Conseil de
l'Union européenne

Bruxelles, le 15 septembre 2017
(OR. en)

12244/17

Dossier interinstitutionnel:
2017/0228 (COD)

TELECOM 213
COMPET 615
MI 637
DATAPROTECT 143
JAI 791
IA 141
CODEC 1407

PROPOSITION

Origine:	Pour le secrétaire général de la Commission européenne, Monsieur Jordi AYET PUIGARNAU, directeur
Date de réception:	13 septembre 2017
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	COM(2017) 495 final
Objet:	Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL concernant un cadre applicable à la libre circulation des données à caractère non personnel dans l'Union européenne

Les délégations trouveront ci-joint le document COM(2017) 495 final.

p.j.: COM(2017) 495 final

COMMISSION
EUROPÉENNE

Bruxelles, le 13.9.2017
COM(2017) 495 final

2017/0228 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

concernant un cadre applicable à la libre circulation des données à caractère non personnel dans l'Union européenne

{SWD(2017) 304 final}
{SWD(2017) 305 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

Les nouvelles technologies numériques, comme l'informatique en nuage, les mégadonnées, l'intelligence artificielle et l'Internet des objets sont conçues pour optimiser l'efficience, permettre les économies d'échelle et favoriser le développement de nouveaux services. Elles procurent aux utilisateurs des avantages tels que la flexibilité, la productivité, la vitesse de déploiement et l'autonomie, notamment par l'apprentissage automatique[1].

Comme indiqué dans la communication de 2017 «Créer une économie européenne fondée sur les données»[2], la valeur du marché des données de l'UE a été estimée, en 2016, à près de 60 milliards d'EUR, soit une augmentation de 9,5 % par rapport à 2015. D'après une étude, ce marché pourrait représenter plus de 106 milliards d'EUR en 2020[3].

Afin d'exploiter ce potentiel, il est proposé de traiter les questions suivantes:

- améliorer la mobilité des données à caractère non personnel à travers les frontières au sein du marché unique, laquelle est aujourd'hui limitée par des restrictions géographiques ou des incertitudes juridiques dans de nombreux États membres;
- veiller à ce que le pouvoir des autorités compétentes de demander et d'obtenir l'accès à des données à des fins de contrôle réglementaire, comme l'inspection et l'audit, reste inchangé; et
- permettre aux utilisateurs professionnels des services de stockage ou de traitement des données de changer de fournisseur et de transférer leurs données plus facilement, sans faire peser de charge excessive sur les fournisseurs de services ni créer de distorsion sur le marché.

Dans l'examen à mi-parcours de la mise en œuvre de la stratégie pour le marché unique numérique[4], il était annoncé une proposition législative sur un cadre européen de coopération pour la libre circulation des données.

L'objectif politique général de l'initiative est de rendre le marché intérieur des services et activités de stockage ou de traitement des données plus concurrentiel et mieux intégré en remédiant aux problèmes ci-dessus. Dans la présente proposition, le stockage et les autres traitements des données s'entendent au sens large, quel que soit le type de système informatique utilisé, qu'ils aient lieu dans les locaux de l'utilisateur ou qu'ils soient externalisés chez un fournisseur de services de stockage ou de traitement des données[5].

---

1 L'apprentissage automatique est une application de l'intelligence artificielle (IA) qui dote les systèmes de la capacité à apprendre automatiquement et à se perfectionner par l'expérience sans être expressément programmés.

2 COM(2017) 9, «Créer une économie européenne fondée sur les données», 10 janvier 2017; voir aussi le document de travail des services de la Commission qui l'accompagne, SWD(2017) 2 du 10 janvier 2017.

3 *IDC and Open Evidence, European Data Market*, rapport final, 1er février 2017 (SMART 2013/0063).

4 Communication de la Commission adoptée le 10 mai 2017 [COM(2017) 228 final].

5 Les autres services de traitement des données comprennent les services fondés sur les données comme l'analyse des données, les systèmes de gestion des données, etc.

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

La proposition poursuit les objectifs fixés dans la stratégie pour un marché unique numérique[6], son examen à mi-parcours, ainsi que les orientations politiques de l'actuelle Commission européenne intitulées «Un nouvel élan pour l'Europe: mon programme pour l'emploi, la croissance, l'équité et le changement démocratique»[7].

La présente proposition porte sur la prestation des services d'hébergement (de stockage) ou de traitement des données, et elle est conforme aux **instruments juridiques existants**. L'initiative a pour objet la création d'un marché unique européen efficace desdits services. Elle est donc conforme à la **directive sur le commerce électronique[8]** qui vise à la création d'un marché unique européen, complet et efficace, des catégories plus générales de services de la société de l'information, et à la directive «Services»[9] qui renforce le marché unique européen des services dans un certain nombre de secteurs.

Plusieurs secteurs concernés sont expressément exclus du champ d'application de cette législation (directive sur le commerce électronique et directive «Services») si bien que seules les dispositions générales du traité s'appliqueraient à la totalité des services d'hébergement (de stockage) et de traitement des données. Cependant, lever les obstacles auxquels ces services se heurtent aujourd'hui est impossible si l'on se fonde uniquement sur l'application directe des articles 49 et 56 du traité sur le fonctionnement de l'Union européenne car, d'une part, y remédier au cas par cas selon des procédures d'infraction à l'encontre des États membres concernés serait extrêmement compliqué pour les institutions nationales et de l'Union et, d'autre part, les supprimer implique, dans de nombreux cas, des règles spécifiques, applicables aux obstacles non seulement publics mais aussi privés, et l'instauration d'une coopération administrative. De plus, le renforcement consécutif de la sécurité juridique semble être particulièrement important pour les utilisateurs de nouvelles technologies[10].

Comme la présente proposition concerne les données électroniques autres que celles à caractère personnel, elle ne remet pas en question le cadre juridique de l'Union en matière de protection des données, en particulier le règlement (UE) 2016/679 (RGPD)[11], la directive (UE) 2016/680 (directive «police»)[12] et la directive 2002/58/CE (directive vie privée et communications électroniques)[13], qui garantissent un niveau élevé de protection des données à caractère personnel et la libre circulation de celles-ci dans l'Union. En conjonction avec ce

---

6 COM(2015) 192 final.

7 Discours d'ouverture de la session plénière du Parlement européen, Strasbourg, 22 octobre 2014.

8 Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects 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).

9 Directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur (JO L 376 du 27.12.2006, p. 36).

10 Étude LE Europe (SMART 2015/0016) et étude IDC (SMART 2013/0063).

11 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).

12 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).

13 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).

cadre juridique, la proposition vise à mettre en place un cadre européen complet et cohérent permettant la libre circulation des données dans le marché unique.

La proposition impliquera de notifier les projets de mesures concernant la localisation des données, en application de la directive (UE) 2015/1535[14] sur la transparence, pour permettre de déterminer si de telles restrictions géographiques se justifient.

Concernant la coopération et l'assistance mutuelle entre les autorités compétentes, la proposition prévoit que tous les mécanismes en la matière s'appliqueront. Dans les cas où il n'existe pas de mécanisme de coopération, la proposition instaure des mesures visant à permettre aux autorités compétentes d'échanger et de consulter des données stockées ou traitées dans d'autres États membres.

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

Concernant le marché unique numérique, la présente initiative vise à lever les obstacles à une économie fondée sur les données en Europe. Conformément à la communication sur l'examen à mi-parcours de la stratégie en la matière, la Commission étudie séparément les questions de l'accessibilité et de la réutilisation des données du secteur public et des données obtenues au moyen de fonds publics et des données détenues par le secteur privé qui sont d'intérêt public, ainsi que de la responsabilité en cas de dommage causé par des produits à forte intensité de données[15].

L'intervention politique se fonde aussi sur le paquet stratégique «**Passage au numérique des entreprises européennes**», qui comprenait l'**initiative européenne sur l'informatique en nuage**[16] visant à déployer des solutions à haute capacité pour le stockage, le partage et la réutilisation des données scientifiques. De plus, l'initiative repose sur la révision du **cadre d'interopérabilité européen**[17], qui vise à améliorer la collaboration numérique entre les administrations publiques en Europe et bénéficiera directement de la libre circulation des données. Elle relève enfin de l'engagement de l'UE en faveur d'un **Internet ouvert**[18].

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

- **Base juridique**

La présente proposition relève d'un domaine de compétence partagée conformément à l'article 4, paragraphe 2, point a), du TFUE. Elle vise à rendre le marché intérieur des services de stockage ou de traitement des données plus concurrentiel et mieux intégré en assurant la libre circulation des données au sein de l'Union. Elle établit 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. La proposition se fonde sur l'article 114 du TFUE, qui constitue la base juridique générale pour l'adoption de telles règles.

---

[14] 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).

[15] COM(2017) 228 final.

[16] COM(2016) 178 final, «Initiative européenne sur l'informatique en nuage – Bâtir une économie compétitive des données et de la connaissance en Europe», 19 avril 2016.

[17] COM(2017) 134 final, «Cadre d'interopérabilité européen – Stratégie de mise en œuvre», 23 mars 2017.

[18] COM(2014) 72 final, «Politique et gouvernance de l'Internet: le rôle de l'Europe à l'avenir », http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=COM:2014:0072:FIN

- **Subsidiarité**

La proposition est conforme au principe de subsidiarité énoncé à l'article 5 du traité sur l'Union européenne (TUE). L'objectif de la présente proposition est d'assurer le bon fonctionnement du marché intérieur des services susmentionnés, lequel ne se limite pas au territoire d'un État membre. La libre circulation des données à caractère non personnel au sein de l'Union ne peut être garantie par les États membres au niveau national car le problème essentiel est la mobilité transfrontière des données.

Les États membres sont à même de limiter le nombre et la portée de leurs propres restrictions en matière de localisation des données, mais ils sont susceptibles de le faire dans des mesures et des conditions différentes, ou de ne pas le faire du tout.

Or, des approches divergentes entraîneraient une multiplication des exigences réglementaires au sein du marché unique de l'UE et un surcoût réel pour les entreprises, notamment les petites et moyennes entreprises (PME).

- **Proportionnalité**

La proposition est conforme au principe de proportionnalité énoncé à l'article 5 du TUE car elle consiste en un cadre efficace qui n'excède pas ce qui est nécessaire pour résoudre les problèmes recensés et elle est proportionnée aux objectifs qu'elle poursuit.

Afin de lever les obstacles à la libre circulation des données à caractère non personnel au sein de l'Union, encore limitée par des exigences de localisation, et de susciter une confiance accrue dans les flux de données transfrontières ainsi que dans les services de stockage ou de traitement des données, la proposition reposera, dans une large mesure, sur les instruments et cadres existants de l'UE: la directive sur la transparence pour ce qui est de la notification des projets de mesures concernant les exigences de localisation des données, et différents cadres garantissant la disponibilité des données à des fins de contrôle réglementaire par les États membres. C'est seulement en l'absence d'autres mécanismes de coopération, et lorsque les autres moyens d'accès auront été épuisés, qu'il sera fait usage du mécanisme de coopération prévu par la proposition afin de traiter les questions de disponibilité des données pour les autorités nationales compétentes.

L'approche proposée relativement à la circulation des données à travers les frontières des États membres et entre les fournisseurs de services / systèmes informatiques internes vise à établir un équilibre entre la réglementation de l'UE et les intérêts des États membres en matière de sécurité publique ainsi qu'entre la réglementation de l'UE et l'autorégulation par le marché.

Plus précisément, afin de remédier aux difficultés rencontrées par les utilisateurs professionnels pour changer de fournisseur et transférer leurs données, l'initiative encourage l'autorégulation selon des codes de conduite concernant les informations à fournir aux utilisateurs des services de stockage ou de traitement des données. De même, il conviendrait d'avoir recours à l'autorégulation pour définir les meilleures pratiques en ce qui concerne les modalités de changement de fournisseur et de portage des données.

La proposition rappelle que les exigences de sécurité imposées par le droit national et de l'Union devraient aussi être respectées lorsque des personnes physiques ou morales externalisent leurs services de stockage ou de traitement des données, y compris dans un autre État membre. Elle rappelle également les pouvoirs d'exécution conférés à la Commission par la directive sur la sécurité des réseaux et des systèmes d'information afin de satisfaire aux exigences de sécurité qui contribuent aussi au fonctionnement du présent règlement. Enfin, s'il est vrai que la proposition exigerait une action de la part des pouvoirs publics des États membres en raison des exigences de notification / réexamen, des exigences de transparence et

de la coopération administrative, elle a été élaborée de façon à limiter une telle action aux besoins de coopération les plus impérieux et, partant, à éviter toute charge administrative inutile.

En instaurant un cadre clair, associé à la coopération entre et avec les États membres ainsi qu'à l'autorégulation, la présente proposition vise à renforcer la sécurité juridique et à relever les niveaux de confiance, en maintenant la pertinence et l'efficacité à long terme du fait de la souplesse du cadre de coopération, sur la base de points de contact uniques dans les États membres.

La Commission entend instituer un groupe d'experts pour la conseiller sur les questions relevant du présent règlement.

- **Choix de l'instrument**

La Commission présente une proposition de règlement, lequel peut garantir que des règles uniformes relatives à la libre circulation des données à caractère non personnel seront applicables dans toute l'Union en même temps. Cela est particulièrement important pour lever les restrictions existantes et éviter que des États membres en imposent de nouvelles, pour garantir la sécurité juridique aux fournisseurs de services et utilisateurs concernés et, ainsi, pour susciter une confiance accrue dans les flux de données transfrontières ainsi que dans les services de stockage ou de traitement des données.

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

- **Consultation des parties intéressées**

Lors d'une **première phase de collecte d'éléments probants**, une **consultation publique** a été réalisée, en 2015, sur l'environnement réglementaire des plateformes, les intermédiaires en ligne, les données et l'informatique en nuage ainsi que l'économie collaborative. Deux tiers des participants – représentant équitablement toutes les catégories de parties intéressées, y compris les PME – ont constaté que les restrictions en matière de localisation des données avaient une incidence sur leur stratégie commerciale[19]. D'autres activités de collecte d'informations ont consisté en des réunions et événements, des ateliers destinés à certains acteurs clés (p. ex. le *Cloud Select Industry Group*) et des ateliers spécialisés dans le cadre d'études.

Une **deuxième phase de collecte d'éléments probants**, qui s'est déroulée entre la fin de 2016 et le second semestre de 2017, comprenait une **consultation publique lancée au titre de la communication «Créer une économie européenne fondée sur les données»** du 10 janvier 2017. D'après les réponses à la consultation publique, 61,9 % des parties intéressées estimaient que les restrictions en matière de localisation des données devaient être levées. La majorité des parties intéressées (55,3 % des participants) pensent qu'une mesure législative est l'instrument le plus adapté pour remédier aux restrictions injustifiées en matière de localisation, et plusieurs participants préconisent expressément un règlement[20]. Les

[19] Une étude sur l'impact économique de l'informatique en nuage en Europe (SMART 2014/0031, Deloitte, «Measuring the economic impact of cloud computing in Europe», 2016) a permis d'obtenir des données économiques supplémentaires.

[20] 289 parties intéressées ont répondu à cette question à choix multiple dans la consultation publique. Il n'était pas demandé aux participants de préciser le *type* de mesure législative, mais 12 parties intéressées ont, de leur propre initiative, saisi l'occasion de préconiser expressément un règlement dans un commentaire écrit. Ce

fournisseurs de services informatiques, tant grands que petits, qu'ils soient établis dans l'UE ou ailleurs, apparaissent comme les partisans les plus fervents d'une mesure réglementaire. Les parties intéressées ont aussi recensé les effets négatifs des restrictions en matière de localisation des données. Outre qu'ils se traduisent par un surcoût pour les entreprises, ces effets se font sentir sur la prestation de service aux entités privées ou publiques (69,6 % des participants ont qualifié l'effet d'«important») ou sur la capacité à entrer sur un nouveau marché (73,9 % des participants ont qualifié l'effet d'«important»). Des parties intéressées venant de tous les horizons répondent à ces questions dans les mêmes proportions. La consultation publique en ligne a également révélé que le problème du changement de fournisseur est répandu car 56,8 % des participants ont déclaré rencontrer des difficultés lorsqu'ils entreprennent un tel changement.

Les dialogues structurés avec les États membres ont permis d'appréhender les problèmes de la même façon et, dans une lettre adressée au président Tusk, 16 États membres ont expressément préconisé une proposition législative.

La proposition prend en compte plusieurs des préoccupations dont des États membres et des entreprises ont fait part, en particulier la nécessité d'établir un principe transversal de libre circulation des données procurant une sécurité juridique; de progresser en matière de disponibilité des données à des fins réglementaires; de permettre aux utilisateurs professionnels de changer de fournisseur de services de stockage ou de traitement des données et de transférer leurs données plus facilement en invitant à plus de transparence au sujet des procédures applicables et des conditions contractuelles mais sans imposer, à ce stade, de normes ou d'obligations précises aux fournisseurs de services.

- **Obtention et utilisation d'expertise**

Des études juridiques et économiques ont été mises à profit concernant divers aspects de la mobilité des données, comme les exigences de localisation des données[21], le changement de fournisseur / portage des données[22] et la sécurité des données[23]. D'autres études ont été commandées sur les effets de l'informatique en nuage[24] et de son adoption[25], ainsi que sur le marché européen des données[26]. Ont aussi été réalisées des études portant sur les mesures de corégulation ou d'autorégulation dans le secteur de l'informatique en nuage[27]. La

---

groupe était divers dans sa composition, car il comprenait 2 États membres, 3 associations professionnelles, 6 fournisseurs de services informatiques et un cabinet d'avocats.

[21] SMART 2015/0054, TimeLex, Spark et Tech4i, «Cross-border Data Flow in the Digital Single Market: Study on Data Location Restrictions», D5. Rapport final (en cours) [Étude TimeLex (SMART 2015/0054)]; SMART 2015/0016, London Economics Europe, Carsa et CharlesRussellSpeechlys, «Facilitating cross border data flow in the Digital Single Market», 2016 (en cours) [Étude LE Europe (SMART 2015/0016)].

[22] SMART 2016/0032, IDC et Arthur's Legal, «Switching between Cloud Service Providers», 2017 (en cours) [Étude IDC et Arthur's Legal (SMART 2016/0032)].

[23] SMART 2016/0029 (en cours), Tecnalia, «Certification Schemes for Cloud Computing», D6.1 rapport initial.

[24] SMART 2014/0031, Deloitte, «Measuring the economic impact of cloud computing in Europe», 2016 [Étude Deloitte (SMART 2014/0031)].

[25] SMART 2013/43, IDC, «Uptake of Cloud in Europe. Follow-up of IDC Study on Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake», 2014, disponible à l'adresse: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9742; SMART 2011/0045, IDC, «Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake» (juillet 2012).

[26] SMART 2013/0063, IDC et Open Evidence, «European Data Market. Data ownership and Access to Data – Key Emerging Issues», 1er février 2017 [Étude IDC (SMART 2013/0063)].

[27] SMART 2015/0018, TimeLex, Spark, «Clarification of Applicable Legal Framework for Full, Co- or Self-Regulatory Actions in the Cloud Computing Sector» (en cours).

Commission a également utilisé des sources externes supplémentaires, comme des études de marché et des statistiques (p. ex. Eurostat).

- **Analyse d'impact**

Pour la présente proposition, il a été réalisé une analyse d'impact dans laquelle les solutions suivantes ont été envisagées: un scénario de référence (aucune intervention) et trois options stratégiques. L'option 1 consistait à recourir à des orientations et/ou à l'autorégulation pour traiter les différents problèmes recensés et impliquait une application plus rigoureuse de la loi concernant divers cas de restrictions injustifiées ou disproportionnées en matière de localisation des données imposées par des États membres. L'option 2 consisterait à établir des principes juridiques concernant les différents problèmes recensés et à prévoir la désignation de points de contact uniques par les États membres et la création d'un groupe d'experts chargé de discuter des approches et pratiques communes et de donner des orientations relatives aux principes instaurés. Il a également été envisagé une sous-option 2a pour permettre d'évaluer une solution associant des mesures législatives établissant le cadre de la libre circulation des données et les points de contact uniques et un groupe d'experts ainsi que des mesures d'autorégulation sur le portage des données. L'option 3 consistait en une initiative législative détaillée visant à établir, entre autres, des évaluations (harmonisées) prédéfinies de ce qui constitue une restriction (in)justifiée et (dis)proportionnée en matière de localisation des données, et un nouveau droit de portage des données.

Le 28 septembre 2016, le comité d'examen de la réglementation a émis un premier avis sur l'analyse d'impact et a demandé qu'elle lui soit soumise à nouveau. L'analyse d'impact a donc été révisée et présentée à nouveau le 11 août 2017 au comité d'examen de la réglementation. Celui-ci, dans son second avis, a pris acte de l'extension du champ d'application, à la suite de la communication de la Commission intitulée «Créer une économie européenne fondée sur les données» [COM(2017) 9 final], ainsi que du matériel supplémentaire sur l'opinion des parties intéressées et les lacunes du cadre actuel. Cependant, le comité a émis un second avis négatif le 25 août 2017, en faisant observer, notamment, l'absence de preuves à l'appui d'un nouveau droit à la portabilité des services informatiques en nuage. Conformément à son mode de fonctionnement, le comité a estimé que son avis était définitif.

La Commission a jugé opportun de présenter une proposition tout en continuant à améliorer son analyse d'impact pour prendre en compte les observations formulées par le comité d'examen de la réglementation dans son second avis. Le champ d'application de la proposition est limité à la libre circulation des données à caractère non personnel dans l'Union européenne. Conformément aux conclusions du comité, selon lequel les faits semblent plaider en faveur d'une solution moins contraignante en ce qui concerne le portage des données, l'option privilégiée au départ dans l'analyse d'impact, à savoir instaurer l'obligation pour les fournisseurs de faciliter le changement de fournisseur ou le portage des données des utilisateurs, a été abandonnée. La Commission a retenu, à la place, une solution moins lourde, consistant en des mesures d'autorégulation qu'elle se chargerait de promouvoir. La proposition est proportionnée et moins contraignante car elle ne crée pas de nouveau droit de portage entre fournisseurs de services de stockage ou de traitement des données, mais repose sur l'autorégulation pour ce qui est de la transparence des conditions techniques et fonctionnelles relatives à la portabilité des données.

Il a aussi été tenu compte de l'avis du comité afin de faire en sorte qu'il n'y ait pas de recoupement ou de double emploi avec le réexamen du mandat de l'Agence européenne

chargée de la sécurité des réseaux et de l'information (ENISA) et la création d'un cadre européen de cybersécurité des TIC.

L'analyse d'impact a démontré que l'option privilégiée, la sous-option 2a, garantirait la levée effective des actuelles restrictions injustifiées en matière de localisation et éviterait efficacement de futures restrictions, du fait de l'application d'un principe juridique clair associé à des exigences de réexamen, de notification et de transparence, tout en accroissant la sécurité juridique et la confiance dans le marché. La charge pour les pouvoirs publics des États membres serait modérée et impliquerait un coût annuel d'environ 33 000 EUR pour les ressources humaines nécessaires au maintien des points de contact uniques, ainsi qu'un coût annuel compris entre 385 et 1 925 EUR pour la préparation des notifications.

La proposition aura un effet positif sur la concurrence car elle favorisera l'innovation en matière de services de stockage ou de traitement des données, incitera davantage d'utilisateurs à y avoir recours et facilitera considérablement, en particulier pour les fournisseurs de services nouveaux et de petite taille, l'accès à des marchés émergents. Elle contribuera également à promouvoir l'utilisation transfrontière et intersectorielle des services de stockage ou de traitement des données et le développement du marché des données. Par conséquent, la proposition permettra de transformer la société et l'économie et offrira de nouvelles possibilités aux particuliers, aux entreprises et aux administrations publiques en Europe.

- **Réglementation affûtée et simplification**

La proposition s'applique aux particuliers, aux administrations nationales et à toutes les entreprises, y compris aux micro-entreprises et aux PME. Toutes les entreprises peuvent tirer avantage des dispositions concernant les obstacles à la mobilité des données. La proposition sera en particulier profitable aux PME, car la libre circulation des données à caractère non personnel fera directement diminuer leurs coûts et leur assurera une position plus compétitive sur le marché. Exempter les PME des règles nuirait à l'efficacité de celles-ci car les PME représentent une proportion importante des fournisseurs de services de stockage ou de traitement des données et sont des moteurs de l'innovation sur ces marchés. En outre, comme il est peu probable que les coûts résultant des règles soient importants, les micro-entreprises ou les PME ne devraient pas être exclues de leur champ d'application.

- **Droits fondamentaux**

Le règlement proposé respecte les droits fondamentaux et les principes reconnus par la Charte des droits fondamentaux de l'Union européenne. Il devrait avoir un effet positif sur la liberté d'entreprise (article 16) car il contribuerait à lever et à éviter les obstacles injustifiés ou disproportionnés à l'utilisation et la prestation des services de données, comme les services informatiques en nuage, ainsi qu'à la configuration des systèmes informatiques internes.

4. INCIDENCE BUDGÉTAIRE

Il s'ensuivra une charge administrative modérée pour les pouvoirs publics des États membres, due à l'affectation de ressources humaines à la coopération entre États membres au moyen des «points de contact uniques» et à l'application des dispositions en matière de réexamen, de notification et de transparence.

5. AUTRES ÉLÉMENTS

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

Une évaluation complète aura lieu cinq ans après le début de l'application des règles, qui permettra d'apprécier leur efficacité et leur proportionnalité. Cette évaluation sera réalisée conformément aux lignes directrices pour une meilleure réglementation.

Il s'agira notamment d'établir si le règlement a contribué à limiter le nombre et la portée des restrictions en matière de localisation des données et à accroître la sécurité juridique et la transparence des exigences (justifiées et proportionnées) restantes. L'évaluation consistera aussi à déterminer si l'initiative politique a contribué à susciter une confiance accrue dans la libre circulation des données à caractère non personnel, si les États membres peuvent raisonnablement avoir accès aux données stockées à l'étranger à des fins de contrôle réglementaire et si le règlement a abouti à une plus grande transparence des conditions de portage des données.

Les points de contact uniques des États membres devraient constituer une source d'informations précieuse au cours de la phase d'évaluation *ex post* de la législation.

Des indicateurs spécifiques (comme proposé dans l'analyse d'impact) serviraient à mesurer les progrès accomplis dans ces domaines. Il est également prévu de recourir aux données Eurostat et à l'indice relatif à l'économie et à la société numériques. Une édition spéciale d'Eurobaromètre peut aussi être envisagée à cette fin.

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

Les **articles 1er à 3** précisent l'**objectif** de la proposition, le **champ d'application** du règlement et les **définitions** applicables aux fins du règlement.

L'**article 4** établit le **principe de libre circulation des données à caractère non personnel** dans l'Union. En vertu de ce principe, toute exigence de localisation des données est interdite à moins qu'elle ne se justifie par des motifs de sécurité publique. De plus, il prévoit le réexamen des exigences existantes, la notification des exigences restantes ou nouvelles à la Commission, et des mesures de transparence.

L'**article 5** vise à assurer la **disponibilité des données à des fins de contrôle réglementaire de la part des autorités compétentes**. À cet effet, les utilisateurs ne peuvent refuser de donner aux autorités compétentes accès à des données au motif que celles-ci sont stockées ou traitées dans un autre État membre. Lorsqu'**une autorité compétente** a épuisé tous les moyens possibles d'avoir accès à des données, elle **peut demander l'assistance** d'une autorité dans un autre État membre s'il n'existe aucun mécanisme de coopération spécifique.

L'**article 6** dispose que la Commission doit encourager les **fournisseurs de services et les utilisateurs professionnels à élaborer et appliquer des codes de conduite** précisant les informations sur les conditions de portage des données (y compris les exigences techniques et fonctionnelles) que les fournisseurs devraient mettre à la disposition de leurs utilisateurs professionnels de façon suffisamment détaillée, claire et transparente avant la conclusion d'un contrat. La Commission procédera au réexamen de l'élaboration et de la mise en œuvre effective de ces codes de conduite au plus tard deux ans après le début de l'application du présent règlement.

Conformément à l'**article 7**, chaque État membre doit désigner un **point de contact unique** qui doit assurer la liaison avec les points de contact des autres États membres et la Commission en ce qui concerne l'application du présent règlement. L'article 7 prévoit aussi

les conditions procédurales applicables à l'assistance entre autorités compétentes envisagée en vertu de l'article 5.

Conformément à l'**article 8**, la Commission doit être assistée par le comité de la libre circulation des données au sens du règlement (UE) n° 182/2011.

L'**article 9** prévoit un **réexamen** au plus tard cinq ans après le début de l'application du règlement.

L'**article 10** prévoit que le règlement commencera à s'appliquer six mois après le jour de sa publication.

2017/0228 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

concernant un cadre applicable à la libre circulation des données à caractère non personnel dans l'Union européenne

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[28],

vu l'avis du Comité des régions[29],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) Avec la transformation numérique de l'économie qui s'accélère, les technologies de l'information et des communications (TIC) 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.

(2) Les chaînes de valeur des données sont le résultat de diverses activités: création et collecte; agrégation et organisation; stockage et traitement; analyse, commercialisation et distribution; utilisation et réutilisation. Le fonctionnement efficace et efficient du stockage et du traitement des données est un élément fondamental de toute chaîne de valeur. Toutefois, un tel fonctionnement 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.

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

(4) Ces obstacles à la libre circulation des services de stockage ou de traitement des données et à la liberté d'établissement des fournisseurs desdits services découlent des exigences, dans le droit national des États membres, de localiser les données dans une zone géographique précise à des fins de stockage ou de traitement. D'autres règles ou pratiques administratives ont un effet équivalent en imposant des exigences

[28] JO C ... du ..., p. .
[29] JO C ... du ..., p. .

spécifiques qui rendent plus difficile de stocker ou traiter des 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. La sécurité juridique quant à la portée des exigences, justifiées et injustifiées, de localisation des données restreint encore le choix offert aux acteurs du marché et au secteur public concernant la localisation du stockage ou du traitement des données.

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

(6) 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 législations nationales, et d'empêcher l'apparition probable d'autres obstacles et distorsions de concurrence importantes, il est dès lors nécessaire d'adopter des règles uniformes applicables dans tous les États membres.

(7) Pour établir les règles de la libre circulation des données à caractère non personnel dans l'Union et les bases pour développer l'économie des données et renforcer la compétitivité des entreprises européennes, il convient d'instaurer un cadre juridique clair, complet et prévisible concernant le stockage et 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'à l'autorégulation, le cadre devrait être assez souple pour permettre de prendre en compte l'évolution des besoins des utilisateurs, des fournisseurs et des autorités nationales dans l'Union. Afin d'éviter le risque de recoupement avec des mécanismes existants et donc un alourdissement de la charge pour les États membres comme pour les entreprises, il conviendrait de ne pas établir de règles techniques détaillées.

(8) Le présent règlement devrait s'appliquer aux personnes morales ou physiques qui fournissent des services de stockage ou 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.

(9) Le cadre juridique de l'Union relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, en particulier le règlement (UE) 2016/679[30], la directive (UE) 2016/680[31] et la directive 2002/58/CE[32], ne devrait pas être remis en question par le présent règlement.

---

30 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).

31 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

(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 justifiait par des motifs de sécurité.

(11) Le présent règlement devrait s'appliquer au stockage et aux autres traitements des données au sens le plus large, quel que soit le type de système informatique utilisé, qu'ils aient lieu dans les locaux de l'utilisateur ou qu'ils soient externalisés chez un fournisseur de services de stockage ou de traitement des données. 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). Ces différents services devraient entrer dans le champ d'application du présent règlement, à moins que le stockage ou traitement soit simplement accessoire à un service de type différent, comme la fourniture de place de marché en ligne servant d'intermédiaire entre fournisseurs et consommateurs ou utilisateurs professionnels.

(12) Les exigences de localisation des données constituent incontestablement un obstacle à la libre prestation des services de stockage ou 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 l'article 52 du traité sur le fonctionnement de l'Union européenne, et respectent le principe de proportionnalité consacré par l'article 5 du traité sur l'Union européenne. Afin de donner effet au principe de libre circulation 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 stockage ou le traitement des données à plusieurs endroits dans l'UE, 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 pas pouvoir invoquer de motifs autres que celui de la sécurité publique.

(13) Afin d'assurer l'application effective du principe de libre circulation 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 notifier à la Commission tout projet d'acte contenant une nouvelle exigence de localisation des données ou modifiant une exigence existante. Ces notifications devraient être transmises et appréciées selon la procédure établie dans la directive (UE) 2015/1535[33].

(14) De plus, afin de supprimer les dispositions pouvant constituer des obstacles, les États membres devraient, durant une période transitoire de 12 mois, procéder à l'examen des actuelles exigences nationales de localisation des données et notifier à la Commission,

---

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).

[32] 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).

[33] 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).

avec une justification, toute exigence de localisation des données qu'ils jugent conforme au présent règlement. Ces notifications devraient permettre à la Commission d'apprécier la conformité de toute exigence de localisation restante.

(15) Afin d'assurer la transparence des exigences de localisation des données en vigueur dans les États membres pour les personnes physiques et morales, comme les fournisseurs et utilisateurs des services de stockage ou de traitement des données, les États membres devraient publier les informations concernant de telles mesures sur un guichet unique d'information en ligne et les mettre à jour régulièrement. Afin que les personnes morales et physiques 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 guichets en ligne. La Commission devrait publier ces informations sur son propre site web.

(16) La raison qui sous-tend les exigences de localisation des données est souvent un manque de confiance dans le stockage ou 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. Par conséquent, le présent règlement devrait clairement établir qu'il n'entame pas le pouvoir des autorités compétentes de demander et d'obtenir l'accès à des données conformément au droit national ou de l'Union, et que cet accès ne peut être refusé aux autorités compétentes au motif que les données sont stockées ou traitées dans un autre État membre.

(17) 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 stockées ou 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 de stockage ou de traitement des données.

(18) Lorsqu'une personne physique ou morale soumise aux obligations de fournir des données ne les respecte pas et que l'autorité compétente a épuisé tous les moyens d'obtenir l'accès aux données, 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 dans le droit de l'Union ou dans les 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 questions administratives - respectivement, la décision-cadre 2006/960[34], la directive 2014/41/UE du Parlement européen et du Conseil[35], la Convention sur la cybercriminalité du Conseil de l'Europe[36], le règlement (CE) n° 1206/2001 du Conseil[37], la directive 2006/112/CE du

[34] 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).

[35] 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).

[36] Convention sur la cybercriminalité du Conseil de l'Europe, STCE n° 185.

Conseil[38] et le règlement (UE) n° 904/2010 du Conseil[39]. 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, pour autant que cela ne soit pas contraire à l'ordre public de l'État membre dont l'assistance est sollicitée.

(19) 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, et notamment à tous les équipements et moyens de stockage ou de traitement des données, cet accès doit être conforme au droit procédural de l'Union ou de l'État membre, y compris toute obligation d'obtenir une autorisation judiciaire préalable.

(20) 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 stockage ou 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 personnes physiques et les consommateurs bénéficient de la législation de l'Union en vigueur, aucune mesure de facilitation ne concerne la possibilité, pour les utilisateurs, de changer de fournisseur de services dans le cadre de leurs activités commerciales ou professionnelles.

(21) 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 stockage ou de traitement des données proposés dans le marché intérieur, notamment en ce qui concerne les conditions 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 et des utilisateurs professionnels des services de stockage ou 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 et facilitée par la Commission, sous la forme de codes de conduite de l'Union pouvant comporter des clauses contractuelles types. Néanmoins, si ces codes de conduite ne sont pas mis en place ni appliqués de manière effective dans un délai raisonnable, la Commission devrait réexaminer la situation.

(22) Afin de contribuer à une bonne coopération entre les États membres, chacun d'entre eux devrait désigner un point de contact unique chargé d'assurer la liaison avec les points de contact des autres États membres et la Commission en ce qui concerne l'application du présent règlement. Lorsqu'une autorité compétente d'un État membre sollicite l'assistance d'un autre État membre pour accéder à des données conformément au présent règlement, elle devrait présenter au point de contact unique désigné dudit État membre une demande dûment motivée, comprenant une explication écrite de la justification et des bases juridiques de sa demande d'accès aux données. Le

---

[37] Règlement (CE) n° 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).

[38] 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).

[39] Règlement (UE) n° 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).

point de contact unique désigné par l'État membre sollicité devrait faciliter l'assistance entre les autorités en identifiant et en transmettant 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 à satisfaire une demande d'assistance ou sur ses raisons de rejeter cette demande.

(23) Afin d'assurer la mise en œuvre effective de la procédure d'assistance entre les autorités compétentes des États membres, la Commission peut adopter des actes d'exécution définissant les formulaires types, les langues utilisées pour les demandes, les délais ou d'autres détails des procédures de demande d'assistance. Ces compétences devraient être exercées conformément au règlement (UE) nº 182/2011 du Parlement européen et du Conseil[40].

(24) Le renforcement de la confiance dans la sécurité du stockage ou 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 les exigences de sécurité applicables lors de l'externalisation de leurs activités de stockage ou de traitement des données, notamment chez des fournisseurs de services dans d'autres États membres.

(25) Toutes les exigences de sécurité relatives au stockage ou 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 stockage ou 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.

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

(27) La directive 2016/1148[41] prévoit des mesures juridiques pour renforcer le niveau global de cybersécurité dans l'Union. Les services de stockage et de traitement des données sont au nombre des services numériques couverts par ladite directive. Son article 16 dispose que 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

[40] Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

[41] 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).

internationales. Ces éléments doivent être complétés par la Commission dans des actes d'exécution adoptés au titre de ladite directive.

(28) Les dispositions du présent règlement devraient être réexaminées périodiquement par la Commission, notamment en vue de déterminer s'il est nécessaire de les modifier pour tenir compte de l'évolution des technologies ou des marchés.

(29) 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 (article 8), à la liberté d'entreprise (article 16) et à la liberté d'expression et d'information (article 11).

(30) Étant donné que l'objectif du présent règlement, à savoir garantir la libre circulation des données à caractère non 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,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier
Objet

Le présent règlement vise à assurer la libre circulation 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 stockage ou tout autre 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 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. Le présent règlement ne s'applique pas aux activités qui ne relèvent pas du champ d'application du droit de l'Union.

Article 3
Définitions

Aux fins du présent règlement, on entend par:

1. «données», les données autres que les données à caractère personnel visées à l'article 4, paragraphe 1, du règlement (UE) 2016/679;

2. «stockage», tout stockage de données sous forme électronique;

3. «projet d'acte», un texte formulé en vue d'être adopté comme une 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 par l'État membre notifiant;

4. «fournisseur», une personne physique ou morale qui fournit des services de stockage ou 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 des États membres, qui impose la localisation du stockage ou du traitement des données sur le territoire d'un État membre donné ou qui entrave le stockage ou le traitement des données dans un autre État membre;

6. «autorité compétente», une autorité d'un État membre qui a le pouvoir d'obtenir l'accès aux données stockées ou traitées par une personne physique ou morale pour l'exécution de ses fonctions officielles, au sens du droit national ou du droit de l'Union;

7. «utilisateur», une personne physique ou morale qui utilise ou demande un service de stockage ou de traitement des données;

8. «utilisateur professionnel», une personne physique ou morale, y compris une entité du secteur public, qui utilise ou demande un service de stockage ou 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. La localisation des données à des fins de stockage ou de traitement au sein de l'Union n'est pas limitée au territoire d'un État membre spécifique, et le stockage ou le traitement dans un autre État membre ne fait l'objet d'aucune interdiction ou restriction, sauf si elle est justifiée par des raisons de sécurité publique.

2. Les États membres notifient 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 dans la législation nationale mettant en œuvre la directive (UE) 2015/1535.

3. Dans un délai de 12 mois après le début de l'application du présent règlement, les États membres veillent à ce que toute exigence de localisation des données non conforme aux dispositions du paragraphe 1 soit abrogée. Si un État membre estime qu'une exigence de localisation des données est conforme aux dispositions du paragraphe 1 et peut donc rester en vigueur, il notifie cette mesure à la Commission, accompagnée d'une justification de son maintien en vigueur.

4. Les États membres publient en ligne les détails de toutes les exigences de localisation des données applicables sur leur territoire, par l'intermédiaire d'un point d'information unique qu'ils tiennent à jour.

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 Web les liens vers ces points d'information unique.

Article 5
Disponibilité des données pour les autorités compétentes

1. Le présent règlement n'affecte pas le pouvoir des autorités compétentes de demander et 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 stockées ou traitées dans un autre État membre.

2. Lorsqu'une autorité compétente a épuisé tous les moyens d'obtenir l'accès aux données, elle peut solliciter l'assistance de l'autorité compétente d'un autre État membre, conformément à la procédure prévue à l'article 7, et l'autorité compétente sollicitée prête assistance conformément à la procédure prévue à l'article 7, pour autant que cela ne soit pas contraire à l'ordre public de l'État membre sollicité.

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, et notamment à tous les équipements et moyens de stockage ou de traitement des données, cet accès est conforme au droit procédural de l'Union ou de l'État membre.

4. Le paragraphe 2 ne s'applique que s'il n'existe pas de mécanisme de coopération spécifique en vertu du droit de l'Union ou d'accords internationaux d'échange de données entre autorités compétentes de différents États membres.

Article 6
Portage des données

1. La Commission encourage et facilite l'élaboration de codes de conduite par autorégulation au niveau de l'Union, afin de définir des lignes directrices concernant les bonnes pratiques pour faciliter le changement de fournisseur et de veiller à ce qu'ils fournissent aux utilisateurs professionnels des informations suffisamment détaillées, claires et transparentes préalablement à la signature d'un contrat de stockage et de traitement des données, en ce qui concerne les questions suivantes:

   (a) les processus, les exigences techniques, les délais et les frais qui s'appliquent dans le cas où un utilisateur professionnel souhaite changer de fournisseur ou transférer ses données pour les rapatrier vers ses propres systèmes informatiques, y compris 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; les garanties d'accès aux données en cas de faillite du fournisseur; et

   (b) les exigences fonctionnelles pour que le changement de fournisseur ou le portage des données s'effectue dans un format structuré, couramment utilisé, et lisible par machine accordant suffisamment de temps à l'utilisateur pour changer de fournisseur ou transférer les données.

2. La Commission encourage les fournisseurs à mettre effectivement en œuvre les codes de conduite visés au paragraphe 1 dans un délai d'un an à compter du début de l'application du présent règlement.

3. La Commission réexamine l'élaboration et la mise en œuvre effective de ces codes de conduite, ainsi que la fourniture effective d'informations par les fournisseurs, au plus tard deux ans après le début de l'application du présent règlement.

Article 7
Points de contact uniques

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. Les États membres veillent à ce que les points de contact uniques disposent des ressources nécessaires à l'application du présent règlement.

3. Lorsqu'une autorité compétente d'un État membre sollicite l'assistance d'un autre État membre pour accéder à des données conformément à l'article 5, paragraphe 2, elle présente au point de contact unique désigné de cet État membre une demande dûment motivée, comprenant une explication écrite de la justification et des bases juridiques de sa demande d'accès aux données.

4. Le point de contact unique identifie l'autorité compétente concernée de son État membre et lui transmet la demande reçue conformément au paragraphe 3. L'autorité ainsi sollicitée veille, sans retard injustifié:

   (a) à répondre à l'autorité compétente qui a présenté la demande et à notifier sa réponse au point de contact unique, et

   (b) à informer le point de contact unique et l'autorité compétente qui a présenté la demande de toute difficulté ou à indiquer, en cas de refus de la demande ou de réponse partielle, les motifs de ce refus ou de cette réponse partielle.

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. La Commission peut adopter des actes d'exécution définissant les formulaires types, les langues utilisées pour les demandes, les délais ou d'autres détails des procédures de demande d'assistance. Ces actes d'exécution sont adoptés conformément à la procédure prévue à l'article 8.

Article 8
Comité

1. La Commission est assistée par le comité de la libre circulation des données. Celui-ci est un comité au sens du règlement (UE) n° 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 182/2011 s'applique.

Article 9
Réexamen

1. Au plus tard le [5 ans après la date visée à l'article 10, paragraphe 2], la Commission procède au réexamen du présent règlement, dont elle présente les principales

conclusions dans un rapport au Parlement européen, au Conseil et au Comité économique et social européen.

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

Article 10
Dispositions finales

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

2. Le présent règlement 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 Bruxelles, le

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*