière des données au sein de l'Union et l'émergence de réserves de données couvrant plusieurs États membres. Les détenteurs de données pourraient autoriser le traitement de leurs données à caractère non personnel

pour une série de finalités non définies au moment où l'autorisation est accordée. Le respect, par de telles organisations altruistes en matière de données reconnues, d'un ensemble d'exigences prévues par le présent règlement devrait susciter la confiance dans le fait que les données mises à disposition à des fins altruistes servent un objectif d'intérêt général. Cette confiance devrait résulter notamment de l'existence d'un lieu d'établissement ou d'un représentant légal dans l'Union, ainsi que de l'obligation pour les entités altruistes en matière de données reconnues d'être des organisations à but non lucratif, des exigences de transparence et des garanties spécifiques mises en place pour protéger les droits et les intérêts des personnes concernées et des entreprises.

D'autres garanties devraient inclure la possibilité de traiter les données pertinentes dans un environnement de traitement sécurisé exploité par les organisations altruistes en matière de données reconnues, des mécanismes de surveillance tels que l'existence de conseils d'éthique ou de conseils d'administration, y compris des représentants de la société civile afin de garantir que le responsable du traitement respecte des normes rigoureuses en matière d'éthique scientifique et de protection des droits fondamentaux, des moyens techniques efficaces et clairement communiqués pour retirer ou modifier son consentement à tout moment, sur la base des obligations d'information incombant aux sous-traitants au titre du règlement (UE) 2016/679, ainsi que des moyens permettant aux personnes concernées de rester informées au sujet de l'utilisation des données qu'elles ont mises à disposition. L'enregistrement en tant qu'organisation altruiste en matière de données reconnue ne devrait pas être une condition préalable à l'exercice d'activités altruistes en matière de données. La Commission devrait, par voie d'actes délégués, préparer un recueil de règles en étroite coopération avec les organisations altruistes en matière de données et les parties prenantes. Le respect de ce recueil de règles devrait constituer une exigence pour l'enregistrement en tant qu'organisation altruiste en matière de données reconnue.

(47) Afin d'aider les personnes concernées et les détenteurs de données à identifier facilement les organisations altruistes en matière de données reconnues et, partant, de renforcer leur confiance en ces dernières, il convient de créer un logo commun reconnaissable dans toute l'Union. Le logo commun devrait s'accompagner d'un code QR comportant un lien vers le registre public de l'Union des organisations altruistes en matière de données reconnues.

(48) Le présent règlement devrait être sans préjudice de l'établissement, de l'organisation et du fonctionnement des entités qui souhaitent s'engager dans l'altruisme en matière de données en vertu du droit national et s'inspirer des exigences imposées par le droit national pour exercer des activités légalement dans un État membre en tant qu'organisation à but non lucratif.

(49) Le présent règlement devrait s'entendre sans préjudice de l'établissement, de l'organisation et du fonctionnement d'entités autres que les organismes du secteur public qui s'engagent dans le partage de données et de contenus sur la base de licences ouvertes, contribuant ainsi à la création de ressources communes accessibles à tous. Cela devrait inclure des plateformes de partage de connaissances collaboratives ouvertes, des référentiels scientifiques et universitaires en libre accès, des plateformes de développement de logiciels ouverts et des plateformes d'agrégation de contenu en libre accès.

(50) Les organisations altruistes en matière de données reconnues devraient être en mesure de collecter des données pertinentes directement auprès de personnes physiques et morales ou de traiter les données collectées par d'autres. Le traitement des données collectées pourrait être effectué par des organisations altruistes en matière de données à des fins qu'elles définissent elles-mêmes ou, le cas échéant, elles pourraient autoriser le traitement par des tiers à ces fins. Lorsque les organisations altruistes en matière de données reconnues sont des responsables du traitement ou des sous-traitants tels qu'ils sont définis dans le règlement (UE) 2016/679, elles devraient respecter ledit règlement. En règle générale, l'altruisme en matière de données reposerait sur le consentement des personnes concernées, au sens de l'article 6, paragraphe 1, point a), et de l'article 9, paragraphe 2, point a), du règlement (UE) 2016/679, qui devrait respecter les exigences régissant un consentement licite énoncées aux articles 7 et 8 dudit règlement. Conformément au règlement (UE) 2016/679, le consentement donné en ce qui concerne certains domaines de recherche scientifique lorsqu'ils respectent des normes éthiques reconnues en matière de recherche scientifique, ou uniquement en ce qui concerne certains domaines de recherche ou certaines parties de projets de recherche, pourrait soutenir les finalités de la recherche scientifique. L'article 5, paragraphe 1, point b), du règlement (UE) 2016/679 précise que le traitement ultérieur à des fins de recherche scientifique ou historique ou à des fins statistiques ne devrait pas être considéré, conformément à l'article 89, paragraphe 1, dudit règlement, comme incompatible avec les finalités initiales. Pour les données à caractère non personnel, les limitations d'utilisation devraient figurer dans l'autorisation donnée par le détenteur de données.

(51) Les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données désignées pour contrôler le respect des exigences du présent règlement par les organisations altruistes en matière de données reconnues devraient être choisies sur la base de leurs capacités et de leur expertise. Elles devraient être indépendantes de toute organisation altruiste en matière de données, transparentes et impartiales dans l'exercice de leurs tâches. Les États membres devraient notifier à la Commission l'identité desdites autorités compétentes pour l'enregistrement des organisations altruistes en matière de données. Les pouvoirs et les compétences des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données devraient être sans préjudice des pouvoirs des autorités chargées de la protection des données. En particulier, pour toute question nécessitant une évaluation du respect du règlement (UE) 2016/679, l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données devrait solliciter, s'il y a lieu, un avis ou une décision de l'autorité de contrôle compétente instituée en application dudit règlement.

(52) Afin de promouvoir la confiance et d'apporter davantage de sécurité juridique et de simplicité à la procédure d'octroi et de retrait du consentement, en particulier dans le cadre de la recherche scientifique et de l'utilisation statistique des données mises à disposition sur une base altruiste, il convient d'élaborer et d'utiliser un formulaire européen de consentement à l'altruisme en matière de données en cas de partage de données altruiste. Un tel formulaire devrait contribuer à accroître la transparence à l'égard des personnes concernées quant au fait que leurs données seront consultées et utilisées conformément à leur consentement et dans le plein respect des règles en matière de protection des données. Il devrait également faciliter l'octroi et le retrait du consentement et être utilisé pour rationaliser l'altruisme en matière de données pratiqué par les entreprises et fournir un mécanisme permettant à ces entreprises de retirer leur autorisation d'utiliser les données. Afin de tenir compte des spécificités de chaque secteur, y compris sur le plan de la protection des données, le formulaire européen de consentement à l'altruisme en matière de données devrait être conçu selon une approche modulaire permettant son adaptation à des secteurs particuliers et pour des finalités différentes.

(53) Afin de mettre en œuvre avec succès le cadre de gouvernance des données, il convient d'instaurer un comité européen de l'innovation dans le domaine des données, sous la forme d'un groupe d'experts. Le comité européen de l'innovation dans le domaine des données devrait être composé de représentants des autorités compétentes pour les services d'intermédiation de données et des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données de tous les États membres, du comité européen de la protection des données, du Contrôleur européen de la protection des données, de l'Agence de l'Union européenne pour la cybersécurité (ENISA), de la Commission, du représentant de l'UE pour les PME ou d'un représentant désigné par le réseau des représentants des PME, et d'autres représentants d'organismes compétents dans des secteurs particuliers ainsi que d'organismes disposant d'une expertise particulière. Le comité européen de l'innovation dans le domaine des données devrait être composé d'un nombre de sous-groupes, y compris d'un sous-groupe chargé de la participation des parties prenantes composé de représentants compétents issus de l'industrie, notamment dans les domaines de la santé, de l'environnement, de l'agriculture, des transports, de l'énergie, de la fabrication industrielle, des médias, des secteurs de la culture et de la création et des statistiques, ainsi que de la recherche, du monde universitaire, de la société civile, des organismes de normalisation, des espaces européens communs de données pertinents et d'autres parties prenantes concernées et de tiers, entre autres d'organismes possédant une expertise spécifique tels que les instituts nationaux de statistique.

(54) Le comité européen de l'innovation dans le domaine des données devrait aider la Commission à coordonner les pratiques et les politiques nationales sur les thèmes couverts par le présent règlement et à soutenir l'utilisation transsectorielle des données, en respectant les principes du cadre d'interopérabilité européen et en ayant recours à des normes et spécifications européennes et internationales, notamment à la plateforme européenne multipartite sur la normalisation des TIC, aux vocabulaires de base et aux blocs constitutifs du MIE, et devrait tenir compte des travaux de normalisation menés dans des secteurs ou domaines spécifiques. Les travaux de normalisation technique pourraient inclure la définition de priorités pour l'élaboration de normes et la création et l'actualisation d'un ensemble de normes techniques et juridiques régissant la transmission de données entre deux environnements de traitement afin d'organiser des espaces de données, notamment en clarifiant et en distinguant les normes et pratiques qui sont intersectorielles et celles qui sont sectorielles. Le comité européen de l'innovation dans le domaine des données devrait coopérer avec des organismes, des réseaux ou des groupes d'experts sectoriels, ou toute autre organisation intersectorielle intervenant dans la réutilisation des données. En ce qui concerne l'altruisme en matière de données, le comité européen de l'innovation dans le domaine des données devrait aider la Commission à élaborer le formulaire européen de consentement à l'altruisme en matière de données, après consultation du comité européen de la protection des données. En proposant des lignes directrices sur les espaces européens communs des données, le comité européen de l'innovation dans le domaine des données devrait soutenir le développement d'une économie européenne des données qui fonctionne sur la base de ces espaces de données, comme le prévoit la stratégie européenne pour les données.

(55) Les États membres devraient fixer des règles en matière de sanctions applicables aux infractions au présent règlement et devraient prendre toutes les mesures nécessaires afin de garantir leur mise en œuvre. Ces sanctions devraient être effectives, proportionnées et dissuasives. D'importantes disparités entre les règles en matière de sanctions pourraient entraîner une distorsion de la concurrence sur le marché unique numérique. L'harmonisation de ces règles pourrait être utile à cet égard.

(56) Afin de garantir une application efficace du présent règlement et de veiller à ce que les prestataires de services d'intermédiation de données et les entités qui souhaitent s'enregistrer en tant qu'organisations altruistes en matière de données reconnues puissent accéder aux procédures de notification et d'enregistrement et les mener à bien intégralement en ligne et par-delà les frontières, ces procédures devraient être proposées par l'intermédiaire du portail numérique unique établi en vertu du règlement (UE) 2018/1724 du Parlement européen et du Conseil ([29]). Il convient d'ajouter ces procédures à la liste des procédures figurant à l'annexe II du règlement (UE) 2018/1724.

(57) Il convient, dès lors, de modifier le règlement (UE) 2018/1724 en conséquence.

([29]) Règlement (UE) 2018/1724 du Parlement européen et du Conseil du 2 octobre 2018 établissant un portail numérique unique pour donner accès à des informations, à des procédures et à des services d'assistance et de résolution de problèmes, et modifiant le règlement (UE) n° 1024/2012 (JO L 295 du 21.11.2018, p. 1).

(58) Afin de garantir l'efficacité du présent règlement, 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 afin de compléter le présent règlement en fixant les conditions particulières applicables aux transferts vers des pays tiers de certaines catégories de données à caractère non personnel considérées comme hautement sensibles dans des actes législatifs de l'Union déterminés et en établissant, pour les organisations altruistes en matière de données reconnues, un recueil de règles que ces organisations doivent respecter, qui fixe les exigences liées aux informations, aux aspects techniques et à la sécurité ainsi que les feuilles de route en matière de communication et les normes d'interopérabilité. 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» ([30]). 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.

(59) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission pour aider les organismes du secteur public et les réutilisateurs à respecter les conditions de réutilisation énoncées dans le présent règlement en élaborant des clauses contractuelles types pour le transfert par des réutilisateurs de données à caractère non personnel vers un pays tiers, pour déclarer que le cadre juridique et le dispositif de surveillance et d'exécution d'un pays tiers sont équivalents à la protection garantie au titre du droit de l'Union, pour concevoir le logo commun destiné aux prestataires de services d'intermédiation de données et le logo commmun destiné aux organisations altruistes en matière de données reconnues et pour créer et élaborer le formulaire européen de consentement à l'altruisme en matière de données. Ces compétences devraient être exercées conformément au règlement (UE) n° 182/2011 du Parlement européen et du Conseil ([31]).

(60) Le présent règlement ne devrait pas avoir d'incidence sur l'application des règles relatives à la concurrence, en particulier les articles 101 et 102 du traité sur le fonctionnement de l'Union européenne. Les mesures prévues par le présent règlement ne devraient pas être utilisées pour restreindre la concurrence d'une manière qui soit contraire au traité sur le fonctionnement de l'Union européenne. Cela concerne en particulier les règles relatives à l'échange d'informations sensibles sous l'angle de la concurrence entre concurrents réels ou potentiels au moyen de services d'intermédiation de données.

(61) 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, paragraphe 1, du règlement (UE) 2018/1725 et ont rendu leur avis le 10 mars 2021.

(62) Le présent règlement a pour principes directeurs le respect des droits fondamentaux et des principes reconnus en particulier par la Charte des droits fondamentaux de l'Union européenne, notamment le respect de la vie privée, la protection des données à caractère personnel, la liberté d'entreprise, le droit de propriété et l'intégration des personnes handicapées. En ce qui concerne ce dernier élément, les organismes de service public et les services relevant du présent règlement devraient, s'il y a lieu, respecter les directives (UE) 2016/2102 ([32]) et (UE) 2019/882 ([33]) du Parlement européen et du Conseil. En outre, il convient de tenir compte de la conception universelle dans le contexte des technologies de l'information et de la communication, qui consiste en un effort délibéré et systématique d'appliquer de manière proactive les principes, méthodes et outils de promotion de la conception universelle dans les technologies informatiques, y compris les technologies basées sur l'internet, ce qui évite que des adaptations a posteriori ou une conception spéciale ne soient nécessaires.

(63) Étant donné que les objectifs du présent règlement, à savoir la réutilisation, au sein de l'Union, de certaines catégories de données détenues par des organismes du secteur public, ainsi que l'établissement d'un cadre de notification et de surveillance pour la fourniture de services d'intermédiation de données, d'un cadre pour l'enregistrement volontaire des entités qui mettent des données à disposition à des fins altruistes et d'un cadre pour l'établissement d'un comité européen de l'innovation dans le domaine des données, ne peuvent pas être atteints de manière suffisante par les États membres mais peuvent, en raison de leurs dimensions et de leurs effets, 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,

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

([31]) 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).

([32]) Directive (UE) 2016/2102 du Parlement européen et du Conseil du 26 octobre 2016 relative à l'accessibilité des sites internet et des applications mobiles des organismes du secteur public (JO L 327 du 2.12.2016, p. 1).

([33]) 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).

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

Dispositions générales

Article premier

Objet et champ d'application

1. Le présent règlement établit:

a) les conditions de réutilisation, au sein de l'Union, de certaines catégories de données détenues par des organismes du secteur public;

b) un cadre de notification et de surveillance pour la fourniture de services d'intermédiation de données;

c) un cadre pour l'enregistrement volontaire des entités qui collectent et traitent les données mises à disposition à des fins altruistes; et

d) un cadre pour l'établissement d'un comité européen de l'innovation dans le domaine des données.

2. Le présent règlement ne crée, pour les organismes du secteur public, aucune obligation d'autoriser la réutilisation des données et ne libère pas les organismes du secteur public des obligations de confidentialité qui leur incombent au titre du droit de l'Union ou du droit national.

Le présent règlement est sans préjudice:

a) des dispositions particulières du droit de l'Union ou du droit national concernant l'accès à certaines catégories de données ou la réutilisation de celles-ci, notamment en ce qui concerne l'octroi de l'accès à des documents officiels et leur divulgation; et

b) de l'obligation incombant aux organismes du secteur public au titre du droit de l'Union ou du droit national d'autoriser la réutilisation des données ou des exigences liées au traitement des données à caractère non personnel.

Lorsque le droit sectoriel de l'Union ou le droit sectoriel national impose aux organismes du secteur public, aux prestataires de services d'intermédiation de données ou aux organisations altruistes en matière de données reconnues de respecter des exigences techniques, administratives ou organisationnelles particulières supplémentaires, notamment au moyen d'un régime d'autorisation ou de certification, ces dispositions dudit droit sectoriel de l'Union ou dudit droit sectoriel national s'appliquent également. Des exigences particulières supplémentaires de ce type sont non discriminatoires, proportionnées et objectivement justifiées.

3. Le droit de l'Union et le droit national en matière de protection des données à caractère personnel s'appliquent à toutes les données à caractère personnel traitées en lien avec le présent règlement. En particulier, le présent règlement est sans préjudice des règlements (UE) 2016/679 et (UE) 2018/1725 et des directives 2002/58/CE et (UE) 2016/680, y compris en ce qui concerne les pouvoirs et compétences des autorités de contrôle. En cas de conflit entre le présent règlement et les dispositions du droit de l'Union en matière de protection des données à caractère personnel ou du droit national adopté 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 prévalent. Le présent règlement ne crée pas de base juridique pour le traitement des données à caractère personnel et ne modifie pas les droits et obligations énoncés dans le règlement (UE) 2016/679 ou (UE) 2018/1725 ou dans la directive 2002/58/CE ou (UE) 2016/680.

4. Le présent règlement est sans préjudice de l'application du droit de la concurrence.

5. Le présent règlement est sans préjudice des compétences des États membres en ce qui concerne leurs activités relatives à la sécurité publique, à la défense et à la sécurité nationale.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

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

2) «réutilisation»: l'utilisation, par des personnes physiques ou morales, de données détenues par des organismes du secteur public, à des fins commerciales ou non commerciales autres que l'objectif initial de la mission de service public pour lequel les données ont été produites, à l'exception de l'échange de données entre des organismes du secteur public aux seules fins de l'exercice de leur mission de service public;

3) «données à caractère 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) «consentement»: le consentement au sens de l'article 4, point 11), du règlement (UE) 2016/679;

6) «autorisation»: le fait d'accorder aux utilisateurs de données le droit au traitement de données à caractère non personnel;

7) «personne concernée»: la personne concernée visée à l'article 4, point 1), du règlement (UE) 2016/679;

8) «détenteur de données»: une personne morale, y compris des organismes du secteur public et des organisations internationales, ou une personne physique qui n'est pas une personne concernée pour ce qui est des données spécifiques considérées, qui, conformément au droit de l'Union ou au droit national applicable, a le droit d'octroyer l'accès à certaines données à caractère personnel ou non personnel;

9) «utilisateur de données»: une personne physique ou morale qui dispose d'un accès licite à certaines données à caractère personnel ou non personnel et qui a le droit, y compris au titre du règlement (UE) 2016/679 lorsqu'il s'agit de données à caractère personnel, d'utiliser ces données à des fins commerciales ou non commerciales;

10) «partage de données»: la fourniture de données à un utilisateur de données par une personne concernée ou un détenteur de données, en vue de l'utilisation conjointe ou individuelle desdites données, sur la base d'accords volontaires ou du droit de l'Union ou du droit national, directement ou via un intermédiaire, par exemple dans le cadre de licences ouvertes ou commerciales, moyennant le paiement d'une redevance ou gratuitement;

11) «service d'intermédiation de données»: un service qui vise à établir des relations commerciales à des fins de partage de données entre un nombre indéterminé de personnes concernées et de détenteurs de données, d'une part, et d'utilisateurs de données, d'autre part, par des moyens techniques, juridiques ou autres, y compris aux fins de l'exercice des droits des personnes concernées en ce qui concerne les données à caractère personnel, à l'exclusion au minimum de ce qui suit:

   a) des services qui obtiennent des données auprès des détenteurs de données et les agrègent, les enrichissent ou les transforment afin d'en accroître substantiellement la valeur et concèdent une licence d'utilisation des données résultantes aux utilisateurs de données, sans établir de relation commerciale directe entre les détenteurs de données et les utilisateurs de données;

   b) des services axés sur l'intermédiation de contenus protégés par le droit d'auteur;

   c) des services qui sont utilisés exclusivement par un seul détenteur de données pour lui permettre d'utiliser les données qu'il détient, ou qui sont utilisés par des personnes morales multiples au sein d'un groupe fermé, y compris dans le cadre de relations de fournisseur ou de client ou de collaborations établies par contrat, en particulier ceux qui ont pour principal objectif de garantir les fonctionnalités d'objets et de dispositifs connectés à l'internet des objets;

   d) des services pour le partage de données proposés par des organismes du secteur public qui ne cherchent pas à établir des relations commerciales;

12) «traitement»: le traitement au sens de l'article 4, point 2), du règlement (UE) 2016/679 en ce qui concerne les données à caractère personnel ou de l'article 3, point 2), du règlement (UE) 2018/1807 en ce qui concerne les données à caractère non personnel;

13) «accès»: l'utilisation de données conformément à des exigences techniques, juridiques ou organisationnelles particulières, sans que cela implique nécessairement la transmission ou le téléchargement de données;

14) «établissement principal»: en ce qui concerne une personne morale, le lieu de son administration centrale dans l'Union;

15) «services de coopératives de données»: les services d'intermédiation de données proposés par une structure organisationnelle constituée de personnes concernées, d'entreprises unipersonnelles ou de PME qui sont membres de cette structure dont les objectifs principaux consistent à aider ses membres à exercer leurs droits à l'égard de certaines données, y compris quant au fait d'opérer des choix en connaissance de cause avant qu'ils ne consentent au traitement de données, à mener des échanges de vues sur les finalités et les conditions du traitement de données qui représenteraient le mieux les intérêts de ses membres en ce qui concerne leurs données, et à négocier les conditions et modalités du traitement des données au nom de ses membres avant que ceux-ci ne donnent l'autorisation de traiter des données à caractère non personnel ou ne donnent leur consentement au traitement de données à caractère personnel;

16) «altruisme en matière de données»: le partage volontaire de données fondé sur le consentement donné par les personnes concernées au traitement de données à caractère personnel les concernant, ou l'autorisation accordée par des détenteurs de données pour l'utilisation de leurs données à caractère non personnel sans demander ni recevoir de contrepartie qui aille au-delà de la compensation des coûts qu'ils supportent lorsqu'ils mettent à disposition leurs données, pour des objectifs d'intérêt général prévus par le droit national, le cas échéant, par exemple les soins de santé, la lutte contre le changement climatique, l'amélioration de la mobilité, la facilitation du développement, de la production et de la diffusion de statistiques officielles, l'amélioration de la prestation de services publics, l'élaboration des politiques publiques ou la recherche scientifique dans l'intérêt général;

17) «organisme du secteur public»: l'État, les autorités régionales ou locales, les organismes de droit public ou les associations formées par une ou plusieurs de ces autorités ou un ou plusieurs de ces organismes de droit public;

18) «organismes de droit public»: les organismes présentant les caractéristiques suivantes:

    a) ils ont été créés pour satisfaire spécifiquement des besoins d'intérêt général et n'ont pas de caractère industriel ou commercial;

    b) ils sont dotés de la personnalité juridique;

    c) ils sont financés majoritairement par l'État, les autorités régionales ou locales ou d'autres organismes de droit public, leur gestion est soumise à un contrôle de ces autorités ou organismes, ou leur organe d'administration, de direction ou de surveillance est composé de membres dont plus de la moitié sont désignés par l'État, les autorités régionales ou locales ou d'autres organismes de droit public;

19) «entreprise publique»: toute entreprise sur laquelle les organismes du secteur public peuvent exercer directement ou indirectement une influence dominante du fait de la propriété de l'entreprise, de la participation financière qu'ils y détiennent ou des règles qui la régissent; aux fins de la présente définition, une influence dominante des organismes du secteur public sur l'entreprise est présumée dans tous les cas suivants lorsque ces organismes, directement ou indirectement:

    a) détiennent la majorité du capital souscrit de l'entreprise;

    b) disposent de la majorité des voix attachées aux parts émises par l'entreprise;

    c) peuvent désigner plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance de l'entreprise;

20) «environnement de traitement sécurisé»: l'environnement physique ou virtuel et les moyens organisationnels pour garantir le respect du droit de l'Union, tel que le règlement (UE) 2016/679, en particulier en ce qui concerne les droits des personnes concernées, les droits de propriété intellectuelle, la confidentialité commerciale et le secret statistique, l'intégrité et l'accessibilité, ainsi que le respect du droit national applicable, et pour permettre à l'entité fournissant l'environnement de traitement sécurisé de déterminer et de surveiller toutes les opérations de traitement de données, notamment l'affichage, le stockage, le téléchargement et l'exportation de données et le calcul de données dérivées au moyen d'algorithmes de calcul;

21) «représentant légal»: une personne physique ou morale établie dans l'Union, expressément désignée pour agir pour le compte d'un prestataire de services d'intermédiation de données ou d'une entité qui collecte pour des objectifs d'intérêt général des données mises à disposition par des personnes physiques ou morales sur le fondement de l'altruisme en matière de données non établi(e) dans l'Union, qui peut être contactée par les autorités compétentes en matière de services d'intermédiation de données et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données en plus du prestataire de services d'intermédiation de données ou de l'entité, ou à leur place, en ce qui concerne les obligations prévues dans le présent règlement, y compris en ce qui concerne le lancement d'une procédure d'exécution à l'encontre d'un prestataire de services d'intermédiation de données ou d'une entité non établi(e) dans l'Union qui ne respecte pas ses obligations.

CHAPITRE II

Réutilisation de certaines catégories de données protégées détenues par des organismes du secteur public

Article 3

Catégories de données

1. Le présent chapitre s'applique aux données détenues par des organismes du secteur public, qui sont protégées pour des motifs:

a) de confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise;

b) de secret statistique;

c) de protection des droits de propriété intellectuelle de tiers; ou

d) de protection des données à caractère personnel, dans la mesure où de telles données ne relèvent pas du champ d'application de la directive (UE) 2019/1024.

2. Le présent chapitre ne s'applique pas:

a) aux données détenues par des entreprises publiques;

b) aux données détenues par des radiodiffuseurs de service public et leurs filiales et par d'autres organismes ou leurs filiales pour l'accomplissement d'une mission de radiodiffusion de service public;

c) aux données détenues par des établissements culturels et des établissements d'enseignement;

d) aux données détenues par des organismes du secteur public qui sont protégées pour des raisons de sécurité publique, de défense ou de sécurité nationale; ou

e) aux données dont la fourniture est une activité qui ne relève pas de la mission de service public dévolue aux organismes du secteur public concernés telle qu'elle est définie par la loi ou par d'autres règles contraignantes en vigueur dans l'État membre concerné ou, en l'absence de telles règles, telle qu'elle est définie conformément aux pratiques administratives courantes dans cet État membre, sous réserve que l'objet des missions de service public soit transparent et soumis à réexamen.

3. Le présent chapitre est sans préjudice:

a) du droit de l'Union, du droit national et des accords internationaux auxquels l'Union ou les États membres sont parties en ce qui concerne la protection des catégories de données visées au paragraphe 1; et

b) du droit de l'Union et du droit national en matière d'accès aux documents.

Article 4

Interdiction des accords d'exclusivité

1. Sont interdits les accords ou autres pratiques relatifs à la réutilisation de données détenues par des organismes du secteur public contenant des catégories de données visées à l'article 3, paragraphe 1, qui octroient des droits d'exclusivité ou qui ont pour objet ou pour effet d'octroyer de tels droits d'exclusivité ou de restreindre la disponibilité des données à des fins de réutilisation par des entités autres que les parties à ces accords ou autres pratiques.

2. Par dérogation au paragraphe 1, un droit d'exclusivité pour la réutilisation des données visées audit paragraphe peut être accordé dans la mesure nécessaire à la fourniture d'un service ou d'un produit d'intérêt général qui, sans cela, ne pourrait pas être obtenu.

3. Un droit d'exclusivité tel qu'il est visé au paragraphe 2 est accordé par le biais d'un acte administratif ou d'un arrangement contractuel conformément au droit de l'Union ou au droit national applicable, dans le respect des principes de transparence, d'égalité de traitement et de non-discrimination.

4. La durée du droit d'exclusivité pour la réutilisation des données ne dépasse pas douze mois. Lorsqu'un contrat est conclu, la durée du contrat est la même que la durée du droit d'exclusivité.

5. L'octroi d'un droit d'exclusivité en vertu des paragraphes 2, 3 et 4, notamment les raisons justifiant la nécessité d'accorder un tel droit, est transparent et est rendu public en ligne, sous une forme qui respecte les dispositions pertinentes du droit de l'Union en matière de marchés publics.

6. Les accords ou autres pratiques tombant sous le coup de l'interdiction visée au paragraphe 1 qui ne remplissent pas les conditions prévues aux paragraphes 2 et 3, et qui ont été respectivement conclus ou convenues avant le 23 juin 2022 prennent fin au terme du contrat applicable et, en tout état de cause, au plus tard le 24 décembre 2024.

Article 5

Conditions applicables à la réutilisation

1. Les organismes du secteur public qui sont compétents en vertu du droit national pour octroyer ou refuser l'accès aux fins de la réutilisation d'une ou de plusieurs des catégories de données visées à l'article 3, paragraphe 1, rendent publiques les conditions d'autorisation de cette réutilisation et la procédure de demande de réutilisation par l'intermédiaire du point d'information unique visé à l'article 8. Lorsqu'ils octroient ou refusent l'accès à des fins de réutilisation, ils peuvent être assistés par les organismes compétents visés à l'article 7, paragraphe 1.

Les États membres veillent à ce que les organismes du secteur public soient dotés des ressources nécessaires pour se conformer au présent article.

2. Les conditions applicables à la réutilisation sont non discriminatoires, transparentes, proportionnées et objectivement justifiées en ce qui concerne les catégories de données et les finalités de la réutilisation, ainsi que la nature des données pour lesquelles la réutilisation est autorisée. Ces conditions ne sont pas utilisées pour restreindre la concurrence.

3. Les organismes du secteur public veillent à ce que, conformément au droit de l'Union et au droit national, le caractère protégé des données soit préservé. Ils peuvent prévoir les exigences suivantes:

a) l'accès aux données à des fins de réutilisation n'est octroyé que lorsque l'organisme du secteur public ou l'organisme compétent, à la suite d'une demande de réutilisation, a fait en sorte que les données:

   i) aient été anonymisées dans le cas des données à caractère personnel; et

   ii) aient été modifiées, agrégées ou traitées selon toute autre méthode de contrôle de la divulgation dans le cas des informations commerciales confidentielles, y compris des secrets d'affaires et des contenus protégés par des droits de propriété intellectuelle;

b) l'accès aux données et leur réutilisation se font à distance dans un environnement de traitement sécurisé qui est fourni ou contrôlé par l'organisme du secteur public;

c) l'accès aux données et leur réutilisation se font dans les locaux où se trouve l'environnement de traitement sécurisé, dans le respect de normes de sécurité élevées, à condition que l'accès à distance ne puisse être autorisé sans qu'il soit porté atteinte aux droits et aux intérêts des tiers.

4. Lorsque la réutilisation est autorisée conformément au paragraphe 3, points b) et c), les organismes du secteur public imposent des conditions qui préservent l'intégrité du fonctionnement des systèmes techniques de l'environnement de traitement sécurisé utilisé. L'organisme du secteur public se réserve le droit de vérifier le processus, les moyens et tout résultat du traitement de données effectué par le réutilisateur afin de préserver l'intégrité de la protection des données et se réserve le droit d'interdire l'utilisation des résultats qui contiennent des informations portant atteinte aux droits et aux intérêts de tiers. La décision d'interdire l'utilisation des résultats est transparente et compréhensible par le réutilisateur.

5. Sauf si le droit national prévoit des garanties spécifiques concernant les obligations de confidentialité applicables en cas de réutilisation des données visées à l'article 3, paragraphe 1, l'organisme du secteur public subordonne la réutilisation des données fournies conformément au paragraphe 3 du présent article au respect par le réutilisateur d'une obligation de confidentialité interdisant la divulgation de toute information compromettant les droits et intérêts de tiers que le réutilisateur peut avoir acquis malgré les garanties mises en place. Il est interdit aux réutilisateurs de rétablir l'identité de toute personne concernée à laquelle se rapportent les données et ils prennent des mesures techniques et opérationnelles pour empêcher toute réidentification et notifier à l'organisme du secteur public toute violation de données ayant pour effet de réidentifier les personnes concernées. En cas de réutilisation non autorisée de données à caractère non personnel, le réutilisateur informe sans retard, au besoin avec l'aide de l'organisme du secteur public, les personnes morales dont les droits et intérêts peuvent être affectés.

6. Lorsqu'il est impossible d'autoriser la réutilisation des données en respectant les obligations prévues aux paragraphes 3 et 4 du présent article et qu'il n'existe pas de base juridique pour la transmission des données au titre du règlement (UE) 2016/679, l'organisme du secteur public met tout en œuvre, conformément au droit de l'Union et au droit national, pour aider les réutilisateurs potentiels à demander le consentement des personnes concernées ou l'autorisation des détenteurs de données dont les droits et intérêts peuvent être affectés par cette réutilisation, lorsque cela est faisable sans charge disproportionnée pour l'organisme du secteur public. Lorsqu'il fournit cette aide, l'organisme du secteur public peut être assisté par les organismes compétents visés à l'article 7, paragraphe 1.

7. La réutilisation des données n'est autorisée que dans le respect des droits de propriété intellectuelle. Les organismes du secteur public n'exercent pas le droit du fabricant d'une base de données prévu à l'article 7, paragraphe 1, de la directive 96/9/CE en vue d'empêcher la réutilisation de données ou de limiter celle-ci au-delà des limites fixées par le présent règlement.

8. Lorsque les données demandées sont considérées comme confidentielles, conformément au droit de l'Union ou au droit national en matière de confidentialité commerciale ou de secret statistique, les organismes du secteur public veillent à ce que les données confidentielles ne soient pas divulguées du fait de l'autorisation à des fins de réutilisation, à moins que cette réutilisation ne soit autorisée conformément au paragraphe 6.

9. Lorsqu'un réutilisateur a l'intention de transférer à un pays tiers des données à caractère non personnel protégées pour les motifs énoncés à l'article 3, paragraphe 1, il informe l'organisme du secteur public de son intention de transférer ces données ainsi que de la finalité de ce transfert au moment de demander la réutilisation desdites données. En cas de réutilisation conformément au paragraphe 6 du présent article, le réutilisateur informe, au besoin avec l'aide de l'organisme du secteur public, la personne morale dont les droits et intérêts peuvent être affectés de cette intention, de la finalité et des garanties appropriées. L'organisme du secteur public n'autorise pas la réutilisation à moins que la personne morale n'autorise le transfert.

10. Les organismes du secteur public ne transmettent des données confidentielles à caractère non personnel ou des données protégées par des droits de propriété intellectuelle à un réutilisateur qui a l'intention de transférer lesdites données vers un pays tiers autre qu'un pays désigné conformément au paragraphe 12 que si le réutilisateur s'engage contractuellement à:

a) respecter les obligations imposées conformément aux paragraphes 7 et 8, même après le transfert des données vers le pays tiers; et

b) admettre la compétence des juridictions de l'État membre de l'organisme du secteur public qui transmet les données en ce qui concerne tout litige lié au respect des paragraphes 7 et 8.

11. Les organismes du secteur public, s'il y a lieu et dans la mesure de leurs capacités, fournissent des conseils et une assistance aux réutilisateurs pour ce qui est de respecter les obligations visées au paragraphe 10 du présent article.

Afin d'aider les organismes du secteur public et les réutilisateurs, la Commission peut adopter des actes d'exécution établissant des clauses contractuelles types pour le respect des obligations visées au paragraphe 10 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 33, paragraphe 3.

12. Lorsque cela est justifié en raison du nombre important de demandes dans l'ensemble de l'Union concernant la réutilisation de données à caractère non personnel dans des pays tiers déterminés, la Commission peut adopter des actes d'exécution déclarant que le cadre juridique et le dispositif de surveillance et d'exécution d'un pays tiers:

a) assurent la protection de la propriété intellectuelle et des secrets d'affaires d'une manière qui est essentiellement équivalente à la protection assurée par le droit de l'Union;

b) sont effectivement appliqués et leur application est contrôlée; et

c) prévoient un recours juridictionnel effectif.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 33, paragraphe 3.

13. Des actes législatifs spécifiques de l'Union peuvent considérer que certaines catégories de données à caractère non personnel détenues par des organismes du secteur public sont hautement sensibles aux fins du présent article, lorsque leur transfert vers des pays tiers peut mettre en péril des objectifs de politique publique de l'Union, tels que la sécurité et la santé publique, ou peut entraîner un risque de réidentification de données anonymisées à caractère non personnel. Lorsqu'un tel acte est adopté, la Commission adopte des actes délégués conformément à l'article 32 afin de compléter le présent règlement en fixant des conditions particulières applicables aux transferts de telles données vers des pays tiers.

Ces conditions particulières sont fondées sur la nature des catégories de données à caractère non personnel identifiées dans l'acte législatif spécifique de l'Union et sur les motifs conduisant à considérer ces catégories comme hautement sensibles, en tenant compte des risques de réidentification de données anonymisées à caractère non personnel. Elles sont non discriminatoires et limitées à ce qui est nécessaire pour atteindre les objectifs de politique publique de l'Union définis dans ledit acte, conformément aux obligations internationales de l'Union.

Lorsque les actes législatifs spécifiques de l'Union visés au premier alinéa l'exigent, de telles conditions particulières peuvent notamment comprendre des conditions applicables au transfert ou des arrangements techniques à cet égard, des limitations en ce qui concerne la réutilisation de données dans des pays tiers ou les catégories de personnes habilitées à transférer ces données vers des pays tiers ou, dans des cas exceptionnels, des restrictions en ce qui concerne les transferts vers des pays tiers.

14. La personne physique ou morale à laquelle le droit de réutiliser des données à caractère non personnel a été accordé ne peut transférer ces données que vers les pays tiers pour lesquels il est satisfait aux exigences énoncées aux paragraphes 10, 12 et 13.

Article 6

Redevances

1. Les organismes du secteur public qui autorisent la réutilisation des catégories de données visées à l'article 3, paragraphe 1, peuvent percevoir des redevances pour autoriser la réutilisation de ces données.

2. Les redevances perçues en vertu du paragraphe 1 sont transparentes, non discriminatoires, proportionnées et objectivement justifiées et ne restreignent pas la concurrence.

3. Les organismes du secteur public font en sorte que les redevances puissent aussi être acquittées en ligne au moyen de services de paiement transfrontaliers largement disponibles, sans discrimination fondée sur le lieu d'établissement du prestataire de services de paiement, le lieu d'émission de l'instrument de paiement ou la localisation du compte de paiement dans l'Union.

4. Lorsque les organismes du secteur public perçoivent des redevances, ils prennent des mesures pour inciter à la réutilisation des catégories de données visées à l'article 3, paragraphe 1, à des fins non commerciales, par exemple à des fins de recherche scientifique, ainsi que par les PME et les jeunes pousses conformément aux règles en matière d'aides d'État. À cet égard, les organismes du secteur public peuvent également mettre ces données à disposition moyennant une redevance réduite ou à titre gratuit, notamment pour les PME, les jeunes pousses, les organisations de la société civile et les établissements d'enseignement. À cette fin, les organismes du secteur public peuvent établir une liste des catégories de réutilisateurs pour lesquelles les données à des fins de réutilisation sont mises à disposition moyennant une redevance réduite ou à titre gratuit. Cette liste, ainsi que les critères utilisés pour l'établir, sont rendus publics.

5. Les redevances sont calculées sur la base des coûts liés à la conduite de la procédure de demande de réutilisation des catégories de données visées à l'article 3, paragraphe 1, et limitées aux coûts nécessaires relatifs:

a) à la reproduction, à la fourniture et à la diffusion des données;

b) à l'acquisition des droits;

c) à l'anonymisation ou à d'autres formes de préparation des données à caractère personnel et des données commerciales confidentielles conformément à l'article 5, paragraphe 3;

d) à la maintenance de l'environnement de traitement sécurisé;

e) à l'acquisition du droit d'autoriser la réutilisation conformément au présent chapitre par des tiers extérieurs au secteur public; et

f) à l'assistance fournie aux réutilisateurs pour obtenir le consentement des personnes concernées et l'autorisation des détenteurs de données dont les droits et intérêts peuvent être affectés par cette réutilisation.

6. Les critères et la méthode de calcul des redevances sont arrêtés par les États membres et publiés. L'organisme du secteur public publie une description des principales catégories de coûts et des règles utilisées pour la répartition des coûts.

Article 7

Organismes compétents

1. En vue d'effectuer les tâches visées au présent article, chaque État membre désigne un ou plusieurs organismes compétents, qui peuvent être compétents pour un secteur particulier, pour aider les organismes du secteur public qui octroient ou refusent l'accès aux fins de la réutilisation des catégories de données visées à l'article 3, paragraphe 1. Les États membres peuvent soit établir un ou plusieurs nouveaux organismes compétents, soit s'appuyer sur des organismes du secteur public ou sur des services internes d'organismes du secteur public existants qui remplissent les conditions fixées par le présent règlement.

2. Les organismes compétents peuvent également être habilités à octroyer l'accès aux fins de la réutilisation des catégories de données visées à l'article 3, paragraphe 1, en application des dispositions du droit de l'Union ou du droit national qui prévoient l'octroi d'un tel accès. Lorsqu'ils octroient ou refusent l'accès à des fins de réutilisation, les articles 4, 5, 6 et 9 s'appliquent à ces organismes compétents.

3. Les organismes compétents disposent des ressources juridiques, financières, techniques et humaines suffisantes pour mener à bien les tâches qui leur sont assignées, y compris des connaissances techniques nécessaires pour être en mesure de respecter le droit de l'Union ou le droit national applicable en ce qui concerne les régimes d'accès pour les catégories de données visées à l'article 3, paragraphe 1.

4. L'assistance prévue au paragraphe 1 consiste notamment, le cas échéant:

a) à fournir une assistance technique en mettant à disposition un environnement de traitement sécurisé pour donner accès à la réutilisation de données;

b) à fournir des orientations et une assistance technique sur la meilleure manière de structurer et de stocker les données pour les rendre facilement accessibles;

c) à fournir un soutien technique pour la pseudonymisation et à garantir le traitement des données d'une manière qui préserve efficacement le caractère privé, la confidentialité, l'intégrité et l'accessibilité des informations contenues dans les données pour lesquelles la réutilisation est autorisée, notamment les techniques d'anonymisation, de généralisation, de suppression et de randomisation des données à caractère personnel ou d'autres méthodes de préservation de la vie privée à la pointe de la technologie, et la suppression des informations commerciales confidentielles, y compris les secrets d'affaires ou les contenus protégés par des droits de propriété intellectuelle;

d) à aider les organismes du secteur public, le cas échéant, à fournir une assistance aux réutilisateurs pour demander le consentement des personnes concernées à la réutilisation ou l'autorisation des détenteurs de données conformément à leurs décisions spécifiques, y compris en ce qui concerne le territoire où le traitement des données est prévu et à aider les organismes du secteur public à mettre en place des mécanismes techniques permettant la transmission des demandes de consentement ou d'autorisation des réutilisateurs, lorsque cela est réalisable en pratique;

e) à fournir aux organismes du secteur public une assistance lorsqu'il s'agit d'évaluer l'adéquation des engagements contractuels pris par un réutilisateur en vertu de l'article 5, paragraphe 10.

5. Chaque État membre notifie à la Commission l'identité des organismes compétents désignés en application du paragraphe 1 au plus tard le 24 septembre 2023. Chaque État membre notifie également à la Commission toute modification ultérieure concernant l'identité de ces organismes compétents.

Article 8

Points d'information unique

1. Les États membres veillent à ce que toutes les informations pertinentes concernant l'application des articles 5 et 6 soient disponibles et facilement accessibles par l'intermédiaire d'un point d'information unique. Les États membres établissent un nouvel organisme ou désignent un organisme existant ou une structure existante en tant que point d'information unique. Le point d'information unique peut être lié à des points d'information sectoriels, régionaux ou locaux. Les fonctions du point d'information unique peuvent être automatisées, à condition que l'organisme du secteur public apporte un soutien adéquat.

2. Le point d'information unique est compétent pour recevoir les demandes d'information ou demandes de réutilisation des catégories de données visées à l'article 3, paragraphe 1, et les transmettre, par des moyens automatisés lorsque cela est possible et opportun, aux organismes du secteur public compétents, ou aux organismes compétents visés à l'article 7, paragraphe 1, le cas échéant. Le point d'information unique met à disposition par voie électronique une liste de ressources consultable contenant un aperçu de toutes les ressources en données disponibles, y compris, le cas échéant, les ressources en données qui sont disponibles au niveau des points d'information sectoriels, régionaux ou locaux, avec des informations pertinentes décrivant les données disponibles, y compris au minimum le format et la taille des données ainsi que les conditions applicables à leur réutilisation.

3. Le point d'information unique peut établir un canal d'information distinct, simplifié et bien documenté pour les PME et les jeunes pousses, afin de répondre à leurs besoins et à leurs capacités en matière de demande de réutilisation des catégories de données visées à l'article 3, paragraphe 1.

4. La Commission établit un point d'accès unique européen mettant à disposition un registre électronique consultable des données disponibles au niveau des points d'information uniques nationaux ainsi que d'autres informations sur la manière de demander des données par l'intermédiaire de ces points d'information uniques nationaux.

Article 9

Procédure relative aux demandes de réutilisation

1. Sauf si des délais plus courts ont été fixés conformément au droit national, les organismes du secteur public compétents ou les organismes compétents visés à l'article 7, paragraphe 1, adoptent une décision sur la demande de réutilisation des catégories de données visées à l'article 3, paragraphe 1, dans un délai de deux mois à compter de la date de réception de la demande.

En cas de demandes de réutilisation exceptionnellement détaillées et complexes, ce délai de deux mois peut être prolongé de trente jours au maximum. En pareils cas, les organismes du secteur public compétents ou les organismes compétents visés à l'article 7, paragraphe 1, informent le demandeur dès que possible de la nécessité d'un délai supplémentaire pour conduire la procédure, ainsi que des raisons qui justifient le retard.

2. Toute personne physique ou morale directement affectée par une décision visée au paragraphe 1 dispose d'un droit de recours effectif dans l'État membre dans lequel est situé ledit organisme. Un tel droit de recours est fixé par le droit national et inclut la possibilité d'un réexamen par un organisme impartial doté des compétences appropriées, telle que l'autorité nationale de la concurrence, l'autorité pertinente d'accès aux documents, l'autorité de contrôle établie conformément au règlement (UE) 2016/679 ou une autorité judiciaire nationale, dont les décisions sont contraignantes pour l'organisme du secteur public concerné ou l'organisme compétent concerné.

CHAPITRE III

Exigences applicables aux services d'intermédiation de données

Article 10

Services d'intermédiation de données

La fourniture des services d'intermédiation de données suivants respecte l'article 12 et est soumise à une procédure de notification:

a) les services d'intermédiation entre les détenteurs de données et les utilisateurs de données potentiels, y compris la mise à disposition des moyens techniques ou autres nécessaires pour permettre la fourniture desdits services; ces services peuvent comprendre des échanges bilatéraux ou multilatéraux de données ou la création de plateformes ou de bases de données permettant l'échange ou l'utilisation conjointe de données, ainsi que la mise en place d'une autre infrastructure spécifique pour l'interconnexion des détenteurs de données avec les utilisateurs de données;

b) les services d'intermédiation entre, d'une part, les personnes concernées qui cherchent à mettre à disposition leurs données à caractère personnel ou des personnes physiques qui cherchent à mettre à disposition des données à caractère non personnel et, d'autre part, les utilisateurs de données potentiels, y compris la mise à disposition des moyens techniques ou autres nécessaires pour permettre la fourniture desdits services, et notamment pour permettre l'exercice des droits des personnes concernées prévus par le règlement (UE) 2016/679;

c) les services de coopératives de données.

Article 11

Notification par des prestataires de services d'intermédiation de données

1. Tout prestataire de services d'intermédiation de données qui a l'intention de fournir les services d'intermédiation de données visés à l'article 10 soumet une notification à l'autorité compétente en matière de services d'intermédiation de données.

2. Aux fins du présent règlement, un prestataire de services d'intermédiation de données qui a des établissements dans plusieurs États membres est considéré comme relevant de la compétence de l'État membre dans lequel il a son établissement principal, sans préjudice du droit de l'Union réglementant les actions transfrontalières en dommages et intérêts et les procédures connexes.

3. Un prestataire de services d'intermédiation de données qui n'est pas établi dans l'Union mais qui propose les services d'intermédiation de données visés à l'article 10 dans l'Union désigne un représentant légal dans l'un des États membres où il propose lesdits services.

Afin de garantir le respect du présent règlement, le représentant légal est mandaté par le prestataire de services d'intermédiation de données pour être contacté, en plus dudit prestataire ou à sa place, par les autorités compétentes pour les services d'intermédiation de données ou les personnes concernées et les détenteurs de données, sur toutes les questions liées aux services d'intermédiation de données fournis. Le représentant légal coopère avec les autorités compétentes pour les services d'intermédiation de données et leur démontre de manière exhaustive, sur demande, les mesures prises et les dispositions mises en place par le prestataire de services d'intermédiation de données pour garantir le respect du présent règlement.

Le prestataire de services d'intermédiation de données est considéré comme relevant de la compétence de l'État membre dans lequel se trouve le représentant légal. La désignation d'un représentant légal par le prestataire de services d'intermédiation de données est sans préjudice d'actions en justice qui pourraient être intentées contre le prestataire de services d'intermédiation de données.

4. Après avoir soumis une notification conformément au paragraphe 1, le prestataire de services d'intermédiation de données peut commencer l'activité sous réserve des conditions énoncées au présent chapitre.

5. La notification visée au paragraphe 1 donne au prestataire de services d'intermédiation de données le droit de fournir des services d'intermédiation de données dans tous les États membres.

6. La notification visée au paragraphe 1 comporte les renseignements suivants:

a) le nom du prestataire de services d'intermédiation de données;

b) le statut juridique, la forme, la structure de propriété et les filiales pertinentes du prestataire de services d'intermédiation de données ainsi que, lorsque le prestataire de services d'intermédiation de données est enregistré dans un registre de commerce ou dans un autre registre public national similaire, son numéro d'enregistrement;

c) l'adresse de l'éventuel établissement principal du prestataire de services d'intermédiation de données dans l'Union et, le cas échéant, de toute succursale dans un autre État membre, ou l'adresse du représentant légal;

d) un site internet public contenant des informations complètes et à jour sur le prestataire de services d'intermédiation de données et ses activités, y compris au minimum les renseignements visés aux points a), b), c) et f);

e) les personnes de contact et les coordonnées du prestataire de services d'intermédiation de données;

f) une description du service d'intermédiation de données que le prestataire de services d'intermédiation de données a l'intention de fournir, ainsi qu'une indication des catégories énumérées à l'article 10 dont relève ce service d'intermédiation de données;

g) une estimation de la date de lancement de l'activité, si celle-ci est différente de la date de la notification.

7. L'autorité compétente en matière de services d'intermédiation de données veille à ce que la procédure de notification soit non discriminatoire et ne fausse pas la concurrence.

8. À la demande du prestataire de services d'intermédiation de données, l'autorité compétente en matière de services d'intermédiation de données délivre, dans un délai d'une semaine à partir du moment où la notification est dûment et entièrement complétée, une déclaration standardisée confirmant que le prestataire de services d'intermédiation de données a soumis la notification visée au paragraphe 4 et que cette notification contient les informations visées au paragraphe 6.

9. À la demande du prestataire de services d'intermédiation de données, l'autorité compétente en matière de services d'intermédiation de données confirme que le prestataire de services d'intermédiation de données respecte le présent article et l'article 12. Dès réception de cette confirmation, ledit prestataire de services d'intermédiation de données peut utiliser le label «prestataire de services d'intermédiation de données reconnu dans l'Union» dans ses communications écrites et orales, ainsi qu'un logo commun.

Afin de garantir que les prestataires de services d'intermédiation de données reconnus dans l'Union sont facilement identifiables dans toute l'Union, la Commission conçoit le logo commun par la voie d'actes d'exécution. Les prestataires de services d'intermédiation de données reconnus dans l'Union affichent clairement le logo commun sur chaque publication en ligne et hors ligne qui se rapporte à leurs activités d'intermédiation de données.

Ces actes d'exécution sont adoptés en conformité avec la procédure consultative visée à l'article 33, paragraphe 2.

10. L'autorité compétente en matière de services d'intermédiation de données notifie à la Commission, sans retard et par voie électronique, toute nouvelle notification. La Commission tient et met régulièrement à jour un registre public de tous les prestataires de services d'intermédiation de données proposant leurs services dans l'Union. Les informations visées au paragraphe 6, points a), b), c), d), f) et g), sont publiées dans le registre public.

11. L'autorité compétente en matière de services d'intermédiation de données peut percevoir des redevances pour la notification conformément au droit national. Ces redevances sont proportionnées et objectives et sont fondées sur les coûts administratifs liés au contrôle du respect des dispositions et aux autres activités de contrôle du marché menées par les autorités compétentes en matière de services d'intermédiation de données en rapport avec les notifications des prestataires de services d'intermédiation de données. Dans le cas des PME et des jeunes pousses, l'autorité compétente en matière de services d'intermédiation de données peut percevoir une redevance réduite ou renoncer à la redevance.

12. Les prestataires de services d'intermédiation de données notifient à l'autorité compétente en matière de services d'intermédiation de données toute modification des renseignements communiqués en vertu du paragraphe 6 dans un délai de quatorze jours à compter de la date de la modification.

13. Lorsqu'un prestataire de services d'intermédiation de données cesse ses activités, il le notifie dans un délai de quinze jours à l'autorité compétente en matière de services d'intermédiation de données concernée, déterminée conformément aux paragraphes 1, 2 et 3.

14. L'autorité compétente en matière de services d'intermédiation de données notifie à la Commission, sans retard et par voie électronique, chaque notification visée aux paragraphes 12 et 13. La Commission met à jour en conséquence le registre public des prestataires de services d'intermédiation de données dans l'Union.

Article 12

Conditions liées à la fourniture de services d'intermédiation de données

La fourniture de services d'intermédiation de données visés à l'article 10 est soumise aux conditions suivantes:

a) le prestataire de services d'intermédiation de données ne peut pas utiliser les données pour lesquelles il fournit des services d'intermédiation de données à des fins autres que leur mise à disposition des utilisateurs de données, et il fournit les services d'intermédiation de données par l'intermédiaire d'une personne morale distincte;

b) les modalités commerciales, y compris la tarification, de la fourniture de services d'intermédiation de données à un détenteur de données ou à un utilisateur de données ne doivent pas être subordonnées au fait que le détenteur de données ou l'utilisateur de données utilise ou non d'autres services fournis par le même prestataire de services d'intermédiation de données ou par une entité liée, et dans l'affirmative, à la mesure dans laquelle le détenteur de données ou l'utilisateur de données utilise ces autres services;

c) les données collectées en ce qui concerne toute activité d'une personne physique ou morale aux fins de la fourniture d'un service d'intermédiation de données, notamment la date, l'heure et les données de géolocalisation, la durée de l'activité et les connexions établies avec d'autres personnes physiques ou morales par la personne qui utilise le service d'intermédiation de données ne doivent être utilisées que pour le développement dudit service d'intermédiation de données, ce qui peut impliquer l'utilisation de données pour la détection de fraudes ou pour la cybersécurité, et sont mises à la disposition des détenteurs de données sur demande;

d) le prestataire de services d'intermédiation de données facilite l'échange des données au format dans lequel il les reçoit d'une personne concernée ou d'un détenteur des données, ne convertit les données dans des formats spécifiques que pour améliorer l'interopérabilité intrasectorielle et transsectorielle, ou si l'utilisateur de données le demande, ou lorsque le droit de l'Union le requiert, ou pour assurer l'harmonisation avec des normes internationales ou européennes en matière de données, et donne aux personnes concernées ou aux détenteurs de données une possibilité de non-participation en ce qui concerne ces conversions, à moins que la conversion ne soit requise par le droit de l'Union;

e) les services d'intermédiation de données peuvent prévoir de fournir aux détenteurs de données ou aux personnes concernées des instruments et services spécifiques supplémentaires dans le but particulier de faciliter l'échange de données, tels que le stockage temporaire, l'organisation, la conversion, l'anonymisation et la pseudonymisation, ces instruments étant uniquement utilisés à la demande expresse ou moyennant l'approbation expresse du détenteur de données ou de la personne concernée et les instruments de tiers proposés dans ce contexte nétant pas utilisés à d'autres fins;

f) le prestataire de services d'intermédiation de données veille à ce que la procédure d'accès à son service soit équitable, transparente et non discriminatoire à l'égard tant des personnes concernées et des détenteurs de données que des utilisateurs de données, y compris en ce qui concerne les prix et les conditions de service;

g) le prestataire de services d'intermédiation de données met en place des procédures pour prévenir les pratiques frauduleuses ou abusives en lien avec des parties cherchant à obtenir un accès via ses services d'intermédiation de données;

h) en cas d'insolvabilité, le prestataire de services d'intermédiation de données assure une continuité raisonnable de la fourniture de ses services d'intermédiation de données et, lorsque ces services d'intermédiation de données assurent le stockage de données, il met en place des mécanismes pour permettre aux détenteurs de données et aux utilisateurs de données d'avoir accès à leurs données, de les transférer ou de les extraire et, lorsque ces services d'intermédiation de données sont fournis entre des personnes concernées et des utilisateurs de données, pour permettre aux personnes concernées d'exercer leurs droits;

i) le prestataire de services d'intermédiation de données prend les mesures appropriées pour assurer l'interopérabilité avec d'autres services d'intermédiation de données, entre autres au moyen de normes ouvertes communément utilisées dans le secteur dans lequel le prestataire de services d'intermédiation de données exerce ses activités;

j) le prestataire de services d'intermédiation de données met en place des mesures techniques, juridiques et organisationnelles appropriées afin d'empêcher le transfert de données à caractère non personnel ou l'accès à celles-ci dans les cas où ils sont illicites au regard du droit de l'Union ou du droit national de l'État membre concerné;

k) le prestataire de services d'intermédiation de données informe sans retard les détenteurs de données en cas de transfert, d'accès ou d'utilisation non autorisés portant sur les données à caractère non personnel qu'il a partagées;

l) le prestataire de services d'intermédiation de données prend les mesures nécessaires pour garantir un niveau de sécurité approprié pour le stockage, le traitement et la transmission de données à caractère non personnel, et le prestataire de services d'intermédiation de données garantit également le niveau de sécurité le plus élevé pour le stockage et la transmission d'informations sensibles sous l'angle de la concurrence;

m) le prestataire de services d'intermédiation de données proposant des services à des personnes concernées agit au mieux de leurs intérêts lorsqu'il facilite l'exercice de leurs droits, notamment en informant et, le cas échéant, en conseillant les personnes concernées de manière concise, transparente, compréhensible et aisément accessible sur les utilisations prévues des données par les utilisateurs de données et sur les conditions générales applicables à ces utilisations, avant que les personnes concernées ne donnent leur consentement;

n) lorsqu'un prestataire de services d'intermédiation de données fournit des outils permettant d'obtenir le consentement de personnes concernées ou l'autorisation de traiter des données mises à disposition par des détenteurs de données, il précise, le cas échéant, la juridiction des pays tiers où l'utilisation des données est prévue et fournit aux personnes concernées des outils permettant à la fois de donner et de retirer leur consentement et aux détenteurs de données des outils permettant à la fois de donner et de retirer l'autorisation de traiter des données;

o) le prestataire de services d'intermédiation de données tient un journal de l'activité d'intermédiation de données.

Article 13

Autorités compétentes en matière de services d'intermédiation de données

1. Chaque État membre désigne une ou plusieurs autorités compétentes pour effectuer les tâches liées à la procédure de notification pour les services d'intermédiation de données et notifie à la Commission l'identité de ces autorités compétentes au plus tard le 24 septembre 2023. Chaque État membre notifie également à la Commission toute modification ultérieure de l'identité de ces autorités compétentes.

2. Les autorités compétentes en matière de services d'intermédiation de données respectent les exigences énoncées à l'article 26.

3. Les pouvoirs des autorités compétentes en matière de services d'intermédiation de données sont sans préjudice des pouvoirs des autorités chargées de la protection des données, des autorités nationales de la concurrence, des autorités chargées de la cybersécurité et des autres autorités sectorielles concernées. Dans le respect de leurs compétences respectives au titre du droit de l'Union et du droit national, ces autorités établissent une coopération solide et échangent les informations qui sont nécessaires à l'accomplissement de leurs tâches en rapport avec les prestataires de services d'intermédiation de données, et visent à assurer la cohérence des décisions prises en application du présent règlement.

Article 14

Contrôle du respect des dispositions

1. Les autorités compétentes en matière de services d'intermédiation de données contrôlent et surveillent le respect par les prestataires de services d'intermédiation de données des exigences énoncées dans le présent chapitre. Les autorités compétentes en matière de services d'intermédiation de données peuvent également contrôler et surveiller le respect par les prestataires de services d'intermédiation de données de leurs obligations, sur la base d'une demande présentée par une personne physique ou morale.

2. Les autorités compétentes en matière de services d'intermédiation de données ont le pouvoir de demander aux prestataires de services d'intermédiation de données ou à leurs représentants légaux toutes les informations nécessaires pour vérifier le respect des exigences énoncées dans le présent chapitre. Toute demande d'information est proportionnée à l'accomplissement de la tâche et est motivée.

3. Lorsque l'autorité compétente en matière de services d'intermédiation de données constate qu'un prestataire de services d'intermédiation de données ne respecte pas une ou plusieurs des exigences énoncées dans le présent chapitre, elle notifie ces constatations audit prestataire de services d'intermédiation de données et lui donne la possibilité d'exposer son point de vue dans un délai de trente jours à compter de la réception de la notification.

4. L'autorité compétente en matière de services d'intermédiation de données a le pouvoir d'exiger qu'il soit mis fin à l'infraction visée au paragraphe 3, dans un délai raisonnable, ou immédiatement dans le cas d'une infraction grave, et prend des mesures appropriées et proportionnées visant à garantir le respect des obligations. À cet égard, les autorités compétentes en matière de services d'intermédiation de données ont le pouvoir, le cas échéant:

a) d'imposer, par le biais de procédures administratives, des sanctions financières dissuasives, pouvant comporter des astreintes et des sanctions avec effet rétroactif, d'engager des procédures judiciaires en vue d'infliger des amendes, ou les deux;

b) d'exiger un report du début de la fourniture du service d'intermédiation de données ou une suspension de cette fourniture jusqu'à ce que les modifications des conditions demandées par l'autorité compétente en matière de services d'intermédiation de données aient été réalisées; ou

c) d'exiger la cessation de la fourniture du service d'intermédiation de données dans le cas où il n'a pas été remédié à des infractions graves ou répétées malgré l'envoi d'une notification préalable conformément au paragraphe 3.

L'autorité compétente en matière de services d'intermédiation de données demande à la Commission de radier le prestataire de services d'intermédiation de données du registre des prestataires de services d'intermédiation de données, une fois qu'elle a ordonné la cessation de la fourniture du service d'intermédiation de données conformément au premier alinéa, point c).

Si un prestataire de service d'intermédiation de données remédie aux infractions, ledit prestataire de service d'intermédiation de données adresse une nouvelle notification à l'autorité compétente en matière de services d'intermédiation de données. L'autorité compétente en matière de services d'intermédiation de données notifie à la Commission chaque nouvelle renotification.

5. Lorsqu'un prestataire de services d'intermédiation de données qui n'est pas établi dans l'Union ne désigne pas de représentant légal ou que ce représentant légal, bien que l'autorité compétente en matière de services d'intermédiation de données lui en fasse la demande, ne fournit pas les informations nécessaires prouvant de manière exhaustive le respect du présent règlement, l'autorité compétente en matière de services d'intermédiation de données a le pouvoir de reporter le début de la fourniture du service d'intermédiation de données ou de suspendre cette fourniture jusqu'à ce que le représentant légal soit désigné ou que les informations nécessaires soient fournies.

6. Les autorités compétentes en matière de services d'intermédiation de données notifient sans retard au prestataire de services d'intermédiation de données concerné les mesures imposées au titre des paragraphes 4 et 5, leur motivation, ainsi que les mesures dont l'adoption est nécessaire pour corriger les manquements constatés, et fixent au prestataire de services d'intermédiation de données concerné un délai raisonnable, ne dépassant pas trente jours, pour se conformer à ces mesures.

7. Si un prestataire de services d'intermédiation de données a son établissement principal ou son représentant légal dans un État membre mais fournit des services dans d'autres États membres, l'autorité compétente en matière de services d'intermédiation de données de l'État membre où est situé l'établissement principal ou dans lequel se trouve le représentant légal et les autorités compétentes en matière de services d'intermédiation de données de ces autres États membres coopèrent et se prêtent assistance. Cette assistance et cette coopération peuvent porter sur les échanges d'informations entre les autorités compétentes en matière de services d'intermédiation de données concernées aux fins de l'accomplissement de leurs tâches au titre du présent règlement et sur les demandes motivées de prendre les mesures visées au présent article.

Lorsqu'une autorité compétente en matière de services d'intermédiation de données dans un État membre sollicite l'assistance d'une autorité compétente en matière de services d'intermédiation de données d'un autre État membre, elle présente une demande motivée. Lorsqu'elle reçoit une telle demande, l'autorité compétente en matière de services d'intermédiation de données fournit une réponse sans retard et dans des délais proportionnés à l'urgence de la demande.

Toutes les informations échangées dans le cadre de la demande d'assistance et fournies au titre du présent paragraphe ne sont utilisées qu'aux fins pour lesquelles elles ont été demandées.

Article 15

Dérogations

Le présent chapitre ne s'applique pas aux organisations altruistes en matière de données reconnues ni aux autres entités sans but lucratif dans la mesure où leurs activités consistent à collecter, pour des objectifs d'intérêt général, des données mises à disposition par des personnes physiques ou morales sur le fondement de l'altruisme en matière de données, à moins que ces organisations et entités ne visent à établir des relations commerciales entre un nombre indéterminé de personnes concernées et de détenteurs de données, d'une part, et des utilisateurs de données, d'autre part.

CHAPITRE IV

Altruisme en matière de données

Article 16

Dispositions nationales relatives à l'altruisme en matière de données

Les États membres peuvent avoir mis en place des dispositions organisationnelles ou techniques, ou les deux, pour faciliter l'altruisme en matière de données. À cette fin, les États membres peuvent élaborer des politiques nationales dans le domaine de l'altruisme en matière de données. Ces politiques nationales peuvent notamment aider les personnes concernées à mettre à disposition volontairement, à des fins d'altruisme en matière de données, des données à caractère personnel les concernant détenues par des organismes du secteur public, et déterminer les informations nécessaires qui doivent être fournies aux personnes concernées en ce qui concerne la réutilisation de leurs données dans l'intérêt général.

Si un État membre élabore de telles politiques nationales, il le notifie à la Commission.

Article 17

Registres publics d'organisations altruistes en matière de données reconnues

1. Chaque autorité compétente pour l'enregistrement des organisations altruistes en matière de données tient et met à jour régulièrement un registre public national des organisations altruistes en matière de données reconnues.

2. La Commission gère, à des fins d'information, un registre public de l'Union des organisations altruistes en matière de données reconnues. Dès lors qu'une entité est enregistrée dans le registre public national des organisations altruistes en matière de données reconnues conformément à l'article 18, elle peut utiliser le label «organisation altruiste en matière de données reconnue dans l'Union» dans ses communications écrites et orales, ainsi qu'un logo commun.

Afin de garantir que les organisations altruistes en matière de données reconnues soient facilement identifiables dans toute l'Union, la Commission conçoit un logo commun par voie d'actes d'exécution. Les organisations altruistes en matière de données reconnues affichent clairement le logo commun sur chaque publication en ligne et hors ligne qui se rapporte à leurs activités altruistes en matière de données. Le logo commun s'accompagne d'un code QR comportant un lien vers le registre public de l'Union des organisations altruistes en matière de données reconnues.

Ces actes d'exécution sont adoptés en conformité avec la procédure consultative visée à l'article 33, paragraphe 2.

Article 18

Conditions générales d'enregistrement

Pour être admise à l'enregistrement dans un registre public national des organisations altruistes en matière de données reconnues, une entité doit:

a) mener des activités altruistes en matière de données;

b) être une personne morale constituée en vertu du droit national pour poursuivre des objectifs d'intérêt général prévus dans le droit national, le cas échéant;

c) exercer ses activités dans un but non lucratif et être juridiquement indépendante de toute entité exerçant des activités dans un but lucratif;

d) mener ses activités altruistes en matière de données par l'intermédiaire d'une structure qui, sur le plan fonctionnel, est distincte de ses autres activités;

e) se conformer au recueil de règles visé à l'article 22, paragraphe 1, au plus tard dix-huit mois après la date d'entrée en vigueur des actes délégués visés audit paragraphe.

Article 19

Enregistrement d'organisations altruistes en matière de données reconnues

1. Une entité qui satisfait aux exigences énoncées à l'article 18 peut présenter une demande d'enregistrement dans le registre public national des organisations altruistes en matière de données reconnues dans l'État membre dans lequel elle est établie.

2. Une entité qui satisfait aux exigences énoncées à l'article 18 et a des établissements dans plusieurs États membres peut présenter une demande d'enregistrement dans le registre public national des organisations altruistes en matière de données reconnues dans l'État membre dans lequel elle a son établissement principal.

3. Une entité qui satisfait aux exigences énoncées à l'article 18 mais qui n'est pas établie dans l'Union désigne un représentant légal dans l'un des États membres dans lesquels les services fondés sur l'altruisme en matière de données sont proposés.

Aux fins de garantir le respect du présent règlement, le représentant légal est mandaté par l'entité pour être contacté, en plus de ladite entité ou à sa place, par les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données ou les personnes concernées et les détenteurs de données, sur toutes les questions liées à ladite entité. Le représentant légal coopère avec les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données et leur démontre de manière exhaustive, sur demande, les mesures prises et les dispositions mises en place par l'entité pour garantir le respect du présent règlement.

L'entité est considérée comme relevant de la compétence de l'État membre dans lequel se trouve son représentant légal. Une telle entité peut présenter une demande d'enregistrement dans le registre public national des organisations altruistes en matière de données reconnues dans cet État membre. La désignation d'un représentant légal par l'entité est sans préjudice d'actions en justice qui pourraient être intentées contre l'entité.

4. Les demandes d'enregistrement visées aux paragraphes 1, 2 et 3 comportent les renseignements suivants:

a) le nom de l'entité;

b) le statut juridique et la forme de l'entité ainsi que, lorsque l'entité est enregistrée dans un registre public national, son numéro d'enregistrement;

c) les statuts de l'entité, le cas échéant;

d) les sources de revenus de l'entité;

e) l'adresse de l'éventuel établissement principal de l'entité dans l'Union et, le cas échéant, de toute succursale dans un autre État membre, ou l'adresse du représentant légal;

f) un site internet public contenant des informations complètes et à jour sur l'entité et ses activités, y compris au minimum les renseignements visés aux points a), b), d), e) et h);

g) les personnes de contact et les coordonnées de l'entité;

h) les objectifs d'intérêt général qu'elle entend promouvoir par la collecte de données;

i) la nature des données que l'entité entend contrôler ou traiter et, dans le cas des données à caractère personnel, une indication des catégories de données à caractère personnel;

j) tout autre document démontrant qu'il est satisfait aux exigences énoncées à l'article 18.

5. Lorsque l'entité a fourni tous les renseignements nécessaires en vertu du paragraphe 4 et après que l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données a évalué la demande d'enregistrement et établi que l'entité satisfait aux exigences énoncées à l'article 18, ladite autorité enregistre l'entité dans le registre public national des organisations altruistes en matière de données reconnues, dans un délai de douze semaines suivant la date de réception de la demande d'enregistrement. L'enregistrement est valable dans tous les États membres.

L'autorité compétente pour l'enregistrement des organisations altruistes en matière de données notifie tout enregistrement à la Commission. La Commission fait figurer l'enregistrement concerné dans le registre public de l'Union des organisations altruistes en matière de données reconnues.

6. Les renseignements visés au paragraphe 4, points a), b), f), g) et h), sont publiés dans le registre public national des organisations altruistes en matière de données reconnues concerné.

7. L'organisation altruiste en matière de données reconnue notifie à l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données concernée toute modification des renseignements communiqués en vertu du paragraphe 4 dans un délai de quatorze jours à compter de la date de la modification.

L'autorité compétente pour l'enregistrement des organisations altruistes en matière de données notifie à la Commission, sans retard et par voie électronique, chaque notification de ce type. Sur la base d'une telle notification, la Commission met à jour, sans retard, le registre public de l'Union des organisations altruistes en matière de données reconnues.

Article 20

Obligations de transparence

1. L'organisation altruiste en matière de données reconnue tient des registres complets et exacts concernant:

a) toutes les personnes physiques ou morales qui se sont vu offrir la possibilité de traiter des données détenues par cette organisation altruiste en matière de données reconnue, ainsi que leurs coordonnées;

b) la date ou la durée du traitement des données à caractère personnel ou de l'utilisation des données à caractère non personnel;

c) la finalité du traitement, telle qu'elle a été déclarée par la personne physique ou morale qui s'est vu offrir la possibilité d'effectuer ce traitement;

d) les éventuelles redevances acquittées par les personnes physiques ou morales traitant les données.

2. L'organisation altruiste en matière de données reconnue établit et transmet à l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données concernée un rapport annuel d'activité qui contient au moins les éléments suivants:

a) des informations sur les activités de l'organisation altruiste en matière de données reconnue;

b) une description de la manière dont les objectifs d'intérêt général pour lesquels des données ont été collectées ont été promus pendant l'exercice considéré;

c) une liste de toutes les personnes physiques et morales qui ont été autorisées à traiter des données qu'elle détient, assortie d'une description sommaire des objectifs d'intérêt général poursuivis par ce traitement de données et de la description des moyens techniques employés en vue de cette utilisation, y compris une description des techniques appliquées pour préserver la vie privée et la protection des données;

d) une synthèse des résultats du traitement des données autorisé par l'organisation altruiste en matière de données reconnue, s'il y a lieu;

e) des informations sur les sources de recettes de l'organisation altruiste en matière de données reconnue, en particulier toutes les recettes résultant de l'autorisation d'accès aux données, et sur les dépenses.

Article 21

Exigences spécifiques visant à préserver les droits et intérêts des personnes concernées et des détenteurs de données quant à leurs données

1. L'organisation altruiste en matière de données reconnue informe les personnes concernées ou les détenteurs de données préalablement à tout traitement de leurs données d'une manière claire et aisément intelligible:

a) des objectifs d'intérêt général et, le cas échéant, de la finalité déterminée, explicite et légitime pour laquelle les données à caractère personnel doivent être traitées et pour laquelle elle autorise le traitement de données les concernant par un utilisateur de données;

b) de la localisation de tout traitement effectué dans un pays tiers et des objectifs d'intérêt général pour lesquels elle autorise ledit traitement, lorsque le traitement est effectué par l'organisation altruiste en matière de données reconnue.

2. L'organisation altruiste en matière de données reconnue n'utilise pas les données pour des objectifs autres que ceux d'intérêt général pour lesquels la personne concernée ou le détenteur des données autorise le traitement. L'organisation altruiste en matière de données reconnue ne recourt pas à des pratiques commerciales trompeuses pour solliciter la fourniture de données.

3. L'organisation altruiste en matière de données reconnue fournit des outils permettant d'obtenir le consentement des personnes concernées ou l'autorisation de traiter des données mises à disposition par des détenteurs de données. L'organisation altruiste en matière de données reconnue fournit également des outils permettant de retirer facilement ce consentement ou cette autorisation.

4. L'organisation altruiste en matière de données reconnue prend des mesures pour assurer un niveau de sécurité approprié pour le stockage et le traitement des données à caractère non personnel qu'elle a collectées sur le fondement de l'altruisme en matière de données.

5. L'organisation altruiste en matière de données reconnue informe, sans retard, les détenteurs de données de tout transfert, de tout accès ou de toute utilisation non autorisés portant sur les données à caractère non personnel qu'elle a partagées.

6. Lorsque l'organisation altruiste en matière de données reconnue facilite le traitement de données par des tiers, y compris en fournissant des outils permettant d'obtenir le consentement de personnes concernées ou l'autorisation de traiter des données mises à disposition par des détenteurs de données, elle précise, le cas échéant, la juridiction du pays tiers où l'utilisation des données est prévue.

Article 22

Recueil de règles

1. La Commission adopte des actes délégués conformément à l'article 32 afin de compléter le présent règlement en établissant un recueil de règles fixant:

a) des exigences appropriées en matière d'information pour veiller à ce que les personnes concernées et les détenteurs de données reçoivent, avant qu'un consentement ou une autorisation ne soit donné pour l'altruisme en matière de données, des informations suffisamment détaillées, claires et transparentes concernant l'utilisation des données, les outils permettant de donner et de retirer le consentement ou l'autorisation, et les mesures prises pour éviter une mauvaise utilisation des données partagées avec l'organisation altruiste en matière de données;

b) des exigences techniques et de sécurité appropriées pour garantir un niveau de sécurité approprié pour le stockage et le traitement des données, ainsi que pour les outils permettant de donner et de retirer le consentement ou l'autorisation;

c) des feuilles de route en matière de communication adoptant une approche pluridisciplinaire pour sensibiliser à l'altruisme en matière de données, à la désignation en tant que «organisation altruiste en matière de données reconnue dans l'Union» et au recueil de règles les parties prenantes concernées, notamment les détenteurs de données et les personnes concernées pouvant potentiellement partager leurs données;

d) des recommandations relatives aux normes d'interopérabilité pertinentes.

2. Le recueil de règles visé au paragraphe 1 est élaboré en étroite coopération avec les organisations altruistes en matière de données et les parties prenantes concernées.

Article 23

Autorités compétentes pour l'enregistrement des organisations altruistes en matière de données

1. Chaque État membre désigne une ou plusieurs autorités compétentes responsables de son registre public national des organisations altruistes en matière de données reconnues.

Les autorités compétentes pour l'enregistrement d'organisations altruistes en matière de données respectent les exigences énoncées à l'article 26.

2. Chaque État membre notifie à la Commission l'identité de leurs autorités compétentes pour l'enregistrement des organisations altruistes en matière de données au plus tard le 24 septembre 2023. Chaque État membre notifie également à la Commission toute modification ultérieure de l'identité desdites autorités compétentes.

3. L'autorité compétente pour l'enregistrement des organisations altruistes en matière de données d'un État membre accomplit ses tâches en coopération avec l'autorité chargée de la protection des données concernée, lorsque ces tâches se rapportent au traitement de données à caractère personnel, et avec les autorités sectorielles concernées dudit État membre.

Article 24

Contrôle du respect des dispositions

1. Les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données contrôlent et surveillent le respect, par les organisations altruistes en matière de données reconnues, des exigences énoncées dans le présent chapitre. L'autorité compétente pour l'enregistrement des organisations altruistes en matière de données peut également contrôler et surveiller le respect par de telles organisations altruistes en matière de données reconnues de leurs obligations sur la base d'une demande présentée par une personne physique ou morale.

2. Les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données ont le pouvoir de demander aux organisations altruistes en matière de données reconnues les informations qui lui sont nécessaires pour vérifier qu'elles respectent les exigences énoncées dans le présent chapitre. Toute demande d'information est proportionnée à l'accomplissement de la tâche et est motivée.

3. Lorsque l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données constate qu'une organisation altruiste en matière de données reconnue ne respecte pas une ou plusieurs des exigences énoncées dans le présent chapitre, elle notifie ces constatations à l'organisation altruiste en matière de données reconnue et lui donne la possibilité d'exposer son point de vue dans un délai de trente jours à compter de la réception de la notification.

4. L'autorité compétente pour l'enregistrement des organisations altruistes en matière de données a le pouvoir d'exiger qu'il soit mis fin à l'infraction visée au paragraphe 3, soit immédiatement soit dans un délai raisonnable, et prend des mesures appropriées et proportionnées pour garantir le respect des dispositions.

5. Si une organisation altruiste en matière de données reconnue ne respecte pas une ou plusieurs des exigences énoncées dans le présent chapitre même après avoir reçu une notification de l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données conformément au paragraphe 3, ladite organisation altruiste en matière de données reconnue:

a) perd le droit d'utiliser le label d'«organisation altruiste en matière de données reconnue dans l'Union» dans toute communication écrite et orale;

b) est radiée du registre public national des organisations altruistes en matière de données reconnues concerné et du registre public de l'Union des organisations altruistes en matière de données reconnues.

Toute décision révoquant le droit d'utiliser le label d'«organisation altruiste en matière de données reconnue dans l'Union» prévue au premier alinéa, point a), est rendue publique par l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données.

6. Si une organisation altruiste en matière de données reconnue a son établissement principal ou son représentant légal dans un État membre mais qu'elle exerce des activités dans d'autres États membres, l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données de l'État membre où est situé l'établissement principal ou dans lequel se trouve le représentant légal et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données de ces autres États membres coopèrent et se prêtent assistance. Cette assistance et cette coopération peuvent porter sur les échanges d'informations entre les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données concernées aux fins de l'accomplissement de leurs tâches au titre du présent règlement et sur les demandes motivées de prendre les mesures visées au présent article.

Lorsqu'une autorité compétente pour l'enregistrement des organisations altruistes en matière de données dans un État membre sollicite l'assistance d'une autorité compétente pour l'enregistrement des organisations altruistes en matière de données dans un autre État membre, elle présente une demande motivée. L'autorité compétente pour l'enregistrement des organisations altruistes en matière de données veille, à la suite d'une telle demande, à fournir une réponse sans retard et dans des délais proportionnés à l'urgence de la demande.

Toutes les informations échangées dans le cadre de la demande d'assistance et fournies au titre du présent paragraphe ne sont utilisées qu'aux fins pour lesquelles elles ont été demandées.

Article 25

Formulaire européen de consentement à l'altruisme en matière de données

1. Afin de faciliter la collecte de données fondée sur l'altruisme en matière de données, la Commission adopte des actes d'exécution établissant et développant un formulaire européen de consentement à l'altruisme en matière de données, après consultation du comité européen de la protection des données, en tenant compte des avis du comité européen de l'innovation dans le domaine des données et en associant dûment les parties prenantes concernées. Le formulaire permet de recueillir le consentement ou l'autorisation dans tous les États membres selon un format uniforme. Ces actes d'exécution sont adoptés en conformité avec la procédure consultative visée à l'article 33, paragraphe 2.

2. Le formulaire européen de consentement à l'altruisme en matière de données est conçu selon une approche modulaire permettant son adaptation à des secteurs particuliers et à des fins différentes.

3. Lorsque des données à caractère personnel sont communiquées, le formulaire européen de consentement à l'altruisme en matière de données garantit que les personnes concernées sont en mesure de donner et de retirer leur consentement à une opération particulière de traitement de données en conformité avec les exigences du règlement (UE) 2016/679.

4. Le formulaire est disponible de manière à pouvoir être imprimé sur papier tout en étant facile à comprendre, ainsi que sous une forme électronique lisible par machine.

CHAPITRE V

Autorités compétentes et dispositions procédurales

Article 26

Exigences relatives aux autorités compétentes

1. Les autorités compétentes en matière de services d'intermédiation de données et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données sont juridiquement distinctes et fonctionnellement indépendantes de tout prestataire de services d'intermédiation de données ou de toute organisation altruiste en matière de données reconnue. Les fonctions des autorités compétentes en matière de services d'intermédiation de données et des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données peuvent être exercées par la même autorité. Les États membres peuvent soit établir une ou plusieurs nouvelles autorités à ces fins, soit s'appuyer sur des autorités existantes.

2. Les autorités compétentes en matière de services d'intermédiation de données et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données accomplissent leurs tâches de manière impartiale, transparente, cohérente, fiable et rapide. Dans l'exercice de leurs tâches, elles préservent une concurrence loyale et veillent à l'absence de discrimination.

3. Les cadres supérieurs et le personnel chargé d'accomplir les tâches concernées des autorités compétentes en matière de services d'intermédiation de données et des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données ne peuvent pas être le concepteur, le fabricant, le fournisseur, l'installateur, l'acheteur, le propriétaire, l'utilisateur ou le responsable de la maintenance des services qu'ils évaluent, ni le représentant autorisé d'aucune de ces parties. Cela n'exclut pas l'utilisation de services évalués qui sont nécessaires au fonctionnement de l'autorité compétente en matière de services d'intermédiation de données et de l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données, ou l'utilisation de ces services à des fins personnelles.

4. Les cadres supérieurs et le personnel des autorités compétentes en matière de services d'intermédiation de données et des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données ne participent à aucune activité susceptible d'entrer en conflit avec l'indépendance de leur jugement ou leur intégrité en lien avec les activités d'évaluation qui leur sont assignées.

5. Les autorités compétentes en matière de services d'intermédiation de données et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données disposent des ressources humaines et financières suffisantes, y compris des connaissances et ressources techniques nécessaires, pour mener à bien les tâches qui leur sont assignées.

6. Sur demande motivée et sans retard, les autorités compétentes en matière de services d'intermédiation de données et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données d'un État membre fournissent à la Commission et aux autorités compétentes en matière de services d'intermédiation de données et aux autorités compétentes pour l'enregistrement des organisations altruistes en matière de données d'autres États membres les informations nécessaires à l'accomplissement des tâches qui leur incombent au titre du présent règlement. Lorsqu'une autorité compétente en matière de services d'intermédiation de données ou une autorité compétente pour l'enregistrement des organisations altruistes en matière de données considère que les informations demandées sont confidentielles selon les dispositions du droit de l'Union et du droit national relatives à la confidentialité commerciale et au secret professionnel, la Commission et toutes les autres autorités compétentes en matière de services d'intermédiation de données ou les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données concernées garantissent cette confidentialité et ce secret.

Article 27

Droit d'introduire une réclamation

1. Les personnes physiques et morales ont le droit d'introduire une réclamation concernant toute question relevant du champ d'application du présent règlement, individuellement ou, le cas échéant, collectivement, auprès de l'autorité compétente en matière de services d'intermédiation de données concernée contre un prestataire de services d'intermédiation de données ou auprès de l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données concernée contre une organisation altruiste en matière de données reconnue.

2. L'autorité compétente en matière de services d'intermédiation de données ou l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données auprès de laquelle la réclamation a été introduite informe l'auteur de la réclamation:

a) de l'état d'avancement de la procédure et de la décision prise; et

b) des recours juridictionnels prévus à l'article 28.

Article 28

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 visées à l'article 14 prises par les autorités compétentes en matière de services d'intermédiation de données dans le domaine de la gestion, du contrôle et de la mise en œuvre du régime de notification pour les prestataires de services d'intermédiation de données et les décisions juridiquement contraignantes visées aux articles 19 et 24 prises par les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données dans le domaine du contrôle des organisations altruistes en matière de données reconnues.

2. Les recours formés en vertu du présent article sont portés devant les juridictions de l'État membre de l'autorité compétente en matière de services d'intermédiation de données ou de l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données 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.

3. Lorsqu'une autorité compétente en matière de services d'intermédiation de données ou une autorité compétente pour l'enregistrement des organisations altruistes en matière de données ne donne pas suite à une réclamation, toute personne physique ou morale lésée a, conformément au droit national, soit le droit à un recours juridictionnel effectif, soit accès à un réexamen réalisé par un organe impartial doté des compétences appropriées.

CHAPITRE VI

Comité européen de l'innovation dans le domaine des données

Article 29

Comité européen de l'innovation dans le domaine des données

1. La Commission institue un comité européen de l'innovation dans le domaine des données sous la forme d'un groupe d'experts, qui se compose de représentants des autorités compétentes en matière de services d'intermédiation de données et des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données de tous les États membres, du comité européen de la protection des données, du Contrôleur européen de la protection des données, de l'ENISA, de la Commission, du représentant de l'UE pour les PME ou d'un représentant désigné par le réseau des représentants des PME, et d'autres représentants d'organismes compétents dans des secteurs particuliers ainsi que d'organismes disposant d'une expertise particulière. Lorsqu'elle nomme des experts individuels, la Commission s'efforce de parvenir à un équilibre entre les hommes et les femmes ainsi qu'à un équilibre géographique parmi les membres du groupe d'experts.

2. Le comité européen de l'innovation dans le domaine des données se compose au moins des trois sous-groupes suivants:

a) un sous-groupe composé des autorités compétentes en matière de services d'intermédiation de données et des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données en vue de s'acquitter des missions prévues à l'article 30, points a), c), j) et k);

b) un sous-groupe chargé des discussions techniques sur la normalisation, la portabilité et l'interopérabilité conformément à l'article 30, points f) et g);

c) un sous-groupe chargé de la participation des parties prenantes, composé de représentants pertinents de l'industrie, de la recherche, des milieux universitaires, de la société civile, des organismes de normalisation, des espaces européens communs de données pertinents et d'autres parties prenantes concernées et de tiers qui conseillent le comité européen de l'innovation dans le domaine des données sur les missions prévues à l'article 30, points d), e), f), g) et h).

3. La Commission préside les réunions du comité européen de l'innovation dans le domaine des données.

4. Le comité européen de l'innovation dans le domaine des données est assisté par un secrétariat assuré par la Commission.

Article 30

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

Le comité européen de l'innovation dans le domaine des données s'acquitte des missions suivantes:

a) conseiller et assister la Commission en ce qui concerne l'élaboration d'une pratique cohérente des organismes du secteur public et des organismes compétents visés à l'article 7, paragraphe 1, pour la gestion des demandes de réutilisation des catégories de données visées à l'article 3, paragraphe 1;

b) conseiller et assister la Commission en ce qui concerne l'élaboration d'une pratique cohérente pour l'altruisme en matière de données dans l'ensemble de l'Union;

c) conseiller et assister la Commission en ce qui concerne l'élaboration d'une pratique cohérente des autorités compétentes en matière de services d'intermédiation de données et des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données quant à l'application des exigences auxquelles sont soumis les prestataires de services d'intermédiation de données et les organisations altruistes en matière de données reconnues;

d) conseiller et assister la Commission en ce qui concerne l'élaboration de lignes directrices cohérentes sur la meilleure façon de protéger, dans le cadre du présent règlement, les données à caractère non personnel commercialement sensibles, notamment les secrets d'affaires, mais aussi les données à caractère non personnel représentant des contenus protégés par des droits de propriété intellectuelle contre un accès illicite susceptible de conduire à un vol de propriété intellectuelle ou à de l'espionnage industriel;

e) conseiller et assister la Commission en ce qui concerne l'élaboration de lignes directrices cohérentes relatives aux exigences en matière de cybersécurité pour l'échange et le stockage de données;

f) conseiller la Commission, notamment en tenant compte de la contribution des organismes de normalisation, sur la hiérarchisation des normes transsectorielles à utiliser et à mettre au point pour l'utilisation de données et le partage de données transsectoriel entre les espaces européens communs de données émergents, la comparaison et l'échange transsectoriels des meilleures pratiques en ce qui concerne les exigences sectorielles de sécurité et les procédures d'accès, en prenant en considération les activités de normalisation transsectorielle, notamment en précisant et en distinguant les normes et pratiques transsectorielles des normes et pratiques sectorielles;

g) aider la Commission, notamment en tenant compte de la contribution des organismes de normalisation, à lutter contre la fragmentation du marché intérieur et de l'économie des données au sein du marché intérieur en améliorant l'interopérabilité transfrontalière et transsectorielle des données ainsi que les services de partage de données entre les différents secteurs et domaines, en tirant parti des normes européennes, internationales ou nationales existantes dans le but, entre autres, d'encourager la création d'espaces européens communs de données;

h) proposer des lignes directrices pour des espaces européens communs de données, à savoir des cadres interopérables pour les différentes finalités ou pour les différents secteurs ou encore transsectoriels de normes et de pratiques communes visant à partager ou à traiter conjointement des données en vue, entre autres, de la mise au point de nouveaux produits et services, de la recherche scientifique ou d'initiatives de la société civile, ces normes et pratiques communes tenant compte des normes existantes, respectant les règles de concurrence et garantissant un accès non discriminatoire à tous les participants, afin de faciliter le partage des données dans l'Union et de tirer parti du potentiel des espaces de données existants et futurs, notamment en ce qui concerne:

   i) les normes transsectorielles à utiliser et à mettre au point pour l'utilisation de données et le partage de données transsectoriel, la comparaison et l'échange transsectoriels des meilleures pratiques en ce qui concerne les exigences sectorielles de sécurité et les procédures d'accès, en tenant compte des activités de normalisation des différents secteurs, notamment en précisant et en distinguant les normes et pratiques transsectorielles des normes et pratiques sectorielles;

   ii) les exigences visant à lutter contre les obstacles à l'entrée sur le marché et à éviter les effets de verrouillage, afin de garantir une concurrence loyale et l'interopérabilité;

iii) une protection adéquate des transferts licites de données vers des pays tiers, y compris des garanties contre tout transfert interdit par le droit de l'Union;

iv) une représentation adéquate et non discriminatoire des parties prenantes concernées dans la gouvernance d'espaces européens communs de données;

v) le respect des exigences de cybersécurité conformément au droit de l'Union;

i) faciliter la coopération entre les États membres en ce qui concerne la définition de conditions harmonisées permettant la réutilisation des catégories de données visées à l'article 3, paragraphe 1, détenues par des organismes du secteur public dans l'ensemble du marché intérieur;

j) faciliter la coopération entre les autorités compétentes en matière de services d'intermédiation de données et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données par le renforcement des capacités et l'échange d'informations, notamment en établissant des méthodes pour l'échange efficace d'informations relatives, d'une part, à la procédure de notification applicable aux prestataires de services d'intermédiation de données et, d'autre part, à l'enregistrement et au contrôle des organisations altruistes en matière de données reconnues, y compris la coordination en ce qui concerne la fixation de redevances ou de sanctions, ainsi que faciliter la coopération entre les autorités compétentes en matière de services d'intermédiation de données et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données en ce qui concerne l'accès international aux données et le transfert international de données;

k) conseiller et assister la Commission pour ce qui est d'évaluer si les actes d'exécution visés à l'article 5, paragraphes 11 et 12, doivent être adoptés;

l) conseiller et assister la Commission en ce qui concerne l'élaboration du formulaire européen de consentement à l'altruisme en matière de données conformément à l'article 25, paragraphe 1;

m) conseiller la Commission en ce qui concerne l'amélioration du cadre réglementaire international des données à caractère non personnel, y compris la normalisation.

CHAPITRE VII

Accès international et transfert international

Article 31

Accès international et transfert international

1. L'organisme du secteur public, la personne physique ou morale à laquelle le droit de réutilisation des données a été accordé en vertu du chapitre II, le prestataire de services d'intermédiation de données ou l'organisation altruiste en matière de données reconnue prend toutes les mesures techniques, juridiques et organisationnelles raisonnables, y compris des arrangements contractuels, afin d'empêcher le transfert international de données à caractère non personnel détenues dans l'Union ou l'accès international des pouvoirs publics à celles-ci 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 d'une juridiction d'un pays tiers et toute décision d'une autorité administrative d'un pays tiers exigeant d'un organisme du secteur public, d'une personne physique ou morale à laquelle le droit de réutilisation des données a été accordé en vertu du chapitre II, d'un prestataire de services d'intermédiation de données ou d'une organisation altruiste en matière de données reconnue qu'il ou elle transfère des données à caractère non personnel détenues dans l'Union ou y donne accès dans le cadre du présent règlement ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou sur tout accord de ce type entre le pays tiers demandeur et un État membre.

3. En l'absence d'accord international tel qu'il est visé au paragraphe 2 du présent article, lorsqu'un organisme du secteur public, une personne physique ou morale à laquelle le droit de réutilisation des données a été accordé en vertu du chapitre II, un prestataire de services d'intermédiation de données ou une organisation altruiste en matière de données reconnue est destinataire d'une décision d'une juridiction d'un pays tiers ou d'une décision d'une autorité administrative d'un pays tiers de transférer des données à caractère non personnel détenues dans l'Union ou d'y donner accès dans le cadre du présent règlement, et lorsque le respect d'une telle décision risque de mettre le destinataire en conflit avec le droit de l'Union ou 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 si:

a) le système du pays tiers exige que les motifs et la proportionnalité de cette décision soient exposés et que cette décision revête un caractère spécifique, par exemple en établissant un lien suffisant avec certaines personnes suspectées, ou avec des infractions;

b) l'objection motivée du destinataire peut faire l'objet d'un réexamen par une juridiction compétente du pays tiers; et

c) la juridiction compétente du pays tiers qui rend la décision ou réexamine la décision d'une autorité administrative est habilitée, en vertu du droit de ce pays tiers, à prendre dûment en compte les intérêts juridiques pertinents du fournisseur des données protégées par le droit de l'Union ou par le droit national de l'État membre concerné.

4. Si les conditions prévues par le paragraphe 2 ou 3 sont réunies, l'organisme du secteur public, la personne physique ou morale à laquelle le droit de réutilisation des données a été accordé en vertu du chapitre II, le prestataire de services d'intermédiation de données ou l'organisation altruiste en matière de données reconnue fournit le volume minimal de données admissible en réponse à une demande, sur la base d'une interprétation raisonnable de la demande.

5. L'organisme du secteur public, la personne physique ou morale à laquelle le droit de réutilisation des données a été accordé en vertu du chapitre II, le prestataire de services d'intermédiation de données et l'organisation altruiste en matière de données reconnue informe le détenteur de données de l'existence d'une demande d'accès à des données le concernant qui émane d'une autorité administrative d'un pays tiers, avant d'y donner suite, 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

Délégation et comité

Article 32

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 5, paragraphe 13, et à l'article 22, paragraphe 1, est conféré à la Commission pour une durée indéterminée à compter du 23 juin 2022.

3. La délégation de pouvoir visée à l'article 5, paragraphe 13, et à l'article 22, paragraphe 1, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

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

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

6. Un acte délégué adopté en vertu de l'article 5, paragraphe 13, et de l'article 22, paragraphe 1, 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 33

Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) nº 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 4 du règlement (UE) nº 182/2011 s'applique.

3. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

CHAPITRE IX

Dispositions finales et transitoires

Article 34

Sanctions

1. Les États membres déterminent le régime des sanctions applicables aux violations des obligations relatives aux transferts de données à caractère non personnel vers des pays tiers en vertu de l'article 5, paragraphe 14, et de l'article 31, de l'obligation de notification incombant aux prestataires de services d'intermédiation de données en vertu de l'article 11, des conditions liées à la fourniture de services d'intermédiation de données en vertu de l'article 12 et des conditions liées à l'enregistrement en tant qu'organisation altruiste en matière de données reconnue en vertu des articles 18, 20, 21 et 22, et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Ces sanctions doivent être effectives, proportionnées et dissuasives. Dans leur régime de sanctions, les États membres tiennent compte des recommandations du comité européen de l'innovation dans le domaine des données. Les États membres informent la Commission, au plus tard le 24 septembre 2023, 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.

2. Les États membres prennent en compte les critères indicatifs et non exhaustifs suivants lorsqu'il s'agit d'imposer des sanctions aux prestataires de services d'intermédiation de données et aux organisations altruistes en matière de données reconnues en cas d'infraction au présent règlement, le cas échéant:

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

b) toute mesure prise par le prestataire de services d'intermédiation de données ou l'organisation altruiste en matière de données reconnue pour atténuer ou réparer le préjudice causé par l'infraction;

c) toute infraction antérieure commise par le prestataire de services d'intermédiation de données ou l'organisation altruiste en matière de données reconnue;

d) les avantages financiers obtenus ou les pertes évitées par le prestataire de services d'intermédiation de données ou l'organisation altruiste en matière de données reconnue 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.

Article 35

Évaluation et réexamen

Au plus tard le 24 septembre 2025, 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. Ce rapport est au besoin accompagné de propositions législatives.

Ce rapport porte en particulier sur:

a) l'application et le fonctionnement du régime de sanctions établi par les États membres en vertu de l'article 34;

b) le niveau de respect du présent règlement par les représentants légaux des prestataires de services d'intermédiation de données et des organisations altruistes en matière de données reconnues qui ne sont pas établis dans l'Union et le niveau d'applicabilité des sanctions imposées à ces prestataires et organisations;

c) le type d'organisations altruistes en matière de données enregistrées au titre du chapitre IV et un aperçu des objectifs d'intérêt général pour lesquels les données sont partagées en vue d'établir des critères clairs à cet égard.

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

Article 36

Modification du règlement (UE) 2018/1724

Dans le tableau figurant à l'annexe II du règlement (UE) 2018/1724, la mention «Démarrage et gestion d'une entreprise, et cessation d'activité» est remplacée par le texte suivant:

Événements	Procédures	Résultat escompté, sous réserve d'une évaluation de la demande par l'autorité compétente conformément au droit national, le cas échéant
Démarrage et gestion d'une entreprise, et cessation d'activité	Notification de l'activité économique, autorisation d'exercer une activité économique, modifications de l'activité économique et cessation de l'activité économique sans procédure d'insolvabilité ou de liquidation, à l'exclusion de l'enregistrement initial d'une activité économique au registre du commerce et hors procédures relatives à la constitution de sociétés ou à tout dépôt de pièces ultérieur par des sociétés au sens de l'article 54, deuxième alinéa, du traité sur le fonctionnement de l'Union européenne	Accusé de réception de la notification ou de la modification, ou de la demande d'autorisation de l'activité économique
	Enregistrement d'un employeur (personne physique) auprès d'un régime obligatoire de pension et d'assurance	Confirmation d'enregistrement ou numéro de sécurité sociale
	Enregistrement de salariés auprès de régimes obligatoires de pension et d'assurance	Confirmation d'enregistrement ou numéro de sécurité sociale
	Soumettre une déclaration d'impôt sur les sociétés	Accusé de réception de la déclaration
	Notification de la fin du contrat de travail d'un salarié au régime de sécurité sociale, à l'exclusion des procédures de licenciement collectif	Accusé de réception de la notification
	Paiement des cotisations sociales pour les salariés	Reçu ou autre mode de confirmation du paiement des cotisations sociales pour les salariés
	Notification d'un prestataire de services d'intermédiation de données	Accusé de réception de la notification
	Enregistrement en tant qu'organisation altruiste en matière de données reconnue dans l'Union	Confirmation de l'enregistrement

Article 37

Dispositions transitoires

Les entités fournissant les services d'intermédiation de données visés à l'article 10 au 23 juin 2022 se conforment aux obligations énoncées au chapitre III au plus tard le 24 septembre 2025.

Article 38

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 24 septembre 2023.

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

Fait à Bruxelles, le 30 mai 2022.

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président*
R. METSOLA	B. LE MAIRE