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

(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) La transformation numérique de l'économie s'accélère. Les technologies de l'information et des communications ne constituent plus un secteur d'activité parmi d'autres, mais la base de tous les systèmes économiques innovants et des sociétés modernes. Les données électroniques sont au centre de ces systèmes et peuvent générer une grande valeur lorsqu'elles sont analysées ou combinées à des services et des produits. Dans le même temps, le développement rapide de l'économie des données et des technologies émergentes telles que l'intelligence artificielle, les produits et les services en lien avec l'internet des objets, les systèmes autonomes et la 5G soulèvent de nouvelles questions juridiques quant à l'accès aux données et à leur réutilisation, à la responsabilité, à l'éthique et à la solidarité. Des travaux devraient être envisagés sur la question de la responsabilité, notamment par la mise en œuvre de codes de conduite par autorégulation et d'autres bonnes pratiques, en tenant compte des recommandations, des décisions et des mesures prises sans interaction humaine tout au long de la chaîne de valeur du traitement des données. Ces travaux pourraient également porter sur des mécanismes appropriés visant à déterminer les responsabilités et à transférer les responsabilités entre services coopérant, les assurances et les audits.

(2) Les chaînes de valeur des données sont le résultat de diverses activités: création et collecte des données; agrégation et organisation des données; traitement des données; analyse, commercialisation et distribution des données; utilisation et réutilisation des données. Le fonctionnement efficace et efficient du traitement des données est un élément fondamental de toute chaîne de valeur. Toutefois, le fonctionnement efficace et efficient du traitement des données et le développement de l'économie des données dans l'Union sont entravés, en particulier, par deux types d'obstacles à la mobilité des données et au marché intérieur: les exigences en matière de localisation des données mises en place par les autorités des États membres et les pratiques menant à une dépendance à l'égard des fournisseurs dans le secteur privé.

(3) La liberté d'établissement et la liberté de prestation de services consacrées par le traité sur le fonctionnement de l'Union européenne s'appliquent aux services de traitement des données. Cependant, la prestation de ces services est entravée ou, parfois, empêchée par certaines exigences nationales, régionales ou locales exigeant que les données soient localisées sur un territoire précis.

(4) Ces obstacles à la libre circulation des services de traitement des données et à la liberté d'établissement des fournisseurs de services découlent des exigences, dans le droit des États membres, visant à localiser les données dans une zone géographique ou un territoire précis à des fins de traitement des données. D'autres règles ou pratiques administratives ont un effet équivalent en imposant des exigences spécifiques qui rendent plus difficile le traitement de données en dehors d'une zone géographique ou d'un territoire précis dans l'Union, telles que les exigences d'utiliser des moyens techniques qui sont certifiés ou agréés dans un État membre particulier. L'absence de sécurité juridique quant à la portée des exigences, légitimes ou non, de localisation des données restreint encore le choix offert aux acteurs du marché et au secteur public concernant la localisation du traitement des données. Le présent règlement ne limite en rien la liberté des entreprises de conclure des contrats précisant où les données doivent être localisées. Le présent règlement vise simplement à sauvegarder cette liberté en permettant de convenir d'une localisation située en tout lieu de l'Union.

[1] JO C 227 du 28.6.2018, p. 78.
[2] Position du Parlement européen du 4 octobre 2018 (non encore parue au Journal officiel) et décision du Conseil du 6 novembre 2018.

(5) En même temps, la mobilité des données dans l'Union est également freinée par des restrictions relevant du secteur privé, à savoir les questions juridiques, contractuelles et techniques qui dissuadent ou empêchent les utilisateurs des services de traitement des données de transférer leurs données d'un fournisseur de services à un autre ou de les rapatrier vers leur propre système informatique, en particulier au terme de leur contrat avec un fournisseur.

(6) La combinaison de ces obstacles a entraîné un manque de concurrence entre les fournisseurs de services informatiques en nuage dans l'Union, divers problèmes de dépendance à l'égard des fournisseurs et un sérieux manque de mobilité des données. De même, les politiques de localisation des données ont entravé la capacité des entreprises de recherche et développement à faciliter la collaboration entre les entreprises, les universités et d'autres organismes de recherche aux fins de la stimulation de l'innovation.

(7) Pour des raisons de sécurité juridique et vu la nécessité de conditions de concurrence égales au sein de l'Union, un ensemble unique de règles applicables à tous les acteurs du marché est un élément essentiel du fonctionnement du marché intérieur. Afin de supprimer les obstacles aux échanges et les distorsions de concurrence qui résultent des divergences entre les droits nationaux, et d'empêcher l'apparition probable d'autres obstacles et distorsions de concurrence importantes, il est nécessaire d'adopter des règles uniformes applicables dans tous les États membres.

(8) Le cadre juridique de l'Union relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, au respect de la vie privée et à la protection des données à caractère personnel dans les communications électroniques, et en particulier le règlement (UE) 2016/679 du Parlement européen et du Conseil ([1]) et les directives (UE) 2016/680 ([2]) et 2002/58/CE ([3]) du Parlement européen et du Conseil, n'est pas remis en question par le présent règlement.

(9) L'essor de l'internet des objets, l'intelligence artificielle et l'apprentissage automatique représentent des sources importantes de données à caractère non personnel, par exemple en raison de leur déploiement dans des processus automatisés de production industrielle. Des exemples spécifiques de données à caractère non personnel sont notamment les ensembles de données agrégées et anonymisées utilisées pour l'analyse des mégadonnées, les données sur l'agriculture de précision qui peuvent aider à contrôler et à optimiser l'utilisation des pesticides et de l'eau, ou encore les données sur les besoins d'entretien des machines industrielles. Si les évolutions technologiques permettent de transformer les données anonymisées en données à caractère personnel, ces données doivent être traitées comme des données à caractère personnel, et le règlement (UE) 2016/679 doit s'appliquer en conséquence.

(10) En vertu du règlement (UE) 2016/679, les États membres ne peuvent ni limiter ni interdire la libre circulation des données à caractère personnel au sein de l'Union pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Le présent règlement établit le même principe de libre circulation, au sein de l'Union, des données à caractère non personnel sauf si une restriction ou une interdiction se justifie par des motifs de sécurité publique. Le règlement (UE) 2016/679 et le présent règlement énoncent un ensemble cohérent de règles concernant la libre circulation de différents types de données. En outre, le présent règlement n'impose pas d'obligation de stocker séparément les différents types de données.

(11) Afin d'établir un cadre applicable au libre flux des données à caractère non personnel dans l'Union et les bases pour développer l'économie des données et renforcer la compétitivité des entreprises de l'Union, il convient d'instaurer un cadre juridique clair, complet et prévisible concernant le traitement des données autres que personnelles dans le marché intérieur. Grâce à une approche fondée sur des principes, prévoyant une coopération entre les États membres ainsi qu'une autorégulation, le cadre devrait être assez souple pour permettre de prendre en compte l'évolution des besoins des utilisateurs, des fournisseurs de services et des autorités nationales dans l'Union. Afin d'éviter le risque de recoupement avec des mécanismes existants et ainsi un alourdissement de la charge pour les États membres comme pour les entreprises, il convient de ne pas établir de règles techniques détaillées.

(12) Le présent règlement ne devrait pas avoir d'incidence sur le traitement des données dès lors qu'il est effectué dans le cadre d'une activité qui ne relève pas du droit de l'Union. Il convient, en particulier, de rappeler que la sécurité nationale relève de la seule responsabilité de chaque État membre conformément à l'article 4 du traité sur l'Union européenne.

([1]) 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).

([2]) 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).

([3]) 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).

(13) Le libre flux des données dans l'Union jouera un rôle important dans la croissance et l'innovation fondées sur les données. À l'instar des entreprises et des consommateurs, les autorités publiques et les organismes de droit public des États membres peuvent bénéficier d'une plus grande liberté de choix pour ce qui est des fournisseurs de services axés sur les données, de prix plus concurrentiels et d'une meilleure fourniture de services aux citoyens. Compte tenu des volumes élevés de données que gèrent les autorités publiques et les organismes de droit public, il est de la plus haute importance qu'ils montrent l'exemple en utilisant les services de traitement des données et qu'ils s'abstiennent de prendre des mesures restrictives en matière de localisation des données lorsqu'ils recourent à des services de traitement des données. Il convient donc que les autorités publiques et les organismes de droit public relèvent du présent règlement. À cet égard, le principe du libre flux des données à caractère non personnel prévu par le présent règlement devrait également s'appliquer aux pratiques administratives générales et cohérentes et aux autres exigences de localisation des données dans le domaine des marchés publics, sans préjudice de la directive 2014/24/UE du Parlement européen et du Conseil ([1]).

(14) À l'instar de la directive 2014/24/UE, le présent règlement est sans préjudice des dispositions législatives, réglementaires et administratives qui concernent l'organisation interne des États membres et qui attribuent aux autorités publiques et aux organismes de droit public des pouvoirs et des responsabilités en matière de traitement des données sans rémunération contractuelle de parties privées, ainsi que des dispositions législatives, réglementaires et administratives des États membres qui prévoient la mise en œuvre de ces pouvoirs et responsabilités. Si les autorités publiques et les organismes de droit public sont encouragés à prendre en considération les avantages économiques et autres bienfaits de l'externalisation vers des prestataires de services extérieurs, ils peuvent avoir des raisons légitimes de choisir l'autoprestation de services ou l'internalisation. Par conséquent, aucune disposition du présent règlement n'oblige les États membres à sous-traiter ou à externaliser la prestation de services qu'ils souhaitent fournir eux-mêmes ou organiser autrement que par des marchés publics.

(15) Le présent règlement devrait s'appliquer aux personnes physiques ou morales qui fournissent des services de traitement des données aux utilisateurs résidant ou ayant un établissement dans l'Union, y compris à celles qui fournissent des services dans l'Union sans y avoir d'établissement. Le présent règlement ne devrait donc pas s'appliquer aux services de traitement des données ayant lieu en dehors de l'Union ni aux exigences de localisation relatives à ces données.

(16) Le présent règlement ne fixe pas de règles relatives à la détermination de la loi applicable en matière commerciale et est donc sans préjudice du règlement (CE) n° 593/2008 du Parlement européen et du Conseil ([2]). En particulier, dès lors que la loi applicable à un contrat n'a pas été choisie conformément audit règlement, un contrat de prestation de services est en principe régi par la loi du pays dans lequel le prestataire de services a sa résidence habituelle.

(17) Le présent règlement devrait s'appliquer au traitement des données au sens le plus large, quel que soit le type de système informatique utilisé, qu'il ait lieu dans les locaux de l'utilisateur ou qu'il soit externalisé chez un fournisseur de services. Il devrait couvrir le traitement des données à différents niveaux d'intensité, depuis le stockage des données (infrastructure à la demande) jusqu'au traitement des données sur des plateformes (plateforme à la demande) ou dans des applications (logiciel à la demande).

(18) Les exigences de localisation des données constituent incontestablement un obstacle à la libre prestation des services de traitement des données dans l'ensemble de l'Union, et au marché intérieur. À ce titre, elles devraient être interdites à moins qu'elles ne se justifient par des motifs de sécurité publique comme prévu par le droit de l'Union, en particulier au sens de l'article 52 du traité sur le fonctionnement de l'Union européenne, et respecter le principe de proportionnalité consacré par l'article 5 du traité sur l'Union européenne. Afin de donner effet au principe du libre flux des données à caractère non personnel à travers les frontières, d'assurer la levée rapide des exigences actuelles de localisation des données et de permettre, pour des raisons fonctionnelles, le traitement des données à plusieurs endroits dans l'Union, et comme le présent règlement prévoit des mesures pour garantir la disponibilité des données à des fins de contrôle réglementaire, les États membres ne devraient pouvoir invoquer que la sécurité publique pour justifier des exigences de localisation des données.

(19) Le concept de sécurité publique, au sens de l'article 52 du traité sur le fonctionnement de l'Union européenne et tel que l'interprète la Cour de justice, englobe à la fois la sécurité intérieure et extérieure d'un État membre, mais aussi les questions de sûreté publique, afin, en particulier, de faciliter la détection des infractions pénales, les enquêtes et les poursuites en la matière. Il présuppose l'existence d'une menace réelle et suffisamment grave portant atteinte à l'un des intérêts fondamentaux de la société, telle qu'une menace pour le fonctionnement des institutions et des services publics essentiels et pour la survie de la population, ainsi que le risque d'une perturbation grave des relations extérieures ou de la coexistence pacifique des nations, ou un risque pour les intérêts militaires. Conformément au principe de proportionnalité, les exigences de localisation des données qui sont justifiées par des motifs de sécurité publique devraient être adaptées à la réalisation de l'objectif poursuivi et ne devraient pas aller au-delà de ce qui est nécessaire pour atteindre cet objectif.

([1]) Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE (JO L 94 du 28.3.2014, p. 65).

([2]) Règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome I) (JO L 177 du 4.7.2008, p. 6).

(20) Afin d'assurer l'application effective du principe du libre flux des données à caractère non personnel à travers les frontières et d'empêcher l'apparition de nouveaux obstacles au bon fonctionnement du marché intérieur, les États membres devraient communiquer immédiatement à la Commission tout projet d'acte prévoyant une nouvelle exigence de localisation des données ou modifiant une exigence existante. Ces projets d'acte devraient être transmis et appréciés conformément à la directive (UE) 2015/1535 du Parlement européen et du Conseil ([1]).

(21) De plus, afin de supprimer les dispositions pouvant constituer des obstacles, les États membres devraient, durant une période transitoire de 24 mois à partir de la date d'application du présent règlement, procéder à l'examen des dispositions législatives, réglementaires ou administratives de nature générale existantes qui énoncent des exigences de localisation des données et communiquer à la Commission toute exigence de localisation des données qu'ils jugent conforme au présent règlement ainsi que sa justification. Cela devrait permettre à la Commission d'examiner la conformité de toute exigence de localisation des données restante. La Commission devrait être à même, le cas échéant, d'adresser des observations à l'État membre concerné. Ces observations pourraient comprendre une recommandation de modifier ou d'abroger l'exigence de localisation des données.

(22) Les obligations établies par le présent règlement de communiquer à la Commission les exigences existantes de localisation des données et les projets d'actes devraient s'appliquer aux exigences réglementaires de localisation des données et aux projets d'actes de nature générale mais pas aux décisions adressées à une personne physique ou morale spécifique.

(23) Afin d'assurer la transparence des exigences de localisation des données en vigueur dans les États membres, qui sont établies dans une disposition législative, réglementaire ou administrative de nature générale, pour les personnes physiques et morales comme les fournisseurs de services et les utilisateurs des services de traitement des données, les États membres devraient publier les informations sur ces exigences sur un point d'information unique en ligne national et les mettre à jour régulièrement. À défaut, les États membres devraient fournir des informations actualisées sur ces exigences à un point d'information central établi au titre d'un autre acte de l'Union. Afin que les personnes physiques et morales soient correctement informées des exigences de localisation des données dans l'ensemble de l'Union, les États membres devraient notifier à la Commission les adresses de ces points d'information uniques. La Commission devrait publier ces informations sur son propre site internet, ainsi qu'une liste consolidée régulièrement mise à jour de toutes les exigences de localisation des données en vigueur dans les États membres, avec une synthèse des informations sur ces exigences.

(24) Les exigences de localisation des données trouvent souvent leur origine dans un manque de confiance dans le traitement transfrontière des données, découlant de l'indisponibilité présumée de celles-ci à des fins d'intervention des autorités compétentes des États membres, comme l'inspection et l'audit dans le cadre d'un contrôle réglementaire ou prudentiel. Un tel manque de confiance ne peut être surmonté uniquement par la nullité des clauses contractuelles interdisant aux autorités compétentes l'accès légal aux données pour l'exercice de leurs fonctions officielles. Par conséquent, le présent règlement devrait clairement préciser qu'il ne porte pas atteinte au pouvoir des autorités compétentes de demander ou d'obtenir l'accès à des données conformément au droit de l'Union ou au droit national, et que les autorités compétentes ne peuvent se voir refuser l'accès aux données au motif que les données sont traitées dans un autre État membre. Les autorités compétentes pourraient imposer des exigences fonctionnelles pour faciliter l'accès aux données et exiger, par exemple, que les descriptions des systèmes doivent demeurer dans l'État membre concerné.

(25) Les personnes physiques ou morales qui sont soumises à l'obligation de fournir des données à des autorités compétentes peuvent s'en acquitter en donnant et en garantissant auxdites autorités un accès effectif et en temps utile, par voie électronique, aux données, indépendamment de l'État membre sur le territoire duquel celles-ci sont traitées. Cet accès peut être garanti par des clauses et conditions contractuelles concrètes entre la personne physique ou morale soumise à l'obligation de donner accès aux données et le fournisseur de services.

(26) Lorsqu'une personne physique ou morale est soumise à une obligation de fournir des données et ne la respecte pas, l'autorité compétente devrait être en mesure de demander l'assistance des autorités compétentes dans d'autres États membres. En pareil cas, les autorités compétentes devraient utiliser des instruments de coopération spécifiques du droit de l'Union ou en vertu d'accords internationaux, en fonction du sujet dans une situation donnée, comme par exemple dans le domaine de la coopération policière, de la justice pénale ou civile ou des

([1]) Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (JO L 241 du 17.9.2015, p. 1).

questions administratives — respectivement, la décision-cadre 2006/960/JAI du Conseil ([1]), la directive 2014/41/UE du Parlement européen et du Conseil ([2]), la convention sur la cybercriminalité du Conseil de l'Europe ([3]), le règlement (CE) nº 1206/2001 du Conseil ([4]), la directive 2006/112/CE du Conseil ([5]) et le règlement (UE) nº 904/2010 du Conseil ([6]). En l'absence de tels mécanismes de coopération spécifiques, les autorités compétentes devraient coopérer les unes avec les autres en vue de fournir l'accès aux données sollicitées par l'intermédiaire de points de contact uniques désignés.

(27) Lorsqu'une demande d'assistance implique d'obtenir, de la part de l'autorité sollicitée, l'accès à tous les locaux d'une personne physique ou morale, y compris à tous les équipements et moyens de traitement des données, cet accès doit être conforme au droit de l'Union ou au droit procédural national, y compris toute obligation d'obtenir une autorisation judiciaire préalable.

(28) Le présent règlement ne devrait pas permettre aux utilisateurs de tenter d'échapper à l'application du droit national. Il devrait dès lors permettre aux États membres d'infliger des sanctions effectives, proportionnées et dissuasives aux utilisateurs qui empêchent les autorités compétentes d'accéder aux données nécessaires à l'accomplissement de leurs missions officielles en vertu du droit de l'Union et du droit national. En cas d'urgence, lorsqu'un utilisateur abuse de son droit, les États membres devraient pouvoir imposer des mesures provisoires strictement proportionnées. Toute mesure provisoire nécessitant la relocalisation de données pendant plus de 180 jours à compter de la relocalisation s'écarterait du principe de libre circulation des données pendant une période importante et devrait dès lors être communiquée à la Commission pour examen de sa compatibilité avec le droit de l'Union.

(29) La capacité de transférer des données sans entrave est un élément clé pour faciliter le choix de l'utilisateur et favoriser une concurrence effective sur les marchés pour les services de traitement des données. Les difficultés réelles ou ressenties concernant le portage transfrontière de données rendent également les utilisateurs professionnels moins confiants à l'égard des offres transfrontières et sapent de ce fait leur confiance dans le marché intérieur. Alors que les consommateurs individuels bénéficient du droit de l'Union en vigueur, il n'existe pas de mesures facilitant le changement de fournisseur de services pour les utilisateurs intervenant dans le cadre de leurs activités commerciales ou professionnelles. Des exigences techniques cohérentes dans l'ensemble de l'Union, que cela concerne l'harmonisation technique, la reconnaissance mutuelle ou l'harmonisation volontaire, contribuent également à la mise en place d'un marché intérieur concurrentiel pour les services de traitement des données.

(30) Pour tirer pleinement parti de l'environnement concurrentiel, les utilisateurs professionnels devraient être en mesure de faire des choix en connaissance de cause et de comparer facilement les différentes composantes des divers services de traitement des données proposés dans le marché intérieur, notamment en ce qui concerne les conditions générales contractuelles de portage des données lors de la résiliation d'un contrat. Afin de s'aligner sur le potentiel d'innovation du marché et de tenir compte de l'expérience et de l'expertise des fournisseurs de services et des utilisateurs professionnels des services de traitement des données, les informations et exigences fonctionnelles détaillées concernant le portage des données devraient être définies par les acteurs du marché dans le cadre de l'autorégulation, encouragée, facilitée et contrôlée par la Commission, sous la forme de codes de conduite de l'Union pouvant comporter des conditions générales contractuelles types.

(31) Pour être efficaces et faciliter les changements de fournisseur de services et le portage des données, de tels codes de conduite devraient être complets et englober au minimum les aspects qui s'avèrent essentiels au cours du processus de portage des données, tels que les processus et la localisation des sauvegardes de données, les formats et supports de données disponibles, la configuration informatique requise et la bande passante minimale du réseau, le délai à prévoir avant le lancement de la procédure de portage et la durée pendant laquelle les données resteront accessibles en vue de leur portage, ainsi que les garanties d'accès aux données en cas de faillite du fournisseur de services. Les codes de conduite devraient aussi indiquer clairement que la dépendance à l'égard des fournisseurs n'est pas une pratique commerciale acceptable, prévoir des technologies renforçant la confiance et être régulièrement mis à jour pour suivre l'évolution technologique. Tout au long du processus, la Commission devrait veiller à consulter toutes les parties prenantes, y compris les associations de petites et moyennes entreprises (PME) et de jeunes pousses, les utilisateurs et les fournisseurs de services en nuage. Elle devrait évaluer l'élaboration de ces codes de conduite et l'efficacité de leur mise en application.

([1]) Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne (JO L 386 du 29.12.2006, p. 89).

([2]) Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale (JO L 130 du 1.5.2014, p. 1).

([3]) Convention sur la cybercriminalité du Conseil de l'Europe, STCE nº 185.

([4]) Règlement (CE) nº 1206/2001 du Conseil du 28 mai 2001 relatif à la coopération entre les juridictions des États membres dans le domaine de l'obtention des preuves en matière civile ou commerciale (JO L 174 du 27.6.2001, p. 1).

([5]) Directive 2006/112/CE du Conseil du 28 novembre 2006 relative au système commun de taxe sur la valeur ajoutée (JO L 347 du 11.12.2006, p. 1).

([6]) Règlement (UE) nº 904/2010 du Conseil du 7 octobre 2010 concernant la coopération administrative et la lutte contre la fraude dans le domaine de la taxe sur la valeur ajoutée (JO L 268 du 12.10.2010, p. 1).

(32) Lorsqu'une autorité compétente d'un État membre sollicite l'assistance d'un autre État membre pour obtenir l'accès à des données conformément au présent règlement, elle devrait présenter, par l'intermédiaire d'un point de contact unique désigné, une demande dûment motivée au point de contact unique désigné dudit État membre, qui devrait comprendre une explication écrite des motifs et des bases juridiques pour demander l'accès aux données. Le point de contact unique désigné par l'État membre sollicité devrait faciliter la transmission de la demande à l'autorité compétente concernée dans l'État membre en question. Afin de garantir une coopération effective, l'autorité à laquelle une demande est transmise devrait fournir une assistance sans retard indu, pour répondre à une demande donnée ou pour fournir des informations sur les difficultés rencontrées pour satisfaire cette demande ou sur ses motifs de rejet.

(33) Le renforcement de la confiance dans la sécurité du traitement transfrontière des données devrait réduire la propension des acteurs du marché et du secteur public à utiliser la localisation des données en lieu et place d'une assurance de sécurité des données. Il devrait également améliorer la sécurité juridique pour les entreprises en ce qui concerne le respect des exigences de sécurité applicables lorsqu'elles externalisent leurs activités de traitement des données à des fournisseurs de services, y compris à ceux qui sont situés dans d'autres États membres.

(34) Toutes les exigences de sécurité relatives au traitement des données qui s'appliquent de manière justifiée et proportionnée sur la base du droit de l'Union ou du droit national en conformité avec le droit de l'Union dans l'État membre de résidence ou d'établissement des personnes physiques ou morales dont les données sont concernées devraient continuer à s'appliquer au traitement des données dans un autre État membre. Ces personnes physiques ou morales devraient pouvoir satisfaire à ces exigences par elles-mêmes ou par des clauses contractuelles dans les contrats conclus avec les fournisseurs de services.

(35) Les exigences de sécurité fixées au niveau national devraient être nécessaires et proportionnées aux risques qui menacent la sécurité du traitement des données dans le domaine d'application du droit national contenant ces exigences.

(36) La directive (UE) 2016/1148 du Parlement européen et du Conseil [1] prévoit des mesures juridiques pour renforcer le niveau global de cybersécurité dans l'Union. Les services de traitement des données sont au nombre des services numériques régis par ladite directive. Selon ladite directive, les États membres doivent veiller à ce que les fournisseurs de service numérique identifient les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent et prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour les gérer. Ces mesures devraient garantir un niveau de sécurité adapté au risque existant et prendre en considération la sécurité des systèmes et des installations, la gestion des incidents, la gestion de la continuité des activités, le suivi, l'audit et le contrôle, ainsi que le respect des normes internationales. Ces éléments doivent être complétés par la Commission dans des actes d'exécution adoptés au titre de ladite directive.

(37) La Commission devrait présenter un rapport sur la mise en œuvre du présent règlement, notamment en vue de déterminer s'il est nécessaire de le modifier pour tenir compte de l'évolution des technologies ou des marchés. Il convient, dans ce rapport, d'évaluer en particulier le présent règlement, spécialement son application aux ensembles de données composés à la fois de données à caractère personnel et de données à caractère non personnel, ainsi que l'application de l'exception relative à la sécurité publique. Avant la mise en application du présent règlement, la Commission devrait également publier des lignes directrices sur la manière de traiter les ensembles de données composés à la fois de données à caractère personnel et de données à caractère non personnel, afin que les entreprises, dont les PME, puissent mieux comprendre l'interaction entre le présent règlement et le règlement (UE) 2016/679 et afin de veiller à ce que les deux règlements soient respectés.

(38) Le présent règlement respecte les droits fondamentaux et observe les principes reconnus, en particulier, par la Charte des droits fondamentaux de l'Union européenne, et devrait être interprété et appliqué dans le respect de ces droits et principes, notamment les droits à la protection des données à caractère personnel, la liberté d'expression et d'information et la liberté d'entreprise.

(39) Étant donné que l'objectif du présent règlement, à savoir garantir le libre flux des données autres que des données à caractère personnel dans l'Union, ne peut pas être atteint de manière suffisante par les États membres mais peut, en raison de ses dimensions et de ses 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 tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif,

[1] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Objet

Le présent règlement vise à assurer le libre flux de données autres que les données à caractère personnel au sein de l'Union, en établissant des règles concernant les exigences de localisation des données, la disponibilité des données pour les autorités compétentes et le portage des données pour les utilisateurs professionnels.

Article 2

Champ d'application

1. Le présent règlement s'applique au traitement de données électroniques autres que les données à caractère personnel dans l'Union, qui est:

a) fourni en tant que service aux utilisateurs résidant ou disposant d'un établissement dans l'Union, par un fournisseur de services établi ou non dans l'Union; ou

b) effectué par une personne physique ou morale résidant ou disposant d'un établissement dans l'Union pour ses propres besoins.

2. Dans le cas d'un ensemble de données composé à la fois de données à caractère personnel et de données à caractère non personnel, le présent règlement s'applique aux données de l'ensemble à caractère non personnel. Lorsque les données à caractère personnel et les données à caractère non personnel d'un ensemble sont inextricablement liées, le présent règlement est sans préjudice de l'application du règlement (UE) 2016/679.

3. Le présent règlement ne s'applique pas aux activités qui ne relèvent pas du champ d'application du droit de l'Union.

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

Article 3

Définitions

Aux fins du présent règlement, on entend par:

1) «données», les données autres que les données à caractère personnel au sens de l'article 4, point 1), du règlement (UE) 2016/679;

2) «traitement», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou à des ensembles de données sous forme électronique, telles que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

3) «projet d'acte», un texte rédigé en vue d'être édicté comme disposition législative, réglementaire ou administrative de nature générale, et se trouvant au stade de la préparation au cours duquel des modifications substantielles peuvent encore être apportées;

4) «fournisseur de services», une personne physique ou morale qui fournit des services de traitement des données;

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

6) «autorité compétente», une autorité d'un État membre ou toute autre entité habilitée en vertu du droit national à exercer une fonction publique ou la puissance publique qui a le pouvoir d'obtenir l'accès aux données traitées par une personne physique ou morale pour l'exécution de ses fonctions officielles, au sens du droit de l'Union ou du droit national;

7) «utilisateur», une personne physique ou morale, y compris une autorité publique ou un organisme de droit public, qui utilise ou demande un service de traitement des données;

8) «utilisateur professionnel», une personne physique ou morale, y compris une autorité publique ou un organisme de droit public, qui utilise ou demande un service de traitement des données à des fins liées à son activité commerciale, industrielle, artisanale, libérale ou à sa mission.

Article 4

Libre circulation des données au sein de l'Union

1. Les exigences de localisation des données sont interdites, sauf si elles sont justifiées par des motifs de sécurité publique dans le respect du principe de proportionnalité.

Le premier alinéa du présent paragraphe est sans préjudice du paragraphe 3 et des exigences de localisation des données établies sur la base du droit en vigueur de l'Union.

2. Les États membres communiquent immédiatement à la Commission tout projet d'acte qui introduit une nouvelle exigence de localisation des données ou modifie une exigence de localisation des données existante conformément aux procédures définies aux articles 5, 6 et 7 de la directive (UE) 2015/1535.

3. Au plus tard le 30 mai 2021, les États membres veillent à ce que toute exigence existante de localisation des données qui est établie dans une disposition législative, réglementaire ou administrative de nature générale et qui n'est pas conforme au paragraphe 1 du présent article soit abrogée.

Au plus tard le 30 mai 2021, si un État membre estime qu'une mesure existante incluant une exigence de localisation des données est conforme au paragraphe 1 du présent article et peut donc rester en vigueur, il communique cette mesure à la Commission, accompagnée d'une justification de son maintien en vigueur. Sans préjudice de l'article 258 du traité sur le fonctionnement de l'Union européenne, la Commission examine, dans un délai de six mois à compter de la date de réception de cette communication, la conformité de cette mesure avec le paragraphe 1 du présent article et adresse, le cas échéant, des observations à l'État membre concerné, y compris en lui recommandant au besoin de modifier ou d'abroger la mesure.

4. Les États membres publient les détails de toutes les exigences de localisation des données, établies dans une disposition législative, réglementaire ou administrative de nature générale et applicables sur leur territoire, par l'intermédiaire d'un point d'information unique en ligne national qu'ils tiennent à jour, ou fournissent des détails actualisés de telles exigences de localisation à un point d'information central établi au titre d'un autre acte de l'Union.

5. Les États membres communiquent à la Commission l'adresse de leur point d'information unique visé au paragraphe 4. La Commission publie sur son site internet les liens vers ces points d'information uniques, ainsi qu'une liste consolidée régulièrement mise à jour de toutes les exigences de localisation des données visées au paragraphe 4, avec une synthèse des informations sur ces exigences.

Article 5

Disponibilité des données pour les autorités compétentes

1. Le présent règlement n'affecte pas le pouvoir des autorités compétentes de demander ou d'obtenir l'accès à des données pour l'accomplissement de leurs fonctions officielles, conformément au droit de l'Union ou au droit national. L'accès aux données par les autorités compétentes ne peut être refusé au motif que les données sont traitées dans un autre État membre.

2. Lorsqu'une autorité compétente, après avoir demandé l'accès aux données d'un utilisateur, n'obtient pas l'accès aux données et qu'il n'existe pas de mécanisme de coopération spécifique en vertu du droit de l'Union ou d'accords internationaux pour l'échange de données entre autorités compétentes de différents États membres, cette autorité compétente peut solliciter l'assistance de l'autorité compétente dans un autre État membre, conformément à la procédure prévue à l'article 7.

3. Lorsqu'une demande d'assistance implique d'obtenir, de la part de l'autorité sollicitée, l'accès à tous les locaux d'une personne physique ou morale, y compris à tous les équipements et moyens de traitement des données, cet accès doit être conforme au droit de l'Union ou au droit procédural national.

4. Les États membres peuvent imposer des sanctions effectives, proportionnées et dissuasives en cas de manquement à l'obligation de fournir des données, conformément au droit de l'Union et au droit national.

Lorsqu'un utilisateur spécifique abuse de ses droits, un État membre peut imposer des mesures provisoires strictement proportionnées à cet utilisateur, lorsque l'urgence de l'accès aux données le justifie et compte tenu des intérêts des parties concernées. Si une mesure provisoire impose la relocalisation des données pour une durée supérieure à 180 jours à compter de la relocalisation, elle est communiquée à la Commission au cours de cette période de 180 jours. La Commission examine, dans les plus brefs délais possibles, la mesure et sa compatibilité avec le droit de l'Union et, le cas échéant, prend les mesures qui s'imposent. La Commission échange des informations sur l'expérience acquise en la matière avec les points de contact uniques des États membres visés à l'article 7.

Article 6

Portage des données

1. La Commission encourage et facilite l'élaboration de codes de conduite par autorégulation au niveau de l'Union (ci-après dénommés «codes de conduite»), afin de contribuer à une économie des données compétitive, fondée sur les principes de transparence et d'interopérabilité et tenant dûment compte des normes ouvertes, concernant, notamment, les aspects suivants:

a) les bonnes pratiques qui facilitent le changement de fournisseurs de services et le portage des données dans des formats structurés, usuels et lisibles par machine, notamment dans des formats standard ouverts, lorsque le fournisseur de services obtenant les données le demande ou l'exige;

b) les exigences minimales d'information afin que les utilisateurs professionnels disposent, préalablement à la conclusion d'un contrat de traitement des données, d'informations suffisamment détaillées, claires et transparentes en ce qui concerne les processus, les exigences techniques, les délais et les frais qui s'appliquent dans le cas où un utilisateur professionnel souhaite changer de fournisseur de services ou transférer ses données pour les rapatrier vers ses propres systèmes informatiques;

c) les approches en matière de dispositifs de certification facilitant la comparaison entre les produits et services de traitement des données pour les utilisateurs professionnels, compte tenu des normes nationales ou internationales établies afin de faciliter la comparabilité de ces produits et services. Ces approches peuvent porter, entre autres, sur la gestion de la qualité, la gestion de la sécurité de l'information, la gestion de la continuité des activités et la gestion environnementale;

d) les feuilles de route de communication axées sur une démarche pluridisciplinaire afin d'informer les parties intéressées sur les codes de conduite.

2. La Commission veille à ce que les codes de conduite soient élaborés en étroite coopération avec toutes les parties intéressées, y compris les associations de PME et de jeunes pousses, les utilisateurs et les fournisseurs de services en nuage.

3. La Commission encourage les fournisseurs de services à terminer le développement des codes de conduite au plus tard le 29 novembre 2019 et à les mettre effectivement en œuvre au plus tard le 29 mai 2020.

Article 7

Procédure de coopération entre les autorités

1. Chaque État membre désigne un point de contact unique qui assure la liaison avec les points de contact uniques des autres États membres et la Commission en ce qui concerne l'application du présent règlement. Les États membres notifient à la Commission les points de contact uniques désignés et toute modification ultérieure les concernant.

2. Lorsqu'une autorité compétente d'un État membre sollicite l'assistance d'un autre État membre, conformément à l'article 5, paragraphe 2, afin d'obtenir l'accès à des données, elle présente au point de contact unique désigné de cet État membre une demande dûment motivée. La demande comprend une explication écrite des motifs et des bases juridiques pour demander l'accès aux données.

3. Le point de contact unique identifie l'autorité compétente concernée de son État membre et lui transmet la demande reçue conformément au paragraphe 2.

4. L'autorité compétente concernée ainsi sollicitée veille, sans retard injustifié et dans des délais proportionnés à l'urgence de la demande, à fournir une réponse en communiquant les données demandées ou en informant l'autorité compétente qui a présenté la demande qu'elle ne considère pas que les conditions requises pour demander une assistance au titre du présent règlement sont réunies.

5. Toutes les informations échangées dans le cadre de la demande d'assistance et fournies en vertu de l'article 5, paragraphe 2, ne sont utilisées qu'aux fins pour lesquelles elles ont été demandées.

6. Les points de contact uniques fournissent aux utilisateurs des informations générales sur le présent règlement, notamment sur les codes de conduite.

Article 8

Évaluation et lignes directrices

1. Au plus tard le 29 novembre 2022, la Commission soumet un rapport au Parlement européen, au Conseil et au Comité économique et social européen faisant état de son évaluation de la mise en œuvre du présent règlement, notamment en ce qui concerne:

a) l'application du présent règlement, en particulier aux ensembles de données composés à la fois de données à caractère personnel et de données à caractère non personnel, à la lumière de l'évolution des marchés et de l'évolution technologique qui pourraient élargir les possibilités de désanonymisation des données;

b) la mise en œuvre par les États membres de l'article 4, paragraphe 1, et en particulier l'exception relative à la sécurité publique; et

c) l'élaboration et la mise en œuvre effective des codes de conduite, ainsi que la fourniture effective d'informations par les fournisseurs de services.

2. Les États membres communiquent à la Commission toutes les informations nécessaires à l'établissement du rapport visé au paragraphe 1.

3. Au plus tard le 29 mai 2019, la Commission publie des lignes directrices sur l'interaction entre le présent règlement et le règlement (UE) 2016/679, en particulier en ce qui concerne les ensembles de données composés à la fois de données à caractère personnel et de données à caractère non personnel.

Article 9

Dispositions finales

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

Il s'applique six mois après la date de sa publication.

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

Fait à Strasbourg, le 14 novembre 2018.

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*
A. TAJANI	K. EDTSTADLER