# COM(2025) 837 final

**ASSEMBLÉE NATIONALE**

**QUINZIÈME LÉGISLATURE**

**SÉNAT**

**SESSION ORDINAIRE DE 2025/2026**

**Reçu à la Présidence de l'Assemblée nationale**
**le 20 janvier 2026**

**Enregistré à la Présidence du Sénat**
**le 20 janvier 2026**

# TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT

Règlement du Parlement européen et du Conseil modifiant les règlements (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 et (UE) 2023/2854 ainsi que les directives 2002/58/CE, (UE) 2022/2555 et (UE) 2022/2557 en ce qui concerne la simplification du cadre législatif numérique, et abrogeant les règlements (UE) 2018/1807, (UE) 2019/1150 et (UE) 2022/868 ainsi que la directive (UE) 2019/1024 (règlement omnibus numérique)

E 20310

COMMISSION
EUROPÉENNE

Bruxelles, le 19.11.2025
COM(2025) 837 final

2025/0360 (COD)

Proposition de

# RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

**modifiant les règlements (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 et (UE) 2023/2854 ainsi que les directives 2002/58/CE, (UE) 2022/2555 et (UE) 2022/2557 en ce qui concerne la simplification du cadre législatif numérique, et abrogeant les règlements (UE) 2018/1807, (UE) 2019/1150 et (UE) 2022/868 ainsi que la directive (UE) 2019/1024 (règlement omnibus numérique)**

{SWD(2025) 836 final}

# EXPOSÉ DES MOTIFS

## 1. CONTEXTE DE LA PROPOSITION

### • Justification et objectifs de la proposition

Dans sa communication sur la mise en œuvre et la simplification («Une Europe plus simple et plus rapide»)[1], la Commission a présenté son approche concernant l'adaptation du cadre réglementaire de l'Union à un monde plus instable: un nouvel élan pour simplifier, clarifier et améliorer l'acquis de l'UE, en tant que mesure essentielle pour soutenir la compétitivité de l'UE.

Cette vision reflète le plan plus large défini par la présidente de la Commission, M[me] von der Leyen, dans ses orientations politiques pour la législature 2024-2029[2]. Comme souligné également dans les rapports Draghi[3] et Letta[4], l'accumulation de règles a parfois eu un effet négatif sur la compétitivité. Des améliorations rapides et visibles sont nécessaires pour les citoyens et les entreprises, grâce à une mise en œuvre de nos règles plus efficiente et plus propice à l'innovation, tout en maintenant des normes élevées et des objectifs partagés.

Dans ses conclusions du 20 mars 2025, le Conseil européen a en outre appelé la Commission à «continuer de réexaminer l'acquis de l'Union et de le soumettre à un test de résistance afin de déterminer les moyens de simplifier et consolider davantage la législation en vigueur»[5]. Il a également souligné la nécessité de présenter d'autres séries d'initiatives de simplification. Dans ses conclusions du 26 juin, le Conseil européen a souligné l'importance d'une législation fondée sur une approche de «simplicité dès la conception», «sans compromettre la prévisibilité, les objectifs stratégiques et les normes élevées»[6]. Dans ses conclusions du 23 octobre 2025, le Conseil européen a réaffirmé «qu'il est urgent de faire progresser, à tous les niveaux — régional, national et de l'UE — et dans tous les domaines, un programme ambitieux et mené horizontalement en matière de simplification et d'amélioration de la réglementation, afin d'assurer la compétitivité de l'Europe». Il a également invité la Commission à «présenter rapidement de nouveaux trains de mesures de simplification ambitieux, notamment dans les domaines [...] du numérique»[7].

Dans sa résolution sur «la mise en œuvre et la rationalisation des règles du marché unique de l'UE pour renforcer le marché unique», votée le 11 septembre en plénière[8], le Parlement

---

1 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Une Europe plus simple et plus rapide: communication sur la mise en œuvre et la simplification, COM(2025) 47 final, 11 février 2025.

2 von der Leyen, U. (2024) *«Le choix de l'Europe: Orientations politiques pour la prochaine Commission européenne 2024-2029*. Disponible à l'adresse suivante: e6cd4328-673c-4e7a-8683-f63ffb2cf648_fr

3 Draghi, M. (2024) *The future of European competitiveness* (L'avenir de la compétitivité européenne). Disponible à l'adresse suivante: Le rapport Draghi sur la compétitivité de l'UE

4 Letta, E. (2024) *Much more than a market* (Bien plus qu'un marché). Disponible à l'adresse suivante: Enrico Letta - Much more than a market (April 2024)

5 Conclusions du Conseil européen, EUCO 1/25, Bruxelles, 20 mars 2025, point 13

6 Conclusions du Conseil européen, EUCO 12/25, Bruxelles, 26 juin 2025, point 30.

7 Conclusions du Conseil européen, EUCO 18/25, Bruxelles, 23 octobre 2025, points 33 et 35.

8 Résolution du Parlement européen du 11 septembre 2025 sur la mise en œuvre et la rationalisation des règles du marché unique de l'UE pour renforcer le marché unique (2025/2009/INI).

européen a souligné la nécessité d'une simplification afin de faciliter la mise en conformité des entreprises sans compromettre les objectifs stratégiques fondamentaux de l'UE.

Dans le cadre des activités de consultation et d'engagement des parties intéressées menées par la Commission autour du programme de simplification, les parties prenantes représentant différents intérêts ont demandé des modifications ciblées de certaines règles dans le domaine du numérique, à la fois pour rationaliser les coûts de mise en conformité et pour clarifier les interactions entre les règles en vigueur dans leur secteur.

Avec une valeur ajoutée de 791 milliards d'EUR pour l'ensemble de l'Union européenne en 2022[9], le secteur des TIC joue un rôle crucial lorsqu'il s'agit de stimuler la compétitivité de l'UE dans tous les secteurs de l'économie, tant par la croissance des entreprises numériques que par l'offre de solutions numériques clés à tous les niveaux. La réglementation en matière numérique a joué un rôle déterminant dans la mise en place d'un environnement équitable pour les entreprises dans l'UE. Elle a permis de créer un véritable marché unique des services numériques. L'UE a été à la pointe en matière de réglementation du numérique et s'est dotée de la norme la plus stricte, qui sert de référence en matière de protection des droits fondamentaux, de sécurité des consommateurs et de protection des valeurs européennes.

La Commission est déterminée à réaliser un «test de résistance» complet du corpus réglementaire numérique tout au long du mandat législatif. L'objectif est très clair: pour faire en sorte que les règles restent adaptées de manière à favoriser l'innovation et la croissance, elles doivent atteindre leurs objectifs et constituer un moteur de la compétitivité. Tout au long de ce processus, la Commission s'efforcera de fournir des solutions convaincantes pour simplifier, clarifier et consolider l'efficacité des règles et leur application en recourant à tous les instruments disponibles, qu'il s'agisse d'ajustements réglementaires, d'une coopération renforcée entre les autorités, de la promotion de solutions numériques destinées à simplifier la conformité réglementaire «dès la conception», ou d'autres mesures d'accompagnement.

**La proposition de règlement omnibus sur le numérique constitue une première étape** dans l'optimisation de l'application du corpus réglementaire numérique. Elle comprend une série de modifications techniques à un vaste corpus législatif numérique, sélectionnées pour apporter un allègement immédiat aux entreprises, aux administrations publiques et aux citoyens, de manière à stimuler la compétitivité. L'objectif immédiat est de faire en sorte que le respect des règles se fasse à moindre coût, atteigne les mêmes objectifs et procure en soi un avantage concurrentiel aux entreprises responsables. Les modifications ont été classées par ordre de priorité sur la base des consultations réalisées auprès des parties prenantes et des premiers dialogues sur la mise en œuvre menés par la vice-présidente exécutive Henna Virkkunen et le commissaire Michael McGrath.

Pour ces raisons, les modifications visent à tirer parti des possibilités qui s'offrent dans l'utilisation des données, en tant que ressource fondamentale au sein de l'économie de l'Union, notamment en vue de favoriser le développement et l'utilisation de solutions d'intelligence artificielle fiables sur le marché de l'Union. Les modifications ciblées des

---

[9] Eurostat (2025) *Statistics explained: ICT sector – value added, employment and R&D*. Disponible à l'adresse suivante: ICT sector - value added, employment and R&D - Statistics Explained - Eurostat.

règles en matière de protection des données et de la vie privée soutiennent cet objectif et constituent des mesures de simplification immédiates pour les entreprises et les particuliers, renforçant ainsi leur capacité à exercer leurs droits.

En outre, les modifications apportées au règlement (UE) 2024/1689 (règlement sur l'intelligence artificielle[10]), présentées dans une proposition législative distincte faisant partie du train de mesures omnibus sur le numérique, visent à faciliter l'application harmonieuse et efficace des règles relatives au développement et à l'utilisation sûrs et dignes de confiance de l'IA.

Le règlement omnibus sur le numérique prévoit également une solution très claire pour rationaliser le signalement des incidents de cybersécurité, en intégrant dans un mécanisme de signalement unique toutes les obligations concernées en matière de signalement.

Enfin, la proposition abroge des règles obsolètes dans la réglementation des plateformes, qui ont été remplacées par des règlements plus récents.

Les modifications visent à rationaliser les règles, à réduire le nombre d'actes législatifs et à harmoniser les dispositions. Elles permettent de réduire les coûts administratifs en simplifiant les dispositions et les procédures. Elles dispensent les petites entreprises à moyenne capitalisation de certaines obligations prévues par la législation sur les données et le règlement (UE) 2024/1689 (règlement sur l'intelligence artificielle[11]), en plus des petites entreprises et des microentreprises qui relèvent déjà d'un régime spécial. Elles stimulent également les possibilités en faveur d'un environnement économique dynamique, en créant davantage de sécurité juridique et d'opportunités, en particulier dans des domaines tels que le partage et la réutilisation des données, le traitement des données à caractère personnel ou l'entraînement des systèmes et modèles d'intelligence artificielle.

Dans le même temps, les modifications proposées conservent un caractère technique, dans la mesure où elles visent à adapter le cadre réglementaire, mais sans en modifier les objectifs sous-jacents. Les mesures sont calibrées de manière à préserver le même niveau de protection des droits fondamentaux.

Parallèlement au règlement omnibus sur le numérique, la Commission présente également sa proposition de **règlement relatif aux portefeuilles européens d'identité numérique pour les entreprises**, qui constitue une initiative essentielle pour simplifier la mise en conformité avec la réglementation et réduire les charges administratives pesant sur les entreprises. Les portefeuilles d'identité numérique pour les entreprises seront conçus comme des outils numériques sécurisés destinés aux entreprises et feront office de plateforme unique afin de simplifier les interactions entre entreprises dans l'ensemble de l'UE. Grâce à la mise en œuvre d'un identifiant univoque et constant, les entreprises seront habilitées à vérifier numériquement les identités, à signer des documents, à horodater et à échanger des informations numériques vérifiées sans discontinuité par-delà les frontières grâce à l'utilisation d'une solution unique. En adoptant des portefeuilles européens d'identité

[10] Conformément à la proposition législative distincte.
[11] Voir la proposition distincte.

numérique pour les entreprises, les entreprises, en particulier les PME, pourront piloter facilement la conformité, de façon à libérer des ressources essentielles susceptibles d'être réorientées vers la croissance et l'innovation.

En tant que seconde étape de son engagement à soumettre à un «test de résistance» le corpus réglementaire numérique, **la Commission procède également actuellement à un bilan de qualité numérique**. Alors que les propositions omnibus sur le numérique sont immédiates et ciblées, l'analyse que la Commission entreprendra dans le cadre du bilan de qualité numérique portera essentiellement sur les effets cumulés des règles numériques, en s'efforçant de déterminer comment elles soutiennent la compétitivité de l'Union et à quels niveaux de nouveaux ajustements devront être proposés au cours de la seconde moitié du mandat législatif.

Le bilan de qualité numérique est entamé en même temps que la proposition de règlement omnibus, et s'accompagnera d'une vaste consultation publique. La Commission s'efforce de dialoguer avec toutes les parties prenantes et de procéder à une large consultation. L'objectif est de disposer ultérieurement d'une vue d'ensemble et d'une vaste cartographie de la manière dont le corpus réglementaire numérique couvre les secteurs stratégiques de l'industrie de l'Union, et d'examiner la manière dont l'effet cumulé des règles a une incidence sur leur compétitivité. Sur cette base, l'analyse approfondira, dans un second temps, les synergies et les domaines qui pourraient être davantage alignés, allant des définitions et des concepts juridiques à l'efficacité et à l'interaction des systèmes de gouvernance et d'autres mesures de soutien.

Le «test de résistance» de l'acquis numérique se poursuivra également dans le cadre de dialogues sur la mise en œuvre et d'**évaluations portant sur l'ensemble des principaux instruments juridiques**. Dans le cadre de la planification actuelle, entre autres initiatives, la Commission prévoit de publier en 2026 une révision du règlement sur les marchés numériques, du programme d'action pour la décennie numérique, du règlement sur les semi-conducteurs, et de la directive «Services de médias audiovisuels», ainsi qu'une évaluation de la directive sur le droit d'auteur. En 2027, les actes pour lesquels une évaluation est prévue comprennent notamment le règlement sur la cybersolidarité, le règlement relatif à l'accès à un internet ouvert, la directive SRI 2 et le règlement sur les services numériques. En 2028, la Commission devrait évaluer le règlement européen sur la liberté des médias ainsi que le règlement sur les données, par exemple, avant de poursuivre en 2029 par une évaluation du règlement sur l'IA et de la clause de caducité du règlement établissant le centre et réseau européens de compétences en matière de cybersécurité.

Les parties prenantes ont souligné à plusieurs reprises que, dans de nombreux cas, l'effort de simplification ne consiste pas tant à modifier les règles qu'à clarifier leur application. **La Commission cible en priorité une série de lignes directrices** visant à favoriser l'application uniforme des règles, sans préjudice des interprétations de la Cour de justice.

En ce qui concerne le cadre réglementaire applicable aux données, la Commission a annoncé qu'elle accordait la priorité à la stratégie pour une union des données, en mettant notamment l'accent sur l'élaboration de lignes directrices pour une compensation raisonnable afin de clarifier ce qui peut être demandé comme rémunération pour le partage de données, de manière à assurer une sécurité juridique tant aux détenteurs qu'aux destinataires de données, ainsi que sur l'élaboration de lignes directrices destinées à clarifier les définitions.

Afin de soutenir l'application du règlement sur l'intelligence artificielle, la Commission continue de donner la priorité à la publication de lignes directrices portant sur plusieurs aspects, comme expliqué plus en détail dans l'exposé des motifs de la proposition de règlement omnibus numérique modifiant le règlement sur l'intelligence artificielle.

***Propositions incluses dans le règlement omnibus sur le numérique***

Au cours des dernières années, **l'«acquis législatif en matière de données»** a été étendu à une série de règlements, créant de la sorte une complexité juridique, notamment certains chevauchements, des définitions non parfaitement alignées, ou des questions sur l'interaction des instruments. En particulier, le règlement (UE) 2018/1807 (règlement sur le libre flux des données à caractère non personnel) a été adopté et a été conçu pour créer un marché unique des services en nuage. Il a été partiellement remplacé par le chapitre VI du règlement (UE) 2023/2854 (règlement sur les données), qui établit des obligations lors du changement de services de traitement de données.

Un autre exemple est le chapitre II du règlement (UE) 2022/868 (règlement sur la gouvernance des données), qui complète les règles relatives à la réutilisation des informations du secteur public énoncées dans la directive (UE) 2019/1024 (directive sur les données ouvertes) pour les données qui ne peuvent pas être réutilisées sans restriction. En outre, d'autres chapitres du règlement (UE) 2022/868 (règlement sur la gouvernance des données) ont créé des règles relatives aux services d'intermédiation de données, à l'altruisme en matière de données, ainsi qu'aux exigences applicables aux demandes d'accès à des données à caractère non personnel introduites par des pouvoirs publics étrangers, et ont créé le comité européen de l'innovation dans le domaine des données. Le règlement (UE) 2023/2854 (règlement sur les données), en revanche, a créé une obligation matérielle pour les fabricants d'appareils connectés et les fournisseurs de services connexes de partager des données avec leurs utilisateurs, ou pour les entreprises de partager des données avec des agences gouvernementales, ainsi que des règles relatives aux contrats équitables de partage de données.

Pour remédier à cette situation, le règlement omnibus sur le numérique propose d'abroger les règles obsolètes, en particulier les règles actuelles du règlement (UE) 2018/1807 (règlement sur le libre flux des données à caractère non personnel), à l'exception de l'interdiction des exigences en matière de localisation des données dans l'Union, ainsi que de consolider et de rationaliser les règles du règlement (UE) 2022/868 (règlement sur la gouvernance des données), telles que les règles relatives à l'altruisme en matière de données et aux services d'intermédiation de données afin de renforcer l'attractivité de ces mécanismes de partage de données. Dans le même temps, les règles du règlement sur la gouvernance des données relatives à la réutilisation des données protégées sont fusionnées avec les règles de la directive (UE) 2019/1024 (directive sur les données ouvertes) afin de créer un cadre unique pour la réutilisation des données détenues par des organismes du secteur public, qui se reflète dans le règlement (UE) 2023/2854 (règlement sur les données). Cette solution présente de nombreux avantages pour les administrations publiques détenant des données du secteur public ainsi que pour les réutilisateurs, car ils peuvent rationaliser les processus et réduire la charge administrative liée à l'interprétation et à la mise en œuvre de diverses législations nationales.

La proposition introduit en outre la possibilité pour les organismes du secteur public de fixer des conditions différentes et de demander le paiement de redevances plus élevées pour la réutilisation par les très grandes entreprises, et en particulier par les entreprises désignées comme contrôleurs d'accès, telles que définies à l'article 3 du règlement (UE) 2022/1925 (règlement sur les marchés numériques), lesquelles détiennent un pouvoir et une influence

considérables sur le marché intérieur. Afin d'empêcher ces entités de tirer parti de leur pouvoir de marché substantiel au détriment d'une concurrence loyale et de l'innovation, les organismes du secteur public seront en mesure de fixer des conditions particulières pour la réutilisation des données et des documents par ces entités.

La proposition inclut les règles consolidées et rationalisées du règlement (UE) 2024/1689 (règlement sur le libre flux des données), du règlement (UE) 2022/868 (règlement sur la gouvernance des données) et de la directive (UE) 2019/1024 (directive sur les données ouvertes) figurant dans le règlement (UE) 2023/2854 (règlement sur les données), créant ainsi un instrument consolidé unique pour l'économie européenne fondée sur les données. Le règlement (UE) 2024/1689 (règlement sur le libre flux des données), la directive (UE) 2019/1024 (directive sur les données ouvertes) et le règlement (UE) 2022/868 (règlement sur la gouvernance des données) sont abrogés. Les règles des quatre instruments sont mieux alignées et rationalisées pour plus de clarté et de cohérence, de manière à accroître leur efficacité et à aider les entreprises à promouvoir l'innovation. La présente initiative est conforme à la stratégie pour une union des données, qui vise fondamentalement à favoriser la simplification du cadre législatif.

En outre, afin d'aider davantage les petites entreprises, les règles qui facilitent la mise en conformité des petites et moyennes entreprises (PME) avec la législation de l'UE sur les données sont étendues aux petites entreprises à moyenne capitalisation. Le règlement (UE) 2023/2854 (règlement sur les données), entré en application le 12 septembre 2025, marque une étape importante vers une économie de l'UE fondée sur les données qui soit équitable et compétitive. Les modifications présentées dans la présente proposition n'ont pas pour but d'apporter des modifications aux résultats obtenus dans le cadre du règlement (UE) 2023/2854 (règlement sur les données).

Toutefois, pour atteindre pleinement son objectif consistant à trouver un équilibre entre l'innovation et la disponibilité des données, d'une part, et la protection des droits et des intérêts des détenteurs de données, d'autre part, quatre éléments clés nécessitent un calibrage. Plus précisément, il est essentiel de veiller à ce que le règlement (UE) 2023/2854 (règlement sur les données) non seulement réduise les charges, mais renforce également la clarté juridique et stimule la compétitivité. Premièrement, il est urgent de renforcer les garanties contre le risque de fuites de secrets d'affaires vers des pays tiers dans le cadre des dispositions obligatoires relatives au partage des données de l'internet des objets (IdO). Deuxièmement, le champ d'application étendu du cadre régissant les relations entre les entreprises et les administrations publiques pourrait potentiellement donner lieu à une ambiguïté juridique. Troisièmement, une insécurité juridique pourrait résulter des dispositions relatives aux exigences essentielles applicables aux contrats intelligents exécutant des accords de partage de données. Enfin, les dispositions du règlement (UE) 2023/2854 (règlement sur les données) relatives au changement de services de traitement de données conservent leur pertinence en tant que contribution essentielle à un marché de l'informatique en nuage plus ouvert et plus compétitif. Néanmoins, ces dispositions ne tenaient pas suffisamment compte de la situation spécifique des services qui, pour pouvoir être utilisés, doivent être fortement personnalisés en fonction des besoins d'un client ou qui sont fournis par des PME ou des petites entreprises à moyenne capitalisation. Les modifications contenues dans la présente proposition conserveront l'objectif visant à supprimer la dépendance à l'égard des fournisseurs, en particulier les frais de changement de fournisseur et les frais de transfert, tout en réduisant la charge administrative pesant sur les fournisseurs des services mentionnés ci-avant. La proposition présente donc des modifications qui renforcent la clarté juridique et sont

étroitement alignées sur les objectifs généraux du règlement (UE) 2023/2854 (règlement sur les données).

En outre, afin d'aider davantage les petites entreprises, les règles qui facilitent la mise en conformité des petites et moyennes entreprises (PME) avec l'acquis de l'Union en matière de données sont étendues aux petites entreprises à moyenne capitalisation.

**En ce qui concerne les données à caractère personnel**, le règlement (UE) 2016/679 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 (règlement général sur la protection des données — RGPD) est entré en vigueur le 25 mai 2018, créant des normes, des règles et des garanties à l'échelle de l'Union applicables au traitement des données à caractère personnel des personnes physiques et aux droits des personnes concernées, ainsi qu'un cadre juridique général pour les personnes qui traitent des données à caractère personnel. Si, d'une manière générale, les parties prenantes ont jugé le règlement (UE) 2016/679 (règlement général sur la protection des données) équilibré, solide et toujours adapté à sa finalité, certaines entités, en particulier les petites entreprises et les associations qui procèdent à un petit nombre d'opérations de traitement à faible intensité de données, souvent à faible risque, ont fait part de leurs préoccupations quant à l'application de certaines obligations du règlement général sur la protection des données. Il peut être remédié à certaines de ces préoccupations en garantissant une interprétation et une application plus cohérentes et harmonisées dans tous les États membres, tandis que, pour d'autres, des modifications ciblées de la législation seront nécessaires. Dans ce contexte, les modifications contenues dans la présente proposition visent à répondre à ces préoccupations, notamment en clarifiant certaines définitions clés, par exemple les notions de données à caractère personnel; en facilitant la mise en conformité, par exemple en aidant les responsables du traitement en ce qui concerne les critères et les moyens permettant de déterminer si les données résultant de la pseudonymisation ne constituent pas des données à caractère personnel, ou en ce qui concerne les exigences en matière d'information et les notifications de violations de données aux autorités de contrôle; ainsi qu'en clarifiant certains aspects du traitement des données à des fins d'entraînement et de développement de l'IA. Les modifications proposées permettent également de remédier au manque de clarté quant aux conditions applicables à la recherche scientifique en fournissant une définition de la recherche scientifique, en expliquant davantage encore que le traitement ultérieur à des fins scientifiques doit être compatible avec la finalité initiale du traitement et en précisant que la recherche scientifique constitue un intérêt légitime. Il est également proposé d'étendre les exceptions accordées dans le cadre de l'obligation d'information aux fins du traitement. Le cas échéant, la présente proposition tient compte des modifications apportées au règlement général sur la protection des données figurant dans le règlement (UE) 2018/1725 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union.

En outre, une solution réglementaire sur la lassitude du consentement et la prolifération des bandeaux relatifs aux cookies est attendue depuis longtemps. La directive 2002/58/CE concernant la protection de la vie privée dans le secteur des communications électroniques (ci-après la directive «vie privée et communications électroniques»), révisée en dernier lieu en 2009, fournit un cadre pour la protection de la confidentialité des communications et précise les dispositions du règlement (UE) 2016/679 (ci-après le «règlement général sur la protection des données» ou «RGPD») lorsque le traitement de données à caractère personnel intervient dans le cadre de communications électroniques. Elle protège également les équipements terminaux des utilisateurs qui peuvent être utilisés pour porter atteinte à la vie privée et recueillir des informations relatives à ces utilisateurs. Une partie essentielle de l'utilisation des

équipements terminaux — tels que les téléphones et les ordinateurs personnels — consiste à consommer du contenu et à utiliser des services en ligne. Bon nombre de ces services en ligne dépendent des recettes de la publicité, y compris de la publicité personnalisée. C'est également le cas pour les services de médias. Les fournisseurs de services en ligne s'appuient sur les «cookies» ou sur des technologies similaires utilisant les capacités de traitement et de stockage des équipements terminaux, de manière à accéder, par exemple, aux informations stockées dans l'équipement terminal ou émises à partir de celui-ci. Ces données sont utilisées à diverses fins, par exemple afin d'optimiser la fourniture du service pour l'équipement terminal en question, afin de garantir la sécurité de l'équipement terminal et le service dans son ensemble, mais aussi pour suivre le comportement et l'interaction des personnes avec différents services en ligne de manière à fournir une publicité personnalisée.

Lorsque le recours à ces technologies n'est pas nécessaire aux fins d'un stockage ou d'un accès techniques visant exclusivement à effectuer ou à faciliter la transmission d'une communication par la voie d'un réseau de communications électroniques, ou lorsqu'il est strictement nécessaire à la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur, la directive 2002/58/CE (directive «vie privée et communications électroniques») exige l'octroi d'un consentement. Ce consentement est généralement demandé au moyen de bandeaux contextuels affichés sur le site web ou l'application mobile. Ces bandeaux contiennent des informations sur les finalités du traitement, souvent liées aux types de cookies et aux destinataires des données, et ils ne sont pas toujours faciles à comprendre pour les personnes. Pour ces raisons, il se peut que ces bandeaux n'atteignent pas leur objectif, à savoir informer la personne et lui donner le contrôle de la protection de sa vie privée et du traitement de ses données à caractère personnel, et qu'ils soient, au contraire, davantage perçus comme une nuisance pour les internautes. Dans le même temps, les fournisseurs de services en ligne doivent faire face à des coûts considérables pour la conception de bandeaux conformes.

Pour ajouter à la complexité, l'article 5, paragraphe 3, de la directive 2002/58/CE (directive «vie privée et communications électroniques») s'applique au placement de cookies ou de technologies similaires permettant d'obtenir des informations à partir de l'équipement terminal d'un utilisateur, tandis que le traitement ultérieur des données à caractère personnel est soumis au règlement (UE) 2016/679 (règlement général sur la protection des données). Si le consentement est requis pour garantir le contrôle des personnes concernées, il ne constitue pas toujours la base juridique la plus appropriée pour un traitement ultérieur, par exemple lorsque le traitement est nécessaire à l'exécution d'un service autre que le service de la société de l'information. Cette situation a entraîné une insécurité juridique ainsi que des coûts de mise en conformité plus élevés pour les responsables du traitement qui traitent des données à caractère personnel obtenues au départ d'équipements terminaux. En outre, le double régime découlant de la directive «vie privée et communications électroniques» et du règlement général sur la protection des données a eu pour effet que des autorités nationales différentes sont compétentes pour superviser les règles des deux cadres juridiques.

Pour ces raisons, il est proposé de simplifier immédiatement l'interaction entre les règles applicables. Le traitement des données à caractère personnel stockées sur des équipements terminaux ou émises à partir de ces équipements ne devrait être régi que par le règlement (UE) 2016/679 (règlement général sur la protection des données), lequel intégrerait également l'exigence claire du consentement pour accéder à l'équipement terminal d'une personne physique lorsque des données à caractère personnel sont collectées. Les modifications proposées prévoient également certaines finalités pour lesquelles il ne devrait pas être nécessaire d'obtenir le consentement et pour lesquelles le traitement ultérieur devrait être

considéré comme licite, en particulier lorsqu'elles présentent un faible risque pour les droits et libertés des personnes concernées ou lorsque le placement de ces solutions technologiques est nécessaire à la fourniture d'un service demandé par la personne concernée.

Enfin, la proposition prévoit l'intégration d'indications automatisées et lisibles par machine quant aux choix individuels ainsi que le respect de ces indications par les fournisseurs de sites web et d'applications mobiles et par les fournisseurs d'applications de téléphonie mobile une fois que des normes seront disponibles. Cette proposition s'appuie sur la modification de 2009 de la directive 2002/58/CE (directive «vie privée et communications électroniques») (voir le considérant 66 de la directive 2009/136/CE), qui incitait déjà à permettre l'expression du consentement de l'utilisateur par l'utilisation des paramètres appropriés d'un navigateur ou d'une autre application lorsque cela était techniquement possible et effectif; sur l'article 21, paragraphe 5, du règlement (UE) 2016/679 (règlement général sur la protection des données); et sur la proposition de la Commission de 2017 relative à un règlement «vie privée et communications électroniques» [COM(2017) 10], qui proposait une gestion des choix de l'utilisateur via les paramètres du navigateur web. La proposition habilite la Commission à demander aux organismes de normalisation d'élaborer un ensemble de normes pour l'encodage d'indications automatisées et lisibles par machine des choix des personnes concernées, ainsi que pour la communication de ces choix depuis les navigateurs vers les sites web et depuis les applications de téléphonie mobile vers les services web. Une fois ces informations disponibles, et après un délai de grâce de six mois, les responsables du traitement utilisant un site web ou des applications mobiles pour fournir leur service seront tenus de respecter les indications automatisées et lisibles par machine qui ont été encodées. Dès lors que les responsables du traitement veillent à ce que leurs sites web ou applications de téléphonie mobile respectent ces normes, ils devraient bénéficier d'une présomption de conformité. Sur cette base, il est attendu que des paramètres pertinents soient également mis au point dans les navigateurs. Les dispositions sont formulées d'une manière neutre sur le plan technologique, de sorte que d'autres outils, tels que l'IA agentique, pourraient également aider les utilisateurs à faire des choix en matière de consentement, pour autant que ces outils soient en mesure de garantir le respect des exigences du RGPD. Compte tenu de l'importance des flux de revenus en ligne pour le journalisme indépendant en tant que pilier indispensable d'une société démocratique, les fournisseurs de services de médias tels que définis dans le règlement (UE) 2024/1083 (règlement européen sur la liberté des médias) ne devraient pas être tenus de respecter ces signaux numériques, de sorte qu'ils puissent informer les utilisateurs et leur permettre de faire leurs choix de consentement dans le cadre d'une interaction directe.

Les modifications proposées dans le présent règlement prévoient l'introduction d'un **guichet unique par l'intermédiaire duquel les entités pourront s'acquitter simultanément des obligations en matière de signalement des incidents qui leur incombent au titre de plusieurs actes juridiques**. En favorisant le principe du «signalement unique pour un partage multiple» (*report once, share many*), le guichet unique réduira la charge administrative pesant sur les entités, tout en garantissant un flux efficace et sûr des informations sur les incidents de sécurité vers les destinataires définis dans la législation concernée.

La proposition établit l'obligation pour l'Agence de l'Union européenne pour la cybersécurité (ENISA) de mettre au point le guichet unique, en tenant compte de la plateforme unique de signalement pour les notifications de vulnérabilités activement exploitées et d'incidents graves au titre du règlement (UE) 2024/2847 (règlement sur la cyberrésilience). Elle impose des exigences spécifiques pour l'outil, en tant que canal sécurisé pour les informations communiquées par les entités et transmises aux autorités compétentes. Elle laisse inchangées

les exigences juridiques sous-jacentes en matière de signalement des incidents, mais optimise considérablement la gestion des tâches et les ressources requises de la part des entités.

La proposition impose également l'utilisation du guichet unique pour une série d'obligations étroitement reliées en matière de signalement des incidents énoncées dans la directive (UE) 2022/2555 (directive SRI 2), le règlement (UE) 2016/679 (RGPD), le règlement (UE) 2022/2554 (DORA), le règlement (UE) nº 910/2014 (règlement eIDAS) et la directive (UE) 2022/2557 (directive CER). D'autres obligations sectorielles en matière de notification, telles que celles énoncées dans le cadre du code de réseau pour les aspects de la cybersécurité des flux transfrontaliers d'électricité (NCCS) et des instruments pertinents pour le secteur de l'aviation, relèveront également du guichet unique une fois que seront modifiés les actes délégués et les actes d'exécution respectifs qui établissent les obligations de notification au titre de ces cadres.

La proposition vise également à rationaliser le contenu des informations communiquées en introduisant des habilitations pour plusieurs actes juridiques, lorsque ceux-ci n'existent pas. Elle précise que, lors de l'élaboration de modèles de signalement communs aux fins de la directive (UE) 2022/2555, de la directive (UE) 2022/2557 ou du règlement (UE) 2016/679, afin de garantir la cohérence, de promouvoir les synergies et de réduire la charge administrative pesant sur les entités en réduisant au minimum le nombre de champs de données que les entités sont tenues de remplir, la Commission devrait tenir dûment compte de l'expérience acquise et des modèles communs élaborés dans le cadre du règlement (UE) 2022/2554 (DORA).

Parallèlement à ces modifications fondamentales, la Commission met la présente proposition à profit pour abroger le règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne (ci-après le règlement «plateforme à entreprise» ou «règlement P2B»). Ce règlement est en application depuis le 12 juillet 2020 et a constitué la première étape vers la mise en place d'un cadre juridique complet pour l'économie des plateformes. Depuis son entrée en application, d'autres actes du droit de l'Union réglementent désormais les services d'intermédiation en ligne et les plateformes en ligne. Il s'agit notamment du règlement (UE) 2022/1925 (règlement sur les marchés numériques) et du règlement (UE) 2022/2065 (règlement sur les services numériques), qui vont bien au-delà des dispositions du règlement P2B. Certaines dispositions du règlement P2B resteront en place afin de garantir la sécurité juridique des actes contenant des références croisées à ces dispositions, par exemple la directive (UE) 2024/2831 relative à l'amélioration des conditions de travail dans le cadre du travail via une plateforme. D'une manière générale, la simplification du cadre réglementaire pour les plateformes en ligne réduira les coûts de mise en conformité découlant de la superposition et du chevauchement de plusieurs règles, ainsi que le demandent les parties prenantes. Les fournisseurs de services intermédiaires en ligne bénéficieront d'une plus grande clarté des dispositions juridiques. L'application de la législation sera plus ciblée.

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

La proposition de règlement est accompagnée d'une seconde proposition modifiant le règlement (UE) 2024/1689 (règlement sur l'IA). Ensemble, elles constituent le train de mesures «omnibus sur le numérique» et marquent la première étape immédiate dans la simplification du corpus réglementaire numérique. Parallèlement au règlement omnibus sur le numérique, la proposition de révision du règlement (UE) 2019/881 (règlement sur la cybersécurité) comprendra, entre autres, le mandat actualisé de l'Agence de l'Union

européenne pour la cybersécurité (ENISA) ainsi que des mesures visant à simplifier la mise en conformité avec les exigences en matière de cybersécurité.

Le règlement omnibus numérique s'inscrit dans le cadre d'une stratégie plus large de simplification réglementaire annoncée dans le train de mesures sur le numérique, présentée plus en détail dans la section introductive du présent exposé des motifs.

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

La proposition fait partie du programme de la Commission pour la simplification du cadre réglementaire de l'Union. Le large champ d'application des actes modifiés montre qu'il existe des possibilités manifestes de simplification en prenant en considération l'interaction entre les différentes règles, y compris lorsqu'elles concernent des domaines d'action différents. C'est le cas, par exemple, de la solution de simplification numérique élaborée dans le cadre du guichet unique pour le signalement des incidents, qui laisse inchangées les obligations réglementaires sous-jacentes, mais rassemble dans une même interface les règles de cybersécurité qui s'appliquent aux entités essentielles, celles applicables au secteur financier, les règles en matière de protection des données, etc.

## 2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

- **Base juridique**

La proposition est fondée sur les articles 114 et 16 du traité sur le fonctionnement de l'Union européenne, lesquels reflètent la base juridique des actes qu'elle modifie. La base juridique appropriée pour les dispositions modifiant le règlement (UE) 2016/679 (règlement général sur la protection des données) et le règlement (UE) 2018/1725 est l'article 16 du traité. Étant donné que tous les autres actes modifiés sont fondés sur l'article 114 du traité, la même base juridique est également appropriée pour les dispositions modificatives correspondantes du présent règlement.

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

Étant donné que les règles modifiées sont des règles de l'Union, elles ne peuvent être modifiées qu'au niveau de l'Union. Les adaptations techniques présentées dans le présent règlement préservent la logique de subsidiarité qui sous-tend les actes modifiés.

En ce qui concerne le règlement (UE) 2023/2854 (règlement sur les données), les modifications renforcent l'objectif du présent règlement consistant à supprimer les obstacles au sein du marché unique pour une économie fondée sur les données. Pour ce faire, elles intègrent les règles existantes dans le présent règlement. Les modifications ciblées dont ces règles font l'objet visent à apporter simplification et clarification ainsi qu'à réduire les charges administratives tant pour le secteur privé que pour les autorités nationales. Elles n'interfèrent pas avec la compétence des États membres ou des institutions de l'Union.

C'est également le cas pour l'abrogation de la directive (UE) 2019/1024 (directive sur les données ouvertes), sachant que les règles de fond de ladite directive sont intégrées dans le

règlement (UE) 2023/2854 (règlement sur les données) sans que soient modifiées substantiellement les compétences conférées aux États membres. Une part importante des données du secteur public est déjà soumise à l'application directe du règlement d'exécution (UE) 2023/138 relatif aux ensembles de données de forte valeur[12]. La conversion en un règlement facilitera l'application uniforme des modifications proposées dans tous les États membres. Cela constituera une aide en particulier pour les administrations publiques détenant des données du secteur public, mais aussi pour les réutilisateurs de ces données, grâce à la rationalisation des processus et à la diminution de la charge administrative liée à l'interprétation et à la mise en œuvre de diverses législations nationales. Le contrôle du respect des règles directement applicables gagnera probablement en cohérence. La proposition ne modifie pas les régimes d'accès nationaux et vise à offrir suffisamment de flexibilité pour les solutions nationales, une prérogative mise en évidence par les États membres.

En ce qui concerne le règlement (UE) 2016/679 (règlement général sur la protection des données) et le règlement (UE) 2018/1725, les modifications proposées visent à apporter clarté et prévisibilité dans l'application des règles existantes et à réduire la charge administrative, dans la mesure du possible, sans compromettre le niveau élevé de protection des données prévu par lesdits règlements. De même, elles laissent inchangées les compétences des États membres et des organes et institutions de l'Union.

Avec l'introduction du guichet unique pour le signalement des incidents, une solution à l'échelle européenne est proposée afin de fournir un canal unique pour les multiples obligations légales imposées aux entreprises concernant le signalement d'un incident qui est substantiellement le même. Cette solution ne modifie en rien les droits et compétences des autorités nationales en tant que destinataires de ces rapports. Au lieu de cela, elle encourage les signalements en fournissant un guichet unique dans une interface facile à utiliser pour le dépôt, en apparence, d'un seul rapport, tout en répondant simultanément à de multiples obligations légales. Étant donné qu'un grand nombre des services concernés sont fournis par-delà les frontières et que les prestataires sont présents dans plusieurs États membres, une solution à l'échelon européen est nécessaire.

- **Proportionnalité**

La proposition comprend les modifications techniques nécessaires pour atteindre les objectifs de clarté réglementaire et de réduction des charges administratives, tout en préservant et en optimisant les objectifs sous-jacents de la législation modifiée. Ces modifications sont proportionnées, en ce qu'elles imposent des coûts de transition et d'adaptation négligeables, sinon nuls, aux entreprises et aux autorités tout en favorisant d'importantes retombées en termes d'économies de coûts au cours des années suivantes.

Plusieurs des modifications proposées dans le présent règlement poursuivent l'objectif de simplification en apportant essentiellement une sécurité juridique et en clarifiant l'application des règles, par exemple en ce qui concerne les précisions apportées aux détenteurs de données sur la protection des secrets d'affaires prévue dans le règlement (UE) 2023/2854 (règlement sur les données), les précisions sur l'entraînement des modèles et systèmes d'IA qui incluent

[12] Règlement d'exécution (UE) 2023/138.

des données à caractère personnel régies par le règlement (UE) 2016/679 (règlement général sur la protection des données), ou encore la notion de données à caractère personnel visée dans le règlement (UE) 2016/679 (règlement général sur la protection des données) et le règlement (UE) 2018/1725. Certaines dispositions visent à codifier les interprétations de la Cour de justice de l'Union européenne, notamment en ce qui concerne la pseudonymisation des données à caractère personnel précisée dans le règlement (UE) 2016/679 (règlement général sur la protection des données). À ce titre, elles comprennent des modifications très ciblées des règles qui, dans le même temps, devraient avoir une incidence importante en apportant une sécurité juridique aux entreprises et aux investisseurs.

Les modifications proposées dans le présent règlement visent également à réduire les coûts directs pour les entreprises et les autorités, sachant que des objectifs réglementaires identiques peuvent être atteints avec des charges moindres et que la proportionnalité des règles sera garantie. Par exemple, le régime obligatoire applicable aux services d'intermédiation de données prévu par le règlement (UE) 2022/868 (règlement sur la gouvernance des données) est transformé, dans le règlement (UE) 2023/2854 (règlement sur les données), en un régime volontaire et favorisant une plus grande confiance.

Avec l'extension aux petites entreprises à moyenne capitalisation de certaines dispositions applicables aux petites et moyennes entreprises, les mesures de simplification sont ciblées et apportent des modifications minimales au champ d'application de ces obligations, tout en offrant une sécurité juridique à un éventail plus large d'entreprises fortement susceptibles de contribuer à la compétitivité de l'Union. La proposition se limite aux modifications nécessaires pour garantir que les petites entreprises à moyenne capitalisation bénéficient du même cadre juridique que les PME.

Le guichet unique pour le signalement des incidents et des violations de données permet aux entreprises de réaliser des économies importantes, tout en s'attaquant au problème généralisé du sous-signalement. La proposition apporte non seulement une solution proportionnée mais aussi une solution de simplification essentielle par l'intermédiaire d'un outil numérique, tout en contribuant à l'efficacité des obligations de signalement couvertes dans le cadre du guichet.

L'abrogation du règlement (UE) 2019/1150 (règlement P2B) est nécessaire pour éliminer la duplication des règles; ledit règlement n'a qu'une valeur résiduelle et, compte tenu de l'approche réglementaire proportionnée poursuivie dans la réglementation des plateformes en ligne, il est nécessaire d'éliminer les obligations qui font double emploi.

- **Choix de l'instrument**

Les modifications sont proposées par voie de règlement, compte tenu de la nature des règles modifiées. Lorsque des directives sont modifiées, les dispositions s'adressent à des organismes européens ou apportent des modifications ciblées, notamment pour se dissocier de dispositions élaborées plus en détail dans des règlements.

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

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

La majeure partie de la législation prise en compte dans la présente proposition est relativement récente et fait l'objet d'une évaluation continue des résultats. Les principales

observations sont résumées dans le document de travail des services de la Commission qui accompagne la proposition.

Une exception à cette règle est le réexamen préliminaire de 2023 du règlement (UE) 2019/1150 (règlement «plateforme à entreprise» ou P2B)[13)]. Le rapport a fait état des effets positifs initiaux en ce qui concerne, par exemple, la transparence contractuelle pour les entreprises utilisatrices et le respect de la procédure dans le traitement des plaintes. Toutefois, le rapport a également mis en évidence un manque de connaissance des entreprises utilisatrices ainsi que des fournisseurs de services d'intermédiation en ligne et de moteurs de recherche en ligne quant à leurs droits et obligations respectifs au titre du règlement (UE) 2019/1150 (règlement P2B). Cette situation, conjuguée également au respect insuffisant des dispositions du règlement (UE) 2019/1150 (règlement P2B), a conduit à un manque de mise en œuvre. Très peu de plaintes ont été reçues jusqu'en 2023 au titre du règlement (UE) 2019/1150 (règlement P2B). Le rapport concluait que «le plein potentiel du règlement (UE) 2019/1150 (règlement P2B) [n'était] pas atteint à l'heure actuelle». Entre-temps, le règlement (UE) 2022/2065 (règlement sur les services numériques) et le règlement (UE) 2022/1925 (règlement sur les marchés numériques) ont commencé à s'appliquer pleinement et sont allés bien au-delà des dispositions du règlement (UE) 2019/1150 (règlement P2B).

- **Consultation des parties intéressées**

Plusieurs consultations ont été menées dans le cadre de l'élaboration de la proposition. Elles ont été conçues pour être complémentaires les unes des autres, couvrant soit différentes thématiques, soit différents groupes de parties prenantes.

Trois consultations publiques et appels à contributions ont été publiés au printemps 2025 sur les principaux piliers de la proposition. Une consultation s'est déroulée du 9 avril au 4 juin[14] sur la stratégie pour l'application de l'IA, une autre a été menée du 11 avril au 20 juin[15] sur la révision du règlement (UE) 2019/881 (règlement sur la cybersécurité), et enfin une autre encore a été organisée du 23 mai au 20 juillet[16] sur la stratégie pour une union européenne des données. Chaque questionnaire comportait une section spécifique (ou parfois plusieurs) sur les préoccupations en matière de mise en œuvre et de simplification, directement en rapport avec les réflexions sur le train de mesures omnibus sur le numérique. Au total, 718 réponses uniques ont été obtenues dans le cadre de ce premier flux de consultation.

---

[13] Document de travail des services de la Commission — Rapport de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur le premier réexamen préliminaire de la mise en œuvre du règlement (UE) 2019/1150 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne {SWD(2023) 300 final}.

[14] Commission européenne (2025), *Appel à contributions sur la stratégie pour l'application de l'IA*. Disponible à l'adresse suivante: Stratégie pour l'application de l'IA — renforcer le continent de l'IA

[15] Commission européenne (2025), *Appel à contributions sur la révision du règlement sur la cybersécurité.* Disponible à l'adresse suivante: Le règlement de l'UE sur la cybersécurité

[16] Commission européenne (2025), *Appel à contributions sur la stratégie pour une union européenne des données*. Disponible à l'adresse suivante: Stratégie pour une union européenne des données

Un appel à contributions relatif au train de mesures omnibus sur le numérique a également été publié du 16 septembre au 14 octobre 2025[17]. L'objectif était de donner aux parties prenantes la possibilité de formuler des observations sur une proposition consolidée relative au champ d'application du règlement omnibus numérique. 513 réponses ont été reçues, présentées par divers groupes de parties prenantes, notamment des entreprises et des associations professionnelles, des représentants de la société civile, des universitaires, des autorités, de même que des contributions individuelles de citoyens.

La vice-présidente exécutive Henna Virkkunen a organisé deux dialogues sur la mise en œuvre portant sur les principaux sujets abordés dans le train de mesures omnibus sur le numérique: le premier était consacré à la politique en matière de données[18] (1er juillet 2025) et le second à la politique en matière de cybersécurité[19] (15 septembre).

Le commissaire McGrath a organisé un dialogue sur la mise en œuvre du RGPD (16 juillet 2025).

Les services de la Commission ont également effectué plusieurs «vérifications sur le terrain» — des groupes de réflexion approfondis avec des entreprises et des représentants de la société civile organisés entre le 15 septembre et le 6 octobre 2025 afin de discuter des difficultés pratiques de mise en œuvre rencontrées au quotidien et d'estimer les coûts de mise en conformité.

Dans l'optique de consulter spécifiquement les petites et moyennes entreprises (PME) et de recueillir leur avis, un panel de PME spécifique a été organisé par l'intermédiaire du réseau Entreprise Europe (EEN)[20] entre le 4 septembre et le 16 octobre 2025.

Enfin, les services de la Commission ont reçu de nombreux documents de prise de position et ont organisé des réunions bilatérales avec diverses parties prenantes. Ils ont également dialogué avec les États membres lors de tables rondes ou dans le cadre de différents groupes de travail du Conseil.

Dans l'ensemble, les réactions des parties prenantes convergeaient quant à la nécessité de simplifier l'application de certaines règles numériques. Les parties prenantes ont salué le fait que l'accent soit mis sur la cohérence et la consolidation des règles, ainsi que sur l'optimisation des coûts de mise en conformité.

Un appel clair a été lancé en faveur d'une rationalisation de l'acquis en matière de données et d'une consolidation des règles. Ce souhait est pris en considération dans la proposition, de même que des modifications ciblées appuyées par des parties prenantes, notamment en ce qui concerne le règlement général sur la protection des données et la lassitude générée par les

---

[17] Commission européenne (2025), *Appel à contributions sur le paquet numérique et omnibus*. Disponible à l'adresse suivante: Simplification — paquet numérique et omnibus

[18] Commission européenne (2025), *«Dialogue sur la mise en œuvre — politique en matière de données*. Disponible à l'adresse suivante: Dialogue sur la mise en œuvre — politique en matière de données — Commission européenne

[19] Commission européenne (2025), *Dialogue sur la mise en œuvre avec la vice-présidente exécutive Henna Virkkunen consacré à la politique en matière de cybersécurité*. Disponible à l'adresse suivante: Dialogue sur la mise en œuvre avec la vice-présidente exécutive Henna Virkkunen consacré à la politique en matière de cybersécurité.

[20] L'EEN est le plus grand réseau de soutien au monde pour les petites et moyennes entreprises. Il est mis en œuvre par l'Agence exécutive pour le Conseil européen de l'innovation et les PME (EISMEA).

bandeaux relatifs aux cookies. En outre, les entreprises ont attiré l'attention sur la nécessité de réaliser de nouvelles évaluations de l'interaction entre les règles en matière de données qui justifient une analyse plus approfondie au moyen des outils relevant de la stratégie d'amélioration de la réglementation, notamment le prochain bilan de qualité numérique.

Les entreprises de différents secteurs ont également mis en évidence les charges injustifiées découlant du double signalement des incidents en vertu de plusieurs cadres juridiques. Cet appel à l'action est pris en considération avec la proposition d'un guichet unique pour le signalement des incidents.

En ce qui concerne le règlement sur l'intelligence artificielle, les parties prenantes ont souligné la nécessité d'une sécurité juridique dans l'application des règles et ont en particulier mis en évidence la nécessité de disposer de normes et d'orientations en amont de l'application des règles. La proposition de règlement distincte présentée dans le cadre du train de mesures omnibus sur le numérique répond à leurs préoccupations.

Enfin, les parties prenantes ne se sont pas exprimées sur l'incidence du règlement sur les relations entre les plateformes et les entreprises, confirmant les résultats du rapport d'évaluation intermédiaire selon lesquels les règles ne sont ni connues ni efficaces pour la réalisation de leur objectif. Le présent règlement propose d'abroger les règles relatives aux relations entre plateformes et entreprises, compte tenu notamment de leur chevauchement avec des règles plus récentes.

Un aperçu détaillé de ces consultations des parties prenantes et de la manière dont elles ont été prises en compte dans la proposition figure dans le document de travail des services de la Commission qui étaye le train de mesures omnibus sur le numérique.

- **Obtention et utilisation d'expertise**

Outre les flux de consultation décrits ci-dessus, la Commission s'est principalement appuyée sur une analyse interne aux fins de la présente proposition. Deux études ont également été commandées pour étayer l'analyse des chapitres de la proposition consacrés aux données. La première était axée sur la mise en œuvre du règlement (UE) 2018/1807 (règlement relatif au libre flux des données à caractère non personnel), de la directive (UE) 2019/1024 (directive sur les données ouvertes) et du règlement (UE) 2022/868 (règlement sur la gouvernance des données). La seconde étude, plus étroitement liée à la communication sur la stratégie pour une union des données (adoptée dans le cadre du même train de mesures de simplification parallèlement au train de mesures omnibus sur le numérique), était axée sur les évolutions de la politique en matière de données liées à l'IA générative, le respect de la réglementation et les dimensions internationales. Ces deux études sont en cours de finalisation et seront publiées ultérieurement.

Les services de la Commission ont également réalisé une étude sur l'interaction entre le règlement (UE) 2022/2065 (règlement sur les services numériques) et d'autres actes législatifs, notamment le règlement (UE) 2019/1150 (règlement P2B). La Commission publie, dans le cadre du train de mesures sur le numérique, le rapport décrivant l'interaction entre le règlement (UE) 2022/2065 (règlement sur les services numériques) et d'autres règles connexes, conformément à l'exigence de l'article 91 du règlement (UE) 2022/2065 (règlement sur les services numériques).

- **Analyse d'impact**

Les modifications proposées dans le présent règlement sont ciblées et de nature technique. Elles sont conçues pour assurer une mise en œuvre plus efficace des règles. Elles ne se prêtent pas à de multiples options stratégiques qui pourraient être testées et comparées de manière

significative et, conformément aux lignes directrices pour une meilleure réglementation, ne sont pas étayées par un rapport d'analyse d'impact complet.

Le document de travail des services de la Commission joint à la proposition aborde de manière approfondie la logique d'intervention adoptée pour les modifications ainsi que le point de vue des parties prenantes sur les différentes mesures, et présente l'analyse coûts-avantages des propositions, y compris les économies de coûts générées et d'autres types d'incidences. Dans de nombreux cas, il s'appuie sur les analyses d'impact respectives qui ont été réalisées à l'origine pour les différents actes.

- **Réglementation affûtée et simplification**

Le règlement proposé donne lieu à une réduction très importante de la charge pesant sur les entreprises, les administrations publiques et les citoyens. Les premières estimations prévoient des économies possibles d'au moins un milliard d'EUR par an, à compter de la date d'entrée en vigueur, avec une économie supplémentaire de coûts ponctuels d'un milliard d'EUR, soit un total d'au moins cinq milliards d'EUR sur trois ans d'ici à 2029. Des avantages non quantifiables sont également largement attendus, découlant notamment de la rationalisation d'un ensemble de règles qui facilitera l'adhésion et le respect des parties concernées. Les calculs excluent également les possibilités économiques créées par l'approche réglementaire proposée.

Si les PME sont déjà exemptées en vertu d'un certain nombre de dispositions figurant dans les actes juridiques modifiés dans le règlement omnibus sur le numérique, d'autres mesures de soutien sont proposées en ce qui concerne les changements de fournisseur de services en nuage. Dans le chapitre consacré à l'harmonisation des règles relatives au partage des données, certaines exemptions déjà accordées aux PME sont étendues aux petites entreprises à moyenne capitalisation.

La proposition est également pleinement cohérente avec le «bilan de qualité numérique» réalisé par la Commission, qui vise à garantir l'alignement adéquat des propositions d'action sur les environnements numériques. De plus amples informations à ce sujet figurent au chapitre 4 de la fiche financière et numérique législative jointe à la proposition.

- **Droits fondamentaux**

Les modifications proposées favorisent les possibilités d'innovation pour les entreprises au sein du marché unique et promeuvent ainsi le droit d'exercer une activité économique dans l'Union.

Certaines dispositions sont également liées à la protection et à la promotion d'autres droits fondamentaux, tels que le droit à la vie privée et à la protection des données à caractère personnel, et ont été calibrées de manière à préserver le niveau de protection le plus élevé et à aider les personnes à exercer effectivement leurs droits, tout en optimisant les coûts et en créant de nouvelles possibilités d'innovation. Ce faisant, la proposition respecte scrupuleusement le principe de proportionnalité consacré à l'article 52 de la Charte.

Dans le cas spécifique des modifications ciblées apportées au règlement (UE) 2016/679 (règlement général sur la protection des données) et au règlement (UE) 2018/1725, les modifications proposées visent à simplifier les exigences applicables au traitement à faible risque, à harmoniser certaines normes et à clarifier certains concepts clés du règlement (UE) 2016/679 (règlement général sur la protection des données) et du règlement (UE) 2018/1725, ce qui permettrait aux responsables du traitement de mettre en œuvre des politiques plus

efficaces en matière de protection des données. Ils pourraient ainsi concentrer leurs ressources sur des activités à plus forte intensité de données et à haut risque pour lesquelles les mesures de protection des données à caractère personnel sont les plus critiques.

En ce qui concerne le respect de la vie privée dans les communications, la proposition préserve le niveau de protection le plus élevé, y compris l'accès aux équipements terminaux fondé sur le consentement. La modification de la directive 2002/58/UE (directive «vie privée et communications électroniques») ne modifie pas les protections essentielles. Elle aligne sur les dispositions du règlement (UE) 2016/679 (règlement général sur la protection des données) les règles relatives au traitement des données à caractère personnel stockées sur des équipements terminaux ou émises à partir de ces équipements. Les règles relatives à l'intégrité des équipements terminaux prévues par la directive sont maintenues lorsque le traitement porte sur des données à caractère non personnel.

## 4. INCIDENCE BUDGÉTAIRE

L'incidence budgétaire de la mise en place et de la maintenance du guichet unique pour le signalement des incidents par l'Agence de l'Union européenne pour la cybersécurité (ENISA) est détaillée dans la révision du règlement (UE) 2019/881 (règlement sur la cybersécurité), dans le cadre des ressources accordées à l'ENISA.

## 5. AUTRES ÉLÉMENTS

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

Sans objet.

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

***Modifications apportées au règlement (UE) 2023/2854 — le règlement sur les données***

Les modifications apportées au cadre juridique applicable aux données consolident au sein du règlement (UE) 2023/2854 (règlement sur les données), d'une manière fortement rationalisée, les dispositions du règlement (UE) 2018/1807 (règlement sur le libre flux des données), du règlement (UE) 2022/868 (règlement sur la gouvernance des données) et de la directive (UE) 2019/1024 (directive sur les données ouvertes). Le chapitre I comprend également des modifications ciblées visant à adapter les règles actuelles du règlement (UE) 2023/2854 (règlement sur les données).

L'article 1er englobe les modifications apportées au règlement (UE) 2023/2854 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828.

**À l'article 1er:**

Le paragraphe 1 actualise le champ d'application du règlement (UE) 2023/2854 (règlement sur les données), dans lequel de nouveaux chapitres seront insérés, comme expliqué plus en détail ci-dessous.

Le paragraphe 2 modifie les définitions et en insère de nouvelles.

Le paragraphe 3 crée une nouvelle règle au titre de l'article 4, paragraphe 8, du règlement (UE) 2023/2854 (règlement sur les données) qui permet aux détenteurs de données de refuser

la divulgation de secrets d'affaires à un utilisateur lorsqu'il existe un risque élevé d'obtention ou d'utilisation illicites ou de divulgation illicite à des pays tiers, ou à des entités placées sous leur contrôle, qui sont soumis à des juridictions offrant des protections plus faibles que celles disponibles dans l'Union.

Le paragraphe 5 introduit la même règle pour l'article 5, paragraphe 11, du règlement (UE) 2023/2854 (règlement sur les données), concernant les détenteurs de données qui divulguent des secrets d'affaires à des tiers.

Les paragraphes 5 à 19 restreignent le champ d'application du chapitre V en remplaçant les «besoins exceptionnels» par les seules «situations d'urgence». Les articles 14 et 15 sont supprimés et un nouvel article 15 *bis* est créé, lequel devient l'article unique régissant les demandes en cas de situations d'urgence dans le cadre du régime B2G du règlement (UE) 2023/2854 (règlement sur les données). Les demandes peuvent être faites lorsque cela est nécessaire afin de réagir à une situation d'urgence (article 15 *bis*, paragraphe 2), ou à des fins d'atténuation ou de rétablissement à la suite d'une situation d'urgence (article 15 *bis*, paragraphe 3). Les références croisées sont adaptées en conséquence, la formulation est simplifiée et clarifiée. L'article 1er, paragraphe 21, crée un nouvel article 22 *bis* qui encadre le régime des réclamations prévu au chapitre V, en fusionnant des dispositions précédemment répétées.

Les paragraphes 20 à 22 prévoient certaines dérogations au chapitre VI du règlement (UE) 2023/2854 (règlement sur les données) (changement de services de traitement de données). À l'article 31, un régime spécifique allégé est inséré pour les services de traitement de données conçus sur mesure, c'est-à-dire des services de traitement de données qui ne sont pas prêts à l'emploi et qui ne fonctionneraient pas sans adaptation préalable aux besoins et à l'écosystème de l'utilisateur, lorsque ces services sont fournis sur la base de contrats conclus avant le 12 septembre 2025. De même, à l'article 31, un nouveau régime spécifique allégé est inséré pour les services de traitement de données fournis par des PME et des petites entreprises à moyenne capitalisation sur la base de contrats conclus avant le 12 septembre 2025, accompagné d'une précision selon laquelle ces fournisseurs peuvent inclure des pénalités de résiliation anticipée dans les contrats à durée déterminée.

Les paragraphes 23 à 25 apportent des modifications à l'article 32 du règlement (UE) 2023/2854 (règlement sur les données) résultant de l'intégration d'organismes actuellement régis par le règlement (UE) 2022/868 (règlement sur la gouvernance des données) dans le règlement (UE) 2023/2854 (règlement sur les données).

Le paragraphe 26 supprime des obligations faites aux fournisseurs de contrats intelligents de se conformer aux exigences essentielles en habilitant la Commission à adopter des normes harmonisées.

Le paragraphe 27 intègre deux régimes juridiques prévus actuellement dans le règlement (UE) 2022/868 (règlement sur la gouvernance des données), un règlement qui sera abrogé une fois que le règlement omnibus sur le numérique entrera en vigueur. Ce point réforme les règles actuelles figurant aux chapitres III et IV du règlement sur la gouvernance des données, qui prévoient un régime de notification obligatoire pour les prestataires de services d'intermédiation de données ainsi qu'un régime d'enregistrement volontaire pour les organisations altruistes en matière de données. Les deux régimes sont insérés en tant que nouveau chapitre VII *bis* dans le règlement (UE) 2023/2854 (règlement sur les données). Compte tenu de la nature émergente du marché des services d'intermédiation de données, les

obligations prévues par le règlement (UE) 2022/868 (règlement sur la gouvernance des données) doivent être assouplies pour permettre le développement de ce marché: premièrement, le régime applicable aux prestataires de services d'intermédiation de données est transformé en un régime volontaire. Deuxièmement, l'obligation la plus essentielle, à savoir l'obligation de maintenir les services d'intermédiation de données juridiquement séparés de tout autre service qu'une entreprise pourrait vouloir offrir, sera remplacée par une obligation de maintenir les services fonctionnellement séparés, assortie d'un ensemble de conditions supplémentaires. Enfin, la liste des obligations est considérablement raccourcie. En ce qui concerne l'altruisme en matière de données, les obligations concernant l'élaboration de rapports et la transparence imposées aux organisations altruistes en matière de données sont abrogées, de même que le principe de compléter les règles du règlement (UE) 2022/868 (règlement sur la gouvernance des données) par un «recueil de règles sur l'altruisme en matière de données» comportant des règles encore plus détaillées.

Un nouveau chapitre VII *ter* est introduit en vertu duquel l'interdiction des exigences de localisation pour les données à caractère non personnel à l'intérieur de l'Union, qui figurait auparavant dans le règlement (UE) 2018/1807 (règlement sur le libre flux des données à caractère non personnel), qui doit être abrogé, est insérée dans le règlement (UE) 2023/2854 (règlement sur les données). L'obligation de notification à la Commission est maintenue, mais le point d'information unique en ligne national où les États membres devraient publier les exigences applicables en matière de localisation des données est supprimé.

Les paragraphes 4 et 33 à 58 introduisent les dispositions fusionnées relatives à la réutilisation des données et des documents détenus par des organismes du secteur public au titre du chapitre II du règlement (UE) 2022/868 (acte sur la gouvernance des données) et de la directive (UE) 2019/1024 (directive sur les données ouvertes):

- Le point 4) introduit des définitions provenant des dispositions insérées dans le règlement (UE) 2023/2854 (règlement sur les données), harmonisant la définition des données et des documents en établissant une délimitation stricte entre les contenus numériques (données) et non numériques (documents).
- Il est introduit un nouveau chapitre VII *quater* sur la réutilisation des données et documents détenus par des organismes du secteur public.
- Il est introduit une nouvelle section 1, qui intègre les principes généraux applicables au chapitre nouvellement inséré.
- L'objet et le champ d'application du chapitre fusionné sont introduits, combinant les règles communes du chapitre II du règlement (UE) 2022/868 (règlement sur la gouvernance des données) et de la directive (UE) 2019/1024 (directive sur les données ouvertes).
- Il est fixé le principe commun de non-discrimination applicable au partage de données ouvertes du secteur public et de certaines catégories de données protégées.
- Il est énoncé l'interdiction d'accords d'exclusivité, commune au régime des données ouvertes du secteur public et à certaines catégories de données protégées.
- Il est énoncé des principes généraux relatifs à la tarification appliquée pour la réutilisation des données ouvertes du secteur public ou de certaines catégories de données protégées. En vertu d'une nouvelle règle, les organismes du secteur public devront veiller à ce que toute redevance puisse également être acquittée en ligne au moyen de services de paiement transfrontières largement disponibles, sans

discrimination en ce qui concerne la réutilisation de données ouvertes du secteur public. Il s'agit d'une extension de la règle qui n'était auparavant connue que pour la réutilisation de certaines catégories de données protégées au titre du chapitre II du règlement (UE) 2022/868 (règlement sur la gouvernance des données).

- Il est prévu le droit des réutilisateurs de données ouvertes du secteur public et de certaines catégories de données protégées d'être informés des voies de recours disponibles lorsqu'il s'agit de décisions ou de pratiques les concernant.
- Il est inséré une section relative aux règles de réutilisation des données ouvertes du secteur public, à savoir les règles anciennement prévues par la directive (UE) 2019/1024 (directive sur les données ouvertes).
- Le champ d'application de la section est déterminé, y compris le fait qu'elle ne s'applique pas à certaines catégories de données protégées relevant du chapitre général sur la réutilisation des données et des documents détenus par des organismes du secteur public.
- Il est énoncé le principe général relatif à la réutilisation des données ouvertes du secteur public.
- Il est fixé des règles pour le traitement des demandes de réutilisation de données ouvertes du secteur public, par l'insertion de l'ancienne disposition de la directive (UE) 2019/1024 (directive sur les données ouvertes).
- Il est introduit des règles relatives aux formats disponibles pour la réutilisation des données ouvertes du secteur public, qui relevaient auparavant de la directive (UE) 2019/1024 (directive sur les données ouvertes).
- Il est introduit des règles régissant la tarification prévue pour les données ouvertes du secteur public, laquelle était auparavant régie par la directive (UE) 2019/1024 (directive sur les données ouvertes). En vertu d'une nouvelle règle, les organismes du secteur public peuvent demander le paiement de redevances plus élevées pour la réutilisation par les très grandes entreprises. Ces redevances doivent être proportionnées et leur montant doit être fondé sur des critères objectifs.
- Il est introduit des règles relatives aux licences types pour la réutilisation des données ouvertes du secteur public, qui figuraient auparavant dans la directive (UE) 2019/1024 (directive sur les données ouvertes). En vertu d'une nouvelle règle, les organismes du secteur public peuvent prévoir des conditions particulières pour les très grandes entreprises. Ces conditions doivent être proportionnées et fondées sur des critères objectifs.
- Il est introduit dans le règlement (UE) 2023/2854 (règlement sur les données) les règles relatives aux modalités pratiques précédemment incluses dans la directive (UE) 2019/1024 (directive sur les données ouvertes), afin de faciliter la recherche de données ou de documents disponibles à des fins de réutilisation.
- Il est introduit dans le règlement (UE) 2023/2854 (règlement sur les données) les règles relatives aux données de recherche précédemment incluses dans la directive (UE) 2019/1024 (directive sur les données ouvertes).
- Il est introduit dans le règlement (UE) 2023/2854 (règlement sur les données) les règles relatives aux ensembles de données de forte valeur, précédemment incluses dans la directive (UE) 2019/1024 (directive sur les données ouvertes).

- Il est créé dans le chapitre une nouvelle section pour la réutilisation de certaines catégories de données protégées afin d'inclure les anciennes règles relevant du chapitre II du règlement (UE) 2022/868 (règlement sur la gouvernance des données). Ce point décrit le champ d'application de cette troisième section, qui exclut les données et documents relevant de la deuxième section, laquelle régit le régime de réutilisation des données ouvertes du secteur public. En vertu d'une nouvelle règle, les documents sont inclus dans le champ d'application de cette section.
- Il est énoncé le principe général relatif à la réutilisation de certaines catégories de données protégées. Il s'agit du principe énoncé au chapitre II du règlement (UE) 2022/868 (règlement sur la gouvernance des données), selon lequel la section ne crée pas d'obligation pour les organismes du secteur public d'autoriser la réutilisation de données protégées, mais fixe plutôt des conditions minimales lorsque les organismes du secteur public décident de mettre ces données à disposition en vue de leur réutilisation.
- Il est introduit, sous une forme simplifiée et rationalisée, les règles relatives aux conditions de réutilisation de certaines catégories de données protégées, précédemment incluses au chapitre II du règlement (UE) 2022/868 (règlement sur la gouvernance des données). Il est précisé les règles applicables en cas d'anonymisation des données à caractère personnel. Les exigences relatives aux transferts de données à caractère non personnel vers des pays tiers sont conservées mais scindées en un nouvel article au point 54).
- Il est introduit dans le règlement (UE) 2023/2854 (règlement sur les données) les règles relatives à la perception de redevances, lesquelles faisaient auparavant partie du chapitre II du règlement (UE) 2022/868 (règlement sur la gouvernance des données). En vertu d'une nouvelle règle, les organismes du secteur public peuvent prévoir des redevances plus élevées pour la réutilisation par les très grandes entreprises. Ces redevances doivent être proportionnées et fondées sur des critères objectifs. Le souci particulier d'encourager la réutilisation des données par les PME est étendu aux petites entreprises à moyenne capitalisation.
- Il est introduit dans le règlement (UE) 2023/2854 (règlement sur les données) les règles relatives aux organismes compétents, lesquelles faisaient auparavant partie du chapitre II du règlement (UE) 2022/868 (règlement sur la gouvernance des données). Les organismes compétents ont pour objet d'aider les organismes du secteur public à répondre aux demandes de réutilisation de données et de documents visés à la section 3.
- Il est introduit dans le règlement (UE) 2023/2854 (règlement sur les données) les règles relatives au point d'information unique, lesquelles faisaient auparavant partie du chapitre II du règlement (UE) 2022/868 (règlement sur la gouvernance des données). Les points d'information uniques sont conçus pour aider les réutilisateurs à trouver facilement des informations sur la réutilisation de certaines catégories de données protégées.
- Il est introduit dans le règlement (UE) 2023/2854 (règlement sur les données) les règles concernant la procédure applicable aux demandes de réutilisation de certaines catégories de données protégées, lesquelles étaient précédemment régies par le chapitre II du règlement (UE) 2022/868 (règlement sur la gouvernance des données).

Le paragraphe 57 intègre les règles de base relatives au comité européen de l'innovation dans le domaine des données (EDIB), un groupe chargé de conseiller la Commission sur

l'application cohérente du règlement sur les données et servant de forum de coordination pour l'élaboration des politiques dans le domaine de l'économie des données. Il intégrera les règles de base dans le règlement sur les données. Ces modifications permettront à la Commission d'adapter les documents fondateurs pertinents de l'EDIB [la décision de la Commission du 20 février 2023 — C(2023) 1074 final] et d'élargir la composition de l'EDIB aux représentants des services chargés de l'élaboration des politiques nationales, en plus des autorités compétentes.

Les paragraphes 61 à 65 apportent des modifications aux dispositions du règlement (UE) 2023/2854 (règlement sur les données) relatives au comité et au pouvoir de délégation, tandis que le paragraphe 66 apporte des modifications au règlement (UE) 2022/868 (règlement sur la gouvernance des données) nécessaires pour introduire dans le règlement (UE) 2023/2854 (règlement sur les données) les dispositions du règlement (UE) 2022/868 (acte sur la gouvernance des données) et de la directive (UE) 2019/1024 (directive sur les données ouvertes).

Le paragraphe 68 étend l'attention particulière accordée aux PME dans le cadre de l'évaluation aux petites entreprises à moyenne capitalisation tandis que le paragraphe 69 introduit l'évaluation des règles nouvellement insérées dans le règlement (UE) 2023/2854 (règlement sur les données).

L'**article 2** introduit les références pertinentes aux services d'intermédiation de données et à l'altruisme en matière de données dans l'annexe du règlement (UE) 2018/174 relative à la rubrique «Démarrage et gestion d'une entreprise, et cessation d'activité».

***Modifications apportées au règlement (UE) 2016/679, au règlement (UE) 2018/1725 et à la directive 2002/58/CE***

L'article 3 de la proposition vise à apporter des modifications ciblées au règlement (UE) 2016/679 («règlement général sur la protection des données»).

**À l'article 3:**

Le paragraphe 1 vise à clarifier la définition des données à caractère personnel figurant à l'article 4 du règlement (UE) 2016/679 (règlement général sur la protection des données) en indiquant que les informations ne doivent pas être considérées comme des données à caractère personnel pour une entité donnée lorsque celle-ci ne dispose pas de moyens pouvant raisonnablement être utilisés pour identifier la personne physique à laquelle les informations se rapportent. Par conséquent, une telle entité ne relèverait en principe pas dudit règlement.

Le paragraphe 2 prévoit deux dérogations supplémentaires au traitement de catégories particulières de données: il prévoit une dérogation à l'interdiction générale de traiter des données biométriques lorsque cela est nécessaire pour confirmer l'identité de la personne concernée et lorsque les données et les moyens permettant cette vérification sont sous le contrôle exclusif de cette personne. Il prévoit également une dérogation pour le traitement résiduel de catégories particulières de données à caractère personnel aux fins du développement et de l'exploitation d'un système d'IA ou d'un modèle d'IA, sous certaines conditions, y compris des mesures organisationnelles et techniques appropriées pour éviter la collecte de catégories particulières de données à caractère personnel ainsi que la suppression de ces données.

Le paragraphe 3 entend clarifier la situation visée à l'article 12 du règlement (UE) 2016/679 (règlement général sur la protection des données) lorsque le droit d'accès est utilisé de manière abusive par les personnes concernées à des fins autres que la protection de leurs

données à caractère personnel. En conséquence, le responsable du traitement pourrait refuser de donner suite à la demande ou exiger le paiement de frais raisonnables. En outre, il vise à clarifier les conditions permettant de démontrer qu'une demande d'accès était excessive.

Le paragraphe 4 porte essentiellement sur l'obligation du responsable du traitement d'informer les personnes concernées du traitement de leurs données à caractère personnel en vertu de l'article 13 du règlement (UE) 2016/679 (règlement général sur la protection des données) en supprimant cette obligation dans les situations où il existe des motifs raisonnables de supposer que la personne concernée dispose déjà des informations, à moins que le responsable du traitement ne transmette les données à d'autres destinataires ou catégories de destinataires, ne transfère les données vers un pays tiers, ne procède à une prise de décision automatisée ou que le traitement ne soit susceptible d'engendrer un risque élevé pour les droits de la personne concernée.

Le paragraphe 5 vise à clarifier les exigences relatives à la prise de décision individuelle automatisée au titre de l'article 22 du règlement (UE) 2016/679 (règlement général sur la protection des données), dans le cadre de la conclusion ou de l'exécution d'un contrat entre la personne concernée et un responsable du traitement, en particulier le fait que l'exigence de «nécessité» est indépendante de la question de savoir si la décision pourrait être prise autrement que par des moyens exclusivement automatisés.

Le paragraphe 6 vise à aligner l'obligation du responsable du traitement de notifier les violations de données à l'autorité de contrôle compétente en vertu de l'article 33 du règlement (UE) 2016/679 (règlement général sur la protection des données) sur l'obligation qui lui incombe d'informer les personnes concernées de ces violations en disposant que la notification n'est requise que si une violation de données est susceptible d'engendrer un risque élevé pour les droits de la personne concernée. Il prolongerait également le délai de notification à 96 heures. Il est également proposé que les responsables du traitement utilisent le guichet unique lorsqu'ils notifient des violations de données à l'autorité de contrôle. En outre, le comité européen de la protection des données serait tenu d'élaborer et de soumettre à la Commission une proposition de modèle commun pour les notifications de violations de données, que la Commission serait habilitée à adopter par voie d'acte d'exécution, après l'avoir révisée, le cas échéant.

Le paragraphe 7 vise à harmoniser les listes des activités de traitement qui nécessitent, ou qui ne nécessitent pas, une analyse d'impact relative à la protection des données en prévoyant qu'une liste unique des opérations de traitement qui nécessitent, ou qui ne nécessitent pas, une analyse d'impact relative à la protection des données soit fournie au niveau de l'Union, contribuant ainsi à l'harmonisation de la notion de risque élevé. Le comité européen de la protection des données serait tenu d'élaborer des propositions pour ces listes. Il serait également tenu d'élaborer des propositions de modèle commun et de méthodologie commune pour la réalisation d'analyses d'impact relatives à la protection des données, que la Commission serait habilitée à adopter par voie d'acte d'exécution, après les avoir révisées, le cas échéant.

Le paragraphe 8 dispose que la Commission peut aider, en collaboration avec le comité européen de la protection des données, les responsables du traitement à évaluer si les données résultant de la pseudonymisation ne constituent pas des données à caractère personnel en précisant les moyens et critères pertinents pour une telle évaluation, y compris l'état de la technique en ce qui concerne les techniques et critères disponibles pour évaluer le risque de réidentification.

Le paragraphe 12 réforme le régime juridique relatif au traitement des données à caractère personnel stockées sur des équipements terminaux ou émises à partir de ces équipements

(«dispositifs connectés»), lequel relève actuellement de la directive 2002/58/CE (directive «vie privée et communications électroniques»). Un nouvel article 88 *bis* est inséré dans le règlement (UE) 2016/679 (règlement général sur la protection des données), qui prévoit l'exigence de consentement pour le stockage de données à caractère personnel ou pour l'accès à des données déjà stockées sur les équipements terminaux des personnes physiques, et qui intègre dans les dispositions du règlement (UE) 2016/679 (règlement général sur la protection des données) le traitement de données à caractère personnel stockées sur les équipements terminaux ou émises à partir de ces équipements. Un nouvel article 88 *ter* est inséré dans le règlement (UE) 2016/679 (règlement général sur la protection des données) concernant les indications automatisées et lisibles par machine des choix individuels, ainsi que le respect de ces indications par les fournisseurs de sites web une fois que des normes seront disponibles.

**À l'article 4:**

L'article 4 de la proposition vise à introduire des modifications ciblées dans le règlement (UE) 2018/1725, afin d'aligner le texte dudit règlement sur les modifications apportées au règlement (UE) 2016/679 et introduites à l'article 3.

**À l'article 5:**

L'article 5 prévoit des modifications de la directive 2002/58/CE, à savoir la directive «vie privée et communications électroniques». L'article 4 de ladite directive est abrogé. Le texte ajouté à l'article 5, paragraphe 3, de ladite directive permet de transférer vers le règlement (UE) 2016/679 (règlement général sur la protection des données) les règles concernant le stockage de données à caractère personnel, ainsi que l'accès à des données à caractère personnel déjà stockées, sur l'équipement terminal d'une personne physique, par l'insertion d'un nouvel article 88 *bis* dans le règlement (UE) 2016/679 (règlement général sur la protection des données), comme décrit ci-dessus.

***guichet unique pour le signalement des incidents***

**À l'article 6**:

Les paragraphes 1 et 2 prévoient la création du guichet unique pour le signalement des incidents, en incluant des exigences particulières pour l'ENISA. En outre, il est établi que le signalement des incidents imposé par la directive SRI 2 devrait être effectué par l'intermédiaire du nouveau guichet unique.

**À l'article 7**: le guichet unique est également obligatoire pour le signalement des incidents au titre du règlement (UE) nº 910/2014 (règlement eIDAS).

**À l'article 8:** le guichet unique est également obligatoire aux fins du règlement (UE) 2022/2554 (DORA).

**À l'article 9**: le guichet unique est également obligatoire aux fins de la directive (UE) 2022/2557 (directive CER).

En outre, conformément à l'article 3, paragraphe 6, le signalement des incidents de violation de données doit transiter par le guichet unique également aux fins du règlement (UE) 2016/679 (règlement général sur la protection des données). Conformément à l'article 5, paragraphe 1, les exigences en matière de rapport prévues par la directive 2002/58/CE (directive «vie privée et communications électroniques») sont abrogées, étant donné qu'elles

sont obsolètes au regard des dispositions du règlement (UE) 2016/679 (règlement général sur la protection des données).

***Abrogations d'actes et dispositions finales***

**À l'article 10**:

Le paragraphe 1 abroge le règlement (UE) 2019/1150 (le règlement P2B), considéré comme présentant une pertinence résiduelle compte tenu des règles récentes qui couvrent dans une large mesure les mêmes questions. Par dérogation, le paragraphe 2 concerne toute référence croisée au règlement (UE) 2019/1150 (règlement P2B) dans d'autres instruments juridiques: ces dispositions resteront en vigueur jusqu'à ce qu'elles soient modifiées dans leurs actes initiaux, au plus tard le 31 décembre 2032, afin d'éviter toute insécurité juridique.

Le paragraphe 3 abroge les textes juridiques intégrés dans le règlement (UE) 2023/2854 (règlement sur les données).

**L'article 11** fixe les dispositions finales du règlement modificatif.

2025/0360 (COD)

Proposition de

# RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

## modifiant les règlements (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 et (UE) 2023/2854 ainsi que les directives 2002/58/CE, (UE) 2022/2555 et (UE) 2022/2557 en ce qui concerne la simplification du cadre législatif numérique, et abrogeant les règlements (UE) 2018/1807, (UE) 2019/1150 et (UE) 2022/868 ainsi que la directive (UE) 2019/1024 (règlement omnibus numérique)

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

vu le traité sur le fonctionnement de l'Union européenne, et notamment ses articles 16 et 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[21],

vu l'avis de la Banque centrale européenne[22],

vu l'avis du Comité des régions[23],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) Dans sa communication intitulée «Une Europe plus simple et plus rapide»[24], la Commission a annoncé son engagement en faveur d'un programme ambitieux visant à promouvoir des politiques innovantes et tournées vers l'avenir qui renforcent la compétitivité de l'Union et allègent radicalement la charge réglementaire pesant sur les citoyens, les entreprises et les administrations, tout en maintenant les normes les plus élevées aux fins de la promotion des valeurs de l'Union. Par conséquent, la Commission a privilégié la proposition visant à apporter des ajustements immédiats à la législation, y compris à la législation numérique, afin de relever le défi de la compétitivité de l'Union.

---

[21] JO C […], […], p. […].

[22] JO C […], […], p. […].

[23] JO C […], […], p. […].

[24] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Une Europe plus simple et plus rapide: communication sur la mise en œuvre et la simplification, COM(2025) 47 final, 11 février 2025.

(2) La législation de l'Union dans le domaine du numérique fixe des normes élevées au sein de l'Union et peut constituer une source puissante d'avantages concurrentiels pour les entreprises qui respectent les règles et qui peuvent ainsi afficher un niveau de qualité, de sécurité et de fiabilité de premier plan au niveau mondial. La réglementation numérique a défini clairement les règles du jeu dans l'Union pour les entreprises responsables, en garantissant l'équité et la transparence dans les relations interentreprises, en stimulant des modèles d'entreprise innovants et en fixant des normes élevées en matière de protection et de sécurité des consommateurs, ainsi que pour la protection des droits fondamentaux, notamment la protection de la vie privée et des données.

(3) La législation numérique de l'Union a évolué progressivement au cours des dernières années, non seulement en réponse à l'empreinte croissante des technologies numériques dans l'économie et la dynamique sociétale de l'Union, mais aussi pour relever les défis émergents et promouvoir les possibilités économiques au sein de l'Union. Nonobstant l'engagement de la Commission en faveur d'un «test de résistance» systématique des règles numériques et d'autres règles de l'Union, qui pourrait conduire à de nouveaux ajustements réglementaires, notamment à la suite du prochain bilan de qualité numérique, mais aussi d'autres évaluations ciblées des règles numériques, des modifications réglementaires immédiates sont nécessaires. Par conséquent, le présent règlement propose une première série de modifications du cadre législatif numérique, afin de fournir des clarifications réglementaires immédiates qui stimulent l'innovation sur le marché de l'Union et réduisent les coûts administratifs de mise en conformité, en particulier pour les entreprises, tout en rationalisant les coûts administratifs et de contrôle pour les autorités de contrôle et les organes consultatifs. Les modifications visent également à apporter de la clarté aux particuliers.

(4) Compte tenu du rôle fondamental des données pour la création de valeur dans l'économie numérique, et conformément aux objectifs de la communication relative à une stratégie pour une union européenne des données, les modifications du cadre législatif relatif aux données présentées dans le présent règlement visent à établir un cadre réglementaire cohérent et uniforme pour la mise à disposition et l'utilisation des données, en rationalisant et en consolidant le cadre réglementaire relatif aux données en deux actes juridiques seulement, à savoir les règlements (UE) 2016/679[25] et (UE) 2023/2854[26] du Parlement européen et du Conseil, au départ de cinq actes différents actuellement en vigueur. Les modifications visent à réduire les coûts administratifs inutiles et à stimuler la mise à disposition des données en tant que condition préalable pour soutenir des entreprises numériques compétitives dans l'Union, tout en maintenant les normes les plus élevées en matière de protection de la vie privée, de protection des données à caractère personnel et de pratiques commerciales équitables,

---

[25] 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)

[26] RÈGLEMENT (UE) 2023/2854 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données).

et en garantissant la poursuite d'objectifs réglementaires fondamentaux, dont le respect du droit de la concurrence de l'Union et des États membres.

(5) Compte tenu de l'évolution itérative des règles horizontales et sectorielles, il est indispensable de remédier également aux chevauchements observés dans certaines dispositions qui entraînent une duplication inutile des charges administratives. Tel est le cas des exigences figurant dans plusieurs règles relatives au signalement d'incidents de cybersécurité ou d'incidents connexes, pour lesquelles des solutions numériques, telles que proposées dans le présent règlement, peuvent apporter un allègement immédiat pour les entreprises de tous les secteurs concernés.

(6) De même, compte tenu de la réglementation itérative des plateformes en ligne au cours des dernières années, des règles plus récentes ont instauré un cadre plus clair et plus ambitieux que certaines des règles antérieures, rendant celles-ci obsolètes. Il est donc nécessaire que le cadre juridique évolue, en éliminant toute duplication inutile qui ajoute de la complexité juridique.

(7) Le règlement (UE) 2022/868 du Parlement européen et du Conseil[27] a établi des règles pour les fonctions intermédiaires dans trois contextes différents: a) les fonctions qui favorisent la réutilisation de données protégées détenues par des organismes du secteur public dans des conditions contrôlées; b) les services d'intermédiation de données qui facilitent le partage de données entre les personnes concernées, les détenteurs de données et les utilisateurs de données; et c) les organisations altruistes en matière de données qui soutiennent l'utilisation des données mises à disposition par les personnes concernées et les détenteurs de données sur une base altruiste ou philanthropique. Les fonctions favorisant la réutilisation des données protégées détenues par le secteur public sont étroitement liées aux règles énoncées dans la directive (UE) 2019/1024 du Parlement européen et du Conseil[28]. Leur interaction a été source de confusion, notamment au sein des organismes du secteur public. Il est donc nécessaire de fusionner les deux ensembles de règles. L'évaluation des règles relatives aux services d'intermédiation de données a montré que la définition des prestataires de services d'intermédiation de données présentait des faiblesses et que les règles étaient trop strictes pour permettre aux prestataires de services de trouver un modèle financier durable. Il est donc également nécessaire de rationaliser ce régime. En ce qui concerne l'altruisme en matière de données, certaines dispositions du règlement (UE) 2022/868, notamment l'obligation pour les États membres de mettre en place des politiques nationales relatives à l'altruisme en matière de données, l'établissement d'un «recueil de règles» et l'élaboration d'un formulaire européen de consentement à l'altruisme en matière de données, semblent inutiles, eu égard également aux travaux en cours du comité européen de la protection des données visé à l'article 68 du règlement (UE)

---

[27] Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) (JO L 152 du 3.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/868/oj).

[28] Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (JO L 172 du 26.6.2019, p. 56, ELI: http://data.europa.eu/eli/dir/2019/1024/oj).

2016/679 du Parlement européen et du Conseil[29] portant sur les orientations relatives au traitement des données à caractère personnel dans le contexte de la recherche scientifique.

(8) Alors que l'importance des services d'intermédiation de données est reconnue dans le cadre de nombreuses initiatives visant à promouvoir le partage de données et la collaboration, il y a lieu de clarifier les règles fixées dans le règlement (UE) 2022/868 concernant les prestataires de services d'intermédiation de données. En particulier, la définition de ces prestataires devrait être plus précise. Elle devrait supprimer les éléments constituant simplement des exemples illustratifs, plutôt que des exceptions. En outre, la définition devrait permettre de remédier aux lacunes résultant de formulations ambiguës, notamment en ce qui concerne la notion de «groupe fermé». Les services ne devraient pas pouvoir être enregistrés en tant que services d'intermédiation de données lorsqu'ils sont exclusivement utilisés par un groupe fermé d'entreprises et que toute extension de ce groupe d'entreprises ne peut être décidée que par ce groupe et non par le prestataire de services. Plus important encore, le fait de soumettre ce marché émergent à un régime obligatoire a engendré des coûts de mise en conformité inutiles. À ce stade du développement du marché, un régime volontaire, permettant aux acteurs neutres de se distinguer des autres acteurs, semble suffisant. En outre, afin de permettre des modèles d'entreprise durables, il convient d'assouplir le régime en supprimant l'exigence d'une séparation juridique entre les services d'intermédiation de données et les autres services à valeur ajoutée qu'un service devrait être autorisé à offrir, pour la remplacer par une séparation fonctionnelle tout en conservant certaines garanties. Le régime de contrôle administratif devrait être simplifié. Au lieu d'un registre public national et d'un registre public de l'Union pour les prestataires de services d'intermédiation de données et les organisations altruistes en matière de données, il ne devrait y avoir que des registres publics de l'Union, à savoir un registre pour les prestataires de services d'intermédiation de données et un registre pour les organisations altruistes en matière de données. Les autorités compétentes chargées de superviser l'attribution du label et le respect, par les entités, des conditions préalables à son obtention devraient être indépendantes dans l'exécution de cette tâche. En d'autres termes, ces autorités devraient être juridiquement et fonctionnellement indépendantes d'un service d'intermédiation de données ou d'une organisation altruiste en matière de données, y compris au niveau de leur encadrement supérieur. Les organisations gouvernementales devraient avoir la possibilité de soutenir financièrement les services d'intermédiation de données ou les organisations altruistes en matière de données, compte tenu notamment de la nature émergente de ces entités, pour autant qu'il s'agisse d'entités juridiquement distinctes. Afin de garantir que les entités reconnues soient facilement identifiables dans l'ensemble de l'Union, la Commission a établi le règlement d'exécution (UE) 2023/1622 relatif à la conception de logos communs permettant d'identifier les

[29] 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

prestataires de services d'intermédiation de données et les organisations altruistes en matière de données reconnus dans l'Union.

(9) Le règlement (UE) 2023/2854 supprime les obstacles à l'accès aux données et à leur utilisation, stimule l'innovation et la compétitivité fondées sur les données et préserve les incitations à investir dans les technologies des données.

(10) Le chapitre II du règlement (UE) 2023/2854 impose aux détenteurs de données de mettre des données, y compris des données protégées en tant que secrets d'affaires, à la disposition des utilisateurs et des tiers de leur choix, à condition que les mesures de confidentialité établies par le détenteur de données soient maintenues. Cette exigence de préservation de la confidentialité complète la directive (UE) 2016/943 du Parlement européen et du Conseil[30], qui fixe la norme en matière de protection des secrets d'affaires au sein de l'Union. Toutefois, la divulgation de secrets d'affaires à des entités de pays tiers peut accroître les risques pour leur intégrité et leur confidentialité en cas d'exposition à des juridictions présentant des mesures de protection insuffisantes ou des difficultés dans leur mise en œuvre effective, ce qui peut entraîner une utilisation non autorisée, des dommages économiques et une insécurité juridique.

(11) Il est nécessaire de renforcer le règlement (UE) 2023/2854 par l'introduction d'un motif supplémentaire permettant aux détenteurs de données de refuser la divulgation de secrets d'affaires, en complétant les dispositions existantes autorisant le refus dès lors que le détenteur de données peut démontrer une forte probabilité de préjudice économique grave. En vertu de la nouvelle disposition, les détenteurs de données peuvent refuser de divulguer des secrets d'affaires s'ils démontrent un risque élevé d'obtention et d'utilisation illicites ou un risque élevé de divulgation illicite à des entités soumises à des régimes de protection insuffisants ou à des cadres juridiques non équivalents ou plus faibles que les règles en vigueur dans l'Union. La nouvelle disposition couvre également les cas dans lesquels le cadre juridique du pays tiers est, en théorie, solide ou va au-delà des règles de l'Union, mais ne fait pas l'objet d'une application appropriée dans la pratique. Ces risques mettent en évidence la possibilité que des secrets d'affaires puissent être obtenus, utilisés ou divulgués en violation du droit de l'Union, menaçant ainsi l'intégrité et la confidentialité de ces secrets d'affaires.

(12) L'activation du mécanisme de refus devrait demeurer volontaire, et la démonstration ne devrait avoir lieu qu'après son activation. Comme condition préalable pour pouvoir justifier leur refus de partager des données ou de divulguer des secrets d'affaires, les détenteurs de données ne devraient pas être tenus de procéder à une analyse ou à une démonstration complètes du niveau de protection des secrets d'affaires garanti dans des pays tiers ou offert par une entité d'un pays tiers. Lors de leur démonstration, les détenteurs de données peuvent prendre en considération divers facteurs, tels que des normes juridiques insuffisantes ou inadéquates, une application insuffisante ou arbitraire, des cas de violation antérieurs, des obligations de divulgation étrangères contraires au droit de l'Union, des voies de recours juridique limitées pour les entités

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

de l'Union, l'utilisation stratégique abusive de tactiques procédurales visant à porter atteinte à des concurrents, ou l'exercice d'une influence politique indue. Compte tenu de la diversité des entités, des pays tiers et des scénarios de partage de données concernés, les détenteurs de données devraient axer leur évaluation et leur démonstration sur les risques pertinents et agir en conséquence, y compris en établissant des garanties appropriées ou en activant le mécanisme de refus. Les refus devraient être clairs, proportionnés et adaptés aux circonstances spécifiques de chaque cas, plutôt qu'être appliqués de manière systématique ou généralisée à l'ensemble d'un pays tiers.

(13) Une protection insuffisante des secrets d'affaires ou des difficultés pour les faire valoir dans les pays tiers peuvent causer un préjudice irréparable aux entreprises européennes. L'objectif est donc de renforcer les garanties applicables aux secrets d'affaires en empêchant leur fuite vers des personnes physiques ou morales qui sont établies dans des juridictions présentant de tels risques ou qui relèvent de telles juridictions. Cela inclut les entités établies dans l'Union contrôlées par des entités de pays tiers, qui peuvent agir de mauvaise foi ou servir de façade pour des entités de pays tiers. En outre, l'objectif est d'éviter une exposition directe à des entités de pays tiers opérant au sein de l'Union, qui relèvent de ces juridictions. Le fait de relever de la juridiction d'un pays tiers signifie que la personne physique ou morale est légalement régie, contrôlée ou liée d'une autre manière par la législation ou l'autorité réglementaire d'un pays tiers. Les filiales ou sociétés apparentées de sociétés mères établies dans un pays tiers peuvent exploiter ces compétences juridictionnelles pour se soustraire à la législation de l'Union ou la contourner. Le contrôle direct ou indirect désigne la capacité d'exercer une influence déterminante ou dominante sur la gestion ou les décisions stratégiques d'une autre entité, que ce soit par la propriété du capital ou les droits de vote, ou par le biais d'une participation financière, d'accords contractuels ou d'entités intermédiaires. Le contrôle peut être exercé directement ou par d'autres moyens, même sans participation majoritaire. Les détenteurs de données devraient tout mettre en œuvre pour obtenir les informations pertinentes, comme par exemple effectuer des recherches dans les registres publics ou adresser une demande directement à l'utilisateur ou à un tiers, tout en veillant à ne pas être indûment intrusifs.

(14) Il est essentiel de protéger les secrets d'affaires contre ces vulnérabilités afin de permettre aux industries européennes de maintenir leur position sur le marché et leur avantage concurrentiel. Si les détenteurs de données peuvent exercer un pouvoir discrétionnaire dans la protection de leurs secrets d'affaires, le refus de partager des données devrait être limité à des circonstances exceptionnelles justifiées, afin de préserver les objectifs du règlement (UE) 2023/2854 consistant à favoriser l'innovation fondée sur les données ainsi qu'une économie numérique prospère dans l'Union. Des garanties contre l'utilisation abusive du mécanisme de refus devraient rester en place, y compris l'obligation pour le détenteur de données de démontrer de manière dûment étayée que la divulgation présente un risque élevé et d'en informer les autorités compétentes. Les éléments de cette démonstration devraient être fournis par écrit sans retard injustifié à l'utilisateur ou au tiers et être proportionnés au cas d'espèce. Toutes les parties concernées devraient garantir le traitement confidentiel de la décision et de la démonstration afin de préserver le caractère confidentiel des secrets d'affaires concernés. Les utilisateurs et les tiers, selon le cas, peuvent contester la décision du détenteur de données auprès de l'autorité compétente, en justice ou par l'intermédiaire d'organes de règlement des litiges.

(15) Afin de simplifier le cadre de partage de données entre les entreprises et les administrations publiques prévu par le règlement (UE) 2023/2854 et de clarifier les ambiguïtés qui imposaient précédemment des obligations plus larges aux entreprises, il est nécessaire de restreindre le champ d'application du chapitre V dudit règlement en remplaçant le «besoin exceptionnel» par les «situations d'urgence». La notion de «situation d'urgence», qui est définie à l'article 2, point 29), du règlement (UE) 2023/2854, garantit ainsi que les obligations énoncées dans ce chapitre ne sont invoquées que dans des situations d'urgence bien définies, réduisant de la sorte les difficultés techniques, administratives et juridiques auxquelles les entreprises étaient confrontées dans le cadre du régime précédent. Cela garantit que les demandes de données sont pertinentes et proportionnées pour réagir aux situations d'urgence, pour les atténuer ou pour se rétablir à la suite d'une situation d'urgence. Étant donné que le cadre actualisé de l'Union relatif aux statistiques européennes au titre du règlement (CE) nº 223/2009 du Parlement européen et du Conseil[31] ne couvre pas les situations d'urgence, il est essentiel de préserver le rôle des statistiques officielles dans le cadre du chapitre V du règlement (UE) 2023/2854 afin de garantir la clarté et l'efficacité dans de telles situations. Il est également nécessaire de clarifier le régime de compensation pour les situations dans lesquelles les microentreprises et les petites entreprises sont tenues de fournir des données afin de faire face à une situation d'urgence, cas dans lesquels ces entreprises sont autorisées à demander une compensation.

(16) Afin d'atténuer les incertitudes juridiques qui pourraient décourager des modèles d'entreprise innovants, il est nécessaire de remédier aux ambiguïtés et aux charges importantes en matière de conformité associées aux dispositions relatives aux contrats intelligents exécutant des accords de partage de données au titre de l'article 36 du règlement (UE) 2023/2854. L'absence de normes harmonisées et de définitions claires pour des concepts clés tels que la «robustesse», le «contrôle d'accès» et la «cohérence avec les dispositions contractuelles», conjuguée à l'exigence d'un «mécanisme de résiliation ou d'interruption en toute sécurité» potentiellement incompatible avec des architectures de chaînes de blocs décentralisées ou publiques reposant sur des registres immuables, a posé des difficultés aux innovateurs du point de vue des coûts et des opportunités. En outre, l'ambiguïté entourant la réalisation de l'évaluation de la conformité au titre de l'article 36, paragraphe 2, dudit règlement risque d'imposer des charges disproportionnées. La suppression de l'article 36 du règlement (UE) 2023/2854 encouragerait donc le développement et l'introduction sur le marché de nouveaux modèles d'entreprise, favoriserait l'innovation et réduirait les obstacles pour les technologies émergentes.

(17) Certains services de traitement de données, qui ne relèvent pas du modèle de fourniture de l'infrastructure à la demande (IaaS), sont conçus sur mesure en fonction

---

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

des besoins ou de l'écosystème d'un client. La fourniture de ces services de traitement de données repose sur des négociations précontractuelles et contractuelles chronophages visant à déterminer les exigences spécifiques du client ainsi que les efforts techniques ultérieurs nécessaires pour personnaliser le service de traitement de données et fournir une solution sur mesure. Il ne s'agit pas de services «prêts à l'emploi» mais de services personnalisés en fonction des besoins d'un client afin de fournir une solution sur mesure dans le cadre de laquelle la majorité des caractéristiques et fonctionnalités du service de traitement de données ont été adaptées par le fournisseur en fonction des besoins spécifiques du client et dans le cadre de laquelle la majorité des caractéristiques et fonctionnalités ne seraient pas utilisables pour le client sans une adaptation préalable par le fournisseur. Ces services se distinguent des services de traitement de données conçus sur mesure visés à l'article 31, paragraphe 1, du règlement (UE) 2023/2854. Les services de traitement de données conçus sur mesure sont des services dont la majorité des caractéristiques principales ont été conçues sur mesure pour répondre aux besoins spécifiques d'un client particulier, ou des services qui ne sont pas proposés à grande échelle sur le plan commercial par l'intermédiaire du catalogue de services du fournisseur. Afin d'éviter des coûts et une charge administrative supplémentaires liés à la nécessité de rouvrir et de renégocier les contrats conclus au plus tard le 12 septembre 2025, il est nécessaire de préciser qu'à l'exception de l'obligation de réduire et, à terme, de supprimer les frais de changement de fournisseur et de transfert, les services conçus sur mesure fournis conformément aux contrats conclus au plus tard le 12 septembre 2025 ne devraient pas relever du chapitre VI du règlement (UE) 2023/2854.

(18) Pour des motifs liés à la planification financière et à l'attraction des investissements, les fournisseurs de services de traitement de données, en particulier les PME et les petites entreprises à moyenne capitalisation, peuvent privilégier et proposer des contrats à durée déterminée. Il est nécessaire de préciser que les fournisseurs de services de traitement de données peuvent inclure dans ces contrats des clauses relatives à des sanctions proportionnées en cas de résiliation anticipée, pour autant qu'elles ne constituent pas un obstacle au changement de fournisseur. En outre, les fournisseurs de services de traitement de données qui sont des PME ou des petites entreprises à moyenne capitalisation sont particulièrement pénalisés par la nécessité d'aligner sur le règlement (UE) 2023/2854 les contrats existants de fourniture de services de traitement de données. Il est donc indispensable d'établir un régime spécifique pour ces fournisseurs s'ils proposent des services de traitement de données ne relevant pas de l'IaaS, sur la base de contrats conclus au plus tard le 12 septembre 2025. Compte tenu de l'objectif du règlement (UE) 2023/2854 consistant à permettre le changement de services de traitement de données et étant donné que les frais de changement de fournisseur, y compris les frais de transfert, constituent un obstacle sérieux au changement de fournisseur, les nouveaux régimes allégés pour les services de traitement de données qui sont conçus sur mesure ou fournis par des PME ou des petites entreprises à moyenne capitalisation ne devraient pas compromettre la suppression progressive de ces frais. Les dispositions contractuelles allant à l'encontre de cet objectif devraient être considérées comme n'ayant jamais existé, dès lors

qu'elles sont incluses dans des accords contractuels relatifs à la prestation de services relevant de ces deux nouveaux régimes spécifiques.

(19) Le règlement (UE) 2018/1807 du Parlement européen et du Conseil[32] a introduit un principe essentiel pour le soutien d'une économie fondée sur les données au sein de l'Union, qui sous-tend concrètement la liberté d'établissement et la libre prestation de services. Le «libre flux des données» dans l'Union, clarifié par l'interdiction d'imposer la localisation des données, demeure un principe fondamental qui apporte une sécurité juridique aux entreprises et qui devrait donc être conservé dans le règlement (UE) 2023/2854. Cette disposition n'affecte pas le traitement des données dès lors que celui-ci est effectué dans le cadre d'une activité qui ne relève pas du droit de l'Union, notamment aux fins de la sécurité nationale, conformément à l'article 4 du traité sur l'Union européenne. Dans le même temps, d'autres dispositions du règlement (UE) 2018/1807 sont remplacées par des règles plus récentes. En particulier, le chapitre VI du règlement (UE) 2023/2854 a introduit un cadre juridique horizontal moderne qui englobe le changement de services de traitement de données et a rendu l'article 6 du règlement (UE) 2018/1807 de fait obsolète. La coexistence de ces dispositions a accru la complexité juridique pour les entreprises. Il convient dès lors d'abroger le règlement (UE) 2018/1807.

(20) 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.

(21) Tant la directive (UE) 2019/1024 que le chapitre II du règlement (UE) 2022/868 régissent la réutilisation des informations du secteur public à des fins d'innovation. L'interaction entre les deux ensembles de règles a créé une insécurité juridique, principalement pour les organismes du secteur public. Un alignement des règles au sein d'un seul instrument juridique est donc nécessaire pour accroître la cohérence et la sécurité juridiques.

(22) Étant donné que tant la directive (UE) 2019/1024 que le règlement (UE) 2022/868 ont en commun l'objectif de renforcer la réutilisation des informations du secteur public, et afin de simplifier les règles tant du point de vue des organismes du secteur public que des réutilisateurs des informations du secteur public, il est rationnel d'abroger la

---

[32] Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne (JO L 303 du 28.11.2018, p. 59), ELI: http://data.europa.eu/eli/reg/2018/1807/oj).

directive (UE) 2019/1024 et le règlement (UE) 2022/868, d'aligner les deux régimes et de consolider les règles dans un chapitre unique relevant du présent règlement. Cette solution renforcera l'harmonisation de ces règles dans l'ensemble de l'Union, réduira la charge administrative liée à l'interprétation et à la mise en œuvre de la législation nationale, et permettra aux entreprises de développer plus facilement des services et des produits par-delà les frontières. Lors de la désignation des organismes compétents, les États membres devraient veiller à ce que, même lorsque des organismes compétents sectoriels sont désignés, tous les secteurs concernés soient couverts à terme. Il convient d'interpréter les modifications apportées au présent règlement de manière à ne pas modifier l'interprétation des différentes définitions et des différents termes, sauf indication contraire.

(23) Les données et documents qui peuvent être mis à la disposition du public en vue de leur réutilisation, ainsi que les données et documents qui sont protégés pour des motifs de confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise, de secret statistique, de protection des droits de propriété intellectuelle de tiers ou de protection des données à caractère personnel, sont souvent détenus par les mêmes organismes du secteur public. Par conséquent, il est nécessaire d'harmoniser les définitions et les principes communs qui s'appliquent à l'ensemble des informations du secteur public et de prendre en considération les questions portant sur l'interaction entre les deux ensembles de règles.

(24) Il y a lieu de rationaliser les règles existantes pour plus de clarté et de cohérence. Néanmoins, les deux régimes de réutilisation devraient rester distincts et leur champ d'application respectif devrait continuer de dépendre des caractéristiques des données ou des documents et du contexte de leur réutilisation. Les organismes du secteur public devraient, dans la mesure du possible, adopter le régime applicable aux données ouvertes. Ce n'est que lorsqu'ils établissent que des données ou un document contiennent des informations correspondant à certaines catégories de données protégées qu'ils devraient limiter leur mise à la disposition du public et envisager de les rendre disponibles en vue de leur réutilisation en tant que données protégées.

(25) Les start-up, les petites entreprises et les entreprises qui sont qualifiées d'entreprises moyennes au titre de l'article 2 de l'annexe de la recommandation 2003/361/CE[33] de la Commission, ainsi que les entreprises de secteurs dont les capacités numériques sont moins développées éprouvent des difficultés face à la réutilisation des données et des documents. Dans le même temps, quelques très grandes entités ont vu le jour, lesquelles disposent d'une puissance économique considérable dans l'économie numérique grâce à l'accumulation et à l'agrégation de volumes importants de données ainsi qu'à l'infrastructure technologique nécessaire à leur monétisation. Ces très grandes entités comprennent des entreprises qui fournissent des services de plateforme essentiels, sont désignées comme contrôleurs d'accès en vertu du règlement (UE) 2022/1925 du Parlement européen et du Conseil[34] et sont soumises à des obligations

---

[33] Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

[34] Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives

spéciales pour remédier aux déséquilibres. Pour remédier à ces déséquilibres et renforcer la concurrence et l'innovation, les organismes du secteur public devraient pouvoir introduire des conditions particulières dans les licences relatives à la réutilisation de données et de documents par les très grandes entreprises. Toute condition de ce type devrait être proportionnée et fondée sur des critères objectifs, en tenant compte de la puissance économique, de la capacité de l'entité à acquérir des données ou de sa désignation en tant que contrôleur d'accès au titre du règlement (UE) 2022/1925, ainsi que d'autres critères de cette nature, le cas échéant. Ces conditions particulières peuvent porter, entre autres, sur les droits et redevances ou sur les finalités de la réutilisation.

(26) Dans le souci de favoriser l'innovation et de maintenir une concurrence loyale sur le marché numérique de l'Union, il est impératif de veiller à ce que l'accès aux données du secteur public et leur réutilisation profitent à un large éventail d'acteurs du marché et ne renforcent pas involontairement des positions dominantes existantes. Les très grandes entreprises, et en particulier les entreprises désignées comme contrôleurs d'accès en vertu du règlement (UE) 2022/1925, exercent un pouvoir et une influence considérables sur le marché intérieur. Afin d'empêcher ces entités de tirer parti de leurs moyens substantiels au détriment d'une concurrence loyale et de l'innovation, les organismes du secteur public devraient pouvoir fixer des droits et redevances plus élevés pour la réutilisation de données ouvertes du service public ou de données protégées. Ces droits et redevances plus élevés devraient être proportionnés et fondés sur des critères objectifs, en tenant compte de la puissance économique et de la capacité de l'entité à acquérir des données. Cette mesure vise à préserver les possibilités pour les petites entreprises et les nouveaux arrivants sur le marché d'innover et d'être compétitifs dans l'économie numérique.

(27) Le présent règlement propose une série de modifications ciblées du règlement (UE) 2016/679 à des fins de clarification et de simplification, tout en préservant le même niveau de protection des données. Selon l'article 4 du règlement (UE) 2016/679, on entend par données à caractère personnel toute information se rapportant à une personne physique identifiée ou identifiable. Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés pour identifier la personne physique directement ou indirectement. Eu égard à la jurisprudence de la Cour de justice de l'Union européenne concernant la définition des données à caractère personnel, il est nécessaire de préciser davantage à quel moment une personne physique devrait être considérée comme identifiable. L'existence d'informations supplémentaires permettant d'identifier la personne concernée ne signifie pas, en soi, que les données pseudonymisées doivent être considérées comme constituant, dans tous les cas et pour chaque personne ou entité, des données à caractère personnel aux fins de l'application du règlement (UE) 2016/679. En particulier, il convient de préciser que les informations ne doivent pas être considérées comme des données à caractère personnel pour une entité donnée lorsque cette entité ne dispose pas de

---

(UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques) (JO L 265 du 12.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).

moyens raisonnablement susceptibles d'être utilisés pour identifier la personne physique à laquelle les informations se rapportent. Une éventuelle transmission ultérieure de ces informations à des tiers qui disposent de moyens leur permettant raisonnablement d'identifier la personne physique à laquelle les informations se rapportent, tels que le recoupement avec d'autres données à leur disposition, ne transforme ces informations en données à caractère personnel que pour les tiers qui disposent de tels moyens. Une entité pour laquelle les informations ne constituent pas des données à caractère personnel ne relève pas, en principe, du règlement (UE) 2016/679. À cet égard, la Cour de justice de l'Union européenne a jugé qu'un moyen d'identification de la personne concernée n'est pas raisonnablement susceptible d'être utilisé lorsque le risque d'identification apparaît en réalité insignifiant, en ce sens que l'identification de cette personne est interdite par la loi ou impossible dans la pratique, par exemple parce qu'elle impliquerait un effort disproportionné en termes de temps, de coût et de main-d'œuvre. Un exemple d'interdiction de réidentification figure dans les obligations imposées aux utilisateurs de données de santé et énoncées à l'article 61, paragraphe 3, du règlement (UE) 2025/327 du Parlement européen et du Conseil[35]. La Commission, en collaboration avec le comité européen de la protection des données, devrait aider les responsables du traitement à appliquer cette définition actualisée en fixant des critères techniques dans un acte d'exécution.

(28) Afin de déterminer si la recherche remplit les conditions caractérisant la recherche scientifique aux fins du présent règlement, il peut être tenu compte d'éléments tels que l'approche méthodologique et systématique appliquée lors de la réalisation de la recherche dans le domaine concerné. La recherche et le développement technologique devraient être menés dans des milieux universitaires, industriels ou autres, y compris au sein de petites et moyennes entreprises (article 179, paragraphe 2, du TFUE), être toujours de haute qualité et respecter les principes de fiabilité, d'honnêteté, de respect et de responsabilité (vérifiabilité).

(29) Il convient de rappeler que le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques devrait être considéré comme une opération de traitement licite compatible. En pareils cas, il n'est pas nécessaire de déterminer, sur la base de l'article 6, paragraphe 4, du règlement (UE) 2016/679, si la finalité du traitement ultérieur est compatible avec la finalité pour laquelle les données à caractère personnel sont initialement collectées.

(30) Une IA digne de confiance est essentielle pour assurer la croissance économique et soutenir l'innovation avec des résultats socialement bénéfiques. Le développement et l'utilisation des systèmes d'IA et des modèles sous-jacents, tels que les grands modèles de langage et les modèles de vidéo générative, reposent sur des données, y compris des données à caractère personnel, qui sont utilisées à différentes phases du cycle de vie de l'IA, telles que les phases d'entraînement, d'essai et de validation, et qui peuvent, dans certains cas, être conservées dans le système d'IA ou le modèle

---

[35] Règlement (UE) 2025/327 du Parlement européen et du Conseil du 11 février 2025 relatif à l'espace européen des données de santé et modifiant la directive 2011/24/UE et le règlement (UE) 2024/2847 (JO L, 2025/327, 5.3.2025, ELI: http://data.europa.eu/eli/reg/2025/327/oj).

d'IA. Le traitement des données à caractère personnel dans ce contexte peut donc, le cas échéant, être effectué aux fins d'un intérêt légitime au sens de l'article 6 du règlement (UE) 2016/679. Cela n'affecte pas l'obligation du responsable du traitement de veiller à ce que le développement ou l'utilisation (déploiement) de l'IA dans un contexte spécifique ou à des fins spécifiques soit conforme à d'autres dispositions du droit de l'Union ou du droit national, ou de veiller à la mise en conformité lorsque son utilisation est explicitement interdite par la loi. Cela n'affecte pas non plus l'obligation qui lui incombe de veiller à ce que toutes les autres conditions de l'article 6, paragraphe 1, point f), du règlement (UE) 2016/679, ainsi que toutes les autres exigences et tous les autres principes dudit règlement, soient respectés.

(31) Lorsque le responsable du traitement, à la lumière de l'approche fondée sur les risques qui sous-tend l'évolutivité des obligations au titre du présent règlement, met en balance l'intérêt légitime poursuivi par le responsable du traitement ou un tiers et les intérêts, droits et libertés de la personne concernée, il convient d'examiner si l'intérêt poursuivi par le responsable du traitement est bénéfique pour la personne concernée et la société dans son ensemble, ce qui peut par exemple être le cas lorsque le traitement de données à caractère personnel est nécessaire pour détecter et éliminer des préjugés, protégeant ainsi les personnes concernées contre la discrimination, ou lorsque le traitement de données à caractère personnel vise à garantir des résultats précis et sûrs en vue d'une utilisation bénéfique, par exemple pour améliorer l'accessibilité à certains services. Il convient également de tenir compte, entre autres, des attentes raisonnables de la personne concernée fondées sur sa relation avec le responsable du traitement, des garanties appropriées prévues pour réduire au minimum l'incidence sur les droits des personnes concernées, telles que le renforcement de la transparence pour les personnes concernées, l'octroi d'un droit inconditionnel de s'opposer au traitement de leurs données à caractère personnel, le respect des indications techniques intégrées dans un service limitant l'utilisation de données à des fins de développement de l'IA par des tiers, l'utilisation d'autres techniques de pointe de préservation de la vie privée pour l'entraînement de l'IA, ou encore des mesures techniques appropriées permettant de réduire réellement au minimum les risques résultant, par exemple, de la régurgitation, de la fuite de données et d'autres actions prévues ou prévisibles.

(32) Le traitement des données à caractère personnel à des fins de recherche scientifique ainsi que l'application des dispositions du RGPD relatives à la recherche scientifique sont subordonnés à l'adoption de garanties appropriées pour les droits et libertés des personnes concernées, conformément à l'article 89, paragraphe 1, du RGPD. À cette fin, le RGPD met en balance le droit à la protection des données à caractère personnel, conformément à l'article 8 de la Charte, et la liberté des sciences, conformément à l'article 13 de la Charte. Le traitement de données à caractère personnel à des fins de recherche scientifique poursuit donc un intérêt légitime au sens de l'article 6, paragraphe 1, point f), du règlement (UE) 2016/679, pour autant que cette recherche ne soit pas contraire au droit de l'Union ou au droit des États membres. Cela est sans préjudice de l'obligation du responsable du traitement de veiller à ce que toutes les autres conditions de l'article 6, paragraphe 1, point f), du règlement (UE) 2016/679 ainsi que toutes les autres exigences et tous les autres principes dudit règlement soient respectés.

(33) Le développement de certains systèmes d'IA et modèles d'IA peut impliquer la collecte de grandes quantités de données, y compris de données à caractère personnel et de catégories particulières de données. Des catégories particulières de données à caractère personnel peuvent être présentes de manière résiduelle dans les jeux de

données d'entraînement, d'essai ou de validation ou être conservées dans le système d'IA ou le modèle d'IA, bien que ces catégories particulières de données à caractère personnel ne soient pas nécessaires aux fins du traitement. Afin de ne pas entraver de manière disproportionnée le développement et le fonctionnement de l'IA et compte tenu des capacités du responsable du traitement à identifier et à supprimer des catégories particulières de données à caractère personnel, il convient d'autoriser une dérogation à l'interdiction de traiter des catégories particulières de données à caractère personnel prévue à l'article 9, paragraphe 2, du règlement (UE) 2016/679. La dérogation ne devrait s'appliquer que lorsque le responsable du traitement a mis en œuvre des mesures techniques et organisationnelles appropriées de manière efficace pour éviter le traitement de ces données, qu'il prend les mesures appropriées tout au long du cycle de vie d'un système d'IA ou d'un modèle d'IA et qu'il supprime effectivement ces données une fois qu'il les a identifiées. Si la suppression devait exiger des efforts disproportionnés, notamment lorsque la suppression de catégories particulières de données mémorisées dans le système d'IA ou le modèle d'IA nécessiterait une réorganisation du système d'IA ou du modèle d'IA, le responsable du traitement devrait protéger efficacement ces données afin qu'elles ne soient pas utilisées pour la déduction de sorties, ne soient pas divulguées ou ne soient pas mises à la disposition de tiers d'une autre manière. Cette dérogation ne devrait pas s'appliquer lorsque le traitement de catégories particulières de données à caractère personnel est nécessaire aux fins du traitement. Dans ce cas, le responsable du traitement devrait se fonder sur les dérogations prévues à l'article 9, paragraphe 2, points a) à j), du règlement (UE) 2016/679.

(34) Les données biométriques, telles que définies à l'article 4, point 14), du règlement (UE) 2016/679, désignent le traitement de certaines caractéristiques d'une personne physique par un moyen technique spécifique, qui permet ou confirme l'identification unique de cette personne. La notion de données biométriques comprend deux fonctions distinctes, à savoir l'identification d'une personne physique ou la vérification (également appelée authentification) de son identité déclarée, qui reposent toutes deux sur des processus techniques différents. Le processus d'identification repose sur une recherche des données biométriques de la personne concernée dans une base de données par comparaison de plusieurs échantillons, tandis que le processus de vérification compare avec un échantillon unique les données biométriques fournies par la personne concernée, laquelle déclare ainsi son identité. La dérogation à l'interdiction de traiter des données biométriques prévue à l'article 9, paragraphe 1, du RGPD devrait également être autorisée lorsque la vérification de l'identité déclarée de la personne concernée est nécessaire à une finalité poursuivie par le responsable du traitement, et que des garanties appropriées s'appliquent pour permettre à la personne concernée d'avoir le contrôle exclusif du processus de vérification. Par exemple, lorsque les données biométriques sont stockées de manière sécurisée uniquement du côté de la personne concernée ou sont stockées de manière sécurisée du côté du responsable du traitement sous une forme cryptée à la pointe de la technologie et que la clé de cryptage ou des moyens équivalents sont détenus uniquement par la personne concernée, ce traitement n'est pas susceptible de créer des risques importants pour les libertés et droits fondamentaux de la personne concernée. Le responsable du traitement n'a pas connaissance des données biométriques ou n'en prend connaissance que pendant une période très limitée au cours du processus de vérification.

(35) L'article 15 du règlement (UE) 2016/679 prévoit que la personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès

auxdites données ainsi qu'à certaines informations. Le droit d'accès devrait permettre à la personne concernée de connaître et de vérifier la licéité du traitement et lui permettre d'exercer ses autres droits au titre du règlement (UE) 2016/679. En revanche, il convient de préciser à l'article 12 du règlement que le droit d'accès, qui est d'emblée octroyé en faveur des personnes concernées, ne devrait pas être exercé de manière abusive en ce sens que les personnes concernées l'utilisent de manière abusive à des fins autres que la protection de leurs données. Par exemple, un tel abus du droit d'accès se produirait lorsque la personne concernée a l'intention d'amener le responsable du traitement à rejeter une demande d'accès, afin d'exiger ultérieurement le paiement d'une indemnisation, éventuellement sous la menace d'introduire une demande de dommages et intérêts. Parmi les autres exemples d'abus figurent les situations dans lesquelles les personnes concernées font un usage excessif du droit d'accès dans la seule intention de causer un dommage ou un préjudice au responsable du traitement ou lorsqu'une personne présente une demande, mais propose en même temps de la retirer en échange d'une forme quelconque d'avantage de la part du responsable du traitement. En outre, afin que la charge des responsables du traitement soit maintenue dans des limites raisonnables, ceux-ci devraient supporter une charge de la preuve moins lourde en ce qui concerne le caractère excessif d'une demande qu'en ce qui concerne le caractère manifestement infondé d'une demande. La raison en est que le caractère manifestement infondé d'une demande dépend de faits qui relèvent principalement de la sphère de responsabilité du responsable du traitement, tandis que le caractère excessif d'une demande concerne le comportement potentiellement abusif d'une personne concernée, qui se situe principalement en dehors de la sphère d'influence du responsable du traitement, de sorte que ce dernier ne sera en mesure de prouver un tel abus que dans des limites raisonnables. En tout état de cause, lors de la demande d'accès au titre de l'article 15 du règlement (UE) 2016/679, la personne concernée devrait être aussi précise que possible. Les demandes trop larges ou génériques devraient également être considérées comme excessives.

(36) L'article 13 du règlement (UE) 2016/679 impose au responsable du traitement de fournir à la personne concernée certaines informations sur le traitement de ses données à caractère personnel ainsi que certaines autres informations nécessaires pour garantir un traitement équitable et transparent, telles que définies aux paragraphes 1, 2 et 3 de ladite disposition. Conformément au paragraphe 4 de l'article 13 du règlement (UE) 2016/679, cette obligation ne s'applique pas lorsque, et dans la mesure où, la personne concernée dispose déjà de ces informations. Afin de réduire encore la charge pesant sur les responsables du traitement, sans compromettre les possibilités dont bénéficie la personne concernée pour exercer ses droits au titre du chapitre III du règlement, cette dérogation devrait être étendue aux situations dans lesquelles le traitement n'est pas susceptible d'engendrer un risque élevé, au sens de l'article 35 du règlement, et lorsqu'il existe des motifs raisonnables de supposer que la personne concernée dispose déjà des informations visées au paragraphe 1, points a) et c), à la lumière du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement. Il devrait s'agir des situations dans lesquelles le contexte entourant la relation entre le responsable du traitement et la personne concernée est très clair et circonscrit et dans lesquelles l'activité du responsable du traitement n'est pas une activité à forte intensité de données, telle que la relation entre un artisan et ses clients, dans le cadre de laquelle la portée du traitement est limitée au minimum de données nécessaires à l'exécution du service. L'activité du responsable du traitement n'est pas une activité à forte intensité de données lorsqu'il s'agit de collecter une faible quantité de données à

caractère personnel et que les opérations de traitement ne sont pas complexes, ce qui n'est pas le cas, par exemple, dans le domaine de l'emploi. En pareilles circonstances, c'est-à-dire lorsque le traitement n'est pas une activité à forte intensité de données, qu'il n'est pas complexe et que le responsable du traitement recueille une faible quantité de données à caractère personnel, il devrait être raisonnable de s'attendre, par exemple, à ce que la personne concernée dispose des informations sur l'identité et les coordonnées du responsable du traitement ainsi que sur la finalité du traitement lorsque ce traitement est effectué aux fins de l'exécution d'un contrat auquel une personne concernée est partie, ou lorsque la personne concernée a donné son consentement à ce traitement, conformément aux exigences énoncées dans le règlement (UE) 2016/679. Il devrait en aller de même pour les associations et les clubs sportifs lorsque le traitement des données à caractère personnel se limite à la gestion des membres, à la communication avec les membres et à l'organisation d'activités. Néanmoins, cette dérogation aux obligations de l'article 13 est sans préjudice des obligations indépendantes incombant au responsable du traitement en vertu de l'article 15 dudit règlement, lequel s'applique dans le cas où la personne concernée demande l'accès sur la base de cette dernière disposition. Lorsque la dérogation aux obligations prévues à l'article 13 ne s'applique pas, afin de trouver un équilibre entre le besoin d'exhaustivité et la nécessité d'une compréhension aisée par la personne concernée, les responsables du traitement peuvent adopter une approche à plusieurs niveaux lorsqu'ils fournissent les informations requises, notamment en permettant aux utilisateurs de s'orienter vers d'autres informations.

(37) Lorsque le traitement est effectué à des fins de recherche scientifique et que la communication d'informations à la personne concernée se révèle impossible ou nécessiterait des efforts disproportionnés, il ne devrait pas être nécessaire de fournir les informations prévues à l'article 13 du présent règlement. Le responsable du traitement devrait s'efforcer, dans la mesure du raisonnable, d'obtenir les coordonnées si celles-ci sont aisément disponibles et si l'acquisition de ces données n'impose pas d'efforts disproportionnés. La communication des informations nécessiterait un effort disproportionné notamment dans les cas où le responsable du traitement, au moment de la collecte des données à caractère personnel, ne savait pas ou ne prévoyait pas qu'il traiterait ultérieurement des données à caractère personnel à des fins de recherche scientifique, auquel cas il pourrait ne pas avoir accès aisément aux coordonnées des personnes concernées. Dans de telles situations, le responsable du traitement devrait informer indirectement les personnes concernées, par exemple en rendant les informations publiquement disponibles. La communication de ces informations devrait permettre d'atteindre le plus grand nombre possible de personnes concernées. Les moyens pertinents pour rendre ces informations publiquement disponibles devraient être déterminés en fonction du contexte du projet de recherche et des personnes concernées.

(38) L'article 22 du règlement (UE) 2016/679 prévoit des règles régissant le traitement des données à caractère personnel lorsque le responsable du traitement prend des décisions fondées exclusivement sur un traitement automatisé et ayant des effets juridiques à l'égard de la personne concernée ou l'affectant de manière significative de façon similaire. Afin d'apporter une plus grande sécurité juridique, il convient de préciser que les décisions fondées uniquement sur un traitement automatisé sont autorisées lorsque des conditions particulières sont remplies, ainsi que le prévoit le règlement (UE) 2016/679. Il convient également de préciser que, lorsqu'il s'agit d'évaluer si une décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement, ainsi que le prévoit l'article 22,

paragraphe 2, point a), du règlement (UE) 2016/679, il ne devrait pas être exigé que la décision ne puisse être prise que sur la base d'un traitement exclusivement automatisé. En d'autres termes, le fait que la décision puisse également être prise par un être humain n'empêche pas le responsable du traitement de prendre la décision sur la base d'un traitement exclusivement automatisé. Lorsqu'il existe plusieurs solutions de traitement automatisé tout aussi efficaces, le responsable du traitement devrait utiliser la solution la moins intrusive.

(39) Afin de réduire la charge pesant sur les responsables du traitement tout en veillant à ce que les autorités de contrôle aient accès aux informations pertinentes et puissent agir en cas de violation du règlement, le seuil de notification d'une violation de données à caractère personnel à l'autorité de contrôle en vertu de l'article 33 du règlement (UE) 2016/679 devrait être aligné sur celui appliqué pour la communication à la personne concernée d'une violation de données à caractère personnel en vertu de l'article 34 dudit règlement. Lorsqu'une violation de données n'est pas susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement ne devrait pas être tenu d'en informer l'autorité de contrôle compétente. Le seuil plus élevé appliqué aux fins de la notification d'une violation de données à l'autorité de contrôle ne porte pas atteinte à l'obligation du responsable du traitement de documenter la violation conformément à l'article 33, paragraphe 5, du règlement (UE) 2016/679, ni à son obligation d'être en mesure de démontrer qu'il respecte ledit règlement, conformément à l'article 5, paragraphe 2, dudit règlement. Afin de faciliter le respect du règlement par les responsables du traitement ainsi qu'une approche harmonisée dans l'Union, le comité devrait élaborer un modèle commun pour la notification des violations de données à l'autorité de contrôle compétente de même qu'une liste commune des circonstances dans lesquelles une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique. La Commission devrait tenir dûment compte des propositions élaborées par le comité et les réviser, le cas échéant, avant leur adoption. Afin de tenir compte des nouvelles menaces pour la sécurité des informations, le modèle commun et la liste devraient être réexaminés au moins tous les trois ans et actualisés au besoin. L'absence d'une liste commune des circonstances dans lesquelles une violation de données à caractère personnel est susceptible d'entraîner un risque élevé pour les droits et libertés d'une personne physique ne devrait pas affecter les obligations faites aux responsables du traitement de notifier ces violations.

(40) L'article 35 du règlement (UE) 2016/679 impose aux responsables du traitement de procéder à une analyse d'impact relative à la protection des données lorsque le traitement de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Les autorités de contrôle instituées dans le cadre dudit règlement sont tenues d'établir et de publier une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise. En outre, le règlement prévoit que les autorités de contrôle puissent établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise. Afin de contribuer efficacement à l'objectif de convergence des économies et de garantir efficacement le libre flux des données à caractère personnel entre les États membres, d'accroître la sécurité juridique, de faciliter le respect du règlement par les responsables du traitement et de garantir une interprétation harmonisée de la notion de risque élevé pour les droits et libertés des personnes concernées, il y a lieu de fournir au niveau de l'UE une liste unique des opérations de traitement, afin de remplacer les listes nationales existantes. En outre, la publication d'une liste des types d'opérations

de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise, qui est actuellement facultative, devrait être rendue obligatoire. Les listes des opérations de traitement devraient être élaborées par le comité et adoptées par la Commission par voie d'acte d'exécution. Afin de faciliter le respect du règlement par les responsables du traitement, le comité devrait également élaborer un modèle commun et une méthodologie commune pour la réalisation des analyses d'impact relatives à la protection des données, que la Commission adoptera par voie d'acte d'exécution. La Commission devrait tenir dûment compte des propositions élaborées par le comité et les réviser, au besoin, avant leur adoption. Afin de tenir compte des évolutions technologiques, les listes ainsi que le modèle commun et la méthodologie commune devraient être réexaminés au moins tous les trois ans et actualisés au besoin.

(41) Le règlement (UE) 2018/1725 du Parlement européen et du Conseil[36] s'applique au traitement des données à caractère personnel par les institutions, organes et organismes de l'Union. La directive (UE) 2016/680 du Parlement européen et du Conseil[37] s'applique au traitement des données à caractère personnel par les autorités compétentes aux fins de la prévention et de la détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou de l'exécution de sanctions pénales. Il convient d'aligner le règlement (UE) 2018/1725 ainsi que la directive (UE) 2016/680 sur les modifications apportées au règlement (UE) 2016/679 par le présent règlement.

(42) Comme précisé au considérant 5 du règlement (UE) 2018/1725, chaque fois que les dispositions du règlement (UE) 2018/1725 suivent les mêmes principes que les dispositions du règlement (UE) 2016/679, ces deux ensembles de dispositions devraient, conformément à la jurisprudence de la Cour de justice de l'Union européenne, être interprétés de manière homogène. Le régime prévu par le règlement (UE) 2018/1725 doit être compris comme étant équivalent au régime défini dans le règlement (UE) 2016/679. Par conséquent, le présent règlement modifie également les dispositions du règlement (UE) 2018/1725 qui sont concernées par les modifications du règlement (UE) 2016/679, dans la mesure où ces dernières modifications sont également pertinentes dans le contexte du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union.

(43) Afin de fournir un cadre solide et cohérent en matière de protection des données dans l'Union, il convient d'apporter, après l'adoption du présent règlement, les adaptations nécessaires à la directive (UE) 2016/680 ainsi qu'à tout autre acte juridique de l'Union

---

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

[37] 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, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

applicable au traitement de données à caractère personnel de manière à permettre une application aussi proche que possible de l'entrée en vigueur des modifications apportées au règlement (UE) 2016/679 et au règlement (UE) 2018/1725.

(44) Le stockage de données à caractère personnel dans un équipement terminal ou l'obtention de l'accès à des données à caractère personnel déjà stockées dans un équipement terminal ainsi que le traitement ultérieur de ces données devraient être régis par un cadre juridique unique, à savoir le règlement (UE) 2016/679, dès lors que l'abonné du service de communications électroniques ou l'utilisateur de l'équipement terminal est une personne physique. Les modifications présentées dans le présent règlement continuent d'offrir les niveaux les plus élevés de protection pour les données à caractère personnel, tout en simplifiant l'expérience vécue par les personnes concernées lors de l'exercice de leurs droits et de l'expression de leurs choix en ligne. Les modifications concernent en particulier le stockage d'informations dans cet équipement, l'accès à des informations stockées dans cet équipement ou leur collecte d'une autre manière, ce qui implique le traitement de données à caractère personnel au moyen de cookies ou de technologies similaires afin d'obtenir des informations provenant de l'équipement terminal. Les règles pertinentes devraient également s'appliquer indépendamment du fait que l'équipement terminal soit la propriété de la personne physique ou d'une autre personne morale ou physique.

Le stockage de données à caractère personnel dans un équipement terminal ou l'obtention de l'accès à des données à caractère personnel déjà stockées dans un équipement terminal ne devraient continuer à être autorisés que sur la base du consentement. À l'instar de l'approche adoptée dans la directive 2002/58/CE, cette exigence ne devrait pas empêcher le stockage de données à caractère personnel, ou l'obtention de l'accès à des données à caractère personnel déjà stockées, dans l'équipement terminal d'une personne physique, dès lors que le traitement est fondé sur le droit de l'Union ou le droit d'un État membre au sens de l'article 6 du règlement (UE) 2016/679, qu'il satisfait à toutes les conditions de licéité énoncées dans ladite disposition et qu'il est effectué aux fins des objectifs énoncés à l'article 23, paragraphe 1, du règlement (UE) 2016/679.

Afin de réduire la charge découlant de la mise en conformité et d'apporter une clarté juridique aux responsables du traitement, et étant donné que certaines finalités du traitement présentent un faible risque pour les droits et libertés des personnes concernées ou que ce traitement peut être nécessaire pour fournir un service demandé par la personne concernée, il est nécessaire de définir une liste limitative de finalités pour lesquelles le traitement devrait être autorisé sans consentement. En ce qui concerne le stockage de données à caractère personnel, ou l'obtention de l'accès à des données à caractère personnel déjà stockées, dans un équipement terminal, ainsi que le traitement ultérieur nécessaire à ces fins, le présent règlement devrait donc prévoir la licéité de ce traitement. Le responsable du traitement, tel qu'un fournisseur de services de médias, peut charger un sous-traitant, tel qu'une société d'études de marché, d'effectuer le traitement pour son compte.

S'agissant du traitement ultérieur de données à caractère personnel à des fins autres que celles définies dans la liste limitative, il convient d'appliquer les dispositions de l'article 6 et, le cas échéant, de l'article 9 du règlement (UE) 2016/679. Il incombe au responsable du traitement, à la lumière du principe de responsabilité, de choisir la base juridique appropriée pour le traitement prévu. Afin de pouvoir invoquer l'intérêt légitime au titre de l'article 6, paragraphe 1, point f), du règlement (UE) 2016/679 comme motif du traitement ultérieur de données à caractère personnel, le responsable

du traitement doit démontrer qu'il poursuit l'intérêt légitime qui est le sien ou celui de tiers, que le traitement est nécessaire à la réalisation de la finalité de cet intérêt légitime et que les intérêts ou les droits fondamentaux de la personne concernée ne prévalent pas sur les intérêts poursuivis par le responsable du traitement. Dans ce cadre, les responsables du traitement devraient tenir le plus grand compte des éléments suivants: le fait que la personne concernée est un enfant ou non; les attentes raisonnables de la personne concernée; l'incidence sur la personne, que ce soit en raison de l'ampleur ou de la sensibilité des données traitées; l'ampleur du traitement en cause, en ce sens que le traitement ne peut être particulièrement étendu en raison de la quantité de données ou de l'éventail de catégories de données; le fait que le traitement devrait reposer sur des données limitées à ce qui est nécessaire et ne peut être fondé sur le suivi d'une grande partie de l'activité en ligne des personnes concernées; et d'autres facteurs pertinents, selon le cas. Le traitement ne devrait pas donner lieu à une surveillance continue de la vie privée de la personne concernée.

Lorsque le responsable du traitement ne peut pas invoquer un intérêt légitime comme fondement juridique pour le traitement ultérieur, le traitement devrait être fondé sur l'un des autres motifs visés à l'article 6, paragraphe 1, en particulier sur le consentement conformément aux articles 6 et 7 du règlement (UE) 2016/679, pour autant que tous les principes du règlement (UE) 2016/679 soient respectés.

(45) Les personnes concernées qui ont refusé de donner suite à une demande de consentement sont souvent confrontées à une nouvelle demande de consentement chaque fois qu'elles consultent le service en ligne d'un même responsable du traitement. Cela peut avoir des effets préjudiciables pour les personnes concernées, lesquelles peuvent donner leur consentement dans le seul but d'éviter des demandes répétitives. Le responsable du traitement devrait donc être tenu de respecter le choix de la personne concernée de ne pas donner suite à une demande de consentement pendant au moins une certaine période.

(46) Les personnes concernées devraient pouvoir utiliser des indications automatisées et lisibles par machine de leur choix quant à l'acceptation ou au refus d'une demande de consentement ou pour s'opposer au traitement des données. Ces moyens devraient être en phase avec l'état de la technique. Ils peuvent être mis en œuvre via les paramètres d'un navigateur web ou intégrés dans le portefeuille européen d'identité numérique, ainsi que le prévoit le règlement (UE) nº 910/2014, ou par tout autre moyen adéquat. Les règles énoncées dans le présent règlement devraient favoriser l'émergence de solutions axées sur le marché et dotées d'interfaces appropriées. Le responsable du traitement devrait être tenu de respecter les indications automatisées et lisibles par machine des choix de la personne concernée dès que des normes seront disponibles. Compte tenu de l'importance du journalisme indépendant dans une société démocratique et afin de ne pas en compromettre le fondement économique, les fournisseurs de services de médias ne devraient pas être tenus de respecter le choix de la personne concernée via des indications lisibles par machine. L'obligation pour les fournisseurs de navigateurs web de fournir les moyens techniques permettant aux personnes concernées de faire des choix en ce qui concerne le traitement ne devrait pas compromettre la possibilité pour les fournisseurs de services de médias de demander le consentement des personnes concernées.

(47) La directive 2002/58/CE concernant la vie privée et les communications électroniques (directive «vie privée et communications électroniques»), révisée en dernier lieu en 2009, fournit un cadre pour la protection du droit à la vie privée, y compris la confidentialité des communications. Elle précise également les dispositions du

règlement (UE) 2016/679 en ce qui concerne le traitement des données à caractère personnel dans le cadre des services de communications électroniques. Elle protège la vie privée et l'intégrité des équipements terminaux de l'utilisateur ou de l'abonné utilisés pour ces communications. La disposition actuelle de l'article 5, paragraphe 3, de la directive 2002/58/CE devrait rester applicable dans la mesure où l'abonné ou l'utilisateur n'est pas une personne physique et où les informations stockées ou consultées ne constituent pas ou n'entraînent pas de traitement de données à caractère personnel.

(48) Il convient d'abroger l'article 4 de la directive 2002/58/CE, lequel exige des fournisseurs de services de communications électroniques accessibles au public qu'ils garantissent la sécurité de leurs services, et prévoit des obligations en matière d'information. Par la suite, la directive (UE) 2022/2555 a fixé de nouvelles exigences pour ces fournisseurs en ce qui concerne les mesures de gestion des risques en matière de cybersécurité et le signalement des incidents. Afin de réduire le chevauchement des obligations imposées aux entités du secteur des communications électroniques, il convient d'abroger l'article 4 de la directive 2002/58/CE. En ce qui concerne la sécurité du traitement des données à caractère personnel conformément à l'article 4, paragraphes 1 et 1 *bis*, de la directive 2002/58/CE, de même que la notification des violations de données à caractère personnel conformément à l'article 4, paragraphes 3 à 5, de ladite directive, le règlement (UE) 2016/679 prévoit déjà des règles complètes et actualisées. Ces règles devraient donc s'appliquer aux fournisseurs de services de communications électroniques accessibles au public et aux fournisseurs de réseaux publics de communications, garantissant de la sorte qu'un régime unique s'applique aux responsables du traitement et aux sous-traitants.

(49) Plusieurs actes juridiques horizontaux ou sectoriels de l'Union exigent la notification d'un même événement à différentes autorités par différents moyens techniques et différents canaux. Le guichet unique pour le signalement des incidents devrait permettre aux entités de s'acquitter de leurs obligations en matière de notification au titre de la directive (UE) 2022/2555, du règlement (UE) 2016/679, du règlement (UE) 2022/2554, du règlement (UE) nº 910/2014 et de la directive (UE) 2022/2557 en transmettant leurs notifications à une interface unique. En outre, le guichet unique devrait permettre aux entités de retrouver les informations qu'elles ont précédemment communiquées en utilisant ce guichet unique, afin d'aider ces entités à suivre l'évolution des mesures prises pour s'acquitter de leurs obligations en matière de signalement d'incidents spécifiques.

(50) Afin de garantir la sécurité du guichet unique, l'ENISA devrait prendre des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées de manière à gérer les risques qui pèsent sur la sécurité du guichet unique et des informations communiquées ou diffusées via le guichet unique. Lorsqu'elle évalue le risque, ainsi que le caractère approprié et proportionné de ces mesures, l'ENISA devrait tenir compte de la nature sensible des informations communiquées ou diffusées en vertu des actes juridiques pertinents de l'Union. L'ENISA devrait consulter les autorités compétentes en vertu des actes juridiques pertinents de l'Union lorsqu'elle élabore les mesures techniques, opérationnelles et organisationnelles nécessaires à la mise en place, à la maintenance et au fonctionnement sécurisé du guichet unique en recourant aux groupes et réseaux de coopération existants institués dans les États membres en vertu de ces actes.

(51) Avant de permettre la notification des incidents, l'ENISA devrait tester le fonctionnement du guichet unique et mener à cet effet des essais approfondis sur les

spécificités et les exigences relatives aux notifications aux fins des actes juridiques pertinents de l'Union. Sur la base des résultats des essais, la Commission devrait évaluer le bon fonctionnement, la fiabilité, l'intégrité et la confidentialité du guichet unique. Lors de cette évaluation, la Commission devrait consulter le réseau des centres de réponse aux incidents de sécurité informatique (CSIRT) ainsi que les autorités compétentes en vertu des actes juridiques pertinents de l'Union, en faisant appel aux groupes et réseaux de coopération existants institués dans les États membres au titre de ces actes. Dès lors que la Commission constate que le guichet unique garantit un bon fonctionnement, ainsi que la fiabilité, l'intégrité et la confidentialité, elle devrait publier un avis à cet effet au Journal officiel de l'Union européenne. Si la Commission estime que le bon fonctionnement, la fiabilité, l'intégrité et la confidentialité ne sont pas garantis, il y a lieu pour l'ENISA de prendre toutes les mesures correctives nécessaires, avant une nouvelle évaluation par la Commission.

(52) Afin d'assurer la continuité et l'interopérabilité avec les solutions techniques qui existent au niveau national et facilitent le signalement des incidents, l'ENISA devrait, dans la mesure du possible, tenir compte de ces solutions lors de l'élaboration des spécifications relatives aux mesures techniques, opérationnelles et organisationnelles nécessaires à la mise en place, à la maintenance et au fonctionnement sécurisé du guichet unique. En outre, l'ENISA devrait envisager des protocoles et outils techniques tels que des interfaces de programmation d'applications et des normes lisibles par machine qui permettent aux entités d'intégrer les obligations de signalement dans les processus opérationnels, et aux autorités de connecter le guichet unique à leurs systèmes nationaux de signalement.

(53) Afin de veiller à ce que le guichet unique permette aux entités concernées de communiquer, sous le format requis, le type d'informations demandé par les actes juridiques pertinents de l'Union, l'ENISA devrait consulter la Commission et les autorités compétentes désignées en vertu de ces actes. Lorsqu'un acte juridique de l'Union n'est pas totalement harmonisé en ce qui concerne le type d'informations et le format des signalements, les États membres devraient informer l'ENISA de leurs dispositions nationales en la matière.

(54) Avec le règlement (UE) 2022/2554, le secteur financier a été un pionnier dans la mise en œuvre d'un cadre harmonisé, complet et efficace, y compris en ce qui concerne le signalement des incidents. Afin de simplifier la mise en conformité, il convient d'aligner le cadre de signalement des incidents établi en vertu du règlement (UE) 2022/2554 sur le guichet unique, tout en garantissant la continuité et la stabilité du cadre de signalement existant, et compte tenu du fait que le guichet unique serait opérationnel après une évaluation confirmant qu'il garantit un bon fonctionnement, la fiabilité, l'intégrité et la confidentialité. En outre, le règlement (UE) 2022/2554 a introduit des modèles de notification normalisés rationalisant le contenu des rapports pour les incidents majeurs liés aux TIC dans le secteur financier. L'expérience acquise lors de l'adoption de ces modèles fournit des informations précieuses et met en évidence de bonnes pratiques qui devraient être prises en considération lors de la spécification du type d'informations, du format et de la procédure de notification aux fins du signalement vers le guichet unique au titre de la directive (UE) 2022/2555, de la directive (UE) 2022/2557 ou du règlement (UE) 2016/679, selon le cas. À cette fin, la Commission devrait tenir dûment compte des normes techniques de réglementation adoptées conformément au règlement (UE) 2022/2554, lesquelles précisent le contenu de la notification initiale, ainsi que des rapports intermédiaires et finaux, concernant les incidents majeurs liés aux TIC. Cette approche vise à garantir la cohérence, à

promouvoir les synergies et à réduire la charge administrative pesant sur les entités en réduisant au minimum le nombre de champs de données que les entités sont tenues de remplir, favorisant ainsi des processus de signalement plus efficaces et rationalisés.

(55) En vertu des actes juridiques pertinents de l'Union, certaines informations spécifiques à un incident doivent être partagées à un stade ultérieur entre les autorités compétentes afin de favoriser une surveillance et une coordination efficaces. Par conséquent, le guichet unique devrait être conçu pour permettre et faciliter l'échange d'informations à ce niveau pour chaque acte juridique pertinent de l'Union, en veillant à ce que des flux de données appropriés entre les autorités soient mis en place de manière sécurisée, rapide et efficace, dans le cas où les États membres décideraient d'utiliser cette fonctionnalité supplémentaire.

(56) Afin de faire en sorte que le signalement des incidents soit effectué par l'intermédiaire du guichet unique, il convient dès lors de modifier en conséquence la directive (UE) 2022/2555, le règlement (UE) 2016/679, le règlement (UE) 2022/2554, le règlement (UE) nº 910/2014 et la directive (UE) 2022/2557. L'utilisation du guichet unique aux fins du signalement prévu par ces actes devrait débuter dans un délai de 18 mois à compter de l'entrée en vigueur du présent règlement. Si la Commission lance le mécanisme de communication reportant la date d'application à 24 mois à compter de l'entrée en vigueur du règlement, les dispositions correspondantes de la directive (UE) 2022/2555, du règlement (UE) nº 910/2014, du règlement (UE) 2022/2554 et de la directive (UE) 2022/2557 devraient continuer de s'appliquer aux fins du respect des obligations en matière de signalement prévues par lesdites dispositions.

(57) Dans le cas exceptionnel où une impossibilité technique empêcherait le signalement d'incidents par l'intermédiaire du guichet unique, les entités devraient s'acquitter de leurs obligations de notification par d'autres moyens. À cette fin, les destinataires des notifications d'incidents au titre des actes juridiques pertinents de l'Union devraient faire en sorte de pouvoir recevoir ces notifications d'incidents par d'autres moyens et devraient mettre à la disposition du public des informations sur ces autres moyens.

(58) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil[38] et a rendu son avis le [DATE]. Le comité européen de la protection des données a été consulté conformément à l'article 42, paragraphe 2, du règlement (UE) 2018/1725 et a rendu un avis le [DATE].

(59) Le règlement (UE) 2019/1150 établit un ensemble ciblé de règles contraignantes à l'échelon de l'Union afin de garantir un environnement équitable, prévisible, durable et inspirant confiance pour l'activité économique en ligne au sein du marché intérieur. Le règlement (UE) 2022/2065 et le règlement (UE) 2022/1925 fournissent un cadre réglementaire complet pour un environnement en ligne sûr, prévisible et de confiance

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

pour tous les utilisateurs finaux de services en ligne, et établissent des conditions de concurrence équitables pour les entreprises sur les marchés numériques. Dans un souci de simplification de la législation de l'Union dans le domaine des services d'intermédiation en ligne et des plateformes en ligne, et étant donné que les objectifs et les dispositions matérielles du règlement sur les relations entre les plateformes et les entreprises sont largement couverts par le règlement sur les services numériques et le règlement sur les marchés numériques, il convient d'abroger le règlement (UE) 2019/1050. Le règlement (UE) 2022/2065 et le règlement (UE) 2022/1925 contribuent à un cadre réglementaire pleinement harmonisé pour les services numériques et les marchés numériques, en rapprochant les mesures nationales concernant les exigences applicables aux fournisseurs de services intermédiaires ainsi que la contestabilité et l'équité des services de plateforme essentiels fournis par les contrôleurs d'accès. À des fins de sécurité juridique, certaines définitions figurant à l'article 2, les dispositions relatives aux restrictions et aux suspensions figurant à l'article 4, ainsi que les dispositions relatives au système interne de traitement des plaintes figurant à l'article 11 du règlement (UE) 2019/1150 qui sont recoupées par d'autres actes juridiques, en particulier la directive (UE) 2024/2831 relative à l'amélioration des conditions de travail dans le cadre du travail via une plateforme, et l'article 15 garantissant le contrôle de l'application, resteront temporairement en vigueur jusqu'à ce que les actes initiaux soient modifiés.

(60) Compte tenu de la nature technique des modifications proposées dans le présent règlement et de l'urgence de mettre en place un cadre juridique simplifié, il convient que le présent règlement entre en vigueur immédiatement après sa publication au Journal officiel. Le cas échéant, des périodes transitoires devraient être prévues pour permettre aux États membres et aux entités réglementées de s'adapter aux règles,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

*Article premier*

*Modifications du règlement (UE) 2023/2854*

Le règlement (UE) 2023/2854 est modifié comme suit:

1. L'article 1er est modifié comme suit:

(a) au paragraphe 1, les points suivants sont ajoutés:

«e *bis*) l'enregistrement volontaire des services d'intermédiation de données;

e *ter*) l'enregistrement volontaire des entités qui collectent et traitent les données mises à disposition à des fins altruistes;

e *quater*) l'établissement d'un comité européen de l'innovation dans le domaine des données;

e *quinquies*) les exigences de localisation des données et la disponibilité des données pour les autorités compétentes;

e *sexies*) la réutilisation de certaines données et de certains documents détenus par des organismes du secteur public ou par certaines entreprises publiques, ainsi que des données de la recherche.»;

(b) au paragraphe 2, les points suivants sont ajoutés:

«g) le chapitre VII *bis* s'applique aux données à caractère personnel et non personnel;

h) le chapitre VII *ter* s'applique à toutes les données à caractère non personnel;

i) le chapitre VII *quater* s'applique aux données à caractère personnel et non personnel, à savoir:

i) les documents détenus par les organismes du secteur public des États membres visés

1) à l'article 32 *decies*, paragraphe 1, point a), ou par les entreprises publiques visées

2) à l'article 32 *decies*, paragraphe 1, point b);

ii) les données de la recherche visées à l'article 32 *decies*, paragraphe 1, point c);

iii) certaines catégories de données protégées visées à l'article 32 *decies*, paragraphe 1, point a).»;

(c) au paragraphe 3, le point g) est remplacé par le texte suivant:

«g) aux participants à des espaces de données.»;

(d) le paragraphe 7 est supprimé;

(e) les paragraphes 11, 12 et 13 suivants sont ajoutés:

«11. Le chapitre VII *ter* du 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.

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

13. En ce qui concerne les données et les documents relevant du champ d'application du chapitre VII *quater*, section II, le chapitre VII *quater* du présent règlement est sans incidence sur la possibilité qu'ont les États membres d'adopter des règles plus détaillées ou plus strictes, pour autant que ces règles permettent une réutilisation plus large des données et des documents.».

2. L'article 2 est modifié comme suit:

(a) les points 4 *bis*), 4 *ter*) et 4 *quater*) suivants sont insérés:

«4 *bis*) “consentement”: le consentement au sens de l’article 4, point 11), du règlement (UE) 2016/679;

4 *ter*) “autorisation”: le fait d’accorder aux utilisateurs de données le droit au traitement de données à caractère non personnel;

4 *quater*) “accès”: l’utilisation de données conformément à des exigences techniques, juridiques ou organisationnelles particulières, sans que cela implique nécessairement la transmission ou le téléchargement de données;»;

(b) le point 13) est remplacé par le texte suivant:

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

(c) les points 28 *bis*) et 28 *ter*) suivants sont insérés:

«28 *bis*) “organisme de droit public”, un organisme présentant toutes les caractéristiques suivantes:

a) il a été créé pour satisfaire spécifiquement des besoins d’intérêt général ayant un caractère autre qu’industriel ou commercial;

b) il est doté de la personnalité juridique;

c) soit il est financé majoritairement par l’État, les autorités régionales ou locales, ou par d’autres organismes de droit public; soit sa gestion est soumise à un contrôle de ces autorités ou organismes, soit son organe d’administration, de direction ou de surveillance est composé de membres dont plus de la moitié sont désignés par l’État, les autorités régionales ou locales ou d’autres organismes de droit public;

«28 *ter*) “entreprise publique”: toute entreprise sur laquelle un organisme du secteur public peut exercer directement ou indirectement une influence dominante du fait de la propriété de l’entreprise, de la participation financière qu’il y détient ou des règles qui la régissent. Une influence dominante des organismes du secteur public sur l’entreprise est présumée dans tous les cas suivants lorsque ces organismes, directement ou indirectement:

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

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

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

(d) les points 38 *bis*) et 38 *ter*) suivants sont insérés:

«38 *bis*) “service d’intermédiation de données”: un service qui vise à établir des relations à caractère économique à des fins de partage de données entre un nombre indéterminé de personnes concernées ou de détenteurs de données et d’utilisateurs de données, par des moyens techniques, juridiques ou autres, y

compris aux fins de l'exercice des droits des personnes concernées en ce qui concerne les données à caractère personnel, et qui:

1) n'a pas pour objet principal l'intermédiation de contenus protégés par le droit d'auteur;

2) ne fait pas l'objet d'une acquisition conjointe par plusieurs personnes morales pour un usage exclusif entre elles;

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

(e) les points 44) à 63) suivants sont ajoutés:

«44) "moyenne entreprise": une moyenne entreprise telle que définie à l'article 2 de l'annexe de la recommandation 2003/361/CE;

«45) "petite entreprise à moyenne capitalisation": une petite entreprise à moyenne capitalisation telle que définie au point 2 de l'annexe de la recommandation de la Commission (UE) 2025/1099;

46) "université": un organisme du secteur public dispensant un enseignement supérieur post-secondaire sanctionné par des diplômes universitaires;

47) "licence type": une série de conditions de réutilisation prédéfinies dans un format numérique, de préférence compatible avec des licences publiques normalisées disponibles en ligne;

48) "document":

a) tout contenu non numérique quel que soit son support (papier ou enregistrement sonore, visuel ou audiovisuel); ou

b) toute partie de ce contenu;

50) "données dynamiques": des données et documents se présentant sous forme numérique et faisant l'objet de mises à jour fréquentes ou en temps réel, notamment en raison de leur volatilité ou de leur obsolescence rapide; les données produites par des capteurs sont généralement considérées comme des données dynamiques;

51) "données de la recherche": des données, autres que des publications scientifiques, qui sont recueillies ou produites au cours d'activités de recherche scientifique et utilisées comme éléments probants dans le processus de recherche, ou dont la communauté scientifique admet communément qu'elles sont nécessaires pour valider des conclusions et résultats de la recherche;

52) “réutilisation”: l’utilisation par des personnes physiques ou morales de documents détenus par:

a) des organismes du secteur public, à des fins commerciales ou non commerciales autres que l’objectif initial de la mission de service public pour lequel les documents ont été produits, à l’exception de l’échange de documents entre des organismes du secteur public aux seules fins de l’exercice de leur mission de service public; ou

b) des entreprises publiques au titre du chapitre VII *quater*, section 2, à des fins commerciales ou non commerciales autres que l’objectif initial de fournir les services d’intérêt général pour lequel les documents ont été produits, à l’exception de l’échange de documents entre des entreprises publiques et des organismes du secteur public aux seules fins de l’exercice de leur mission de service public;

53) “ensembles de données de forte valeur”: des données et documents dont la réutilisation est associée à d’importantes retombées positives au niveau de la société, de l’environnement et de l’économie, en particulier parce qu’ils se prêtent à la création de services possédant une valeur ajoutée, d’applications et de nouveaux emplois décents et de grande qualité, ainsi qu’en raison du nombre de bénéficiaires potentiels des services et applications à valeur ajoutée fondés sur ces données et documents;

54) “certaines catégories de données protégées”: des données et documents détenus par des organismes du secteur public, qui sont protégés pour des motifs:

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

b) de secret statistique;

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

d) de protection des données à caractère personnel, dans la mesure où ces données ne relèvent pas du champ d’application du chapitre VII *quater*, section 2;

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

57) “réutilisateur”: une personne physique ou morale qui a obtenu le droit de réutiliser des données ou des documents détenus par un organisme du secteur public ou une entreprise publique au titre du chapitre VII *quater*, des données de la recherche ou certaines catégories de données protégées;

58) “format lisible par machine”: un format de fichier structuré de telle manière que des applications logicielles puissent facilement identifier, reconnaître et extraire des données spécifiques, notamment chaque énoncé d’un fait et sa structure interne;

59) “format ouvert”: un format de fichier indépendant des plates-formes utilisées et mis à la disposition du public sans restriction empêchant la réutilisation des documents;

60) “norme formelle ouverte”: une norme établie par écrit, précisant en détail les exigences relatives à la manière d’assurer l’interopérabilité des logiciels;

61) “retour sur investissement raisonnable”: un pourcentage de la redevance globale, en sus du montant nécessaire au recouvrement des coûts éligibles, ne dépassant pas de plus de cinq points de pourcentage le taux d’intérêt fixe de la BCE;

62) “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;

63) “pseudonymisation”: la pseudonymisation telle qu’elle est visée à l’article 4, point 5), du règlement (UE) 2016/679.».

3. À l’article 4, le paragraphe 8 est remplacé par le texte suivant:

«8. Dans des circonstances exceptionnelles, lorsque le détenteur de données qui est un détenteur de secret d’affaires peut démontrer que, malgré les mesures techniques et organisationnelles prises par l’utilisateur en vertu du paragraphe 6 du présent article, il est très probable qu’il subisse un préjudice économique grave du fait de la divulgation de secrets d’affaires ou que la divulgation de secrets d’affaires à l’utilisateur crée un risque élevé d’obtention, d’utilisation ou de divulgation illicites à des entités de pays tiers, ou à des entités établies dans l’Union sous le contrôle direct ou indirect de ces entités, qui sont soumises à des juridictions assurant une protection plus faible ou non équivalente à celle prévue par le droit de l’Union, ce détenteur de données peut refuser, au cas par cas, une demande d’accès aux données spécifiques en question. Cette démonstration est dûment étayée sur la base d’éléments objectifs, tels que l’opposabilité de la protection des secrets d’affaires dans les pays tiers, la nature et le niveau de confidentialité des données demandées, ainsi que le caractère unique et neuf du produit connecté. Elle est fournie par écrit à l’utilisateur sans retard injustifié. Lorsque le détenteur de données refuse de partager des données en vertu du présent paragraphe, il adresse une notification à l’autorité compétente désignée en vertu de l’article 37.».

4. À l’article 5, le paragraphe 11 est remplacé par le texte suivant:

«11. Dans des circonstances exceptionnelles, lorsque le détenteur de données qui est un détenteur de secret d’affaires peut démontrer que, malgré les mesures techniques et organisationnelles prises par le tiers en vertu du paragraphe 9 du présent article, il est très probable qu’il subisse un préjudice économique grave du fait de la divulgation de secrets d’affaires ou que la divulgation de secrets d’affaires

au tiers crée un risque élevé d'obtention, d'utilisation ou de divulgation illicites à des entités de pays tiers, ou à des entités établies dans l'Union sous le contrôle direct ou indirect de ces entités, qui sont soumises à des juridictions assurant une protection plus faible ou non équivalente à celle prévue par le droit de l'Union, ce détenteur de données peut refuser, au cas par cas, une demande d'accès aux données spécifiques en question. Cette démonstration est dûment étayée sur la base d'éléments objectifs, tels que l'opposabilité de la protection des secrets d'affaires dans les pays tiers, la nature et le niveau de confidentialité des données demandées, ainsi que le caractère unique et neuf du produit connecté. Elle est fournie par écrit au tiers sans retard injustifié. Lorsque le détenteur de données refuse de partager des données en vertu du présent paragraphe, il adresse une notification à l'autorité compétente désignée en vertu de l'article 37.».

5. le titre du chapitre V est remplacé par le texte suivant:

**«MISE À LA DISPOSITION D'ORGANISMES DU SECTEUR PUBLIC, DE LA COMMISSION, DE LA BANQUE CENTRALE EUROPÉENNE ET D'ORGANES DE L'UNION DE DONNÉES SUR LE FONDEMENT D'UNE SITUATION D'URGENCE».**

6. Les articles 14 et 15 sont supprimés.

7. L'article 15 *bis* suivant est inséré:

«Article 15 *bis*

*Obligation incombant aux détenteurs de données de mettre des données à disposition sur le fondement d'une situation d'urgence*

1. Lorsqu'un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union démontre l'existence d'un besoin exceptionnel d'utiliser certaines données pour exercer ses fonctions statutaires à des fins d'intérêt public dans le cadre de la réaction à une situation d'urgence, de l'atténuation d'une situation d'urgence ou du soutien au rétablissement à la suite d'une situation d'urgence, il ou elle peut demander aux détenteurs de données qui sont des personnes morales, autres que des organismes du secteur public, de mettre ces données à disposition, y compris les métadonnées nécessaires à l'interprétation et à l'utilisation de ces données. Sur la base d'une telle demande dûment motivée, les détenteurs de données mettent les données et métadonnées à la disposition de l'organisme du secteur public demandeur, de la Commission, de la Banque centrale européenne ou de l'organe de l'Union. Ces demandes peuvent également être présentées lorsque la production de statistiques officielles est requise dans le cadre d'une situation d'urgence.

2. Lorsque les données demandées sont nécessaires pour réagir à une situation d'urgence et que l'organisme demandeur visé au paragraphe 1 n'est pas en mesure d'obtenir ces données par d'autres moyens en temps utile et de manière efficace et dans des conditions équivalentes, la demande porte sur des données à caractère non personnel. Lorsque la fourniture de données à caractère non personnel est insuffisante pour faire face à la situation d'urgence, des données à caractère personnel peuvent également être demandées et, si possible, mises à disposition sous

une forme pseudonymisée, sous réserve que leur protection soit garantie par des mesures techniques et organisationnelles appropriées.

3. Lorsque les données demandées sont nécessaires pour atténuer une situation d'urgence ou soutenir le rétablissement à la suite d'une situation d'urgence, un organisme demandeur visé au paragraphe 1 agissant sur la base du droit de l'Union ou du droit national peut demander des données à caractère non personnel spécifiques, dont l'absence l'empêche d'atténuer une situation d'urgence ou de soutenir le rétablissement à la suite d'une situation d'urgence. Ces demandes n'ont pas pour destinataires des microentreprises et de petites entreprises.».

8. À l'article 16, le paragraphe 2 est remplacé par le texte suivant:

«2. Le présent chapitre ne s'applique pas aux activités exercées par les organismes du secteur public, la Commission, la Banque centrale européenne ou les organes de l'Union concernant la prévention et la détection des infractions pénales ou administratives, les enquêtes ou les poursuites en la matière, ou l'exécution de sanctions pénales, ni à l'administration douanière ou fiscale. Le présent chapitre est sans incidence sur le droit de l'Union ou le droit national régissant ces activités.».

9. L'article 17 est modifié comme suit:

a) le paragraphe 1 est modifié comme suit:

i) la partie introductive est remplacée par le texte suivant:

«Lorsqu'un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union demande des données en vertu de l'article 15 *bis*, il ou elle:»;

ii) les points b) et c) sont remplacés par le texte suivant:

«b) démontre que les conditions d'introduction d'une demande au titre de l'article 15 *bis* sont remplies;

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

b) le paragraphe 2 est modifié comme suit:

i) le point c) est remplacé par le texte suivant:

«c) est proportionnée à la situation d'urgence et dûment motivée, en ce qui concerne la granularité et le volume des données demandées, ainsi que la fréquence d'accès aux données demandées;»;

ii) le point e) est supprimé;

c) les paragraphes 5 et 6 sont supprimés.

10. L'article 18 est modifié comme suit:

a) au paragraphe 2, la partie introductive est remplacée par le texte suivant:

«2. Sans préjudice des besoins spécifiques concernant la disponibilité des données définis dans le droit de l'Union ou le droit national, un détenteur de données peut rejeter la demande de mise à disposition de données ou demander sa modification dans le cadre du présent chapitre, sans retard injustifié et, en

tout état de cause, dans un délai maximal de cinq jours ouvrables suivant la réception d'une demande au titre de l'article 15 *bis*, paragraphe 2, sans retard injustifié et, en tout état de cause, dans un délai maximal de trente jours ouvrables suivant la réception d'une demande au titre de l'article 15 *bis*, paragraphe 3, pour l'un quelconque des motifs suivants:»;

b) le paragraphe 5 est supprimé.

11. L'article 19 est modifié comme suit:

a) au paragraphe 1, la partie introductive est remplacée par le texte suivant:

«Un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union qui reçoit des données à la suite d'une demande présentée en vertu de l'article 15 *bis*:»;

b) le paragraphe 3 est remplacé par le texte suivant:

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

12. L'article 20 est remplacé par le texte suivant:

«Article 20

*Compensation pour la mise à disposition de données en vertu du chapitre V*

1. Les détenteurs de données mettent gratuitement à disposition les données nécessaires pour réagir à une situation d'urgence conformément à l'article 15 *bis*, paragraphe 2. L'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union qui a reçu des données accorde une reconnaissance publique au détenteur de données si celui-ci lui en fait la demande.

2. Le détenteur de données dispose d'un droit à une juste compensation pour la mise à disposition de données à la suite d'une demande présentée au titre de l'article 15 *bis*, paragraphe 3. Une telle compensation couvre les coûts techniques et organisationnels encourus pour donner suite à la demande, y compris, le cas échéant, les coûts d'anonymisation, de pseudonymisation, d'agrégation et d'adaptation technique, et une marge raisonnable. À la demande de l'organisme du secteur public, de la Commission, de la Banque centrale européenne ou de l'organe de l'Union, le détenteur de données fournit des informations sur la base du calcul des coûts et de la marge raisonnable.

3. Par dérogation au paragraphe 1 du présent article, un détenteur de données qui est une microentreprise ou une petite entreprise peut demander une

compensation pour la mise à disposition de données en réponse à une demande au titre de l'article 15 *bis*, paragraphe 2, conformément aux conditions énoncées au paragraphe 2 du présent article.

4. Les détenteurs de données ne sont pas habilités à recevoir une compensation pour la mise à disposition de données à la suite d'une demande présentée au titre de l'article 15 *bis*, paragraphe 3, lorsque la mission spécifique effectuée dans l'intérêt public consiste en la production de statistiques officielles et que l'achat de données n'est pas autorisé par le droit national. Les États membres adressent une notification à la Commission lorsque le droit national n'autorise pas l'achat de données en vue de la production de statistiques officielles.».

13. L'article 21 est modifié comme suit:

a) le titre est remplacé par le texte suivant:

«**Partage de données obtenues dans le cadre d'une situation d'urgence avec des organismes de recherche ou des organismes statistiques**»;

b) le paragraphe 5 est remplacé par le texte suivant:

«5. Lorsqu'un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union a l'intention de transmettre ou de mettre des données à disposition en vertu du paragraphe 1, il ou elle adresse sans retard injustifié une notification au détenteur de données auprès duquel les données ont été obtenues, en précisant ce qui suit:

a) l'identité et les coordonnées de l'organisme ou du particulier destinataire des données;

b) la finalité de la transmission ou de la mise à disposition des données;

c) la période pendant laquelle les données doivent être utilisées et la protection technique;

d) les mesures organisationnelles prises, y compris lorsque des données à caractère personnel ou des secrets d'affaires sont concernés.».

14. L'article 22 *bis* suivant est inséré avant le chapitre VI:

«Article 22 *bis*

*Droit d'introduire une réclamation*

Lorsqu'un litige survient concernant une demande de données au titre de l'article 15 *bis*, y compris son refus, sa modification, le niveau de la compensation ou la transmission ou la mise à disposition des données, le détenteur de données, l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union peut introduire une réclamation auprès de l'autorité compétente, désignée en application de l'article 37, de l'État membre dans lequel le détenteur de données est établi.».

15. À l'article 31, les paragraphes 1 *bis* et 1 *ter* suivants sont insérés:

«1 *bis*. Les obligations prévues au chapitre VI, à l'exception de l'article 29, et à l'article 34 ne s'appliquent pas aux services de traitement de données autres

que ceux visés à l'article 30, paragraphe 1, lorsque la majorité des caractéristiques et fonctionnalités du service de traitement de données ont été adaptées par le fournisseur aux besoins spécifiques du client, si la fourniture de ces services est fondée sur un contrat conclu au plus tard le 12 septembre 2025.

Le fournisseur de ces services de traitement de données n'est pas tenu de renégocier ou de modifier un contrat relatif à la fourniture de ces services avant son expiration si ce contrat a été conclu au plus tard le 12 septembre 2025. Toute disposition contractuelle figurant dans ce contrat qui est contraire à l'article 29, paragraphes 1, 2 ou 3, est considérée comme nulle et non avenue.

1 ter. Le fournisseur d'un service de traitement de données peut inclure des dispositions prévoyant des pénalités de résiliation anticipée proportionnées dans un contrat à durée déterminée portant sur la fourniture de services de traitement de données autres que ceux visés à l'article 30, paragraphe 1.

Lorsque le fournisseur de services de traitement de données est une petite entreprise, une moyenne entreprise ou une petite entreprise à moyenne capitalisation, les obligations prévues au chapitre VI, à l'exception de l'article 29, et à l'article 34 ne s'appliquent pas aux services de traitement de données autres que ceux visés à l'article 30, paragraphe 1, si la fourniture de ces services est fondée sur un contrat conclu au plus tard le 12 septembre 2025.

Lorsque le fournisseur d'un service de traitement de données est une petite entreprise, une moyenne entreprise ou une petite entreprise à moyenne capitalisation, il n'est pas tenu de renégocier ou de modifier un contrat relatif à la fourniture d'un service de traitement de données autre que ceux visés à l'article 30, paragraphe 1, avant son expiration si ce contrat a été conclu au plus tard le 12 septembre 2025. Toute disposition contractuelle figurant dans ce contrat qui est contraire à l'article 29, paragraphes 1, 2 ou 3, est considérée comme nulle et non avenue.».

16. L'article 32 est modifié comme suit:

a) les paragraphes 1 et 2 sont remplacés par le texte suivant:

«1. Les fournisseurs de services de traitement de données, l'organisme du secteur public qui met à disposition des données ou des documents conformément au chapitre VII *quater*, section 3, la personne physique ou morale à laquelle a été accordé le droit de réutiliser des données ou des documents conformément au chapitre VII *quater*, section 3, un prestataire de services d'intermédiation de données ou une organisation altruiste en matière de données reconnue prennent toutes les mesures techniques, organisationnelles et juridiques adéquates, y compris des contrats, afin d'empêcher l'accès international des autorités publiques et l'accès des autorités publiques des pays tiers aux données à caractère non personnel détenues dans l'Union et le transfert de ces données lorsque ce transfert ou cet accès risque d'être en conflit avec le droit de l'Union ou le droit national de l'État membre concerné, sans préjudice du paragraphe 2 ou 3.

2. Toute décision ou tout jugement d'une juridiction d'un pays tiers et toute décision d'une autorité administrative d'un pays tiers exigeant d'un fournisseur de services de traitement de données, de l'organisme du secteur public qui met à disposition des données ou des documents conformément au chapitre VII *quater*, section 3, de la personne physique ou morale à laquelle a

été accordé le droit de réutiliser des données ou des documents conformément au chapitre VII *quater*, section 3, d'un prestataire de services d'intermédiation de données ou d'une organisation altruiste en matière de données reconnue qu'il ou elle transfère des données à caractère non personnel relevant du champ d'application du présent règlement et détenues dans l'Union ou qu'il ou elle donne accès à ces données ne sont reconnus ou rendus exécutoires de quelque manière que ce soit que s'ils sont fondés sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union, ou tout accord de ce type entre le pays tiers demandeur et un État membre.»;

b) au paragraphe 3, premier alinéa, la partie introductive est remplacée par le texte suivant:

«3. En l'absence d'un accord international tel qu'il est visé au paragraphe 2, lorsqu'un fournisseur de services de traitement de données, l'organisme du secteur public qui met à disposition des données ou des documents conformément au chapitre VII *quater*, section 3, la personne physique ou morale à laquelle a été accordé le droit de réutiliser des données ou des documents conformément au chapitre VII *quater*, section 3, un prestataire de services d'intermédiation de données ou une organisation altruiste en matière de données reconnue est destinataire d'une décision ou d'un jugement d'une juridiction d'un pays tiers ou d'une décision d'une autorité administrative d'un pays tiers imposant de transférer des données à caractère non personnel relevant du champ d'application du présent règlement et détenues dans l'Union ou d'y donner accès, et lorsque le respect d'une telle décision ou d'un tel jugement risquerait de mettre le destinataire en conflit avec le droit de l'Union ou avec le droit national de l'État membre concerné, le transfert de ces données vers cette autorité d'un pays tiers ou l'accès à ces données par cette même autorité n'a lieu que s'il est satisfait aux conditions suivantes:»;

c) les paragraphes 4 et 5 sont remplacés par le texte suivant:

«4. Si les conditions énoncées au paragraphe 2 ou 3 sont remplies, le fournisseur de services de traitement de données, l'organisme du secteur public qui met à disposition des données ou des documents conformément au chapitre VII *quater*, section 3, la personne physique ou morale à laquelle a été accordé le droit de réutiliser des données ou des documents conformément au chapitre VII *quater*, section 3, le prestataire de services d'intermédiation de données ou l'organisation altruiste en matière de données reconnue fournit le volume minimal de données admissible en réponse à une demande, sur la base de l'interprétation que peut raisonnablement donner de cette demande le fournisseur ou l'autorité nationale ou l'organisme national concernés visés au paragraphe 3, deuxième alinéa.

5. Le fournisseur de services de traitement de données, l'organisme du secteur public qui met à disposition des données ou des documents conformément au chapitre VII *quater*, section 3, la personne physique ou morale à laquelle a été accordé le droit de réutiliser des données ou des documents conformément au chapitre VII *quater*, section 3, le prestataire de services d'intermédiation de données ou l'organisation altruiste en matière de données reconnue informe la personne physique ou morale dont les droits et intérêts pourraient être affectés de l'existence d'une demande d'accès à des données la concernant qui émane d'une autorité d'un pays tiers avant de donner suite à cette demande, sauf

lorsque cette demande sert des fins répressives et aussi longtemps que cela est nécessaire pour préserver l'efficacité de l'action répressive.»;

17. L'article 36 est supprimé.

18. Les chapitres VII *bis*, VII *ter* et VII *quater* suivants sont insérés:

**«CHAPITRE VII *bis***
**SERVICES D'INTERMEDIATION DE DONNEES ET ORGANISATIONS ALTRUISTES EN MATIERE DE DONNEES»**

Article 32 *bis*

*Registres publics de l'Union*

1) La Commission tient et met régulièrement à jour des registres publics de l'Union:

   a) des prestataires de services d'intermédiation de données reconnus et

   b) des organisations altruistes en matière de données reconnues.

2) Les prestataires de services d'intermédiation de données enregistrés dans le registre public de l'Union visé au paragraphe 1, point a), peuvent utiliser le label "prestataire de services d'intermédiation de données reconnu dans l'Union" dans leurs communications écrites et orales, ainsi qu'un logo commun visé au paragraphe 4.

3) Les organisations altruistes en matière de données enregistrées dans le registre public de l'Union visé au paragraphe 1, point b), peuvent utiliser le label "organisation altruiste en matière de données reconnue dans l'Union" dans leurs communications écrites et orales, ainsi que le logo commun visé au paragraphe 4.

4) Afin que les prestataires de services d'intermédiation de données reconnus dans l'Union soient facilement identifiables dans toute l'Union, la Commission est habilitée à adopter des actes d'exécution établissant le modèle du logo commun. Ces actes d'exécution sont adoptés en conformité avec la procédure consultative visée à l'article 46, paragraphe 1 *bis*.

Article 32 *ter*

*Autorités compétentes pour l'enregistrement des prestataires de services d'intermédiation de données et des organisations altruistes en matière de données*

1) Chaque État membre désigne une ou plusieurs autorités compétentes chargées de l'application et de l'exécution du présent chapitre conformément à l'article 37, paragraphe 1.

2) Les autorités compétentes sont constituées de manière à garantir leur indépendance par rapport à tout prestataire de services d'intermédiation de données reconnu ou à toute organisation altruiste en matière de données reconnue.

Article 32 *quater*

*Exigences générales relatives à l'enregistrement des prestataires de services d'intermédiation de données reconnus*

Pour pouvoir être enregistré dans le registre public de l'Union visé à l'article 32 *bis*, paragraphe 1, point a), un prestataire de services d'intermédiation de données satisfait à l'ensemble des exigences suivantes:

a) il n’utilise pas les données pour lesquelles il fournit des services d’intermédiation de données à d’autres fins que de les mettre à la disposition des utilisateurs de données;

b) les données qu’il collecte en ce qui concerne toute activité d’une personne physique ou morale aux fins de la fourniture du service d’intermédiation de données, notamment la date, l’heure et les données de géolocalisation, la durée de l’activité et les connexions établies avec d’autres personnes physiques ou morales par la personne qui utilise le service d’intermédiation de données ne sont utilisées que pour le développement dudit service d’intermédiation de données;

c) lorsqu’il prévoit de fournir aux détenteurs de données ou aux personnes concernées des instruments et services supplémentaires dans le but particulier de faciliter l’échange de données, tels que le stockage temporaire, l’organisation, la conversion, le cryptage, l’anonymisation et la pseudonymisation, ces instruments et services ne sont utilisés qu’à la demande expresse ou moyennant l’approbation expresse du détenteur de données ou de la personne concernée;

d) lorsque les prestataires de services d’intermédiation de données qui ne sont pas des microentreprises et des petites entreprises prévoient de fournir à leurs clients des services à valeur ajoutée autres que les services visés au point c), ils remplissent les conditions suivantes:

   i) les services à valeur ajoutée sont expressément demandés par l’utilisateur;

   ii) les données ne sont pas utilisées à d’autres fins que la prestation du service à valeur ajoutée;

   iii) les services à valeur ajoutée sont fournis par l’intermédiaire d’une entité fonctionnellement distincte;

   iv) l’entreprise proposant les services à valeur ajoutée n’est pas désignée comme étant un contrôleur d’accès en vertu de l’article 3 du règlement (UE) 2022/1925;

   v) les conditions commerciales, y compris la tarification, de la fourniture de services d’intermédiation de données à un détenteur de données ou à un utilisateur de données ne sont pas subordonnées au fait que le détenteur de données ou l’utilisateur de données utilise ou non des services à valeur ajoutée fournis par le prestataire de services d’intermédiation de données ou par une entité liée;

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

Article 32 *quinquies*

*Exigences générales relatives à l’enregistrement des organisations altruistes en matière de données reconnues*

Pour pouvoir être enregistrée dans le registre public de l'Union visé à l'article 32 *bis*, paragraphe 1, point b), une organisation altruiste en matière de données satisfait à l'ensemble des exigences suivantes:

a) elle mène des activités altruistes en matière de données;

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

c) elle exerce ses activités dans un but non lucratif et est juridiquement indépendante de toute entité exerçant des activités dans un but lucratif;

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

Article 32 *sexies*

*Enregistrement*

1) Un prestataire de services d'intermédiation de données qui satisfait aux exigences énoncées à l'article 32 *quater* peut présenter une demande d'enregistrement dans le registre public de l'Union des prestataires de services d'intermédiation de données reconnus à l'autorité compétente visée à l'article 32 *ter* dans l'État membre dans lequel il a son établissement principal.

   Une organisation altruiste en matière de données qui satisfait aux exigences énoncées à l'article 32 *quinquies* peut présenter une demande d'enregistrement dans le registre public de l'Union des organisations altruistes en matière de données reconnues à l'autorité compétente visée à l'article 32 *ter* dans l'État membre dans lequel elle a son établissement principal.

2) Les prestataires de services d'intermédiation de données et les organisations altruistes en matière de données qui n'ont pas d'établissement principal dans l'Union désignent un représentant légal dans l'un des États membres. Le représentant légal est mandaté pour servir d'interlocuteur, en complément ou en lieu et place du prestataire de services d'intermédiation de données ou de l'organisation altruiste en matière de données, aux autorités compétentes ou aux personnes concernées et détenteurs de données. Le représentant légal coopère avec l'autorité compétente et lui démontre de manière exhaustive, sur demande, les mesures prises et les dispositions mises en place par le prestataire de services d'intermédiation de données ou l'organisation altruiste en matière de données pour garantir le respect du présent règlement.

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

3) Les autorités compétentes établissent les formulaires de demande nécessaires.

4) Lorsqu'un prestataire de services d'intermédiation de données a communiqué toutes les informations nécessaires conformément au paragraphe 3 du présent article et satisfait aux exigences énoncées à l'article 32 *quater*, l'autorité compétente décide, dans un délai de 12 semaines à compter de la réception de la demande d'enregistrement, si le prestataire satisfait ou non aux critères énoncés à

l'article 32 *quater*. Si le prestataire satisfait aux critères, l'autorité compétente communique les informations pertinentes à la Commission, qui enregistre le prestataire dans le registre public de l'Union en tant que prestataire de services d'intermédiation de données reconnu.

Le premier alinéa s'applique également lorsqu'une organisation altruiste en matière de données a communiqué toutes les informations nécessaires en vertu du paragraphe 2 et respecte les exigences en matière d'enregistrement énoncées à l'article 32 *quinquies*.

L'enregistrement dans le registre public de l'Union est valable dans tous les États membres.

5) L'autorité compétente peut percevoir des redevances pour l'enregistrement conformément au droit national. Ces redevances sont proportionnées et objectives et sont fondées sur les coûts administratifs liés au contrôle du respect des dispositions. Dans le cas des petites entreprises à moyenne capitalisation, des petites et moyennes entreprises et des jeunes pousses, l'autorité compétente peut appliquer une redevance réduite ou renoncer à la redevance.

6) Les entités enregistrées notifient à l'autorité compétente toute modification ultérieure des informations fournies au cours de la procédure de demande ou la cessation de leurs activités d'intermédiation de données ou d'activités altruistes en matière de données dans l'Union.

7) L'autorité compétente notifie sans délai et par voie électronique à la Commission toute notification effectuée en vertu du paragraphe 6. La Commission met à jour le registre public de l'Union dans les meilleurs délais.

Article 32 *septies*

*Fonctions des organisations altruistes en matière de données reconnues*

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

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

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

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

3) Les organisations altruistes en matière de données reconnues fournissent des moyens électroniques pour obtenir le consentement des personnes concernées ou l'autorisation de traiter les données mises à disposition par les détenteurs de données, ainsi que pour les retirer.

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

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

Article 32 *octies*

*Contrôle du respect des dispositions*

1) Les autorités compétentes visées à l’article 32 *ter* contrôlent et surveillent, soit de leur propre initiative, soit à la demande d’une personne physique ou morale, si les prestataires de services d’intermédiation de données reconnus et les organisations altruistes en matière de données reconnues respectent les exigences énoncées dans le présent chapitre, y compris s’ils continuent de respecter les exigences en matière d’enregistrement qui y sont énoncées.

2) Les autorités compétentes ont le pouvoir de demander aux prestataires de services d’intermédiation de données reconnus ou aux organisations altruistes en matière de données reconnues, ou à leur représentant légal, toutes les informations nécessaires pour vérifier le respect des exigences énoncées dans le présent chapitre. Toute demande d’information est proportionnée à l’accomplissement de la tâche et est motivée.

3) Lorsqu’une autorité compétente constate qu’un prestataire de services d’intermédiation de données reconnu ou une organisation altruiste en matière de données reconnue ne respecte pas une ou plusieurs des exigences énoncées dans le présent chapitre, elle notifie ces constatations à l’entité ou à son représentant légal et lui donne la possibilité d’exposer son point de vue dans un délai de trente jours à compter de la réception de la notification.

4) L’autorité compétente a le pouvoir d’exiger qu’il soit mis fin au non-respect visé au paragraphe 3, soit immédiatement soit dans un délai raisonnable, et prend des mesures appropriées et proportionnées visant à garantir la mise en conformité.

5) Si un prestataire de services d’intermédiation de données reconnu ou une organisation altruiste en matière de données reconnue ne respecte pas une ou plusieurs des exigences énoncées dans le présent chapitre même après avoir reçu une notification conformément au paragraphe 3, ladite entité:

a) perd le droit d’utiliser le label visé à l’article 32 *bis* dans ses communications écrites et orales;

b) est radiée du registre public de l’Union visé à l’article 32 *bis*.

Toute décision révoquant le droit d’utiliser le label visé au premier alinéa, point a), est rendue publique par l’autorité compétente.

# CHAPITRE VII *ter*

# Libre flux des données à caractère non personnel dans l'Union

Article 32 *nonies*

*Exigences en matière d'interdiction de localisation applicables aux données à caractère non personnel au sein de l'Union*

1) Les exigences de localisation des données à caractère non personnel sont interdites, sauf si elles sont justifiées par des motifs de sécurité publique conformément au principe de proportionnalité ou établies sur la base du droit de l'Union.

2) Les États membres communiquent immédiatement à la Commission tout projet d'acte instaurant une nouvelle exigence de localisation des données ou apportant des modifications à une exigence de localisation des données existante conformément aux procédures prévues aux articles 5, 6 et 7 de la directive (UE) 2015/1535 du Parlement européen et du Conseil.

# CHAPITRE VII *quater*

# Réutilisation de données et de documents détenus par des organismes du secteur public

## SECTION 1

## DISPOSITIONS GENERALES

Article 32 *decies*

*Objet et champ d'application*

1) Le présent chapitre fixe un ensemble de règles concernant la réutilisation et les modalités pratiques destinées à faciliter la réutilisation des éléments suivants:

   a) les données et documents existants détenus par des organismes du secteur public des États membres, y compris certaines catégories de données protégées;

   b) les données et documents existants détenus par des entreprises publiques:

      i) exerçant des activités dans les domaines visés au chapitre II de la directive 2014/25/UE du Parlement européen et du Conseil;

      ii) agissant en qualité d'opérateurs de services publics conformément à l'article 2 du règlement (CE) nº 1370/2007 du Parlement européen et du Conseil;

      iii) agissant en qualité de transporteurs aériens remplissant des obligations de service public conformément à l'article 16, du règlement (CE) nº 1008/2008 du Parlement européen et du Conseil; ou

iv) agissant en qualité d'armateurs communautaires remplissant des obligations de service public conformément à l'article 4 du règlement (CEE) nº 3577/92 du Conseil;

c) les données de la recherche, conformément aux conditions définies à l'article 32 *unvicies*.

2) Le présent chapitre ne s'applique pas:

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

b) aux données et documents détenus par des entreprises publiques et:

i) dont la production ne relève pas de la fourniture de services d'intérêt général au sens de la loi ou d'autres règles contraignantes en vigueur dans les États membres;

ii) relatifs aux activités directement exposées à la concurrence et qui par conséquent, conformément à l'article 34 de la directive 2014/25/UE, ne sont pas soumises aux règles relatives à la passation des marchés;

c) aux données et documents, tels que les données sensibles, dont l'accès est exclu conformément aux règles d'accès en vigueur dans l'État membre pour des motifs de protection de la sécurité nationale (c'est-à-dire de sécurité de l'État), de défense ou de sécurité publique;

d) aux données et documents détenus par des radiodiffuseurs de service public et leurs filiales et par d'autres organismes ou leurs filiales pour l'accomplissement d'une mission de radiodiffusion de service public.

3) La section 2 du présent chapitre ne s'applique pas:

a) aux données ou documents, tels que les données ou documents sensibles, dont l'accès est exclu conformément aux règles d'accès en vigueur dans l'État membre, y compris pour des motifs:

i) de secret statistique;

ii) de confidentialité des informations commerciales (notamment secret d'affaires, secret professionnel ou secret d'entreprise);

b) aux données ou documents dont l'accès est limité en vertu des règles d'accès en vigueur dans les États membres,

i) notamment dans les cas où les citoyens ou les personnes morales doivent justifier d'un intérêt particulier pour obtenir l'accès aux documents;

ii) pour des motifs de protection des données à caractère personnel, et aux parties de données ou de documents accessibles en vertu desdites règles qui contiennent des données à caractère personnel dont la réutilisation a été définie par la loi comme étant incompatible avec la législation concernant la protection des personnes physiques à l'égard du traitement des données à caractère personnel ou comme portant atteinte à la

protection de la vie privée et de l'intégrité de la personne concernée, en particulier au regard des dispositions de droit de l'Union ou de droit national sur la protection des données à caractère personnel; aux logos, aux armoiries ou aux insignes;

c) aux données ou documents dont des tiers détiennent les droits de propriété intellectuelle;

d) aux données ou documents détenus par des établissements culturels autres que des bibliothèques, y compris des bibliothèques universitaires, des musées et des archives;

e) aux données ou documents détenus par des établissements d'enseignement de niveau secondaire et au-dessous et, dans le cas de tous les autres établissements d'enseignement, aux données autres que celles visées au paragraphe 1, point c);

f) aux données ou documents autres que ceux visés au paragraphe 1, point c), détenus par des organismes exerçant une activité de recherche et des organisations finançant une activité de recherche, y compris des organisations créées pour le transfert des résultats de la recherche;

g) aux données ou documents dont l'accès est exclu ou limité pour des motifs d'informations relatives à la protection des entités critiques ou des infrastructures critiques au sens de l'article 2, points 1) et 4), de la directive (UE) 2022/2557.

4) La section 3 du présent chapitre ne s'applique pas:

a) aux données et documents qui ne constituent pas certaines catégories de données protégées;

b) aux données ou documents détenus par des entreprises publiques;

c) aux données ou documents détenus par des établissements culturels et des établissements d'enseignement;

d) aux données et documents relevant de la section 2 du présent chapitre.

5) Le présent chapitre s'appuie sur les règles d'accès de l'Union et nationales en vigueur et ne les affecte en rien, en particulier en ce qui concerne l'octroi de l'accès aux documents officiels et leur divulgation.

6) Les obligations imposées conformément au présent chapitre ne s'appliquent que dans la mesure où elles sont compatibles avec les dispositions des accords internationaux sur la protection des droits de propriété intellectuelle, notamment la convention de Berne pour la protection des œuvres littéraires et artistiques (convention de Berne), l'accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (accord sur les ADPIC) et le traité de l'Organisation mondiale de la propriété intellectuelle sur le droit d'auteur (WCT).

7) Les organismes du secteur public n'exercent pas le droit prévu à l'article 7, paragraphe 1, de la directive 96/9/CE pour le fabricant d'une base de données aux fins d'empêcher la réutilisation de données et de documents ou de limiter celle-ci au-delà des limites fixées par le présent chapitre.

8) Le présent chapitre régit la réutilisation des données et documents existants détenus par les organismes du secteur public et les entreprises publiques des États membres,

y compris les données et documents relevant de la directive 2007/2/CE du Parlement européen et du Conseil.

9) Le présent chapitre est sans préjudice du droit de l'Union, du droit national et des accords internationaux auxquels l'Union ou les États membres sont parties en ce qui concerne la protection des catégories de données ou de documents visées à l'article 2, point 54).

Article 32 *undecies*

*Non-discrimination*

1) Toutes les conditions applicables à la réutilisation des données ou des documents sont non discriminatoires, transparentes, proportionnées et objectivement justifiées en ce qui concerne les catégories de données ou de documents et les finalités de la réutilisation, ainsi que la nature des données ou des documents pour lesquels la réutilisation est autorisée. Ces conditions ne sont pas utilisées pour restreindre la concurrence. Ce principe s'applique dans une égale mesure aux catégories de réutilisation comparables, notamment la réutilisation transfrontière.

2) Lorsqu'un organisme du secteur public réutilise des données ou des documents dans le cadre de ses activités commerciales étrangères à sa mission de service public, les conditions tarifaires et autres applicables à la fourniture des données ou documents destinés à ces activités sont celles qui s'appliquent aux autres réutilisateurs.

Article 32 *duodecies*

*Accords d'exclusivité*

1) La réutilisation des données ou des documents est ouverte à tous les acteurs potentiels du marché, même si un ou plusieurs d'entre eux exploitent déjà des produits à valeur ajoutée basés sur ces données ou ces documents. Sont interdits les accords ou autres dispositifs ou pratiques relatifs à la réutilisation de données ou de documents qui ont pour objet ou pour effet d'octroyer des droits d'exclusivité ou de restreindre la disponibilité des données ou documents à des fins de réutilisation par des entités autres que les parties à ces accords, arrangements ou pratiques.

2) Par dérogation au paragraphe 1, lorsqu'un droit d'exclusivité est nécessaire à la fourniture d'un service d'intérêt général, ce droit peut être accordé dans la mesure nécessaire à la fourniture du service ou du produit, moyennant le respect des conditions suivantes:

   a) le droit d'exclusivité est accordé au moyen d'un acte administratif ou d'un accord contractuel conformément au droit de l'Union et au droit national applicables et dans le respect des principes de transparence, d'égalité de traitement et de non-discrimination;

   b) les accords octroyant le droit d'exclusivité, y compris les motifs pour lesquels il est nécessaire d'octroyer ce droit, sont transparents et rendus publics en ligne, sous une forme qui respecte le droit de l'Union applicable en matière de marchés publics et le droit national applicable;

   c) sauf en ce qui concerne les droits d'exclusivité liés à la numérisation des ressources culturelles, le bien-fondé de l'octroi de droits d'exclusivité

concernant les données et documents relevant du champ d'application de la section 2 fait l'objet d'un réexamen régulièrement et, en toute hypothèse, tous les trois ans;

d) les accords d'exclusivité conclus le 16 juillet 2019 ou après cette date sont rendus publics en ligne au moins deux mois avant leur prise d'effet. Les termes définitifs de ces accords sont transparents et sont rendus publics en ligne.

3) Par dérogation au paragraphe 1, lorsqu'un droit d'exclusivité concerne la numérisation de ressources culturelles, la période d'exclusivité ne dépasse pas, en général, dix ans. Lorsque ladite période est supérieure à dix ans, sa durée est conforme au droit de l'Union et au droit national applicables et fait l'objet d'un réexamen au cours de la onzième année et ensuite, le cas échéant, tous les sept ans.

4) Dans le cas d'un droit d'exclusivité visé au paragraphe 3, une copie des ressources culturelles numérisées est adressée gratuitement à l'organisme du secteur public dans le cadre des accords conclus. À l'expiration de la période d'exclusivité, ladite copie est mise à disposition à des fins de réutilisation.

5) En ce qui concerne certaines catégories de données protégées, la durée du droit d'exclusivité pour la réutilisation des données ne dépasse pas douze mois. Lorsqu'un contrat est conclu, la durée du contrat est la même que la durée du droit d'exclusivité.

6) Les accords ou autres dispositifs ou pratiques qui, sans accorder expressément de droit d'exclusivité, visent à restreindre la disponibilité de données et de documents relevant du champ d'application de la section 2 à des fins de réutilisation par des entités autres que les parties à ces dispositifs, ou qui peuvent raisonnablement être considérés comme susceptibles de la restreindre, sont rendus publics en ligne au moins deux mois avant leur entrée en vigueur. L'effet de tels dispositifs juridiques ou pratiques sur la disponibilité des données à des fins de réutilisation fait l'objet régulièrement et, en toute hypothèse, tous les trois ans, d'un réexamen. Les termes définitifs de ces accords sont transparents et sont rendus publics en ligne.

7) En ce qui concerne les accords d'exclusivité existants, les dispositions suivantes s'appliquent:

a) les accords d'exclusivité concernant des données et des documents relevant du champ d'application de la section 2 en place le 17 juillet 2013, qui ne relèvent pas des exceptions énoncées aux paragraphes 2 et 3 et qui ont été passés par des organismes du secteur public prennent fin à la date d'échéance du contrat et, en tout état de cause, au plus tard le 18 juillet 2043;

b) les accords d'exclusivité concernant des données et des documents relevant du champ d'application de la section 2 en place le 16 juillet 2019, qui ne relèvent pas des exceptions énoncées aux paragraphes 2 et 3 et qui ont été passés par des entreprises publiques prennent fin à la date d'échéance du contrat et, en tout état de cause, au plus tard le 17 juillet 2049.

Article 32 *terdecies*

*Principes généraux relatifs à la tarification*

1) Les redevances fixées au titre de la section 2 ou de la section 3 sont transparentes, non discriminatoires, proportionnées et objectivement justifiées et ne restreignent pas la concurrence.

2) Dans le cas de redevances types applicables en matière de réutilisation des données ou documents, les conditions applicables et le montant effectif desdites redevances, y compris la base de calcul utilisée pour lesdites redevances, sont fixés à l'avance et publiés, dans la mesure du possible et s'il y a lieu, sous forme électronique.

3) Dans le cas de redevances applicables en matière de réutilisation autres que celles visées au paragraphe 1, les facteurs qui sont pris en compte dans le calcul desdites redevances sont indiqués d'emblée. Sur demande, le détenteur des données ou documents concernés indique également la manière dont lesdites redevances ont été calculées dans le cadre d'une demande particulière de réutilisation.

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

Article 32 *quaterdecies*

*Informations relatives aux voies de recours*

Les organismes du secteur public veillent à ce que les demandeurs de réutilisation de données ou de documents soient informés des voies de recours dont ils disposent pour contester des décisions ou des pratiques qui les concernent.

## SECTION 2

## REUTILISATION DES DONNEES OUVERTES DU SECTEUR PUBLIC

### Sous-section 1 - Champ d'application et principes généraux

Article 32 *quindecies*

*Principe général concernant la réutilisation des données ouvertes du secteur public*

1) Les données ou documents relevant du champ d'application de la présente section sont réutilisables à des fins commerciales ou non commerciales conformément à la section 1 et à la section 2, sous-section 3.

2) Pour les données ou les documents à l'égard desquels des bibliothèques, y compris des bibliothèques universitaires, des musées et des archives sont titulaires de droits de propriété intellectuelle et pour les données ou documents détenus par des entreprises publiques, les États membres veillent à ce que, lorsque la réutilisation de ces données ou documents est autorisée, ils puissent être réutilisés à des fins commerciales ou non commerciales conformément à la section 1 et à la section 2, sous-section 3.

### Sous-section 2

### Demandes de réutilisation

Article 32 *sexdecies*

*Traitement des demandes de réutilisation*

1) Les organismes du secteur public traitent les demandes de réutilisation et mettent le document à la disposition du demandeur en vue de la réutilisation, si possible et s'il y a lieu sous forme électronique, ou, si une licence est nécessaire, présentent au demandeur l'offre de licence définitive dans un délai raisonnable qui correspond au délai de réponse applicable aux demandes d'accès aux données ou documents.

2) Dans les cas où il n'est pas prévu de limite dans le temps ou d'autres règles régissant la mise à disposition des données ou documents dans les délais prévus, les organismes du secteur public traitent la demande et fournissent les données ou les documents au demandeur en vue de la réutilisation ou, si une licence est nécessaire, présentent au demandeur l'offre de licence définitive dès que possible, et en tout état de cause dans les vingt jours ouvrables à compter de la réception de la demande. Ce délai peut être prolongé de vingt jours ouvrables supplémentaires pour des demandes importantes ou complexes. En pareils cas, dès que possible et, en tout état de cause, dans les trois semaines qui suivent la demande initiale, le demandeur est informé de la nécessité d'un délai supplémentaire pour traiter la demande, ainsi que des raisons qui justifient ce délai.

3) En cas de décision négative, les organismes du secteur public communiquent au demandeur les raisons du refus fondé sur les dispositions applicables du système d'accès en vigueur dans ledit État membre ou sur les dispositions du présent règlement, notamment l'article 32 *decies*, paragraphe 2, points a) à c), et l'article 32 *decies*, paragraphe 3, points a) à d), ou l'article 32 *quindecies* (section de la directive concernant les données ouvertes relative au principe général). En cas de décision négative fondée sur l'article 32 *decies*, paragraphe 3, point d), l'organisme du secteur public fait mention de la personne physique ou morale titulaire des droits, si elle est connue, ou, à défaut, du donneur de licence auprès duquel il a obtenu le document en question. Les bibliothèques, y compris les bibliothèques universitaires, les musées et les archives, ne sont pas tenus d'indiquer cette mention.

4) Les voies de recours incluent la possibilité d'un réexamen réalisé par un organisme de réexamen impartial doté des compétences appropriées, telle que l'autorité nationale de la concurrence, l'autorité pertinente d'accès aux données ou documents, l'autorité de contrôle établie conformément au règlement (UE) 2016/679 ou une autorité judiciaire nationale, dont les décisions sont contraignantes pour l'organisme du secteur public concerné.

5) Aux fins du présent article, les États membres établissent des dispositions pratiques visant à faciliter une réutilisation efficace des données ou des documents. Ces dispositions peuvent inclure, en particulier, les moyens de fournir des informations appropriées sur les droits prévus par le présent règlement et d'offrir une assistance et des conseils pertinents.

6) Le présent article ne s'applique pas aux entités suivantes:

   a) les entreprises publiques;

   b) les établissements d'enseignement, les organismes exerçant une activité de recherche et les organisations finançant une activité de recherche.

Sous-section 3

Conditions applicables à la réutilisation

Article 32 *septdecies*

*Formats disponibles*

1) Sans préjudice de la sous-section 5, les organismes du secteur public et les entreprises publiques mettent leurs données ou leurs documents à disposition dans tout format ou toute langue préexistants et, si possible et s'il y a lieu, sous forme électronique, dans des formats qui sont ouverts, lisibles par machine, accessibles, traçables et réutilisables, en les accompagnant de leurs métadonnées. Tant le format que les métadonnées répondent, autant que possible, à des normes formelles ouvertes.

2) Les États membres encouragent les organismes du secteur public et les entreprises publiques à produire et mettre à disposition des données ou des documents qui relèvent du champ d'application de la présente section conformément au principe d'ouverture dès la conception et par défaut.

3) Le paragraphe 1 n'emporte pas l'obligation pour les organismes du secteur public de créer ou d'adapter des données ou des documents ni de fournir des extraits pour se conformer audit paragraphe, lorsque cela entraîne des efforts disproportionnés dépassant le stade de la simple manipulation.

4) Les organismes du secteur public ne sont pas tenus de poursuivre la production et la conservation d'un certain type de données ou de documents en vue de leur réutilisation par une organisation du secteur privé ou public.

5) Les organismes du secteur public mettent les données dynamiques à disposition aux fins de réutilisation aussitôt qu'elles ont été recueillies, en recourant à des API appropriées et, le cas échéant, sous la forme d'un téléchargement de masse.

6) Lorsque la mise à disposition des données dynamiques aux fins de réutilisation immédiatement après la collecte, comme prévu au paragraphe 5, excéderait les capacités financières et techniques de l'organisme du secteur public, en imposant de ce fait un effort disproportionné, ces données dynamiques sont mises à disposition aux fins de réutilisation dans un délai ou avec des restrictions techniques temporaires qui ne portent pas indûment atteinte à l'exploitation de leur potentiel économique et social.

7) Les paragraphes 1 à 6 s'appliquent à des données ou documents existants détenus par des entreprises publiques qui sont disponibles aux fins de réutilisation.

8) Les ensembles de données de forte valeur, dont la liste est établie conformément à l'article 32 *tervicies*, paragraphe 1, sont mis à disposition à des fins de réutilisation dans des formats lisibles par machine, en recourant à des API appropriées et, le cas échéant, sous la forme d'un téléchargement de masse.

Article 32 *octodecies*

*Principes régissant la tarification en matière de données ouvertes du secteur public*

1) Le coût de la réutilisation des données ou des documents relevant du champ d'application de la présente section est nul. Toutefois, le recouvrement, par l'organisme du secteur public détenant les données, des coûts marginaux occasionnés par la reproduction, la mise à disposition et la diffusion de ces données ou documents, ainsi que par l'anonymisation de données à caractère personnel et les mesures prises pour protéger des informations confidentielles à caractère commercial, peut être autorisé.

2) Le paragraphe 1 ne s'applique pas aux entités suivantes:

a) les organismes du secteur public qui sont tenus de générer des recettes destinées à couvrir une part substantielle des coûts liés à l'accomplissement de leurs missions de service public;

b) les bibliothèques, y compris les bibliothèques universitaires, les musées et les archives;

c) les entreprises publiques.

3) Les États membres publient une liste des organismes du secteur public visés au paragraphe 2, point a).

4) Dans les cas visés au paragraphe 2, points a) et c), le montant total des redevances est calculé conformément à des critères objectifs, transparents et vérifiables. Ces critères sont définis par les États membres. Le total des recettes provenant de la fourniture et des autorisations de réutilisation des données ou des documents pendant la période comptable appropriée ne dépasse pas le coût de leur collecte, de leur production, de leur reproduction, de leur diffusion et du stockage de données, tout en permettant un retour sur investissement raisonnable, ainsi que, le cas échéant, d'anonymisation de données à caractère personnel et de mesures prises pour protéger des informations confidentielles à caractère commercial. Les redevances sont calculées conformément aux principes comptables applicables.

5) Lorsque des redevances sont appliquées par les organismes du secteur public visés au paragraphe 2, point b), le total des recettes provenant de la fourniture et des autorisations de réutilisation des données ou des documents pendant la période comptable appropriée ne dépasse pas le coût de collecte, de production, de reproduction, de diffusion, de stockage de données, de conservation et d'acquisition des droits, ainsi que, le cas échéant, d'anonymisation de données à caractère personnel et de mesures prises pour protéger des informations confidentielles à caractère commercial, tout en permettant un retour sur investissement raisonnable. Les redevances sont calculées conformément aux principes comptables applicables aux organismes du secteur public concernés.

6) Les organismes du secteur public peuvent fixer des redevances plus élevées que celles prévues aux paragraphes 1, 4 et 5 pour la réutilisation des données et des documents par les très grandes entreprises. Ces redevances sont proportionnées et fondées sur des critères objectifs, en tenant compte de la puissance économique ou de la faculté dont dispose l'entité d'acquérir des données, y compris, en particulier, une désignation en tant que contrôleur d'accès en vertu du règlement (UE) 2022/1925. Outre les éléments énumérés au paragraphe 1 du présent article, ces redevances peuvent couvrir les coûts de collecte, de production, de reproduction, de diffusion et de stockage des données et, le cas échéant, d'anonymisation ou de mesures visant à protéger la confidentialité de données ou de documents, tout en permettant un retour sur investissement raisonnable.

7) La réutilisation des éléments suivants est gratuite pour l'utilisateur:

a) sous réserve de l'article 32 *tervicies*, paragraphes 3, 4 et 5, les ensembles de données de forte valeur, dont la liste est établie conformément au paragraphe 1 dudit article;

b) les données de la recherche visées à l'article 32 *decies*, paragraphe 1, point c).

Article 32 *novodecies*

*Licences types*

1) La réutilisation de données ou de documents n'est pas soumise à conditions, à moins que celles-ci ne soient objectives, proportionnées, non discriminatoires et justifiées sur la base d'un objectif d'intérêt général.

2) Lorsque la réutilisation est soumise à conditions, ces conditions ne limitent pas indûment les possibilités de réutilisation et ne sont pas utilisées pour restreindre la concurrence.

3) Dans les États membres où des licences sont utilisées, les organismes du secteur public veillent à ce que des licences types pour la réutilisation de données ou de documents du secteur public, qui peuvent être adaptées à des demandes de licences particulières, soient proposées et utilisables sous forme électronique.

4) Les organismes du secteur public peuvent fixer des conditions particulières pour la réutilisation des données et des documents par les très grandes entreprises. Ces conditions sont proportionnées et fondées sur des critères objectifs. Elles sont établies en tenant compte de la puissance économique ou de la faculté dont dispose l'entité d'acquérir des données, y compris, en particulier, une désignation en tant que contrôleur d'accès en vertu du règlement (UE) 2022/1925.

Article 32 *vicies*

*Modalités pratiques*

1) Les États membres adoptent des dispositions pratiques pour faciliter la recherche de données ou de documents disponibles à des fins de réutilisation, telles que des listes de ressources des données ou documents principaux accompagnés des métadonnées pertinentes, accessibles, dans la mesure du possible et s'il y a lieu, en ligne et sous un format lisible par machine, et des portails liés aux listes de ressources. Dans la mesure du possible, les États membres facilitent la recherche interlinguistique des données ou des documents, notamment en permettant l'agrégation de métadonnées au niveau de l'Union.

Les États membres encouragent également les organismes du secteur public à mettre en œuvre des dispositions pratiques permettant de faciliter la conservation de données ou de documents disponibles à des fins de réutilisation.

2) Les États membres poursuivent, en coopération avec la Commission, les efforts visant à simplifier l'accès aux ensembles de données, en particulier en mettant en place un point d'accès unique et en mettant à disposition, progressivement, des ensembles de données appropriés détenus par des organismes du secteur public, en ce qui concerne les données ou documents auxquels la présente section s'applique, ainsi que des données détenues par des institutions de l'Union, dans des formats accessibles, traçables et réutilisables sous forme électronique.

Sous-section 4

Données de la recherche

Article 32 *unvicies*

*Données de la recherche*

1) Les États membres encouragent la mise à disposition des données de la recherche en adoptant les politiques et en prenant les mesures nécessaires à l'échelon national afin de rendre librement accessibles les données résultant de la recherche financée au moyen de fonds publics ("politiques de libre accès") qui respectent le principe d'ouverture par défaut et sont compatibles avec les principes FAIR. Dans ce

contexte, il y a lieu de tenir compte des préoccupations liées aux droits de propriété intellectuelle, à la protection des données à caractère personnel et à la confidentialité, à la sécurité et aux intérêts commerciaux légitimes dans le respect du principe “aussi ouvert que possible, mais aussi fermé que nécessaire”. Ces politiques de libre accès visent les organismes exerçant une activité de recherche et les organisations finançant une activité de recherche.

2) Sans préjudice de l’article 32 *quindecies*, paragraphe 3, point d), les données de la recherche sont réutilisables à des fins commerciales ou non commerciales, conformément à la section 1 et à la section 2, sous-section 3, dans la mesure où elles sont financées au moyen de fonds publics et où des chercheurs, des organismes exerçant une activité de recherche ou des organisations finançant une activité de recherche les ont déjà rendues publiques par l’intermédiaire d’une archive ouverte institutionnelle ou thématique. À cette fin, il est tenu compte des intérêts commerciaux légitimes, des activités de transmission des connaissances et des droits de propriété intellectuelle préexistants.

Sous-section 5

Ensembles de données de forte valeur

Article 32 *duovicies*

*Catégories thématiques d’ensembles de données de forte valeur*

1) Les catégories thématiques d’ensembles de données de forte valeur sont définies à l’annexe I.

2) La Commission est habilitée à adopter des actes délégués conformément à l’article 45, paragraphe 2 *bis*, afin de modifier l’annexe I en y ajoutant de nouvelles catégories thématiques d’ensembles de données de forte valeur reflétant les progrès technologiques et l’évolution du marché.

Article 32 *tervicies*

*Ensembles de données spécifiques de forte valeur et modalités de publication et de réutilisation*

1) La Commission adopte des actes d’exécution dressant une liste d’ensembles de données de forte valeur particuliers relevant des catégories figurant à l’annexe I et détenus par des organismes du secteur public et des entreprises publiques parmi les données ou les documents auxquels s’applique la présente section.

Ces ensembles de données de forte valeur:

a) sont mis à disposition gratuitement, sous réserve des paragraphes 3, 4 et 5;

b) sont lisibles par machine;

c) sont fournis en recourant à des API; et

d) sont fournis sous la forme d’un téléchargement de masse, le cas échéant.

Ces actes d’exécution peuvent préciser les modalités de publication et de réutilisation d’ensembles de données de forte valeur. Ces modalités sont compatibles avec les licences types ouvertes.

Les modalités peuvent comporter des conditions applicables à la réutilisation, aux formats de données et de métadonnées et aux modalités techniques de diffusion. Les

investissements effectués par les États membres en matière d'approches en ce qui concerne les données ouvertes, tel que les investissements portant sur l'élaboration et la mise en œuvre de certaines normes, sont pris en compte et mis en balance avec les avantages potentiels de l'ajout sur la liste.

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

2) L'identification d'ensembles de données de forte valeur particuliers en vertu du paragraphe 1 est fondée sur l'évaluation de leur aptitude potentielle à:

a) générer des avantages socioéconomiques ou environnementaux importants et des services innovants;

b) bénéficier à un grand nombre d'utilisateurs, notamment des PME et des petites entreprises à moyenne capitalisation;

c) contribuer à générer des recettes; et

d) être associés à d'autres ensembles de données.

Afin d'identifier de tels ensembles de données de forte valeur, la Commission procède à des consultations appropriées, y compris au niveau des experts, effectue une analyse d'impact et veille à la complémentarité avec des actes juridiques existants, tels que la directive 2010/40/UE du Parlement européen et du Conseil, en ce qui concerne la réutilisation de données ou de documents. Cette analyse d'impact comprend une analyse coûts-avantages et une analyse visant à déterminer si la fourniture d'ensembles de données de forte valeur à titre gratuit par des organismes du secteur public qui sont tenus de générer des recettes destinées à couvrir une partie substantielle de leurs coûts liés à l'exécution de leurs missions de service public aurait une incidence importante sur le budget de ces organismes. En ce qui concerne les ensembles de données de forte valeur détenues par des entreprises publiques, l'analyse d'impact prend tout particulièrement en considération le rôle des entreprises publiques dans un environnement économique concurrentiel.

3) Par dérogation au paragraphe 1, deuxième alinéa, point a), les actes d'exécution visés audit paragraphe prévoient que la mise à disposition d'ensembles de données de forte valeur à titre gratuit ne s'applique pas aux ensembles de données de forte valeur particuliers détenus par des entreprises publiques dans le cas où cela entraînerait une distorsion de concurrence sur les marchés pertinents.

4) L'exigence de mise à disposition d'ensembles de données de forte valeur à titre gratuit conformément au paragraphe 1, deuxième alinéa, point a), ne s'applique pas aux bibliothèques, y compris les bibliothèques universitaires, aux musées et aux archives.

5) Si la mise à disposition d'ensembles de données de forte valeur à titre gratuit par des organismes du secteur public qui sont tenus de générer des recettes destinées à couvrir une partie substantielle de leurs coûts liés à l'exécution de leurs missions de service public a une incidence importante sur le budget des organismes concernés, les États membres peuvent exempter ces organismes de l'obligation de mettre à disposition ces ensembles de données de forte valeur à titre gratuit pour une durée n'excédant pas deux ans à compter de l'entrée en vigueur de l'acte d'exécution correspondant adopté conformément au paragraphe 1.

Section 3

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

Article 32 *quatervicies*

*Conditions applicables à la réutilisation*

1) Les organismes du secteur public qui sont compétents en vertu du droit national pour octroyer ou refuser l'accès aux fins de la réutilisation de données ou de documents appartenant à certaines catégories de données protégées rendent publiques les conditions d'autorisation de cette réutilisation et la procédure de demande de réutilisation par l'intermédiaire du point d'information unique visé à l'article 32 *octovicies*. Lorsqu'ils octroient ou refusent l'accès à des fins de réutilisation, ils peuvent être assistés par les organismes compétents visés à l'article 32 *septvicies*, paragraphe 1.

   Les États membres veillent à ce que les organismes du secteur public soient dotés des ressources nécessaires pour se conformer au présent article et à l'article 32 *quinvicies*.

2) La réutilisation des données ou des documents est sans incidence sur le caractère protégé de ces données ou de ces documents et est uniquement autorisée:

   a) dans le respect des droits de propriété intellectuelle;

   b) sans divulgation, à la suite de l'autorisation de réutilisation, de données qui sont considérées comme confidentielles conformément au droit de l'Union ou au droit national en matière de confidentialité commerciale ou de secret statistique, sauf si cette réutilisation est autorisée sur la base du consentement de la personne concernée ou de l'autorisation du détenteur de données conformément au paragraphe 5;

   c) dans le respect du règlement (UE) 2016/679.

3) Pour assurer la préservation du caractère protégé visé au paragraphe 2, les organismes du secteur public peuvent prévoir les exigences suivantes:

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

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

      ii) aient fait l'objet d'autres formes de préparation des données à caractère personnel;

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

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

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

Lorsque la réutilisation est autorisée conformément au premier alinéa, point a), i), la réutilisation des données ou des documents est soumise aux règles relatives aux données ouvertes du secteur public énoncées à la section 2. Cette disposition est sans préjudice de l'article 32 *sexvicies*, qui prévaut en cas de divergence.

Lorsque la réutilisation est autorisée conformément au premier alinéa, points b) et c), les organismes du secteur public imposent des conditions qui préservent l'intégrité du fonctionnement des systèmes techniques de l'environnement de traitement sécurisé utilisé.

4) L'organisme du secteur public se réserve le droit de vérifier le processus, les moyens et tout résultat du traitement de données ou de documents effectué par le réutilisateur afin de préserver l'intégrité de la protection des données ou des documents. Il se réserve également le droit d'interdire l'utilisation des résultats qui contiennent des informations portant atteinte aux droits et aux intérêts de tiers. La décision d'interdire l'utilisation des résultats est transparente et compréhensible par le réutilisateur.

Sauf si le droit national prévoit des garanties spécifiques concernant les obligations de confidentialité applicables en cas de réutilisation de certaines catégories de données protégées, l'organisme du secteur public subordonne la réutilisation des données ou des documents fournis conformément au paragraphe 3 au respect par le réutilisateur d'une obligation de confidentialité interdisant la divulgation de toute information qui compromet les droits et intérêts de tiers et que le réutilisateur peut avoir acquise malgré les garanties mises en place. En cas de réutilisation non autorisée de données à caractère non personnel, le réutilisateur est tenu d'informer sans retard, au besoin avec l'aide de l'organisme du secteur public, les personnes physiques ou morales dont les droits et intérêts peuvent être affectés.

5) Lorsqu'il est impossible d'autoriser la réutilisation des données ou des documents dans le respect des paragraphes 3 et 4, elle est uniquement possible:

a) s'il n'existe pas de base juridique autre que le consentement pour la transmission des données au titre du règlement (UE) 2016/679, moyennant le consentement des personnes concernées;

b) moyennant l'autorisation des détenteurs de données dont les droits et intérêts peuvent être affectés par cette réutilisation.

L'organisme du secteur public met tout en œuvre, conformément au droit de l'Union et au droit national, pour aider les réutilisateurs potentiels à demander le consentement des personnes concernées ou l'autorisation des détenteurs de données dont les droits et intérêts peuvent être affectés par cette réutilisation, lorsque cela est faisable sans charge disproportionnée pour l'organisme du secteur public.

Lorsqu'il fournit cette aide, l'organisme du secteur public peut être assisté par les organismes compétents visés à l'article 32 *septvicies*.

Article 32 *quinvicies*

*Exigences applicables aux transferts de données à caractère non personnel vers des pays tiers par les réutilisateurs*

1) Lorsqu'un réutilisateur a l'intention de transférer à un pays tiers certaines catégories de données protégées à caractère non personnel, il informe l'organisme du secteur public de son intention de transférer ces données ainsi que de la finalité de ce transfert au moment de demander la réutilisation des données. En cas de réutilisation fondée sur l'autorisation du détenteur de données, le réutilisateur informe, au besoin

avec l'aide de l'organisme du secteur public, la personne physique ou morale dont les droits et intérêts peuvent être affectés de cette intention, de la finalité et des garanties appropriées. L'organisme du secteur public n'autorise pas la réutilisation à moins que la personne physique ou morale n'autorise le transfert.

2) Les organismes du secteur public ne transmettent des données confidentielles à caractère non personnel ou des données protégées par des droits de propriété intellectuelle à un réutilisateur qui a l'intention de transférer lesdites données vers un pays tiers autre qu'un pays désigné conformément au paragraphe 7 que si le réutilisateur s'engage contractuellement à:

   a) respecter les obligations imposées conformément aux droits de propriété intellectuelle et au droit de l'Union ou au droit national en matière de confidentialité commerciale ou de secret statistique, même après le transfert des données vers le pays tiers;

   b) admettre la compétence des juridictions de l'État membre de l'organisme du secteur public qui transmet les données en ce qui concerne tout litige lié au respect des droits de propriété intellectuelle et du droit de l'Union ou du droit national en matière de confidentialité commerciale ou de secret statistique.

3) La Commission peut adopter des actes d'exécution établissant des clauses contractuelles types pour le respect des obligations visées au paragraphe 2 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 46, paragraphe 2.

4) Les organismes du secteur public, s'il y a lieu et dans la mesure de leurs capacités, fournissent des conseils et une assistance aux réutilisateurs pour ce qui est de respecter les obligations visées au paragraphe 2.

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

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

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

   c) prévoient un recours juridictionnel effectif.

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

7) Des actes législatifs spécifiques de l'Union peuvent considérer que certaines catégories de données à caractère non personnel détenues par des organismes du secteur public sont hautement sensibles aux fins du présent article, lorsque leur transfert vers des pays tiers peut mettre en péril des objectifs de politique publique de l'Union, tels que la sécurité et la santé publique, ou peut entraîner un risque de réidentification de données anonymisées à caractère non personnel. Lorsqu'un tel acte est adopté, la Commission adopte des actes délégués conformément à l'article 45 afin de compléter le présent règlement en fixant des conditions particulières applicables aux transferts de telles données vers des pays tiers.

Lorsqu'un acte législatif spécifique de l'Union visé au premier alinéa l'exige, de telles conditions particulières peuvent notamment comprendre des conditions applicables au transfert ou des arrangements techniques à cet égard, des limitations en ce qui concerne la réutilisation de données dans des pays tiers ou les catégories de personnes habilitées à transférer ces données vers des pays tiers ou, dans des cas exceptionnels, des restrictions en ce qui concerne les transferts vers des pays tiers.

Le réutilisateur auquel a été accordé le droit de réutiliser des données à caractère non personnel ne peut transférer ces données que vers les pays tiers pour lesquels il est satisfait aux exigences énoncées aux paragraphes 2, 4 et 5.

Article 32 *sexvicies*
*Redevances*

1) Les organismes du secteur public qui autorisent la réutilisation de certaines catégories de données protégées peuvent percevoir des redevances pour autoriser la réutilisation de ces données.

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

3) Les redevances sont calculées sur la base des coûts liés à la conduite de la procédure de demande de réutilisation de certaines catégories de données protégées et limitées aux coûts nécessaires relatifs:

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

   b) à l'acquisition des droits;

   c) à l'anonymisation ou à d'autres formes de préparation des données à caractère personnel et des données commerciales confidentielles conformément à l'article 32 *quatervicies*, paragraphe 3 (conditions applicables à la réutilisation);

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

   e) à l'acquisition du droit d'autoriser la réutilisation conformément à la présente section par des tiers extérieurs au secteur public; et à l'assistance fournie aux réutilisateurs pour obtenir le consentement des personnes concernées et l'autorisation des détenteurs de données dont les droits et intérêts peuvent être affectés par cette réutilisation.

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

5) Les organismes du secteur public peuvent appliquer des redevances plus élevées que celles autorisées conformément aux paragraphes 2 et 3 du présent article à l'égard des très grandes entreprises, sur la base de critères objectifs, en tenant compte de la puissance économique ou de la faculté dont dispose l'entité d'acquérir des données, y compris, en particulier, une désignation en tant que contrôleur d'accès au titre du règlement (UE) 2022/1925. Les redevances ainsi calculées sont proportionnées. Outre les éléments énumérés au paragraphe 3 du présent article, elles peuvent couvrir les coûts de collecte et de production des données, tout en permettant un retour sur investissement raisonnable.

Article 32 *septvicies*

*Organismes compétents*

1) En vue d'effectuer les tâches visées au présent article, chaque État membre désigne un ou plusieurs organismes compétents conformément à l'article 37, paragraphe 1, qui peuvent être compétents pour un secteur particulier mais sont tenus de couvrir collectivement tous les secteurs, pour aider les organismes du secteur public qui octroient ou refusent l'accès aux fins de la réutilisation de certaines catégories de données protégées. Les États membres peuvent soit établir un ou plusieurs nouveaux organismes compétents, soit s'appuyer sur des organismes du secteur public ou sur des services internes d'organismes du secteur public existants qui remplissent les conditions fixées par la présente section.

2) Les organismes compétents peuvent également être habilités à octroyer l'accès aux fins de la réutilisation de certaines catégories de données protégées en application des dispositions du droit de l'Union ou du droit national qui prévoient l'octroi d'un tel accès. Lorsqu'ils octroient ou refusent l'accès à des fins de réutilisation, ces organismes compétents sont soumis aux articles 32 *duodecies*, 32 *quatervicies*, 32 *quinvicies*, 32 *sexvicies* et 32 *novovicies*.

3) Les organismes compétents disposent des ressources juridiques, financières, techniques et humaines suffisantes pour mener à bien les tâches qui leur sont assignées, y compris des connaissances techniques nécessaires pour être en mesure de respecter le droit de l'Union ou le droit national applicable en ce qui concerne les régimes d'accès pour les catégories de données protégées visées à l'article 2, point 54).

4) L'assistance visée au paragraphe 1 consiste notamment, le cas échéant:

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

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

   c) à fournir un soutien technique pour l'anonymisation, la pseudonymisation et les méthodes de préservation de la vie privée à la pointe de la technologie, non seulement pour les données à caractère personnel, mais aussi pour les informations commerciales confidentielles, y compris les secrets d'affaires ou les contenus protégés par des droits de propriété intellectuelle;

   d) à aider les organismes du secteur public, le cas échéant, à fournir une assistance aux réutilisateurs pour demander le consentement des personnes

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

e) à fournir aux organismes du secteur public une assistance lorsqu'il s'agit d'évaluer l'adéquation des engagements contractuels pris par un réutilisateur en vertu de l'article 32 *quinvicies*, paragraphe 2.

Article 32 *octovicies*

*Point d'information unique*

1) Chaque État membre désigne un point d'information unique. Ce point rend facilement accessibles les informations concernant l'application des articles 32 *quatervicies*, 32 *quinvicies* et 32 *sexvicies*.

2) Le point d'information unique est compétent pour recevoir les demandes d'information ou demandes de réutilisation de certaines catégories de données protégées et les transmettre, par des moyens automatisés lorsque cela est possible et opportun, aux organismes du secteur public compétents, ou aux organismes compétents visés à l'article 32 *septvicies*, paragraphe 1, le cas échéant.

3) Le point d'information unique peut comprendre un canal d'information distinct, simplifié et bien documenté pour les PME, les petites entreprises à moyenne capitalisation, les jeunes pousses et les organismes de recherche, afin de répondre à leurs besoins et à leurs capacités en matière de demande de réutilisation des catégories de données visées à l'article 2, point 54.

4) Le point d'information unique met à disposition par voie électronique une liste de ressources consultable contenant un aperçu de toutes les ressources en documents disponibles, y compris, le cas échéant, les ressources en documents qui sont disponibles au niveau des points d'information sectoriels, régionaux ou locaux, avec des informations pertinentes décrivant les données ou documents disponibles, y compris au minimum le format et la taille des données ainsi que les conditions applicables à leur réutilisation.

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

Article 32 *novovicies*

*Procédure relative aux demandes de réutilisation*

1) Sauf si des délais plus courts ont été fixés conformément au droit national, les organismes du secteur public compétents ou les organismes compétents visés à l'article 32 *septvicies*, paragraphe 1, adoptent une décision sur la demande de réutilisation de certaines catégories de données protégées dans un délai de deux mois à compter de la date de réception de la demande.

2) En cas de demandes de réutilisation exceptionnellement détaillées et complexes, ce délai de deux mois peut être prolongé de trente jours au maximum. En pareils cas, les organismes du secteur public compétents ou les organismes compétents visés à l'article 32 *septvicies*, paragraphe 1, informent le demandeur dès que possible de la nécessité d'un délai supplémentaire pour conduire la procédure, ainsi que des raisons qui justifient le retard.

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

19. L'article 38 est remplacé par le texte suivant:

1) «Sans préjudice de tout autre recours administratif ou juridictionnel, les personnes physiques et morales ont le droit d'introduire une réclamation, individuellement ou, le cas échéant, collectivement:

   a) auprès de l'autorité compétente concernée dans l'État membre dans lequel se trouve leur résidence habituelle, leur lieu de travail ou leur établissement, si elles considèrent qu'il a été porté atteinte aux droits que leur confère le présent règlement;

   b) pour toute question relevant du champ d'application du présent règlement, spécifiquement à l'encontre d'un prestataire de services d'intermédiation de données reconnu ou d'une organisation altruiste en matière de données reconnue, auprès de l'autorité compétente concernée pour l'enregistrement des services d'intermédiation de données ou de l'autorité compétente concernée pour l'enregistrement des organisations altruistes en matière de données.

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

3) L'autorité compétente auprès de laquelle la réclamation a été introduite informe l'auteur de la réclamation, conformément au droit national:

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

   b) des recours juridictionnels prévus à l'article 39.».

20. À l'article 40, le paragraphe 6 suivant est inséré:

«6. Le présent article ne s'applique pas au chapitre VII *quater*.».

21. Le titre suivant est inséré après l'article 41:

## «CHAPITRE IX *bis*

## Comité européen de l'innovation dans le domaine des données».

22. L'article 41 *bis* suivant est inséré:

«Article 41 *bis*

*Comité européen de l'innovation dans le domaine des données*

1) Le comité européen de l'innovation dans le domaine des données est institué afin de conseiller et d'assister la Commission dans la coordination du contrôle de l'application du présent règlement et de servir de forum de discussion pour l'élaboration d'une économie européenne fondée sur les données et de politiques en matière de données.

2) Il est composé au moins de représentants des États membres compétents pour les questions liées aux données, des autorités compétentes pour le contrôle de l'application des chapitres II, III, V, VII *bis* et VII *quater* du présent règlement, du comité européen de la protection des données, du Contrôleur européen de la protection des données, de l'ENISA et du représentant de l'UE pour les PME ou d'un représentant désigné par le réseau des représentants des PME. La Commission peut décider d'ajouter des catégories de membres supplémentaires. Lorsqu'elle nomme des experts individuels, la Commission s'efforce de parvenir à un équilibre entre les hommes et les femmes ainsi qu'à un équilibre géographique parmi les membres du groupe.

3) La Commission décide de la composition des différentes formations dans lesquelles le comité exécutera ses missions.

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

23. L'article 42 est remplacé par le texte suivant:

«Article 42

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

1) Le comité européen de l'innovation dans le domaine des données favorise l'application cohérente du présent règlement:

   a) en servant de forum pour des discussions stratégiques sur les politiques en matière de données, la gouvernance des données, les flux internationaux de données et les évolutions transsectorielles importantes pour l'économie européenne fondée sur les données;

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

   c) en facilitant la coopération entre les autorités compétentes par le renforcement des capacités et l'échange d'informations;

   d) en favorisant l'échange d'expériences et de bonnes pratiques entre les États membres dans le domaine de la réutilisation des informations du secteur public, en coopération avec d'autres organes de gouvernance compétents.».

24. L'article 45 est modifié comme suit:

   a) le paragraphe 2 est remplacé par le texte suivant:

   «2. Le pouvoir d'adopter des actes délégués visé à l'article 29, paragraphe 7, à l'article 32 *duovicies*, paragraphe 2, et à l'article 33, paragraphe 2, est conféré à la Commission pour une durée indéterminée.»;

b) le paragraphe 3 est remplacé par le texte suivant:

«3. La délégation de pouvoir visée à l'article 29, paragraphe 7, à l'article 32 *duovicies*, paragraphe 2, et à l'article 33, paragraphe 2, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.»;

c) le paragraphe 6 est remplacé par le texte suivant:

«6. Un acte délégué adopté en vertu de l'article 29, paragraphe 7, de l'article 32 *duovicies*, paragraphe 2, ou de l'article 33, paragraphe 2, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de trois mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de trois mois à l'initiative du Parlement européen ou du Conseil.».

25. L'article 46 est modifié comme suit:

a) au paragraphe 1, la première phrase est remplacée par le texte suivant:

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

b) le paragraphe 1 *bis* suivant est inséré:

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

26. L'article 49 est modifié comme suit:

a) le paragraphe 1 est modifié comme suit:

i) la partie introductive est remplacée par le texte suivant:

«1. Au plus tard le 12 septembre 2028, la Commission procède à une évaluation des chapitres II, III, IV, V, VI, VII et VIII et présente ses principales conclusions dans un rapport au Parlement européen et au Conseil, ainsi qu'au Comité économique et social européen. Cette évaluation porte, en particulier, sur les aspects suivants:»;

ii) le point m) est remplacé par le texte suivant:

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

b) Le paragraphe 2 *bis* suivant est inséré:

«2 *bis*. Au plus tard le [date = entrée en vigueur plus cinq ans], la Commission procède à une évaluation des chapitres VII *bis*, VII *ter* et VII *quater* et présente ses principales conclusions dans un rapport au Parlement européen et au Conseil ainsi qu'au Comité économique et social européen.

Ce rapport porte, en particulier, sur les aspects suivants:

a) l'état des enregistrements de services d'intermédiation de données et le type de services qu'ils proposent;

b) le type d'organisations altruistes en matière de données enregistrées et un aperçu des objectifs d'intérêt général pour lesquels les données sont partagées en vue d'établir des critères clairs à cet égard;

c) le champ d'application et l'incidence sociale et économique du chapitre VII *quater*, section 2, y compris

d) l'importance de l'augmentation de la réutilisation des documents du secteur public auxquels s'applique le chapitre VII *quater*, section 2, en particulier par les PME et les petites entreprises à moyenne capitalisation;

e) l'incidence des ensembles de données de forte valeur;

f) l'interaction entre les dispositions relatives à la protection des données et les possibilités de réutilisation.

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

c) le paragraphe 5 est remplacé par le texte suivant:

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

27. L'annexe I, dont le texte figure à l'annexe II du présent règlement, est ajoutée.

*Article 2*

*Modifications du règlement (UE) 2018/1724*

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

| Événements | Procédures | Résultat escompté, sous réserve d'une évaluation de la demande par l'autorité compétente conformément au droit national, le cas échéant |
|---|---|---|
| Démarrage et gestion d'une entreprise, et cessation d'activité | Notification de l'activité économique, autorisation d'exercer une activité économique, modifications de l'activité économique et cessation de l'activité économique sans procédure d'insolvabilité ou de liquidation, à l'exclusion de l'enregistrement initial d'une activité économique au registre du commerce et hors procédures relatives à la constitution de sociétés ou à tout dépôt de pièces ultérieur par des sociétés au sens de l'article 54, deuxième alinéa, du traité sur le | Accusé de réception de la notification ou de la modification, ou de la demande d'autorisation de l'activité économique |

| | |
|---|---|
| fonctionnement de l'Union européenne | |
| Enregistrement d'un employeur (personne physique) auprès d'un régime obligatoire de pension et d'assurance | Confirmation d'enregistrement ou numéro de sécurité sociale |
| Enregistrement de salariés auprès de régimes obligatoires de pension et d'assurance | Confirmation d'enregistrement ou numéro de sécurité sociale |
| Soumettre une déclaration d'impôt sur les sociétés | Accusé de réception de la déclaration |
| Notification de la fin du contrat de travail d'un salarié au régime de sécurité sociale, à l'exclusion des procédures de licenciement collectif | Accusé de réception de la notification |
| Paiement des cotisations sociales pour les salariés | Reçu ou autre mode de confirmation du paiement des cotisations sociales pour les salariés |
| Enregistrement en tant que prestataire de services d'intermédiation de données | Confirmation de l'enregistrement |
| Enregistrement en tant qu'organisation altruiste en matière de données reconnue dans l'Union | Confirmation de l'enregistrement |

*Article 3*

*Modifications du règlement (UE) 2016/679 (RGPD)*

Le règlement (UE) 2016/679 est modifié comme suit:

1. L'article 4 est modifié comme suit:

(a) au point 1), les phrases suivantes sont ajoutées:

«Les informations relatives à une personne physique ne sont pas nécessairement des données à caractère personnel pour toute autre personne ou entité du simple fait qu'une autre entité peut identifier cette personne physique. Les informations ne revêtent pas de caractère personnel pour une entité donnée lorsque ladite entité ne peut identifier la personne physique à laquelle elles se rapportent, compte tenu des moyens raisonnablement susceptibles d'être utilisés par cette entité. Ces informations ne se muent pas en informations à caractère personnel pour cette entité du simple fait qu'un destinataire ultérieur éventuel dispose de moyens raisonnablement susceptibles d'être utilisés pour identifier la personne physique à laquelle les informations se rapportent.»;

(b) les points suivants sont ajoutés:

«32) “équipement terminal”, un équipement terminal au sens de l’article 1er, point 1), de la directive 2008/63/CE de la Commission;

33) en ce qui concerne les “réseaux de communications électroniques”, la définition de l’article 2, point 1), de la directive (UE) 2018/1972 s’applique;

34) “navigateur internet”, un navigateur internet au sens de l’article 2, point 11), du règlement (UE) 2022/1925;

35) “service de médias”, un service de médias au sens de l’article 2, point 1), du règlement (UE) 2024/1083;

36) “fournisseur de service de médias”, un fournisseur de service de médias au sens de l’article 2, point 2), du règlement (UE) 2024/1083;

37) “interface en ligne”, une interface en ligne au sens de l’article 3, point m), du règlement (UE) 2022/2065;

38) “recherche scientifique”, toute recherche pouvant également soutenir l’innovation, dont le développement technologique et la démonstration. Ces travaux contribuent aux connaissances scientifiques existantes ou appliquent les connaissances existantes de manière inédite, ont pour objet de contribuer à l’accroissement des connaissances et du bien-être généraux de la société et respectent les normes éthiques dans le domaine de recherche concerné. Cela n’exclut pas que la recherche puisse également viser à promouvoir un intérêt commercial.».

2. L’article 5, paragraphe 1, point b), est remplacé par le texte suivant:

«collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d’une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l’intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques est considéré, conformément à l’article 89, paragraphe 1, comme compatible avec les finalités initiales, indépendantes des conditions prévues à l’article 6, paragraphe 4, du présent règlement (limitation des finalités);».

3. L’article 9 est modifié comme suit:

(a) au paragraphe 2, les points suivants sont ajoutés:

«k) le traitement dans le cadre du développement et de l’exploitation d’un système d’IA au sens de l’article 3, point 1), du règlement (UE) 2024/1689 ou d’un modèle d’IA, sous réserve des conditions visées au paragraphe 5;

l) le traitement de données biométriques est nécessaire à la confirmation de l’identité d’une personne concernée (vérification), lorsque les données biométriques ou les moyens nécessaires à la vérification sont sous le seul contrôle de la personne concernée.»;

(b) le paragraphe suivant est ajouté:

«5. Pour le traitement visé au paragraphe 2, point k), des mesures organisationnelles et techniques appropriées sont mises en œuvre pour éviter la collecte et tout autre traitement de catégories particulières de données à caractère personnel. Lorsque, malgré la mise en œuvre de ces mesures, le responsable du traitement constate la présence de catégories particulières de

données à caractère personnel dans les ensembles de données utilisés à des fins d'entraînement, d'essais ou de validation ou dans le système d'IA ou le modèle d'IA, il supprime ces données. Si la suppression de ces données nécessite des efforts disproportionnés, le responsable du traitement protège en tout état de cause ces données de façon efficace et sans retard injustifié afin d'empêcher qu'elles soient utilisées pour produire des sorties ou qu'elles soient divulguées ou mises à la disposition de tiers d'une autre manière.».

4. À l'article 12, le paragraphe 5 est remplacé par le texte suivant:

«5. Aucun paiement n'est exigé pour fournir les informations au titre des articles 13 et 14 et pour procéder à toute communication et prendre toute mesure au titre des articles 15 à 22 et de l'article 34. Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, ou également, lorsqu'il s'agit de demandes au titre de l'article 15, parce que la personne concernée abuse des droits conférés par le présent règlement à des fins autres que la protection de ses données, le responsable du traitement peut:

a) exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées; ou

b) refuser de donner suite à ces demandes.

Il incombe au responsable du traitement de démontrer que la demande est manifestement infondée ou qu'il existe des motifs raisonnables de croire qu'elle est excessive.».

5. À l'article 13, le paragraphe 4 est remplacé par le texte suivant:

«4. Les paragraphes 1, 2 et 3 ne s'appliquent pas lorsque les données à caractère personnel ont été collectées dans le cadre d'une relation claire et circonscrite entre des personnes concernées et un responsable du traitement exerçant une activité sans usage intensif de données et qu'il existe des motifs raisonnables de supposer que la personne concernée dispose déjà des informations visées au paragraphe 1, points a) et c), sauf si le responsable du traitement transmet les données à d'autres destinataires ou catégories de destinataires, les transfère vers un pays tiers, pratique la décision automatisée, y compris le profilage, au sens de l'article 22, paragraphe 1, ou que le traitement est susceptible de comporter un risque élevé pour les droits et libertés des personnes concernées au sens de l'article 35.».

6. À l'article 13, le paragraphe 5 suivant est ajouté:

«5. Lorsque le traitement a lieu à des fins de recherche scientifique et que la fourniture des informations visées aux paragraphes 1, 2 et 3 se révèle impossible ou nécessiterait un effort disproportionné sous réserve des conditions et des garanties visées à l'article 89, paragraphe 1, ou dans la mesure où l'obligation visée au paragraphe 1 du présent article est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement, le responsable du traitement n'est pas tenu de fournir les informations visées aux paragraphes 1, 2 et 3. En pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles.».

7. À l'article 22, les paragraphes 1 et 2 sont remplacés par le texte suivant:

«1. Une décision qui produit des effets juridiques à l'égard d'une personne concernée ou l'affecte de manière significative de façon similaire ne peut être fondée exclusivement sur un traitement automatisé, y compris le profilage, que si cette décision:

a) est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement, que la décision puisse ou non être prise autrement que par des moyens exclusivement automatisés;

b) est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée; ou

c) est fondée sur le consentement explicite de la personne concernée.».

8. L'article 33 est modifié comme suit:

(a) le paragraphe 1 est remplacé par le texte suivant:

«1. En cas de violation de données à caractère personnel susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement la notifie à l'autorité de contrôle compétente conformément à l'article 55 et à l'article 56, dans les meilleurs délais et, si possible, 96 heures au plus tard après en avoir pris connaissance, par l'intermédiaire du guichet unique mis en place en application de l'article 23 *bis* de la directive (UE) 2022/2555. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 96 heures, elle est accompagnée des motifs du retard.»;

(b) le paragraphe suivant est ajouté:

«1 *bis*. Jusqu'à la mise en place du guichet unique en application de l'article 23 *bis* de la directive (UE) 2022/2555, les responsables du traitement continuent de notifier les violations de données à caractère personnel directement à l'autorité de contrôle compétente conformément à l'article 55 et à l'article 56.»;

(c) les paragraphes suivants sont ajoutés:

«6. Le comité élabore et transmet à la Commission une proposition contenant un modèle commun pour la notification d'une violation de données à caractère personnel à l'autorité de contrôle compétente visée au paragraphe 1, ainsi qu'une liste des circonstances dans lesquelles une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique. La proposition est soumise à la Commission dans un délai de [OP: date = neuf mois à compter de la date d'application du présent règlement]. La Commission, après l'avoir dûment examinée, la révise s'il y a lieu et est habilitée à l'adopter au moyen d'un acte d'exécution en conformité avec la procédure d'examen prévue à l'article 93, paragraphe 2.

7. Le modèle et la liste visés au paragraphe 6 sont réexaminés au moins tous les trois ans et, s'il y a lieu, mis à jour. Le comité soumet en temps utile son

évaluation et d'éventuelles propositions de mise à jour à la Commission. La Commission, après les avoir dûment examinées, révise les propositions et est habilitée à adopter les éventuelles mises à jour conformément à la procédure visée au paragraphe 6.»

9. L'article 35 est modifié comme suit:

(a) les paragraphes 4, 5 et 6 sont remplacés par le texte suivant:

«4. Le comité élabore et transmet à la Commission une proposition de liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise en vertu du paragraphe 1.

5. Le comité élabore et transmet à la Commission une proposition de liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise.

6. Le comité élabore et transmet à la Commission une proposition de modèle commun et de méthode commune pour la réalisation d'analyses d'impact relatives à la protection des données.»;

(b) les paragraphes suivants sont insérés:

«6 *bis*. Les propositions relatives aux listes visées aux paragraphes 4 et 5 et au modèle et à la méthode visés au paragraphe 6 sont soumises à la Commission dans un délai de [OP date = 9 mois à compter de la date d'application du présent règlement]. La Commission, après les avoir dûment examinées, les révise s'il y a lieu et est habilitée à les adopter au moyen d'un acte d'exécution en conformité avec la procédure d'examen prévue à l'article 93, paragraphe 2.

6 *ter*. Les listes ainsi que le modèle et la méthode visés au paragraphe 6 *bis* sont réexaminés au moins tous les trois ans et, s'il y a lieu, mis à jour. Le comité soumet en temps utile son évaluation et d'éventuelles propositions de mise à jour à la Commission. La Commission, après les avoir dûment examinées, révise les propositions et est habilitée à adopter les éventuelles mises à jour conformément à la procédure visée au paragraphe 6 *bis*.»

6 *quater* Les listes, établies et rendues publiques par les autorités de contrôle, des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise et des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise restent valables jusqu'à ce que la Commission adopte l'acte d'exécution visé au paragraphe 6 *bis*.».

10. L'article suivant est ajouté:

«Article 41 *bis*

1) La Commission peut adopter des actes d'exécution afin de préciser les moyens et les critères permettant de déterminer si les données résultant de la pseudonymisation ne constituent plus des données à caractère personnel pour certaines entités.

2) Aux fins du paragraphe 1, la Commission:

a) évalue l'état des techniques disponibles;

b) élabore des critères et/ou des catégories permettant aux responsables du traitement et aux destinataires d'évaluer le risque de réidentification à l'égard des destinataires types des données.

3) La mise en œuvre des moyens et des critères définis dans un acte d'exécution est un élément pouvant servir à démontrer que les données ne sauraient conduire à une réidentification des personnes concernées.

4) La Commission associe étroitement le comité européen de la protection des données à la préparation des actes d'exécution. Le comité européen de la protection des données émet un avis sur les projets d'actes d'exécution dans un délai de 8 semaines à compter de la réception du projet de la Commission.

5) Les actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 93, paragraphe 3.».

11. L'article 57, paragraphe 1, est modifié comme suit:

(a) le point k) est supprimé.

12. À l'article 64, paragraphe 1, le point a) est supprimé.

13. À l'article 70, paragraphe 1, le point h) est supprimé.

14. À l'article 70, paragraphe 1, les points suivants sont insérés:

«h *bis*) d'élaborer et de transmettre à la Commission une proposition de liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise et pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise, conformément à l'article 35;

h *ter*) d'élaborer et de transmettre à la Commission une proposition de modèle commun et de méthode commune pour la réalisation d'analyses d'impact relatives à la protection des données, conformément à l'article 35;

h *quater*) d'élaborer et de transmettre à la Commission une proposition contenant un modèle commun pour la notification d'une violation de données à caractère personnel à l'autorité de contrôle compétente, ainsi qu'une liste des circonstances dans lesquelles une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, conformément à l'article 33.».

15. Les articles suivants sont insérés après l'article 88:

«Article 88 *bis*

*Traitement des données à caractère personnel dans l'équipement terminal des personnes physiques*

1) Le stockage de données à caractère personnel, ou l'obtention de l'accès à des données à caractère personnel déjà stockées, dans l'équipement terminal d'une personne physique n'est permis que si cette personne a donné son consentement, conformément au présent règlement.

2) Le paragraphe 1 ne fait pas obstacle au stockage de données à caractère personnel, ou à l'obtention de l'accès à des données à caractère personnel déjà stockées, dans l'équipement terminal d'une personne physique, sur la base du droit de l'Union ou

du droit d'un État membre au sens de l'article 6 et sous réserve des conditions qui y sont énoncées, afin de préserver les objectifs visés à l'article 23, paragraphe 1.

3) Le stockage de données à caractère personnel, ou l'obtention de l'accès à des données à caractère personnel déjà stockées, dans l'équipement terminal d'une personne physique à défaut de consentement, ainsi que leur traitement ultérieur, sont licites dans la mesure où ils sont nécessaires pour:

   a) effectuer la transmission d'une communication électronique par la voie d'un réseau de communications électroniques;

   b) fournir un service expressément demandé par la personne concernée;

   c) créer des informations agrégées sur l'utilisation d'un service en ligne afin de mesurer l'audience de ce service, lorsque cette action est effectuée par le responsable du traitement de ce service en ligne pour son propre usage exclusif;

   d) maintenir ou rétablir la sécurité d'un service fourni par le responsable du traitement et demandé par la personne concernée ou l'équipement terminal utilisé pour la fourniture de ce service.

4) Lorsque le stockage de données à caractère personnel, ou l'obtention de l'accès à des données à caractère personnel déjà stockées, dans l'équipement terminal d'une personne physique est fondé sur le consentement, les dispositions suivantes s'appliquent:

   a) la personne concernée est en mesure de rejeter les demandes de consentement d'une manière simple et compréhensible au moyen d'un bouton à simple clic ou par un moyen équivalent;

   b) si la personne concernée donne son consentement, le responsable du traitement ne présente pas de nouvelle demande de consentement pour la même finalité pendant la période au cours de laquelle le responsable du traitement peut licitement se fonder sur le consentement de la personne concernée;

   c) si la personne concernée rejette une demande de consentement, le responsable du traitement ne présente pas de nouvelle demande de consentement pour la même finalité pendant une période d'au moins six mois.

   Le présent paragraphe s'applique également au traitement ultérieur des données à caractère personnel fondé sur un consentement.

5) Le présent article est applicable à partir du [OP: prière d'insérer la date correspondant à 6 mois après la date d'entrée en vigueur du présent règlement].

Article 88 *ter*

*Indications automatisées et lisibles par machine quant aux choix de la personne concernée en ce qui concerne le traitement de données à caractère personnel dans l'équipement terminal des personnes physiques*

1) Les responsables du traitement veillent à ce que leurs interfaces en ligne permettent aux personnes concernées:

   a) de donner leur consentement par des moyens automatisés et lisibles par machine, pour autant que les conditions applicables au consentement énoncées dans le présent règlement soient remplies;

b) de rejeter une demande de consentement et d'exercer le droit d'opposition conformément à l'article 21, paragraphe 2, par des moyens automatisés et lisibles par machine.

2) Les responsables du traitement respectent les choix effectués par les personnes concernées conformément au paragraphe 1.

3) Les paragraphes 1 et 2 ne s'appliquent pas aux responsables du traitement qui sont des fournisseurs de services de médias lorsqu'ils fournissent un service de médias.

4) Conformément à l'article 10, paragraphe 1, du règlement (UE) nº 1025/2012, la Commission demande à une ou plusieurs organisations européennes de normalisation d'élaborer des normes pour l'interprétation des indications lisibles par machine quant aux choix des personnes concernées.

Les interfaces en ligne de responsables du traitement conformes à des normes harmonisées ou à des parties de normes harmonisées dont les références ont été publiées au *Journal officiel de l'Union européenne* sont présumées conformes aux exigences couvertes par ces normes ou parties de normes visées au paragraphe 1.

5) Les paragraphes 1 et 2 sont applicables à partir du [OP: prière d'insérer la date correspondant à 24 mois après la date d'entrée en vigueur du présent règlement].

6) Les fournisseurs de navigateurs internet qui ne sont pas des PME fournissent les moyens techniques permettant aux personnes concernées de donner leur consentement, de refuser une demande de consentement et d'exercer leur droit d'opposition en vertu de l'article 21, paragraphe 2, par les moyens automatisés et lisibles par machine visés au paragraphe 1 du présent article, en application des paragraphes 2 à 5 du présent article.

7) Le paragraphe 6 est applicable à partir du [OP: prière d'insérer la date correspondant à 48 mois après la date d'entrée en vigueur du présent règlement].

Article 88 *quater*

*Traitement dans le cadre du développement et de l'exploitation de l'IA*

Lorsque le traitement de données à caractère personnel est nécessaire aux intérêts du responsable du traitement dans le cadre du développement et de l'exploitation d'un système d'IA au sens de l'article 3, point 1), du règlement (UE) 2024/1689 ou d'un modèle d'IA, ce traitement peut être réalisé aux fins d'intérêts légitimes au sens de l'article 6, paragraphe 1, point f), du règlement (UE) 2016/679, le cas échéant, à moins que le consentement soit expressément requis par d'autres dispositions du droit de l'Union ou du droit national et à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Ce traitement éventuel fait l'objet de mesures organisationnelles et techniques et de garanties appropriées pour les droits et libertés de la personne concernée, consistant notamment à veiller au respect de la minimisation des données au cours de la phase de sélection des sources et lors de l'entraînement et de l'essai d'un système d'IA ou d'un modèle d'IA, à prévenir la non-divulgation des données conservées de manière résiduelle dans le système d'IA ou le

modèle d'IA, à garantir une transparence renforcée aux personnes concernées et à leur donner le droit inconditionnel de s'opposer au traitement de leurs données à caractère personnel.».

*Article 4*

*Modifications du règlement (UE) 2018/1725*

Le règlement (UE) 2018/1725 est modifié comme suit:

1. L'article 3 est modifié comme suit:

(a) au point 1), les phrases suivantes sont ajoutées:

«Les informations relatives à une personne physique ne sont pas nécessairement des données à caractère personnel pour toute autre personne ou entité du simple fait qu'une autre entité peut identifier cette personne physique. Les informations ne revêtent pas de caractère personnel pour une entité donnée lorsque ladite entité ne peut identifier la personne physique à laquelle elles se rapportent, compte tenu des moyens raisonnablement susceptibles d'être utilisés par cette entité. Ces informations ne se muent pas en informations à caractère personnel pour cette entité du simple fait qu'un destinataire ultérieur éventuel dispose de moyens raisonnablement susceptibles d'être utilisés pour identifier la personne physique à laquelle les informations se rapportent.»;

(b) le point 25) est remplacé par le texte suivant:

«25) en ce qui concerne les "réseaux de communications électroniques", la définition de l'article 2, point 1), de la directive (UE) 2018/1972 s'applique;

(c) les points suivants sont ajoutés:

27) "application mobile": une application mobile au sens de l'article 3, point 2), du règlement (UE) 2016/2102;

28) "interface en ligne": une interface en ligne au sens de l'article 3, point m), du règlement (UE) 2022/2065;

29) "recherche scientifique", toute recherche pouvant également soutenir l'innovation, dont le développement technologique et la démonstration. Ces travaux contribuent aux connaissances scientifiques existantes ou appliquent les connaissances existantes de manière inédite, ont pour objet de contribuer à l'accroissement des connaissances et du bien-être généraux de la société et respectent les normes éthiques dans le domaine de recherche concerné. Cela n'exclut pas que la recherche puisse également viser à promouvoir un intérêt commercial.».

2. L'article 4, paragraphe 1, point b), est remplacé par le texte suivant:

«b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques est considéré, conformément à l'article 13, comme compatible avec les finalités initiales, indépendantes des conditions prévues à l'article 6 du présent règlement (limitation des finalités);».

3. L’article 10 est modifié comme suit:

(a) au paragraphe 2, les points suivants sont ajoutés:

«k) le traitement dans le cadre du développement et de l’exploitation d’un système d’IA au sens de l’article 3, point 1), du règlement (UE) 2024/1689 ou d’un modèle d’IA, sous réserve des conditions visées au paragraphe 4; ;

l) le traitement de données biométriques est nécessaire à la confirmation de l’identité d’une personne concernée (vérification), lorsque les données biométriques ou les moyens nécessaires à la vérification sont sous le seul contrôle de la personne concernée.»;

(b) le paragraphe 4 suivant est ajouté:

«4. Pour le traitement visé au paragraphe 2, point k), des mesures organisationnelles et techniques appropriées sont mises en œuvre pour éviter la collecte et tout autre traitement de catégories particulières de données à caractère personnel. Lorsque, malgré la mise en œuvre de ces mesures, le responsable du traitement constate la présence de catégories particulières de données à caractère personnel dans les ensembles de données utilisés à des fins d’entraînement, d’essais ou de validation ou dans le système d’IA ou le modèle d’IA, il supprime ces données. Si la suppression de ces données nécessite des efforts disproportionnés, le responsable du traitement protège en tout état de cause ces données de façon efficace et sans retard injustifié afin d’empêcher qu’elles soient utilisées pour produire des sorties, divulguées ou mises à la disposition de tiers d’une autre manière.».

4. À l’article 14, le paragraphe 5 est remplacé par le texte suivant:

«5. Aucun paiement n’est exigé pour fournir les informations au titre des articles 15 et 16 et pour procéder à toute communication et prendre toute mesure au titre des articles 17 à 24 et de l’article 35. Lorsque les demandes d’une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, ou également, lorsqu’il s’agit de demandes au titre de l’article 17, parce que la personne concernée abuse des droits conférés par le présent règlement à des fins autres que la protection de ses données, le responsable du traitement peut refuser de donner suite à ces demandes. Il incombe au responsable du traitement de démontrer que la demande est manifestement infondée ou qu’il existe des motifs raisonnables de croire qu’elle est excessive.».

5. à l’article 15, le nouveau paragraphe 5 suivant est ajouté:

«5. Lorsque le traitement a lieu à des fins de recherche scientifique et que la fourniture des informations visées aux paragraphes 1, 2 et 3 se révèle impossible ou nécessiterait un effort disproportionné sous réserve des conditions et des garanties visées à l’article 13, ou dans la mesure où l’obligation visée au paragraphe 1 du présent article est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement, le responsable du traitement n’est pas tenu de fournir les informations visées aux paragraphes 1, 2 et 3. En pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles.».

6. À l'article 24, les paragraphes 1 et 2 sont remplacés par le texte suivant:

«1. Une décision qui produit des effets juridiques à l'égard d'une personne concernée ou l'affecte de manière significative de façon similaire ne peut être fondée exclusivement sur un traitement automatisé, y compris le profilage, que si cette décision:

a) est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement, que la décision puisse ou non être prise autrement que par des moyens exclusivement automatisés;

b) est autorisée par le droit de l'Union auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée; ou

c) est fondée sur le consentement explicite de la personne concernée.».

7. À l'article 34, le paragraphe 1 est remplacé par le texte suivant:

«1. En cas de violation de données à caractère personnel susceptible d'engendrer un risque élevé pour les droits et libertés de personnes physiques, le responsable du traitement la notifie au Contrôleur européen de la protection des données dans les meilleurs délais et, si possible, 96 heures au plus tard après en avoir pris connaissance. Lorsque la notification au Contrôleur européen de la protection des données n'a pas lieu dans les 96 heures, elle est accompagnée des motifs du retard.».

8. À l'article 37, les paragraphes suivants sont ajoutés:

«2. Le stockage de données à caractère personnel, ou l'obtention de l'accès à des données à caractère personnel déjà stockées, dans l'équipement terminal d'une personne physique n'est permis que si cette personne a donné son consentement, conformément au présent règlement.

3. Le paragraphe 1 ne fait pas obstacle au stockage de données à caractère personnel, ou à l'obtention de l'accès à des données à caractère personnel déjà stockées, dans l'équipement terminal d'une personne physique, sur la base du droit de l'Union au sens de l'article 5 et sous réserve des conditions qui y sont énoncées, afin de préserver les objectifs visés à l'article 25, paragraphe 1.

4. Le stockage de données à caractère personnel, ou l'obtention de l'accès à des données à caractère personnel déjà stockées, dans l'équipement terminal d'une personne physique à défaut de consentement, ainsi que leur traitement ultérieur, sont licites dans la mesure où ils sont nécessaires pour:

a) effectuer la transmission d'une communication électronique par la voie d'un réseau de communications électroniques;

b) fournir un service expressément demandé par la personne concernée;

c) créer des informations agrégées sur l'utilisation d'un service en ligne afin de mesurer l'audience de ce service, lorsque cette action est effectuée par le responsable du traitement de ce service en ligne pour son propre usage exclusif;

d) maintenir ou rétablir la sécurité d'un service fourni par le responsable du traitement et demandé par la personne concernée ou l'équipement terminal utilisé pour la fourniture de ce service.

5. Lorsque le stockage de données à caractère personnel, ou l'obtention de l'accès à des données à caractère personnel déjà stockées, dans l'équipement terminal d'une personne physique est fondé sur le consentement, les dispositions suivantes s'appliquent:

a) la personne concernée est en mesure de rejeter les demandes de consentement d'une manière simple et compréhensible au moyen d'un bouton à simple clic ou par un moyen équivalent;

b) si la personne concernée donne son consentement, le responsable du traitement ne présente pas de nouvelle demande de consentement pour la même finalité pendant la période au cours de laquelle le responsable du traitement peut licitement se fonder sur le consentement de la personne concernée;

c) si la personne concernée rejette une demande de consentement, le responsable du traitement ne présente pas de nouvelle demande de consentement pour la même finalité pendant une période d'au moins six mois.

Le présent paragraphe s'applique également au traitement ultérieur des données à caractère personnel fondé sur un consentement.

6. Le présent article est applicable à partir du [OP: prière d'insérer la date correspondant à 6 mois après la date d'entrée en vigueur du présent règlement].

7) Les responsables du traitement veillent à ce que leurs interfaces en ligne permettent aux personnes concernées:

a) de donner leur consentement par des moyens automatisés et lisibles par machine, pour autant que les conditions de consentement énoncées dans le présent règlement soient remplies;

b) de rejeter une demande de consentement par des moyens automatisés et lisibles par machine.

8. Les responsables du traitement respectent les choix effectués par les personnes concernées conformément au paragraphe 7.

9. Les interfaces en ligne de responsables du traitement conformes à des normes harmonisées ou à des parties de normes harmonisées visées à l'article 88 *ter*, paragraphe 4, du règlement (UE) 2016/679 sont présumées conformes aux exigences couvertes par ces normes ou parties de normes visées au paragraphe 7.

10. Les paragraphes 7 à 9 sont applicables à partir du [OP: prière d'insérer la date correspondant à 24 mois après la date d'entrée en vigueur du présent règlement].

8) L'article 39 est modifié comme suit:

a) le paragraphe 4 est remplacé par le texte suivant:

«4. Les listes, le modèle et la méthode adoptés par la Commission et visés à l'article 35, paragraphe 6 *bis*, du règlement (UE) 2016/679 devraient s'appliquer au traitement des données à caractère personnel au titre du présent règlement.»

b) les paragraphes 5 et 6 sont supprimés.

9) L'article suivant est ajouté:

«Article 45 *bis*

Les critères communs adoptés par la Commission et visés à l'article 41 *bis* du règlement (UE) 2016/679 devraient s'appliquer au traitement des données à caractère personnel au titre du présent règlement.».

*Article 5*

*Modifications de la directive 2002/58/CE (directive "vie privée et communications électroniques")*

La directive 2002/58/CE est modifiée comme suit:

1. L'article 4 est supprimé.

2. À l'article 5, paragraphe 3, l'alinéa suivant est ajouté:

«Le présent paragraphe ne s'applique pas si l'abonné ou l'utilisateur est une personne physique et que le stockage des informations ou leur accès constituent un traitement de données à caractère personnel ou y donnent lieu.».

*Article 6*

*Modifications de la directive (UE) 2022/2555*

La directive (EU) 2022/2555 est modifiée comme suit:

1. L'article 23 *bis* suivant est ajouté:

«Article 23 *bis*

*Guichet unique pour le signalement des incidents*

1) L'ENISA crée et gère un guichet unique pour la prise en charge de l'obligation de notifier les incidents et événements connexes en vertu des actes juridiques de l'Union lorsque lesdits actes le prévoient (ci-après le "guichet unique"). Sans préjudice de l'article 16 du règlement (UE) 2024/2847 du Parlement européen et du Conseil, l'ENISA peut faire en sorte que le guichet unique s'appuie sur la plateforme unique de signalement mise en place en vertu dudit règlement.

2) L'ENISA prend des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques pesant sur la sécurité du guichet unique et des informations soumises ou diffusées par l'intermédiaire du guichet unique. L'ENISA tient compte du caractère sensible des informations transmises ou diffusées en vertu des actes juridiques de l'Union visés au paragraphe 1 et veille à ce que les autorités compétentes en vertu de ces actes juridiques de l'Union aient accès aux informations et les traitent selon les exigences de ces actes juridiques de l'Union.

3) L'ENISA fournit et met en œuvre les spécifications relatives aux mesures techniques, opérationnelles et organisationnelles concernant la mise en place, la maintenance et le fonctionnement sécurisé du guichet unique. L'ENISA élabore les spécifications en coopération avec la Commission, le réseau des CSIRT et les autorités compétentes en vertu des actes juridiques de l'Union visés au paragraphe 1. Les spécifications garantissent que:

a) les capacités nécessaires pour assurer l'interopérabilité à l'égard des autres obligations d'information pertinentes visées au paragraphe 1 sont présentes;

b) des dispositions techniques sont prévues pour permettre aux entités et autorités concernées en vertu des actes juridiques de l'Union visés au paragraphe 1 d'accéder aux informations provenant du guichet unique, de les soumettre, de les récupérer, de les transmettre ou, d'une manière générale, de les traiter et comprennent des protocoles et outils techniques qui permettent aux entités et autorités d'effectuer un traitement ultérieur des informations reçues au sein de leurs systèmes;

c) les spécificités des exigences en matière de signalement des incidents énoncées dans les actes juridiques de l'Union visés au paragraphe 1 sont dûment prises en compte;

d) le cas échéant, le guichet unique est interopérable et compatible avec les portefeuilles européens d'identité numérique pour les entreprises visés dans *[la proposition de règlement: insérer le titre de la proposition]* et les portefeuilles européens d'identité numérique pour les entreprises peuvent être utilisés au moins pour identifier et authentifier les entités utilisant le guichet unique;

e) les entités utilisant le guichet unique peuvent récupérer et compléter les informations qu'elles ont précédemment soumises par l'intermédiaire du guichet unique;

f) une notification unique des informations soumises par une entité par l'intermédiaire du guichet unique peut être utilisée pour remplir les obligations de signalement énoncées dans tout autre acte juridique de l'Union qui prévoit le signalement d'incidents au guichet unique.

4) Sauf disposition contraire des actes juridiques de l'Union visés au paragraphe 1 du présent article, l'ENISA n'a pas accès aux notifications soumises par l'intermédiaire du guichet unique.

5) Dans un délai de [18] mois à compter de l'entrée en vigueur du présent règlement, l'ENISA pilote le fonctionnement du guichet unique pour chaque acte juridique de l'Union ajouté, y compris les essais tenant compte des spécificités et des exigences relatives aux notifications énoncées dans chaque acte juridique de l'Union concerné, et après consultation de la Commission et des autorités compétentes concernées en vertu des actes juridiques respectifs de l'Union. L'ENISA ne permet la notification d'incidents au titre de chaque acte juridique de l'Union visé au paragraphe 1 qu'après avoir piloté le fonctionnement et après que la Commission a publié un avis conformément au paragraphe 6.

6) La Commission, en coopération avec l'ENISA, évalue le bon fonctionnement, la fiabilité, l'intégrité et la confidentialité du guichet unique. Si la Commission, après consultation du réseau des CSIRT et des autorités compétentes en vertu des actes juridiques de l'Union visés au paragraphe 1, constate que le bon fonctionnement, la

fiabilité, l'intégrité et la confidentialité du guichet unique sont assurés, elle publie un avis à cet effet au Journal officiel de l'Union européenne.

7) Si la Commission constate, dans son évaluation, que le bon fonctionnement, la fiabilité, l'intégrité ou la confidentialité du guichet unique ne sont pas assurés, l'ENISA prend, en coopération avec la Commission et sans retard injustifié, toutes les mesures correctives nécessaires pour en garantir sans retard le bon fonctionnement, la fiabilité, l'intégrité ou la confidentialité sans retard et informe la Commission des résultats. Ensuite, la Commission réévalue le bon fonctionnement, la fiabilité, l'intégrité ou la confidentialité du guichet unique et publie un avis conformément au paragraphe 6.»

2. L'article 23 est modifié comme suit:

a) au paragraphe 1, la première phrase est remplacée par le texte suivant:

«Chaque État membre veille à ce que les entités essentielles et importantes notifient, sans retard injustifié, à son CSIRT ou, selon le cas, à son autorité compétente, conformément au paragraphe 4 du présent article, tout incident ayant un impact important sur leur fourniture des services visés au paragraphe 3 du présent article (ci-après dénommé "incident important") par l'intermédiaire du guichet unique mis en place en application de l'article 23 *bis*.»;

a) le paragraphe 12 suivant est ajouté:

«Lorsqu'un fabricant notifie un incident grave conformément à l'article 14, paragraphe 3, du règlement (UE) 2024/2847 et que le signalement d'incident au titre dudit article contient des informations pertinentes requises par le paragraphe 4 du présent article, le signalement du fabricant en application de l'article 14, paragraphe 3, du règlement (UE) 2024/2847constitue un signalement d'informations au titre du paragraphe 4 du présent article.».

3. À l'article 30, le paragraphe 1 est remplacé par le texte suivant:

«1. Les États membres veillent à ce que, outre l'obligation de notification prévue à l'article 23, des notifications puissent être transmises à titre volontaire, par l'intermédiaire du guichet unique mis en place en application de l'article 23 *bis*, aux CSIRT ou, s'il y a lieu, aux autorités compétentes par:

a) les entités essentielles et importantes en ce qui concerne les incidents, les cybermenaces et les incidents évités;

b) les entités autres que celles visées au point a), indépendamment du fait qu'elles relèvent ou non du champ d'application de la présente directive, en ce qui concerne les incidents importants, les cybermenaces ou les incidents évités.».

*Article 7*

*Modification du règlement (UE) nº 910/2014*

Le règlement (UE) nº 910/2014 est modifié comme suit:

1. À l'article 19 *bis*, le paragraphe 1 *bis* suivant est ajouté:

«1 *bis*. Les notifications au titre du paragraphe 1, point b), du présent article à l'organe de contrôle et, le cas échéant, à d'autres autorités compétentes concernées sont effectuées par l'intermédiaire du guichet unique mis en place en application de l'article 23 *bis* de la directive (UE) 2022/2555.».

2. À l'article 24, le paragraphe 2 *bis* suivant est ajouté:

«2 *bis*. Les notifications au titre du paragraphe 2, point f *ter*), du présent article à l'organe de contrôle et, le cas échéant, à d'autres organismes compétents concernés sont effectuées par l'intermédiaire du guichet unique mis en place en application de l'article 23 *bis* de la directive (UE) 2022/2555.».

3. À l'article 45 *bis*, le paragraphe 3 *bis* suivant est ajouté:

«3 *bis.* Les notifications au titre du paragraphe 3 à la Commission et à l'organe de contrôle compétent sont effectuées par l'intermédiaire du guichet unique mis en place en application de l'article 23 *bis* de la directive (UE) 2022/2555.».

*Article 8*

*Modifications du règlement (UE) 2022/2554*

L'article 19 du règlement (UE) 2022/2554 est modifié comme suit:

1. au paragraphe 1, le premier alinéa est remplacé par le texte suivant:

«Les entités financières déclarent à l'autorité compétente pertinente visée à l'article 46, par l'intermédiaire du guichet unique mis en place en application de l'article 23 *bis* de la directive (UE) 2022/2555, les incidents majeurs liés aux TIC, conformément au paragraphe 4 du présent article.»;

2. au paragraphe 2, le premier alinéa est remplacé par le texte suivant:

«Les entités financières peuvent notifier, à titre volontaire, par l'intermédiaire du guichet unique mis en place en application de l'article 23 *bis* de la directive (UE) 2022/2555, les cybermenaces importantes à l'autorité compétente concernée lorsqu'elles estiment que la menace est pertinente pour le système financier, les utilisateurs de services ou les clients. L'autorité compétente concernée peut communiquer ces informations à d'autres autorités compétentes conformément au paragraphe 6.».

*Article 9*

*Modifications de la directive (UE) 2022/2557*

L'article 15 de la directive (UE) 2022/2557 est modifié comme suit:

1. au paragraphe 1, la première phrase est remplacée par le texte suivant:

«Les États membres veillent à ce que les entités critiques notifient sans retard injustifié à l'autorité compétente, par l'intermédiaire du guichet unique mis en place en application de l'article 23 *bis* de la directive (UE) 2022/2555, les incidents qui perturbent ou sont susceptibles de perturber de manière importante la fourniture de services essentiels.»;

2. au paragraphe 2, l'alinéa suivant est ajouté:

«La Commission peut adopter des actes d'exécution précisant le type et le format des informations notifiées en application de l'article 15, paragraphe 1. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen prévue à l'article 24, paragraphe 2.».

*Article 10*

*Abrogations et dispositions transitoires*

1. Le règlement (UE) 2019/1150 est abrogé avec effet au [date = date d'application du présent règlement].

2. Par dérogation au paragraphe 1, les dispositions suivantes continuent à s'appliquer jusqu'au 31 décembre 2032:

   (a) article 2, point 1);

   (b) article 2, point 2);

   (c) article 2, point 5);

   (d) article 4;

   (e) article 11;

   (f) article 15.

3. Les actes suivants sont abrogés avec effet au [date alignée sur la date d'application des modifications]:

   a) règlement (UE) 2022/868;

   b) règlement (UE) 2018/1807;

   c) directive (UE) 2019/1024.

4. Les références au règlement (UE) 2022/868, au règlement (UE) 2018/1807 et à la directive (UE) 2019/1024 sont à lire selon le tableau de correspondance figurant à l'annexe I du présent règlement.

*Article 11*

*Dispositions finales*

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

Nonobstant le paragraphe 3, l'article 5, paragraphe 2, entre en application 6 mois après sa publication au Journal officiel de l'Union européenne.

L'article 3, paragraphe 8, points a) à c), les articles 6, paragraphes 2 et 3, et les articles 7 à 9 entrent en application 18 mois après l'entrée en vigueur du présent règlement. Nonobstant la première phrase, lorsque la Commission constate, dans son évaluation effectuée conformément à l'article 23 *bis*, paragraphe 7, de la directive (UE) 2022/2555, que le bon

fonctionnement, la fiabilité, l'intégrité ou la confidentialité du guichet unique ne sont pas assurés, les obligations de signalement par l'intermédiaire du guichet unique énoncées à l'article 23, paragraphe 4, de la directive (UE) 2022/2555, à l'article 19 *bis*, paragraphe 1 *bis*, à l'article 24, paragraphe 2 *bis*, et à l'article 45 *bis*, paragraphe 3 *bis*, du règlement (UE) nº 910/2014, à l'article 33, paragraphe 1, du règlement (UE) 2016/679, à l'article 19, paragraphes 1 et 2, du règlement (UE) 2022/2554 et à l'article 15, paragraphe 1, de la directive (UE) 2022/2557 entrent en application 24 mois après l'entrée en vigueur du présent règlement.

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* |
| *La présidente* | *Le président/La présidente* |

**FICHE FINANCIÈRE ET NUMÉRIQUE LÉGISLATIVE**

## 1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

### 1.1. Dénomination de la proposition/de l'initiative

Proposition de règlement du Parlement européen et du Conseil relatif à la simplification de l'acquis numérique, modifiant le règlement (UE) 2023/2854, le règlement (UE) 2016/679, le règlement (UE) 2024/1689 ainsi que la directive 2002/58/CE et la directive (UE) 2022/2555, et abrogeant le règlement (UE) 2022/868, le règlement (UE) 2018/1807, le règlement (UE) 2019/1150 et la directive (UE) 2019/1024 (règlement omnibus numérique sur l'acquis numérique)

### 1.2. Domaine(s) politique(s) concerné(s)

Réseaux de communication, contenu et technologies;

Marché intérieur, industrie, entrepreneuriat et PME

### 1.3. Objectif(s)

*1.3.1. Objectif général / objectifs généraux*

Simplification de l'application de l'acquis numérique et économies de coûts pour les entreprises

*1.3.2. Objectif(s) spécifique(s)*

Objectif spécifique nº 1

Renforcer la gouvernance et l'application effective de l'acquis numérique en réduisant la complexité des règles, les coûts administratifs pour les entreprises et les administrations, et en abrogeant certains actes législatifs

Objectif spécifique nº 2

Fournir un guichet unique pour le signalement des incidents en vertu de plusieurs cadres juridiques

*1.3.3. Résultat(s) et incidence(s) attendus*

*Préciser les effets que la proposition/l'initiative devrait avoir sur les bénéficiaires/la population visée.*

Réduction des coûts pour les entreprises liée à la diminution de la complexité de la législation et à la rationalisation du signalement

*1.3.4. Indicateurs de performance*

*Préciser les indicateurs permettant de suivre l'avancement et les réalisations.*

Indicateur nº 1

Réductions de coûts calculées pour les entreprises

Indicateur nº 2

Économies de coûts liées au signalement des incidents par les entreprises

Indicateur nº 3

### 1.4. La proposition/l'initiative porte sur:

☐ une action nouvelle

☐ une action nouvelle suite à un projet pilote/une action préparatoire[39]

☒ la prolongation d'une action existante

☐ une fusion ou une réorientation d'une ou de plusieurs actions vers une autre action/une action nouvelle

### 1.5. Justification(s) de la proposition/de l'initiative

*1.5.1. Besoin(s) à satisfaire à court ou à long terme, assorti(s) d'un calendrier détaillé pour la mise en œuvre de l'initiative*

*L'entrée en vigueur est prévue dans un délai de 3 jours à compter de la publication au Journal officiel. L'entrée en application devrait être immédiate, avec des exceptions notables pour les règles qui nécessitent une période transitoire. En ce qui concerne le chapitre III sur le signalement des incidents et les règles relatives aux plateformes, une période suffisante pour la mise en œuvre est requise, adaptée aux besoins des entreprises, des États membres et des organes de l'UE.*

*1.5.2. Valeur ajoutée de l'intervention de l'UE (celle-ci peut résulter de différents facteurs, par exemple gains de coordination, sécurité juridique, efficacité accrue, complémentarités, etc.). Aux fins de la présente section, on entend par «valeur ajoutée de l'intervention de l'UE» la valeur découlant de l'intervention de l'UE qui vient s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres.*

Les raisons de l'action au niveau de l'UE tiennent au fait que les modifications concernent la législation existante de l'UE et réduisent la complexité du droit de l'UE (ex ante)

La valeur ajoutée européenne escomptée (ex post) est la rationalisation du droit de l'UE, ainsi que la réduction de la charge administrative et des coûts pour les entreprises.

Concernant la mise en place du guichet unique pour le signalement des incidents, la valeur ajoutée particulière réside dans la fourniture d'une solution au niveau de l'Union qui réponde à des exigences nationales. Les coûts pour les entreprises sont optimisés par la mise en place d'un point unique, quel que soit le lieu où l'entité déclarante est située dans l'Union et quelles que soient les autorités chargées de recevoir les rapports de signalement.

*1.5.3. Leçons tirées d'expériences similaires*

*Les modifications apportées aux règlements respectifs s'appuient sur l'expérience pratique acquise dans la mise en œuvre des règles, comme indiqué dans le document de travail des services de la Commission qui accompagne la présente proposition. Elles s'appuient sur une vaste consultation des parties prenantes, axée principalement sur l'application quotidienne des règles.*

[39] Tel(le) que visé(e) à l'article 58, paragraphe 2, point a) ou b), du règlement financier.

*1.5.4. Compatibilité avec le cadre financier pluriannuel et synergies éventuelles avec d'autres instruments appropriés*

| |
|---|
| Les modifications sont compatibles avec le cadre financier pluriannuel étant donné qu'aucune dépense supplémentaire n'est prévue. |

*1.5.5. Évaluation des différentes possibilités de financement disponibles, y compris des possibilités de redéploiement*

| |
|---|
| Sans objet. |

**1.6. Durée de la proposition/de l'initiative et de son incidence financière**

5. ☐ durée limitée

☐ En vigueur à partir de/du [JJ/MM]AAAA jusqu'en/au [JJ/MM]AAAA

☐ Incidence financière de AAAA jusqu'en AAAA pour les crédits d'engagement et de AAAA jusqu'en AAAA pour les crédits de paiement.

6. ☒ durée illimitée

Mise en œuvre avec une période de montée en puissance de AAAA jusqu'en AAAA, puis un fonctionnement en rythme de croisière au-delà.

**1.7. Mode(s) d'exécution budgétaire prévu(s)[40]**

7. ☒ **Gestion directe** par la Commission

☒ dans ses services, y compris par l'intermédiaire de son personnel dans les délégations de l'Union;

☐ par les agences exécutives.

8. ☐ **Gestion partagée** avec les États membres

9. ☐ **Gestion indirecte** en confiant des tâches d'exécution budgétaire:

☐ à des pays tiers ou des organismes qu'ils ont désignés

☐ à des organisations internationales et à leurs agences (à préciser)

☐ à la Banque européenne d'investissement et au Fonds européen d'investissement

☐ aux organismes visés aux articles 70 et 71 du règlement financier

☐ à des établissements de droit public

☐ à des entités de droit privé investies d'une mission de service public, pour autant qu'elles soient dotées de garanties financières suffisantes

☐ à des entités de droit privé d'un État membre qui sont chargées de la mise en œuvre d'un partenariat public-privé et dotées de garanties financières suffisantes

☐ à des organismes ou des personnes chargés de l'exécution d'actions spécifiques relevant de la politique étrangère et de sécurité commune, en vertu du titre V du traité sur l'Union européenne, identifiés dans l'acte de base concerné

☐ à des entités établies dans un État membre, régies par le droit privé d'un État membre ou par le droit de l'Union et qui peuvent se voir confier, conformément à la réglementation sectorielle, l'exécution des fonds de l'Union ou des garanties budgétaires, dans la mesure où ces entités sont contrôlées par des établissements de droit public ou par des entités de droit privé investies d'une mission de service public et disposent des garanties financières appropriées sous la forme d'une

[40] Les explications sur les modes d'exécution budgétaire ainsi que les références au règlement financier sont disponibles sur le site BUDGpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

responsabilité solidaire des entités de contrôle ou des garanties financières équivalentes et qui peuvent être, pour chaque action, limitées au montant maximal du soutien de l'Union.

I

## 2. MESURES DE GESTION

### 2.1. Dispositions en matière de suivi et de compte rendu

10. Les modifications feront l'objet d'un suivi dans le cadre de la législation modifiée

### 2.2. Système(s) de gestion et de contrôle

*2.2.1. Justification du (des) mode(s) d'exécution budgétaire, du (des) mécanisme(s) de mise en œuvre du financement, des modalités de paiement et de la stratégie de contrôle proposée*

11. Les systèmes de gestion et de contrôle qui s'appliquent à la législation existante garantissent un contrôle efficace également pour les modifications

*2.2.2. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer*

12. Aucun risque supplémentaire n'a été recensé

| |
|---|
| |

*2.2.3. Estimation et justification du rapport coût/efficacité des contrôles (rapport entre les coûts du contrôle et la valeur des fonds gérés concernés), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)*

13. Le coût des contrôles ne sera pas différent du coût précédent

### 2.3. Mesures de prévention des fraudes et irrégularités

14. Les mêmes mesures préventives continuent de s'appliquer pour les modifications

## 3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

### 3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

Lignes budgétaires existantes

15. Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

| Rubrique du cadre financier pluriannuel | Ligne budgétaire | Nature de la dépense | Participation | | | |
|---|---|---|---|---|---|---|
| | Numéro | CD/CND[41]. | de pays AELE[42] | de pays candidats et pays candidats potentiels[43] | d'autres pays tiers | autres recettes affectées |
| | 20 02 06 Dépenses de gestion | CND | NON | NON | NON | NON |
| | | | | | | |
| | | | | | | |

Nouvelles lignes budgétaires, dont la création est demandée

16. Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

| Rubrique du cadre financier pluriannuel | Ligne budgétaire | Nature de la dépense | Participation | | | |
|---|---|---|---|---|---|---|
| | Numéro | CD/CND | de pays AELE | de pays candidats et pays candidats potentiels | d'autres pays tiers | autres recettes affectées |
| | | | | | | |
| | | | | | | |
| | | | | | | |

[41] CD = crédits dissociés / CND = crédits non dissociés.
[42] AELE: Association européenne de libre-échange.
[43] Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

### 3.2. Incidence financière estimée de la proposition sur les crédits

*3.2.1. Synthèse de l'incidence estimée sur les crédits opérationnels*

☒ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

☐ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après

3.2.1.1. Crédits issus du budget voté

En Mio EUR (à la 3e décimale)

| **Rubrique du cadre financier pluriannuel** | Numéro | |
|---|---|---|

| DG: <…….> | | | Année **2024** | Année **2025** | Année **2026** | Année **2027** | **TOTAL CFP 2021-2027** |
|---|---|---|---|---|---|---|---|
| Crédits opérationnels | | | | | | | |
| Ligne budgétaire | Engagements | (1a) | | | | | **0,000** |
| | Paiements | (2a) | | | | | **0,000** |
| Ligne budgétaire | Engagements | (1b) | | | | | **0,000** |
| | Paiements | (2b) | | | | | **0,000** |
| Crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques[44] | | | | | | | |
| Ligne budgétaire | | (3) | | | | | **0,000** |
| **TOTAL des crédits pour la DG** <…….> | Engagements | =1 a+1b+3 | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |
| | Paiements | =2a+2b+3 | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |

[44] Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

==========

Cette partie est à compléter en utilisant les «données budgétaires de nature administrative», à introduire d'abord dans l'annexe de la fiche financière et numérique législative (annexe 5[45] de la décision de la Commission relative aux règles internes sur l'exécution de la section «Commission» du budget général de l'Union européenne), à charger dans DECIDE pour les besoins de la consultation interservices.

| DG: <…….> | | Année **2024** | Année **2025** | Année **2026** | Année **2027** | **TOTAL CFP 2021-2027** |
|---|---|---|---|---|---|---|
| • Ressources humaines | | 0,000 | 0,000 | 0,000 | 0,000 | **0,000** |
| •Autres dépenses administratives | | 0,000 | 0,000 | 0,000 | 0,000 | **0,000** |
| **TOTAL DG** <…….> | Crédits | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |

| DG: <…….> | | Année **2024** | Année **2025** | Année **2026** | Année **2027** | **TOTAL CFP 2021-2027** |
|---|---|---|---|---|---|---|
| • Ressources humaines | | 0,000 | 0,000 | 0,000 | 0,000 | **0,000** |
| •Autres dépenses administratives | | 0,000 | 0,000 | 0,000 | 0,000 | **0,000** |
| **TOTAL DG** <…….> | Crédits | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |

| | | | | | | |
|---|---|---|---|---|---|---|
| **TOTAL des crédits pour la RUBRIQUE 7 du cadre financier pluriannuel** | (Total engagements = Total paiements) | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |

En Mio EUR (à la 3e décimale)

| | Année | Année | Année | Année | **TOTAL CFP** |
|---|---|---|---|---|---|

[45] Si vous faites état de l'utilisation de crédits de la rubrique 7, vous êtes tenu(e) de remplir l'annexe 5.

| | | 2024 | 2025 | 2026 | 2027 | 2021-2027 |
|---|---|---|---|---|---|---|
| **TOTAL des crédits pour les RUBRIQUES 1 à 7** | Engagements | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |
| du cadre financier pluriannuel | Paiements | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |

3.2.1.2. Crédits issus de recettes affectées externes

En Mio EUR (à la 3e décimale)

| **Rubrique du cadre financier pluriannuel** | Numéro | |
|---|---|---|

| DG: <…….> | | | Année 2024 | Année 2025 | Année 2026 | Année 2027 | **TOTAL CFP 2021-2027** |
|---|---|---|---|---|---|---|---|
| Crédits opérationnels | | | | | | | |
| Ligne budgétaire | Engagements | (1a) | | | | | **0,000** |
| | Paiements | (2a) | | | | | **0,000** |
| Ligne budgétaire | Engagements | (1b) | | | | | **0,000** |
| | Paiements | (2b) | | | | | **0,000** |
| Crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques[46] | | | | | | | |
| Ligne budgétaire | | (3) | | | | | **0,000** |
| **TOTAL des crédits pour la DG** <…….> | Engagements | =1a+1b+3 | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |
| | Paiements | =2a+2b+3 | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |

[46] Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

| Rubrique du cadre financier pluriannuel | 7 | «Dépenses administratives»[47] |
|---|---|---|

En Mio EUR (à la 3e décimale)

| DG: <…….> | | Année **2024** | Année **2025** | Année **2026** | Année **2027** | **TOTAL CFP 2021-2027** |
|---|---|---|---|---|---|---|
| • Ressources humaines | | 0,000 | 0,000 | 0,000 | 0,000 | **0,000** |
| •Autres dépenses administratives | | 0,000 | 0,000 | 0,000 | 0,000 | **0,000** |
| **TOTAL DG** <…….> | Crédits | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |

| DG: <…….> | | Année **2024** | Année **2025** | Année **2026** | Année **2027** | **TOTAL CFP 2021-2027** |
|---|---|---|---|---|---|---|
| • Ressources humaines | | 0,000 | 0,000 | 0,000 | 0,000 | **0,000** |
| •Autres dépenses administratives | | 0,000 | 0,000 | 0,000 | 0,000 | **0,000** |
| **TOTAL DG** <…….> | Crédits | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |

| **TOTAL des crédits pour la RUBRIQUE 7 du cadre financier pluriannuel** | (Total engagements = Total paiements) | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |
|---|---|---|---|---|---|---|

En Mio EUR (à la 3e décimale)

| | Année **2024** | Année **2025** | Année **2026** | Année **2027** | **TOTAL CFP 2021-2027** |
|---|---|---|---|---|---|

[47] Pour déterminer les crédits nécessaires, il convient de recourir aux chiffres relatifs au coût moyen annuel qui sont disponibles sur la page web correspondante de BUDGpedia.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **TOTAL des crédits pour les RUBRIQUES 1 à 7** | Engagements | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |
| du cadre financier pluriannuel | Paiements | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |

*3.2.2. Estimation des réalisations financées à partir des crédits opérationnels (cette section ne doit pas être complétée pour les organismes décentralisés)*

Crédits d'engagement en Mio EUR (à la 3e décimale)

| **Indiquer les objectifs et les réalisations** ⇩ | | | Année **2024** | | Année **2025** | | Année **2026** | | Année **2027** | | Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. section 1.6) | | | | | | **TOTAL** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **RÉALISATIONS (outputs)** | | | | | | | | | | | | | | | | | |
| | Type [48] | Coût moyen | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre total | Coût total |
| OBJECTIF SPÉCIFIQUE nº 1[49]... | | | | | | | | | | | | | | | | | | |
| - Réalisation | | | | | | | | | | | | | | | | | | |
| - Réalisation | | | | | | | | | | | | | | | | | | |
| - Réalisation | | | | | | | | | | | | | | | | | | |
| Sous-total objectif spécifique nº 1 | | | | | | | | | | | | | | | | | | |
| OBJECTIF SPÉCIFIQUE nº 2… | | | | | | | | | | | | | | | | | | |

[48] Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

[49] Tel que décrit dans la section 1.3.2. «Objectif(s) spécifique(s)».

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| - Réalisation | | | | | | | | | | | | | | | | | | |
| Sous-total objectif spécifique nº 2 | | | | | | | | | | | | | | | | | | |
| **TOTAUX** | | | | | | | | | | | | | | | | | | |

*3.2.3. Synthèse de l'incidence estimée sur les crédits administratifs*

☒ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

☐ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après

3.2.3.1. Crédits issus du budget voté

| CRÉDITS VOTÉS | Année 2024 | Année 2025 | Année 2026 | Année 2027 | TOTAL 2021-2027 |
|---|---|---|---|---|---|
| **RUBRIQUE 7** | | | | | |
| Ressources humaines | 0,000 | 0,000 | 0,000 | 0,000 | **0,000** |
| Autres dépenses administratives | 0,000 | 0,000 | 0,000 | 0,000 | **0,000** |
| **Sous-total RUBRIQUE 7** | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |
| **Hors RUBRIQUE 7** | | | | | |
| Ressources humaines | 0,000 | 0,000 | 0,000 | 0,000 | **0,000** |
| Autres dépenses de nature administrative | 0,000 | 0,000 | 0,000 | 0,000 | **0,000** |
| **Sous-total hors RUBRIQUE 7** | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |
| | | | | | |
| **TOTAL** | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |

Les besoins en crédits pour les ressources humaines et les autres dépenses de nature administrative seront couverts par les crédits de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

*3.2.4. Besoins estimés en ressources humaines*

☒ La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

☐ La proposition/l'initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après

3.2.4.1. Financement sur le budget voté

*Estimation à exprimer en équivalents temps plein (ETP)*[50]

17.

| CRÉDITS VOTÉS | Année 2024 | Année 2025 | Année 2026 | Année 2027 |
|---|---|---|---|---|
| **• Emplois du tableau des effectifs (fonctionnaires et agents temporaires)** | | | | |
| 20 01 02 01 (Au siège et dans les bureaux de représentation de la Commission) | 0 | 0 | 0 | 0 |
| 20 01 02 03 (Délégations de l'UE) | 0 | 0 | 0 | 0 |

[50] Veuillez préciser en dessous du tableau combien, sur le nombre d'ETP indiqué, sont déjà affectés à la gestion de l'action et/ou peuvent être redéployés au sein de votre DG, et quels sont vos besoins nets.

| | | | | | |
|---|---|---|---|---|---|
| 01 01 01 01 (Recherche indirecte) | | 0 | 0 | 0 | 0 |
| 01 01 01 11 (Recherche directe) | | 0 | 0 | 0 | 0 |
| Autres lignes budgétaires (à préciser) | | 0 | 0 | 0 | 0 |
| **• Personnel externe (en ETP)** | | | | | |
| 20 02 01 (AC, END de l'«enveloppe globale») | | 0 | 0 | 0 | 0 |
| 20 02 03 (AC, AL, END et JPD dans les délégations de l'UE) | | 0 | 0 | 0 | 0 |
| Ligne d'appui administratif [XX.01.YY.YY] | - au siège | 0 | 0 | 0 | 0 |
| | - dans les délégations de l'UE | 0 | 0 | 0 | 0 |
| 01 01 01 02 (AC, END - Recherche indirecte) | | 0 | 0 | 0 | 0 |
| 01 01 01 12 (AC, END - Recherche directe) | | 0 | 0 | 0 | 0 |
| Autres lignes budgétaires (à préciser) - Rubrique 7 | | 0 | 0 | 0 | 0 |
| Autres lignes budgétaires (à préciser) - Hors rubrique 7 | | 0 | 0 | 0 | 0 |
| **TOTAL** | | **0** | **0** | **0** | **0** |

### *3.2.5. Vue d'ensemble de l'incidence estimée sur les investissements liés aux technologies numériques*

18. Obligatoire: il convient d'indiquer dans le tableau figurant ci-dessous la meilleure estimation des investissements liés aux technologies numériques découlant de la proposition/de l'initiative.

19. À titre exceptionnel, lorsque la mise en œuvre de la proposition/de l'initiative l'exige, les crédits de la rubrique 7 doivent être présentés sur la ligne spécifique.

20. Les crédits des rubriques 1-6 doivent être présentés comme des «Dépenses pour les systèmes informatiques soutenant une politique consacrées aux programmes opérationnels». Ces dépenses correspondent au budget opérationnel à affecter à la réutilisation/à l'achat/au développement de plateformes et d'outils informatiques directement liés à la mise en œuvre de l'initiative et aux investissements qui y sont associés (par exemple, licences, études, stockage de données, etc.). Les informations figurant dans ce tableau doivent être cohérentes avec les données détaillées présentées à la section 4 «Dimensions numériques».

| **TOTAL des crédits numériques et informatiques** | Année **2024** | Année **2025** | Année **2026** | Année **2027** | **TOTAL CFP 2021-2027** |
|---|---|---|---|---|---|
| **RUBRIQUE 7** | | | | | |
| Dépenses informatiques (institutionnelles) | 0,000 | 0,000 | 0,000 | 0,000 | **0,000** |
| **Sous-total RUBRIQUE 7** | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |
| **Hors RUBRIQUE 7** | | | | | |
| Dépenses pour les systèmes informatiques soutenant une politique consacrées aux programmes opérationnels | 0,000 | 0,000 | 0,000 | 0,000 | **0,000** |
| **Sous-total hors RUBRIQUE 7** | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |
| | | | | | |
| **TOTAL** | **0,000** | **0,000** | **0,000** | **0,000** | **0,000** |

*3.2.6. Compatibilité avec le cadre financier pluriannuel actuel*

21. La proposition/l'initiative:

☒ peut être intégralement financée par voie de redéploiement au sein de la rubrique concernée du cadre financier pluriannuel (CFP).

☐ nécessite l'utilisation de la marge non allouée sous la rubrique correspondante du CFP et/ou le recours aux instruments spéciaux comme le prévoit le règlement CFP.

☐ nécessite une révision du CFP.

*3.2.7. Participation de tiers au financement*

22. La proposition/l'initiative:

☒ ne prévoit pas de cofinancement par des tierces parties

☐ prévoit le cofinancement par des tierces parties estimé ci-après:

Crédits en Mio EUR (à la 3e décimale)

| | Année **2024** | Année **2025** | Année **2026** | Année **2027** | Total |
|---|---|---|---|---|---|
| Préciser l'organisme de cofinancement | | | | | |
| TOTAL crédits cofinancés | | | | | |

3.3. Incidence estimée sur les recettes

☒ La proposition/l'initiative est sans incidence financière sur les recettes.

– ☐ La proposition/l'initiative a une incidence financière décrite ci-après:

– ☐ sur les ressources propres

– ☐ sur les autres recettes

– ☐ veuillez indiquer si les recettes sont affectées à des lignes de dépenses

En Mio EUR (à la 3e décimale)

| Ligne budgétaire de recettes: | Montants inscrits pour l'exercice en cours | Incidence de la proposition/de l'initiative[51] | | | |
|---|---|---|---|---|---|
| | | Année **2024** | Année **2025** | Année **2026** | Année **2027** |

[51] En ce qui concerne les ressources propres traditionnelles (droits de douane, cotisations sur le sucre), les montants indiqués doivent être des montants nets, c'est-à-dire des montants bruts après déduction de 20 % de frais de perception.

| | | | | | |
|---|---|---|---|---|---|
| Article ……. | | | | | |

23. Pour les recettes affectées, préciser la(les) ligne(s) budgétaire(s) de dépenses concernée(s).

24. […]

25. Autres remarques (relatives par exemple à la méthode/formule utilisée pour le calcul de l'incidence sur les recettes ou toute autre information).

26. […]

27. 4. DIMENSIONS NUMÉRIQUES

**4.1. Exigences pertinentes en matière numérique**

*Description générale des exigences pertinentes en matière numérique et des catégories connexes (données, numérisation et automatisation des processus, solutions numériques et/ou services publics numériques)*

| **Référence à l'exigence** | **Description de l'exigence** | **Acteurs visés ou concernés par l'exigence** | **Processus généraux** | **Catégories** |
|---|---|---|---|---|
| Article 1er | Modification de l'article 1er, paragraphe 1, du règlement sur les données, élargissant son champ d'application à l'établissement des éléments suivants:<br>• un cadre pour l'enregistrement des services d'intermédiation de données;<br>• un cadre pour l'enregistrement volontaire des entités qui collectent et traitent les données mises à disposition à des fins altruistes;<br>• un cadre pour l'établissement d'un comité européen de l'innovation dans le domaine des données. | Commission européenne<br>Services d'intermédiation de données<br>Entités chargées de la collecte et du traitement des données | Extension du champ d'application du règlement sur les données | Service public numérique |
| Article 1er | Modification de l'article 4, paragraphe 8, et de l'article 5, paragraphe 11, du règlement sur les données. Les détenteurs de données qui refusent de partager des données en vertu de l'exception relative aux secrets | Détenteurs de données (détenteurs de secrets d'affaires)<br>Auteurs des demandes | Notification | Données |

| | | | | |
|---|---|---|---|---|
| | d'affaires sont tenus de notifier dûment cette décision. | d'accès | | |
| Article 1er | Insertion de l'article 15 *bis* dans le règlement sur les données. Obligation de mettre des données à disposition sur le fondement d'une situation d'urgence. | Organisme du secteur public<br>Commission européenne<br>Banque centrale européenne<br>Organe de l'Union<br>Détenteurs de données | Mise à disposition des données | Données |
| Article 1er | Modification de l'article 21, paragraphe 5, du règlement sur les données. Exigences concernant le partage de données obtenues dans le cadre d'une situation d'urgence avec des organismes de recherche ou des organismes statistiques.<br>Insertion de l'article 22 *bis* dans le règlement sur les données, afin de permettre l'introduction de réclamations en ce qui concerne le chapitre V («*Mise à la disposition d'organismes du secteur public, de la Commission, de la Banque centrale européenne et d'organes de l'Union de données sur le fondement d'un besoin exceptionnel*»). | Organisme du secteur public<br>Commission européenne<br>Banque centrale européenne<br>Organe de l'Union<br>Détenteur de données<br>Autorité compétente nationale | Partage des données<br>Plaintes | Données |

| | | | | |
|---|---|---|---|---|
| Article 1er | Modifications de l'article 32, paragraphes 1 à 5, du règlement sur les données concernant l'accès des pays tiers à des données à caractère non personnel. | Fournisseurs des services de traitement de données<br>Prestataires de services d'intermédiation de données<br>Organisations altruistes en matière de données<br>Organismes ou autorités à l'échelon national | Accès international aux données et transfert international des données par les autorités publiques | Données<br>Service public numérique |
| Article 1er | Modification de l'article 35, paragraphe 5, du règlement sur les données, permettant à la Commission d'adopter des spécifications communes en ce qui concerne l'interopérabilité des services de traitement des données. | Fournisseurs des services de traitement de données<br>Commission européenne | Adoption de spécifications communes | Service public numérique |
| Article 1er | Modifications des articles 32 *bis* à 32 *sexies* du règlement sur les données afin d'intégrer le chapitre VII *bis* sur le cadre réglementaire régissant le label européen pour les services d'intermédiation de données, y compris en ce qui concerne la notification, la création d'un registre public, les conditions de prestation de services, la désignation des autorités compétentes et le contrôle de la conformité.<br>Modifications de l'article 32 *nonies* du | Prestataires de services d'intermédiation de données<br>Personnes concernées, détenteurs de données, utilisateurs de données<br>États membres<br>Autorités compétentes<br>Commission européenne | Création du label européen pour les services d'intermédiation de données<br>Établissement du libre flux des données au sein de l'Union européenne | Données<br>Solution numérique<br>Transition numérique des processus<br>Service public numérique |

| | | | | |
|---|---|---|---|---|
| | règlement sur les données afin d'intégrer le chapitre VII *ter* sur le libre flux des données au sein de l'Union, y compris en ce qui concerne l'interdiction des exigences de localisation des données, les obligations de notification à la Commission et la publication d'une liste consolidée. | | | |
| Article 1er | Modifications de l'article 32 *nonies* du règlement sur les données afin d'intégrer le chapitre VII *ter* sur le libre flux des données au sein de l'Union, y compris en ce qui concerne l'interdiction des exigences de localisation des données, les obligations de notification à la Commission et la publication d'une liste consolidée. | États membres<br>Commission européenne | Établissement du libre flux des données au sein de l'Union européenne | Données<br>Transition numérique des processus<br>Service public numérique |
| Article 1er | Insertion de l'article 32 *decies* dans le règlement sur les données, définissant le champ d'application du chapitre VII *quater*. Un ensemble de règles minimales est ainsi établi afin de régir la réutilisation des données et les modalités | États membres<br>Détenteurs de données<br>Utilisateurs de données | Définition de l'objet et du champ d'application<br>Non- | Service public numérique |

| | | | | |
|---|---|---|---|---|
| | pratiques visant à faciliter la réutilisation des données.<br>Insertion de l'article 32 *undecies* dans le règlement sur les données; disposition relative à la non-discrimination en ce qui concerne la réutilisation des données et des documents. | | discrimination | |
| Article 1er | Insertion de l'article 32 *duodecies* dans le règlement sur les données. Règles relatives aux accords d'exclusivité pour la réutilisation des données. Inclut l'obligation de rendre publiques les conditions définitives des accords. | Acteurs potentiels sur le marché<br>Organismes du secteur public<br>Parties à ces accords | | Service public numérique<br>Données |
| Article 1er | Modifications du règlement sur les données:<br>• (41): insertion de l'article 32 *quindecies* sur le principe général de réutilisation des données ouvertes du secteur public<br>• (42): insertion de l'article 32 *sexdecies* relatif au traitement des demandes de réutilisation des données<br>• (43): insertion de l'article 32 *septdecies* sur les formats à utiliser pour la réutilisation des données<br>• (46): insertion de l'article 32 *vicies* | Détenteurs de données<br>Utilisateurs de données<br>États membres (organismes du secteur public)<br>Commission européenne | Règles régissant la réutilisation des données | Service public numérique<br>Données<br>Transition numérique des processus |

| | | | | |
|---|---|---|---|---|
| | sur les modalités pratiques facilitant la recherche de données ou de documents disponibles en vue de leur réutilisation | | | |
| Article 1er | Insertion de l'article 32 *unvicies* dans le règlement sur les données; obligation de faciliter la mise à disposition de données de recherche. | États membres<br>Organismes de recherche<br>Utilisateurs de données | Règles régissant la réutilisation des données | Service public numérique<br>Données |
| Article 1er | Insertion de l'article 32 *duovicies* dans le règlement sur les données. Établissement des modalités relatives à la publication et à la réutilisation d'ensembles de données de forte valeur spécifiques. | Commission européenne<br>Organismes du secteur public, entreprises publiques | Règles régissant la réutilisation des données | Service public numérique<br>Données |
| Article 1er | Insertion de l'article 32 *quatervicies* dans le règlement sur les données. Établissement des conditions applicables à la réutilisation de certaines catégories de données. Les procédures de demande et les conditions régissant l'autorisation de la réutilisation de cette catégorie de données sont mises à la disposition du public par l'intermédiaire du point d'information unique. | Organismes du secteur public<br>Utilisateurs de données | Règles régissant la réutilisation des données | Service public numérique<br>Données |
| Article 1er | Insertion de l'article 32 *quinvicies* dans le règlement sur les données; exigences | Réutilisateurs de données<br>Organismes du secteur | Transfert de données vers | Service public numérique |

| | | | | |
|---|---|---|---|---|
| | applicables aux transferts de données à caractère non personnel vers des pays tiers par les réutilisateurs. | public<br>Personnes physiques/morales dont les droits peuvent être affectés | des pays tiers | Données |
| Article 1er | Modifications du règlement sur les données:<br>• (55): insertion de l'article 32 *septvicies*; mesures organisationnelles relatives aux organismes compétents.<br>• (57): insertion de l'article 32 *novovicies* relatif aux procédures de demande de réutilisation des données.<br>• (58): remplacement de l'article 38, paragraphes 1 et 2, relatif au droit d'introduire une réclamation. | Organismes compétents<br>États membres<br>Organismes du secteur public | Mise en place d'organismes compétents<br>Procédures de demande<br>Plaintes | Service public numérique<br>Données |
| Article 1er | Insertion de l'article 32 *octovicies* dans le règlement sur les données. Imposition de l'utilisation d'un point d'information unique pour faciliter la réutilisation des données. | États membres<br>Détenteurs de données<br>Utilisateurs de données<br>Commission européenne. | Mise en place d'un point d'accès unique | Solutions numériques<br>Service public numérique<br>Transition numérique des processus<br>Données |

| | | | | |
|---|---|---|---|---|
| Article 1er | Modifications apportées aux articles 41 *bis*, 42, 45, 46, 48 *bis*, 49 et 49 *bis* du règlement sur les données afin d'introduire le chapitre IX *bis* établissant le comité européen de l'innovation dans le domaine des données (EDIB) en tant que groupe d'experts chargé de coordonner l'application du règlement et de faciliter le développement d'une économie européenne fondée sur les données, comprenant les exigences en matière de composition, le rôle, la facilitation de la coopération entre les autorités compétentes, et le soutien à une application cohérente des exigences juridiques. | Commission européenne, comité européen de l'innovation dans le domaine des données (EDIB)<br>Représentants des États membres compétents pour la politique en matière d'économie fondée sur les données<br>Autorités compétentes pour l'application des chapitres II, III et V<br>Autorités compétentes pour la réutilisation des informations du secteur public (directive sur les données ouvertes)<br>Autorités compétentes en matière de services d'intermédiation de données<br>Autorités compétentes pour l'enregistrement des organisations altruistes en matière de données<br>Comité européen de la protection des données (EDPB), Contrôleur | Création du comité européen de l'innovation dans le domaine des données (EDIB) | Service public numérique<br>Données |

| | | | | |
|---|---|---|---|---|
| | | européen de la protection des données (CEPD)<br>Agence de l'Union européenne pour la cybersécurité (ENISA)<br>Représentant de l'UE pour les PME ou représentant du réseau des représentants des PME<br>Autres représentants d'organismes compétents dans des secteurs spécifiques<br>Organismes ayant une expertise spécifique<br>Organisations de normalisation<br>Parlement européen, Conseil de l'Union européenne, Comité économique et social européen<br>Prestataires de services d'intermédiation de données<br>Organisations altruistes en matière de données | | |

| | | | | |
|---|---|---|---|---|
| | | qui sont reconnues | | |
| Article 3 | Modification de l'article 33 du règlement (UE) 2016/679 (RGPD), en ce qui concerne les notifications de violations de données à caractère personnel. Imposition, entre autres, de l'utilisation du guichet unique mis en place en vertu de l'article 23 *bis* de la directive (UE) 2022/2555 et prévision de l'utilisation de modèles de notification. | Personnes concernées<br>Responsables du traitement des données<br>Autorités de contrôle<br>Comité européen de la protection des données<br>Commission européenne | Notification | Données |

| | | | | |
|---|---|---|---|---|
| Article 3 | Modification de l'article 35 et de l'article 70, paragraphe 1, du règlement (UE) 2016/679 (RGPD). Obligation pour le comité européen de la protection des données de transmettre à la Commission des propositions en vue de poursuivre la mise en œuvre de certains aspects de l'analyse d'impact relative à la protection des données. Celles-ci comprennent notamment un modèle commun pour ces évaluations. | Comité européen de la protection des données<br>Commission européenne | Propositions du comité transmises à la Commission | Données |
| Article 3 | Insertion de l'article 88 *ter* dans le règlement (UE) 2016/679 (RGPD); les personnes concernées sont en mesure de donner leur consentement/d'exercer leur droit d'opposition par des moyens automatisés et lisibles par machine. Il est prévu que les normes soient élaborées par une ou plusieurs organisations européennes de normalisation. | Personnes concernées<br>Responsables du traitement des données<br>Organisations européennes de normalisation<br>Commission européenne | Indications automatisées et lisibles par machine des choix de la personne concernée | Solutions numériques<br>Automatisation des processus |
| Article 6 | Modification de la directive (UE) 2022/2555 (SRI 2):<br>• (1): insertion d'un article 23 *bis* sur la mise au point et la maintenance d'un guichet unique pour le signalement des incidents;<br>• (3): modification de l'article 23, paragraphe 4, afin de rendre obligatoire l'utilisation du guichet | Notifiants (entités essentielles et importantes)<br>CSIRT/autorités compétentes (selon le cas)<br>Commission européenne<br>ENISA | Notification | Données<br>Solutions numériques<br>Service public numérique |

| | | | | |
|---|---|---|---|---|
| | unique pour les notifications d'incidents graves;<br>• (4): insertion de l'article 23, paragraphe 12, qui garantit que les incidents graves ne sont signalés qu'une seule fois (soit dans le cadre de la directive SRI 2, soit dans le cadre du règlement sur la cyberrésilience);<br>• (5): modification de l'article 30, paragraphe 1, de sorte que le guichet unique puisse être utilisé, sur une base volontaire, pour les notifications effectuées par différentes entités. | | | |
| Article 7 | Modification du règlement (UE) nº 910/2014 (portefeuille européen d'identité numérique) imposant l'utilisation du guichet unique, conformément à l'article 23 *bis* de la directive (UE) 2022/2555, pour:<br>• article 19 *bis*, paragraphe 1 *bis*: les notifications visées au paragraphe 1, point b);<br>• article 24, paragraphe 2 *bis*: les notifications visées au paragraphe 2, point f *ter*); article 45 *bis*, paragraphe 3 *bis*: les notifications visées au paragraphe 3. | Notifiants (prestataires de services de confiance non qualifiés; prestataires de services de confiance qualifiés; fournisseurs d'un navigateur web)<br>Organes de contrôle<br>Autres autorités/organismes compétents concernés<br>Commission européenne | Notification | Données |

| | | | | |
|---|---|---|---|---|
| Article 8 | Modification du règlement (UE) 2022/2554 (DORA) imposant l'utilisation du guichet unique, conformément à l'article 23 *bis* de la directive (UE) 2022/2555, pour:<br>• article 19, paragraphe 1: les incidents majeurs liés aux TIC;<br>• article 19, paragraphe 2: les notifications volontaires de cybermenaces importantes. | Notifiants (entités financières)<br>Organes de contrôle<br>Autres autorités/organismes compétents concernés<br>Commission européenne<br>ENISA | Notification | Données |
| Article 9 | Modification de la directive (UE) 2022/2557 (CER) imposant l'utilisation du guichet unique, conformément à l'article 23 *bis* de la directive (UE) 2022/2555, pour:<br>• article 15, paragraphe 1: les incidents qui perturbent ou sont susceptibles de perturber de manière importante la fourniture de services essentiels. | Notifiants (entités critiques)<br>Organes de contrôle<br>Autres autorités/organismes compétents concernés<br>Commission européenne<br>ENISA | Notification | Données |

**4.2. Données**

*Description générale des données relevant du champ d'application*

| **Type de données** | **Référence à la ou aux exigences** | **Norme et/ou spécification (le cas échéant)** |
|---|---|---|
| Refus d'une demande d'accès à des données fondé sur l'exception relative aux secrets d'affaires (*et notification de ce refus à l'autorité compétente*) | Article 1er | Refus à dûment justifier sur la base d'éléments objectifs. |
| Données à mettre à disposition dans le cadre d'une situation d'urgence | Article 1er | Inclusion des métadonnées nécessaires à l'interprétation et à l'utilisation des données. Dans le cas de données à caractère personnel, pseudonymisation dans la mesure du possible. |
| Notification de l'intention de mettre des données à disposition dans le cadre d'une situation d'urgence | Article 1er | Indication de l'identité et des coordonnées de l'organisation ou de la personne qui reçoit les données, de la finalité de la transmission ou de la mise à disposition des données, de la période pendant laquelle les données doivent être utilisées et des mesures techniques de protection et d'organisation qui ont été prises. |
| Réclamations dans le cadre du chapitre V («*Mise à la disposition d'organismes du secteur public, de la Commission, de la Banque centrale européenne et d'organes de l'Union de données sur le fondement d'un besoin exceptionnel*») | Article 1er | // |
| Données à caractère non personnel détenues dans l'Union européenne | Article 1er | // |

| | | |
|---|---|---|
| Données à fournir en réponse à une demande de réutilisation des données | Article 1er | Fourniture du volume minimal de données admissible. |
| Notification de la demande de réutilisation des données sur le point d'être acceptée | Article 1er | // |
| Données pour lesquelles des services d'intermédiation sont fournis (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er | Format reçu de la personne concernée/du détenteur de données. Conversions uniquement pour améliorer l'interopérabilité ou se conformer aux normes internationales/européennes en matière de données |
| Informations sur les utilisations et les conditions d'utilisation des données (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er | Informations à fournir de manière concise, transparente, intelligible et aisément accessible. |
| Demandes d'enregistrement dans le registre public de l'Union et modifications des informations communiquées (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er | Établissement des formulaires de demande nécessaires par les autorités compétentes. |
| Demandes d'enregistrement acceptées à ajouter au registre public de l'Union (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er | // |
| Notification des modifications ultérieures apportées aux informations fournies au cours de la procédure de demande (label européen pour les services d'intermédiation de données et les organisations | Article 1er | // |

| | | |
|---|---|---|
| altruistes en matière de données) | | |
| Réception de la notification de modifications ultérieures (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er | // |
| Informations fournies aux personnes concernées/détenteurs de données avant le traitement (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er | // |
| Consentement (ou retrait du consentement) pour le traitement de données par une organisation altruiste en matière de données reconnue (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er | À obtenir par voie électronique |
| Informations sur la juridiction du pays tiers dans lequel l'utilisation des données est prévue | Article 1er | // |
| Notification des transferts, accès ou utilisation non autorisés de données à caractère non personnel (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er | // |
| Informations aux fins du contrôle de la conformité (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er | Les demandes doivent être proportionnées et motivées |

| | | |
|---|---|---|
| Notification de non-conformité (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er | // |
| Décision de révoquer le droit d'utilisation du label (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er | // |
| Projets d'actes relatifs aux exigences en matière de localisation des données | Article 1er | // |
| Conditions définitives des accords d'exclusivité | Article 1er | // |
| Données (et/ou notifications) relatives à une demande de réutilisation | Article 1er | Dans tout format ou toute langue préexistants et, si possible et s'il y a lieu, sous forme électronique, dans des formats qui sont ouverts, lisibles par machine, accessibles, traçables et réutilisables, en les accompagnant de leurs métadonnées. |
| Données de la recherche financée par des fonds publics | Article 1er | Disponibles de manière ouverte, selon le principe «ouvert par défaut», et compatibles avec les principes FAIR. |
| Ensembles de données de forte valeur spécifiques | Article 1er | Disponibles sans frais; lisibles par machine; fournies via une API et sous la forme d'un téléchargement de masse (le cas échéant). Les actes d'exécution suivront; ceux-ci peuvent inclure des formats de données et de métadonnées. |

| | | |
|---|---|---|
| Conditions applicables aux fins de l'autorisation de la réutilisation de données ou de documents visés à l'article 2, point 54) | Article 1er | Accessibles au public. |
| Notification de réutilisation non autorisée de données à caractère non personnel | Article 1er | // |
| Notification de l'intention de transférer des données à caractère non personnel vers un pays tiers et finalité de ce transfert (*à l'organisme du secteur public*) | Article 1er | // |
| Notification de l'intention de transférer des données à caractère non personnel vers un pays tiers, finalité de ce transfert et garanties appropriées (*à la personne physique ou morale dont les droits et intérêts peuvent être affectés*) | Article 1er | // |
| Toutes les informations pertinentes concernant l'application des articles 32 *septvicies* [conditions de réutilisation], 32 *octovicies* [pays tiers] et 32 *novovicies* [redevances] du règlement sur les données. | Article 1er | Disponibles et aisément accessibles par l'intermédiaire d'un point d'information unique. |
| Réclamation déposée par des personnes physiques/morales en cas de violation de leurs droits en vertu du règlement sur les données ou en ce qui concerne d'autres questions pertinentes | Article 1er | // |
| Informations sur l'état d'avancement des procédures/recours juridictionnels liés à une | Article 1er | // |

| | | |
|---|---|---|
| réclamation introduite au titre du règlement sur les données | | |
| Données sur l'expérience acquise et les bonnes pratiques (EDIB) | Article 1er | // |
| Évaluation des chapitres II, III, IV, V, VI, VII et VIII du règlement sur les données<br>Évaluation des chapitres VII *bis*, VII *ter* et VII *quater* du règlement sur les données | Article 1er<br>Article 1er | Des exigences relatives au contenu minimal des rapports sont prévues. |
| Notifications des violations de données à caractère personnel | Article 3 | Par l'intermédiaire (et donc dans le respect des spécifications) du guichet unique établi conformément à l'article 23 *bis* de la directive (UE) 2022/2555.<br>Le comité européen de la protection des données élabore une proposition de modèle commun (*voir l'entrée suivante*). |
| Proposition du comité européen de la protection des données relative à un modèle commun pour la notification des violations de données | Article 3 | // |
| Propositions du comité européen de la protection des données concernant l'analyse d'impact relative à la protection des données | Article 3 | // |
| Rapports sur les incidents importants conformément à la directive SRI 2 | Article 6 | Par l'intermédiaire (et donc dans le respect des spécifications) du guichet unique établi conformément à l'article 23 *bis* de la directive (UE) |

| | | |
|---|---|---|
| | | 2022/2555. |
| Notifications des violations de données à caractère personnel | Article 3 | Par l'intermédiaire (et donc dans le respect des spécifications) du guichet unique établi conformément à l'article 23 *bis* de la directive (UE) 2022/2555. |
| Notifications d'incidents majeurs liés aux TIC conformément au règlement DORA; notifications volontaires de cybermenaces importantes conformément au règlement DORA | Article 8 | Par l'intermédiaire (et donc dans le respect des spécifications) du guichet unique établi conformément à l'article 23 *bis* de la directive (UE) 2022/2555. |
| Notifications d'incidents qui perturbent ou sont susceptibles de perturber de manière importante la fourniture de services essentiels, conformément à la directive CER | Article 9 | Par l'intermédiaire (et donc dans le respect des spécifications) du guichet unique établi conformément à l'article 23 *bis* de la directive (UE) 2022/2555. |

**Alignement sur la stratégie européenne pour les données**

*Expliquer comment la ou les exigences sont alignées sur la stratégie européenne pour les données*

Les modifications apportées au règlement sur les données introduisent l'EDIB (chapitre IX *bis*), chargé de coordonner l'application des règles et d'élaborer des lignes directrices pour les espaces européens communs sectoriels de données; les labels européens pour les services d'intermédiation de données et les organisations altruistes en matière de données (chapitre VII *bis*), qui créent un écosystème fiable pour le partage des données et la protection des droits mise en place; le chapitre VII *ter*, qui met en œuvre le libre flux des données à caractère non personnel en interdisant les exigences injustifiées en matière de localisation des données; le chapitre VII *quater*, qui rationalise les règles relatives à la réutilisation des données du secteur public, en fusionnant les dispositions de la directive sur les données ouvertes et du règlement sur la gouvernance des données; les règles relatives aux transferts internationaux de données, qui renforcent la souveraineté numérique européenne en protégeant les données contre tout accès non autorisé par des pays tiers; enfin, des exemptions pour les PME ainsi que la présence du représentant de l'UE pour les PME au sein de l'EDIB, qui garantissent que l'économie fondée sur les données est également plus accessible aux petites entreprises.

**Alignement sur le principe «une fois pour toutes»**

*Expliquer comment le principe «une fois pour toutes» a été pris en considération et de quelle manière la possibilité de réutiliser des données existantes a été étudiée*

Les modifications apportées soutiennent le principe «une fois pour toutes» en créant des infrastructures permettant une réutilisation efficace des données: l'EDIB élabore des normes d'interopérabilité dans l'ensemble des espaces européens communs des données afin de réduire les doublons dans la communication des données; les services d'intermédiation de données agissent en tant qu'intermédiaires de confiance permettant le partage sécurisé des données existantes, en éliminant des collectes redondantes; les organisations altruistes en matière de données facilitent le partage volontaire de données dans l'intérêt public, en mettant à disposition des données réutilisables pour la recherche et les services publics; les dispositions relatives au libre flux des données empêchent les barrières exigeant un stockage en double aux différents endroits; et les garanties relatives aux transferts internationaux préservent l'accessibilité des données par-delà les frontières tout en maintenant les mesures de protection, permettant ainsi collectivement aux particuliers et aux entreprises de fournir leurs données une seule fois, sachant que les besoins ultérieurs auront été satisfaits au moyen de mécanismes de partage sécurisés et respectueux des droits. Dans le même temps, les dispositions relatives au guichet unique permettent également d'appliquer le principe «une fois pour toutes» en ce qui concerne le signalement des incidents.

*Expliquer comment les données nouvellement créées sont faciles à trouver, accessibles, interopérables et réutilisables, et répondent à des normes de qualité élevée*

Les modifications apportées garantissent que les données nouvellement créées respectent les principes FAIR ainsi que les normes de qualité au moyen de mécanismes coordonnés: l'EDIB élabore des spécifications techniques communes ainsi que des protocoles d'interopérabilité accessibles entre les espaces de données sectoriels; les dispositions relatives au libre flux des données empêchent une fragmentation qui nuit à la qualité des données; le rôle de coordination de l'EDIB peut permettre une mise en œuvre harmonisée des normes relatives aux métadonnées, des exigences techniques et des critères de qualité dans l'ensemble des États membres.

**Flux de données**

*Description générale des flux de données*

*NB: la plupart des flux de données détaillés ci-dessous sont des flux préexistants qui sont déplacés d'un règlement à un autre. En effet, les dispositions du règlement sur la gouvernance des données sont transférées vers le règlement sur les données.*

| **Type de données** | **Référence(s) à l'exigence ou aux exigences** | **Acteurs qui fournissent les données** | **Acteurs qui reçoivent les données** | **Déclencheur de l'échange de données** | **Fréquence (le cas échéant)** |
|---|---|---|---|---|---|
| Refus d'une demande d'accès à des données fondé sur l'exception relative aux secrets d'affaires (*et notification de ce refus à l'autorité compétente*) | Article 1er<br>*Modification de l'article 4, paragraphe 8, et de l'article 5, paragraphe 11, du règlement sur les données* | Détenteur de données | Utilisateur des données (auteur de la demande); l'autorité compétente désignée conformément à l'article 37 | Refus d'une demande d'accès à des données fondé sur l'exception relative aux secrets d'affaires | Ad hoc |
| Données à mettre à disposition dans le cadre d'une situation d'urgence | Article 1er<br>*Insertion de l'article 15 bis dans le règlement sur les données* | Détenteur de données | Organisme du secteur public; Commission européenne; Banque centrale européenne; organe de l'Union | Situation d'urgence + demande d'accès aux données remplissant les conditions nécessaires | Ad hoc |
| Notification de l'intention de mettre des données à disposition dans le cadre d'une situation d'urgence | Article 1er<br>*Modification de l'article 21, paragraphe 5, du règlement sur les données* | Organisme du secteur public; Commission européenne; Banque centrale européenne; organe de l'Union | Détenteur des données auprès duquel les données reçues ont été demandées | Situation d'urgence + intention de transmettre ou mettre à disposition des données | Ad hoc |
| Réclamations dans le cadre du chapitre V («Mise à la | Article 1er<br>*Insertion de* | Détenteur de données; | Autorité compétente de | Lorsqu'un litige survient concernant | Ad hoc |

| | | | | | |
|---|---|---|---|---|---|
| disposition d'organismes du secteur public, de la Commission, de la Banque centrale européenne et d'organes de l'Union de données sur le fondement d'un besoin exceptionnel») | *l'article 22 bis dans le règlement sur les données* | organisme du secteur public; Commission européenne; Banque centrale européenne; organe de l'Union | l'État membre dans lequel le détenteur de données est établi | une demande de données au titre de l'article 15 *bis* du règlement sur les données | |
| Données à caractère non personnel détenues dans l'Union européenne | Article 1er<br>*Modification de l'article suivant du règlement sur les données:*<br>*article 32, paragraphes 1, 3 et 4* | Fournisseurs de services de traitement de données, prestataires de services d'intermédiation de données, organisations altruistes en matière de données | Juridictions des pays tiers,<br>autorités administratives des pays tiers, clients (détenteurs de données/personnes concernées) | Demande d'un pays tiers fondée sur un accord international, demande d'un pays tiers remplissant les conditions énoncées à l'article 32, paragraphe 3, demande d'accès du client à ses propres données | Ad hoc |
| Données à fournir en réponse à une demande de réutilisation des données | Article 1er<br>*Modification de l'article 32, paragraphes 4 et 5, du règlement sur les données* | Prestataire de services d'intermédiation de données ou organisation altruiste en matière de données reconnue | L'autorité d'origine de la demande de réutilisation des données (autorité du pays tiers) | Acceptation de la demande de réutilisation des données | Ad hoc |

| | | | | | |
|---|---|---|---|---|---|
| Notification de la demande de réutilisation des données sur le point d'être acceptée | Article 1er<br>*Modification de l'article 32, paragraphes 4 et 5, du règlement sur les données* | Prestataire de services d'intermédiation de données ou organisation altruiste en matière de données reconnue | Client | Acceptation de la demande de réutilisation émanant de l'autorité d'un pays tiers (*sauf si la demande sert des fins répressives*) | Ad hoc |
| Informations à publier dans les registres publics (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er<br>*Insertion de l'article 32 bis dans le règlement sur les données* | Commission européenne | Public | Des informations sur les services d'intermédiation de données reconnus ou les organisations altruistes en matière de données reconnues deviennent disponibles ou doivent être modifiées | Régulière (registre régulièrement mis à jour) |
| Données pour lesquelles des services d'intermédiation sont fournis (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er<br>*Insertion de l'article 32 quater dans le règlement sur les données* | Personnes concernées<br>Détenteurs de données | Utilisateur de données (via un prestataire de services d'intermédiation de données) | Consentement de la personne concernée<br>Autorisation du détenteur de données<br>Demande de l'utilisateur de données | Conformément à l'accord/au contrat conclu entre les parties |

| | | | | | |
|---|---|---|---|---|---|
| Informations sur les utilisations et les conditions d'utilisation des données (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er<br>*Insertion de l'article 32 quater dans le règlement sur les données* | Prestataire de services d'intermédiation de données | Personnes concernées | Avant que la personne concernée ne donne son consentement à l'utilisation des données | Chaque fois avant la demande de consentement |
| Demandes d'enregistrement dans le registre public de l'Union et modifications des informations communiquées (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er<br>*Insertion de l'article 32 sexies dans le règlement sur les données* | Prestataires de services d'intermédiation de données<br>Organisations altruistes en matière de données | Autorité compétente de l'État membre de l'établissement principal | Demande | Ad hoc |
| Demandes d'enregistrement acceptées à ajouter au registre public de l'Union (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er<br>*Insertion de l'article 32 sexies dans le règlement sur les données* | Autorité compétente | Commission européenne | Demande approuvée | Ad hoc (dans un délai de 12 semaines à compter de la réception de la demande, pour autant que la décision soit positive) |
| Notification des modifications ultérieures apportées aux informations fournies au cours de | Article 1er<br>*Insertion de* | Entités enregistrées | Autorité compétente | Modifications apportées aux informations fournies | Ad hoc |

| | | | | | |
|---|---|---|---|---|---|
| la procédure de demande (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | *l'article 32 sexies dans le règlement sur les données* | | | ou lorsque les entités cessent leurs activités dans l'Union | |
| Réception de la notification de modifications ultérieures (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er<br>*Insertion de l'article 32 sexies dans le règlement sur les données* | Autorité compétente | Commission européenne | Notification des modifications par les entités enregistrées (voir entrée ci-dessus) | Ad hoc, sans délai |
| Informations fournies aux personnes concernées/détenteurs de données avant le traitement (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er<br>*Insertion de l'article 32 septies dans le règlement sur les données* | Organisation altruiste en matière de données reconnue | Personnes concernées<br>Détenteurs de données | Avant tout traitement de leurs données | Avant chaque activité de traitement (doivent être claires et facilement compréhensibles) |
| Consentement (ou retrait du consentement) pour le traitement des données par une organisation altruiste en matière de données reconnue (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er<br>*Insertion de l'article 32 septies dans le règlement sur les données* | Personnes concernées<br>Détenteurs de données (si données à caractère non personnel) | Organisation altruiste en matière de données | Consentement de la personne concernée/autorisation du détenteur de données nécessaire pour les activités de traitement | Lors du consentement/de l'octroi de l'autorisation, avec possibilité de retrait à tout moment |
| Informations sur la juridiction du | Article 1er | Organisation | Détenteurs de | Lorsque l'organisation | Ad hoc |

| | | | | | |
|---|---|---|---|---|---|
| pays tiers dans lequel l'utilisation des données est prévue | *Insertion de l'article 32 septies dans le règlement sur les données* | altruiste en matière de données | données | altruiste en matière de données facilite le traitement des données par des tiers | |
| Notification des transferts, accès ou utilisation non autorisés de données à caractère non personnel (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er<br>*Insertion de l'article 32 septies dans le règlement sur les données* | Organisation altruiste en matière de données | Détenteurs de données | Action non autorisée | Ad hoc, sans délai |
| Informations aux fins du contrôle de la conformité (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er<br>*Insertion de l'article 32 octies dans le règlement sur les données* | Prestataires de services d'intermédiation de données<br>Organisations altruistes en matière de données | Autorités compétentes | Demande de l'autorité compétente<br>Demande d'une personne physique ou morale | Ad hoc (sur demande, laquelle doit être proportionnée et motivée) |
| Notification de non-conformité (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er<br>*Insertion de l'article 32 octies dans le règlement sur les données* | Autorité compétente | Entité jugée non conforme | L'autorité compétente constate la non-conformité d'un prestataire de services d'intermédiation de données reconnu ou d'une organisation altruiste en matière de | Ad hoc (avec possibilité ultérieure pour l'entité d'exprimer son point de vue dans un délai de 30 jours) |

| | | | | | |
|---|---|---|---|---|---|
| | | | | données reconnue | |
| Décision de révoquer le droit d'utilisation du label (label européen pour les services d'intermédiation de données et les organisations altruistes en matière de données) | Article 1er<br><br>*Insertion de l'article 32 octies dans le règlement sur les données* | Autorité compétente | Public | À la suite de la décision de révocation du label | Ad hoc |
| Projets d'actes relatifs aux exigences en matière de localisation des données | Article 1er | États membres | Commission européenne | Création d'un projet d'acte introduisant une nouvelle exigence en matière de localisation des données ou apportant des modifications à une exigence existante en matière de localisation des données | Ad hoc, immédiatement |
| Conditions définitives des accords d'exclusivité | Article 1er | Parties à l'accord | Public | Accords d'exclusivité conclus au plus tôt le 16 juillet 2019 | Ad hoc, au moins deux mois avant l'entrée en vigueur d'un accord |
| Données (et/ou notifications) relatives à une demande de réutilisation | Article 1er<br>*Insertion de l'article 32 septdecies dans le règlement sur* | Organismes du secteur public | Auteurs des demandes de réutilisation des données | Dans le cas de documents, l'un des documents suivants doit être fourni: | Ad hoc |

| | | | | | |
|---|---|---|---|---|---|
| | *les données* | | | données/documents demandés; offre de licence; avis de retard; notification d'une décision négative. | |
| Conditions définitives des accords d'exclusivité | Article 1er<br>*Insertion de l'article 32 duodecies dans le règlement sur les données* | Parties à un accord d'exclusivité | Grand public | Conclusion des conditions définitives d'un accord d'exclusivité | Ad hoc |
| Conditions applicables aux fins de l'autorisation de la réutilisation de données ou de documents visés à l'article 2, point 54) | Article 1er<br>*Insertion de l'article 32 septvicies dans le règlement sur les données* | Organismes du secteur public (compétents pour accorder ou refuser les demandes d'accès) | Grand public | Lors de l'acceptation de la réutilisation des données ou des documents | Ad hoc |
| Notification de réutilisation non autorisée de données à caractère non personnel | Article 1er<br>*Insertion de l'article 32 septvicies dans le règlement sur les données* | Réutilisateur (éventuellement avec l'aide de l'organisme du secteur public) | Personnes physiques ou morales dont les droits et intérêts peuvent être affectés | Réutilisation non autorisée effectuée | Ad hoc |
| Notification de l'intention de transférer des données à caractère non personnel vers un | Article 1er<br>*Insertion de l'article 32 octovicies* | Réutilisateur | Organisme du secteur public | Intention de transférer des données vers un | Ad hoc |

| | | | | | |
|---|---|---|---|---|---|
| pays tiers et finalité de ce transfert (à l'organisme du secteur public) | *dans le règlement sur les données* | | | pays tiers | |
| Notification de l'intention de transférer des données à caractère non personnel vers un pays tiers, finalité de ce transfert et garanties appropriées (à la personne physique ou morale dont les droits et intérêts peuvent être affectés) | Article 1er<br>*Insertion de l'article 32 octovicies dans le règlement sur les données* | Réutilisateur (éventuellement avec l'aide de l'organisme du secteur public) | Personne physique ou morale dont les droits et intérêts peuvent être affectés | Intention de transférer des données vers un pays tiers | Ad hoc |
| Toutes les informations pertinentes concernant l'application des articles 32 *septvicies* [conditions de réutilisation], 32 *octovicies* [pays tiers] et 32 *novovicies* [redevances] du règlement sur les données. | Article 1er<br>*Insertion de l'article 32 untricies dans le règlement sur les données* | États membres | À la disposition des utilisateurs du point d'information unique | Des informations pertinentes doivent être fournies | Ad hoc |
| Réclamation déposée par des personnes physiques/morales en cas de violation de leurs droits en vertu du règlement sur les données ou en ce qui concerne d'autres questions pertinentes | Article 1er<br>*Modification de l'article 38, paragraphes 1 et 2, du règlement sur les données* | Personnes physiques ou morales | Autorité compétente concernée dans l'État membre concerné | Réclamation à introduire | Ad hoc |
| Informations sur l'état d'avancement des procédures/recours | Article 1er<br>*Modification de* | Autorité compétente | Personnes physiques ou | Plainte déposée | Ad hoc |

| | | | | | |
|---|---|---|---|---|---|
| juridictionnels liés à une réclamation introduite au titre du règlement sur les données | *l'article 38, paragraphes 1 et 2, du règlement sur les données* | concernée | morales à l'origine de la réclamation | | |
| Données sur l'expérience acquise et les bonnes pratiques (EDIB) | Article 1er<br>*Insertion du chapitre IX bis dans le règlement sur les données* | Comité européen de l'innovation dans le domaine des données | Commission; Autorités compétentes | Données à fournir | Ad hoc |
| Évaluation des chapitres II, III, IV, V, VI, VII et VIII du règlement sur les données<br>Évaluation des chapitres VII *bis*, VII *ter* et VII *quater* du règlement sur les données | Article 1er<br>*Modification de l'article 49, paragraphe 1, du règlement sur les données*<br>Article 1er<br>*Modification de l'article 49, paragraphe 2, du règlement sur les données* | Commission européenne | Parlement européen; Conseil; Comité économique et social européen | Réalisation de l'évaluation du règlement sur les données | Au plus tard le 12 septembre 2028<br>Au plus tard le [date d'entrée en vigueur plus 5 ans] |
| Notifications des violations de données à caractère personnel | Article 3<br>*Modification de l'article 33, paragraphe 1, du RGPD* | Responsable du traitement des données | Autorité de contrôle | Violation de données | Ad hoc |

| | | | | | |
|---|---|---|---|---|---|
| Proposition du comité européen de la protection des données relative à un modèle commun pour la notification des violations de données | Article 3<br>*Modification de l'article 33, paragraphe 1, du RGPD* | Comité européen de la protection des données | Commission | Proposition à soumettre | Dans un délai de [mois] à compter de l'entrée en application du présent règlement<br>Tous les trois ans |
| Propositions du comité européen de la protection des données concernant l'analyse d'impact relative à la protection des données | Article 3<br>*Modification de l'article 70, paragraphe 1, du RGPD* | Comité européen de la protection des données | Commission | Proposition à soumettre | Ad hoc |
| Rapports sur les incidents importants conformément à la directive SRI 2 | Article 6<br>*Insertion des articles 23 bis et 23 ter, modification de l'article 23 et de l'article 30, paragraphe 1, de la directive SRI 2* | Entités essentielles et importantes | CSIRT/autorités compétentes (selon le cas) | Circonstances décrites à l'article 23, paragraphe 3, de la directive SRI 2 | Ad hoc |
| Notifications des violations de données à caractère personnel | Article 3<br>*Modification de l'article 33 du RGPD* | Responsables du traitement des données | Autorité de contrôle | Violation de données à caractère personnel | Ad hoc |
| Notifications d'incidents majeurs liés aux TIC conformément au | Article 8<br>*Modification de* | Entités du secteur financier | Autorité compétente | Incidents majeurs liés aux TIC; | Ad hoc |

| | | | | | |
|---|---|---|---|---|---|
| règlement DORA; notifications volontaires de cybermenaces importantes conformément au règlement DORA | *l'article 19 du règlement DORA* | | concernée | cybermenaces importantes | |
| Notifications d'incidents qui perturbent ou sont susceptibles de perturber de manière importante la fourniture de services essentiels conformément à la directive CER | Article 9<br>*Modification de l'article 15 de la directive CER* | Entités critiques | Autorité compétente | Incidents qui perturbent ou sont susceptibles de perturber de manière importante la fourniture de services essentiels | Ad hoc |

**4.3. Solutions numériques**

*Description générale des solutions numériques*

*NB: toutes les solutions numériques détaillées ci-dessous sont des solutions préexistantes dont la base juridique est déplacée d'un règlement à un autre. En effet, les dispositions du règlement sur la gouvernance des données sont transférées vers le règlement sur les données.*

| **Solution numérique** | **Référence(s) à l'exigence ou aux exigences** | **Principales fonctionnalités requises** | **Organisme responsable** | **Comment l'accessibilité est-elle prise en compte?** | **Comment la possibilité de réutilisation est-elle envisagée?** | **Utilisation des technologies de l'IA (le cas échéant)** |
|---|---|---|---|---|---|---|
| Registre public de l'Union des services d'intermédiation de données et des organisations altruistes en matière de données | *Insertion de l'article 32 bis dans le règlement sur les données* | Stockage et publication des informations obligatoires | Commission européenne | // | // | s.o. |
| Point d'information unique (en vertu du règlement sur les données) | Article 1er<br>*Insertion de l'article 32 untricies dans le règlement sur les données* | Informations à mettre à disposition et à rendre accessibles.<br>Est compétent pour recevoir les demandes d'information ou les demandes de réutilisation des | Commission européenne | Point d'accès unique mettant à disposition un registre électronique consultable des données disponibles au niveau des points | Disponibilité par voie électronique d'une liste de ressources consultable contenant un aperçu de toutes les ressources en données | s.o. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | catégories de données protégées.<br>Transmet les demandes, par des moyens automatisés lorsque cela est possible et opportun, aux organismes du secteur public compétents.<br>Met à disposition par voie électronique une liste de ressources consultable contenant un aperçu de toutes les ressources documentaires disponibles. | | d'information uniques nationaux ainsi que d'autres informations sur la manière de demander des données par l'intermédiaire de ces points d'information uniques nationaux | disponibles [...] et des conditions applicables à leur réutilisation. | |
| guichet unique pour les notifications d'incidents | Article 6<br>*Insertion de l'article 23 bis dans la directive SRI 2* | Permettre le signalement des incidents conformément aux actes pertinents au niveau de l'Union. | Commission européenne; ENISA | Interopérabilité et compatibilité avec les portefeuilles européens d'identité | Possibilité de prévoir le signalement des incidents en vertu de différents actes juridiques; | s.o. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Garantir l'interopérabilité et la compatibilité avec les portefeuilles européens d'identité numérique pour les entreprises. | | numérique pour les entreprises et avec leurs propres moyens d'accessibilité | possibilité d'intégrer à l'avenir d'autres bases juridiques dans la solution fondée sur le guichet unique | |

*Pour chaque solution numérique, expliquer comment la solution numérique est conforme aux politiques numériques et aux dispositions législatives applicables*

**Registre public de l'Union des services d'intermédiation de données et des organisations altruistes en matière de données**

| **Politique numérique et/ou sectorielle (le cas échéant)** | **Expliquer de quelle manière la solution s'aligne sur l'élément en question** |
|---|---|
| ***Règlement sur l'IA*** | s.o. |
| ***Cadre de l'UE en matière de cybersécurité*** | s.o. |
| ***eIDAS*** | s.o. |
| ***Portail numérique unique et IMI*** | Modification du règlement (UE) 2018/1724 afin d'ajouter à l'annexe II les procédures «Enregistrement en tant que prestataire de services d'intermédiation de données» et «Enregistrement en tant qu'organisation altruiste en matière de données reconnue dans l'Union». |
| ***Autres*** | s.o. |

**Point d'information unique (en vertu du règlement sur les données)**

| Politique numérique et/ou sectorielle (le cas échéant) | Expliquer de quelle manière la solution s'aligne sur l'élément en question |
|---|---|
| ***Règlement sur l'IA*** | s.o. |
| ***Cadre de l'UE en matière de cybersécurité*** | Les organismes du secteur public peuvent prévoir une exigence pour l'accès à distance aux données et aux documents, ainsi que pour leur réutilisation, dans un environnement de traitement sécurisé qui est fourni ou contrôlé par l'organisme du secteur public. En pareils cas, les organismes du secteur public imposent des conditions qui préservent l'intégrité du fonctionnement des systèmes techniques de l'environnement de traitement sécurisé utilisé. |
| ***eIDAS*** | s.o. |
| ***Portail numérique unique et IMI*** | s.o. |
| ***Autres*** | Le point d'information unique est conforme au règlement (UE) 2016/679 (RGPD). Les organismes du secteur public peuvent prévoir des exigences pour accorder l'accès en vue de la réutilisation de données ou de documents uniquement lorsque ceux-ci ont été anonymisés et/ou soumis à une autre forme de préparation pertinente. En outre, en cas de réutilisation non autorisée de données à caractère non personnel, le réutilisateur est tenu d'informer les personnes physiques dont les droits et intérêts peuvent être affectés. |

**guichet unique pour les notifications d'incidents**

| Politique numérique et/ou sectorielle (le cas échéant) | Expliquer de quelle manière la solution s'aligne sur l'élément en question |
|---|---|

| | |
|---|---|
| ***Règlement sur l'IA*** | s.o. |
| ***Cadre de l'UE en matière de cybersécurité*** | Dans le cadre de la modification apportée à la directive SRI 2, l'accent est naturellement mis sur la cybersécurité. Plus généralement, le guichet unique est censé servir de point d'accès, acheminant tous les rapports d'incidents liés à la cybersécurité vers les autorités compétentes respectives, en vertu de plusieurs actes juridiques de l'Union. |
| ***eIDAS*** | Le guichet unique est également obligatoire pour le signalement des incidents au titre du règlement (UE) nº 910/2014 (règlement eIDAS).<br>L'ENISA veille à ce que le guichet unique soit interopérable et compatible avec les portefeuilles européens d'identité numérique pour les entreprises et à ce que ces portefeuilles puissent être utilisés au moins pour identifier et authentifier les entités utilisant le guichet unique. L'initiative stratégique relative au portefeuille européen d'identité numérique pour les entreprises s'appuiera sur le cadre du règlement eIDAS. |
| ***Portail numérique unique et IMI*** | s.o. |
| ***Autres*** | La proposition a tenu compte de l'ensemble de l'acquis numérique, y compris des politiques relatives aux données, à la cybersécurité et aux télécommunications. |

**4.4. Évaluation de l'interopérabilité**

*Description générale du ou des services publics numériques concernés par les exigences*

| **Service public numérique ou catégorie de services publics numériques** | **Description** | **Référence(s) à l'exigence ou aux exigences** | **Solution(s) interopérable(s) pour l'Europe**<br>**(SANS OBJET)** | **Autre(s) solution(s) d'interopérabilité** |
|---|---|---|---|---|
| Infrastructure européenne en matière de gouvernance et de transparence des données | Service public numérique permettant la mise en place d'infrastructures en matière de gouvernance et de transparence des données et exploitant, entre autres, un registre public européen des services d'intermédiation de données et des organisations altruistes en matière de données, ainsi qu'un point d'information unique destiné à aider les réutilisateurs à trouver des informations sur la réutilisation de certaines catégories de données protégées.<br>Catégorie de services publics numériques selon la CFAP 04.9.0 — Affaires économiques n.c.a. (SC) | Article 1er | // | // |
| Signalement des incidents | Service public numérique permettant le signalement d'incidents par l'intermédiaire du | Article 6 | // | Portefeuilles européens d'identité numérique pour les entreprises |

| | | | | |
|---|---|---|---|---|
| | guichet unique.<br>Catégorie de services publics numériques selon la CFAP 03.6.0 Ordre et sécurité publics n.c.a. | | | |

*Incidence de l'exigence ou des exigences sur l'interopérabilité transfrontière pour chaque service public numérique*

***NB: dans l'analyse qui suit, les numéros d'article fournis tout au long de la section «Mesure(s)» renvoient à l'acte ou aux actes objet de la modification. La correspondance avec les exigences du règlement omnibus est effectuée une fois, en haut de chaque cellule.***

**Service public numérique # 1 — Infrastructure européenne en matière de gouvernance et de transparence des données**

| **Évaluation** | **Mesure(s)** | **Obstacles potentiels restants (le cas échéant)** |
|---|---|---|
| **Alignement sur les politiques numériques et sectorielles existantes**<br>**Énumérer les politiques numériques et sectorielles applicables recensées** | Article 1er<br>L'alignement sur les politiques numériques et sectorielles existantes se reflète dans les considérants du règlement sur la gouvernance des données:<br>Portail numérique unique [règlement (UE) 2018/1724, considérant 56]: les procédures de notification pour les services d'intermédiation de données et les procédures d'enregistrement pour les organisations altruistes en matière de données doivent être mises à disposition par l'intermédiaire du portail numérique unique, de manière à garantir un accès en ligne par-delà les frontières.<br>Cadre d'interopérabilité européen (considérant 54): l'infrastructure numérique doit respecter les principes du cadre d'interopérabilité européen afin de garantir une utilisation transfrontière et transsectorielle des données.<br>Éléments constitutifs du MIE (infrastructures de services numériques dans le cadre du mécanisme pour l'interconnexion en Europe) (considérant 54): références «aux vocabulaires de base et aux blocs constitutifs du MIE». Le service numérique devrait exploiter les blocs constitutifs du MIE (tels que eDelivery, eID, eSignature) aux fins de la | |

| | | |
|---|---|---|
| | mise en œuvre technique.<br><br>Exigences en matière d'accessibilité [directives (UE) 2016/2102 et (UE) 2019/882] (considérant 62). Directive (UE) 2016/2102 (directive sur l'accessibilité du web): les registres publics et les services numériques doivent être accessibles aux personnes handicapées; directive (UE) 2019/882 (acte législatif sur l'accessibilité): les services numériques doivent être conformes aux exigences en matière d'accessibilité.<br><br>RGPD [règlement (UE) 2016/679] (considérants 4 et 35): tous les services numériques traitant des données à caractère personnel doivent respecter les exigences du RGPD en matière de protection des données, de respect de la vie privée et de sécurité.<br><br>Règlement (UE) 2018/1725 (considérant 4): lorsque les institutions de l'UE traitent des données par l'intermédiaire de ces registres, elles doivent se conformer au présent règlement.<br><br>Directive sur les données ouvertes [directive (UE) 2019/1024] (considérants 6 et 10): «La directive (UE) 2019/1024 et le droit sectoriel de l'Union garantissent que les organismes du secteur public rendent facilement accessibles un volume accru des données qu'ils produisent, à des fins d'utilisation et de réutilisation»: le service numérique complète la directive sur les données ouvertes en englobant les catégories de données protégées qui n'entrent pas dans son champ d'application, tout en veillant à ce que les organismes du secteur public suivent les principes d'«ouverture dès la conception et par défaut», le cas échéant.<br><br>Politiques sectorielles relatives aux espaces européens des données et aux données sectorielles, dont l'espace européen des données de santé, l'espace européen des données relatives à la mobilité, les données relatives au pacte vert pour l'Europe/au climat et à l'énergie, les données relatives à l'industrie manufacturière, les données relatives aux services financiers, les données relatives à l'agriculture, l'espace de données pour l'administration publique et l'espace de données relatives aux compétences. | |

| | | |
|---|---|---|
| **Mesures organisationnelles en faveur d'une fourniture transfrontière sans heurts de services publics numériques**<br><br>**Énumérer les mesures de gouvernance prévues** | Article 1er<br><br>**Désignation de l'autorité compétente et coordination**<br><br>- Article 32 *ter*: chaque État membre désigne une ou plusieurs autorités compétentes chargées de l'enregistrement des prestataires de services d'intermédiation de données et des organisations altruistes en matière de données. Ces autorités compétentes préservent leur indépendance à l'égard de tout prestataire de services d'intermédiation de données reconnu ou de toute organisation altruiste en matière de données reconnue.<br><br>Article 32 *tricies*: chaque État membre désigne un ou plusieurs organismes compétents chargés d'assister les organismes du secteur public qui accordent ou refusent l'accès aux fins de la réutilisation de catégories de données protégées.<br><br>Article 32 *octies*: les autorités compétentes contrôlent et supervisent le respect des dispositions du règlement sur les données par les prestataires de services d'intermédiation de données reconnus et les organisations altruistes en matière de données reconnues.<br><br>**Mécanisme de compétence transfrontière**<br><br>Articles 32 *sexies*: les services d'intermédiation de données relèvent de la compétence de l'autorité compétente de l'État membre de l'établissement principal. Le même principe s'applique aux organisations altruistes en matière de données.<br><br>**Reconnaissance mutuelle et enregistrement unique**<br><br>Article 32 *sexies*: l'enregistrement en tant que service d'intermédiation de données/qu'organisation altruiste en matière de données est valable dans l'ensemble des États membres.<br><br>Article 32 *bis*: utilisation d'un logo commun<br><br>**Registres centralisés au niveau de l'UE aux fins de la collecte et de la transparence des données** | |

| | | |
|---|---|---|
| | Article 32 *bis*: registres publics de l'Union de tous les prestataires de services d'intermédiation de données reconnus et de toutes les organisations altruistes en matière de données reconnues.<br><br>Article 32 *sexies*: les autorités compétentes notifient sans délai par voie électronique à la Commission les nouveaux enregistrements, modifications et suppressions, et la Commission met à jour les registres de l'Union en conséquence.<br><br>**Coordination du suivi et de l'application du règlement**<br><br>Autorités nationales compétentes<br><br>Comité européen de l'innovation dans le domaine des données<br><br>**Gouvernance du transfert de données vers des pays tiers**<br><br>Article 32 *octovicies*: exigences applicables aux transferts de données à caractère non personnel vers des pays tiers par les réutilisateurs.<br><br>**Accords d'exclusivité**<br><br>Article 32 *duodecies*: définit l'admissibilité des accords d'exclusivité relatifs à la réutilisation de données ou de documents détenus par des organismes du secteur public. Exige la transparence des conditions définitives. | |
| **Mesures prises pour garantir une compréhension commune des données**<br><br>**Énumérer ces mesures** | Article 1er<br><br>**Normes communes et cadres interopérables**<br><br>- L'EDIB conseille la Commission européenne sur les activités de normalisation à entreprendre en ce qui concerne les aspects transsectoriels du partage des données, y compris au regard de l'émergence d'espaces européens communs des données, en envisageant des activités de normalisation sectorielles.<br>  o Article 42: l'EDIB contribue à l'adoption de «lignes directrices établissant des cadres interopérables et des pratiques communes pour le fonctionnement des espaces européens communs des données». | |

| | | |
|---|---|---|
| | - Logo commun pour l'identification des services d'intermédiation de données et des organisations altruistes en matière de données.<br>- Article 32 *octodecies*: les organismes du secteur public et les entreprises publiques mettent leurs données ou documents à disposition dans tout format ou toute langue préexistants et, si possible et s'il y a lieu, sous forme électronique, dans des formats qui sont ouverts, lisibles par machine, accessibles, traçables et réutilisables, en les accompagnant de leurs métadonnées. Tant le format que les métadonnées répondent, autant que possible, à des normes formelles ouvertes.<br><br>**Autres mesures pertinentes:**<br><br>- Article 32 *unvicies*: les États membres, en coopération avec la Commission, poursuivent les efforts visant à simplifier l'accès aux ensembles de données, en mettant à disposition des ensembles de données appropriés dans des formats accessibles, traçables et réutilisables sous forme électronique.<br>- Article 32 *duovicies*: les États membres encouragent la mise à disposition des données de la recherche d'une manière compatible avec les principes FAIR. | |
| **Utilisation de spécifications et de normes techniques ouvertes convenues d'un commun accord.**<br>**Énumérer ces mesures** | Article 1er<br><br>**Mesures relatives aux données lisibles par machine:**<br><br>- article 32 *bis*: registre de l'Union européenne lisible par machine des prestataires de services d'intermédiation de données;<br>- article 32 *bis*: registre de l'Union européenne lisible par machine des organisations altruistes en matière de données;<br>- article 32 *octodecies*: les organismes du secteur public mettent leurs données/documents à disposition, dans la mesure du possible, dans des formats qui sont ouverts, lisibles par machine, accessibles, traçables et réutilisables, en les accompagnant de leurs métadonnées. Tant le format que les métadonnées répondent, autant que possible, à des normes formelles ouvertes; | |

| | | |
|---|---|---|
| | - article 32 *octodecies*: les ensembles de données de forte valeur sont mis à disposition à des fins de réutilisation dans des formats lisibles par machine, en recourant à des API appropriées et, le cas échéant, sous la forme d'un téléchargement de masse;<br>- article 32 *unvicies*: les États membres adoptent des dispositions pratiques pour faciliter la recherche de données ou de documents disponibles à des fins de réutilisation, telles que des listes de ressources des données ou documents principaux accompagnés des métadonnées pertinentes, accessibles, dans la mesure du possible et s'il y a lieu, en ligne et sous un format lisible par machine, et des portails liés aux listes de ressources. Dans la mesure du possible, les États membres facilitent la recherche interlinguistique des données ou documents;<br>- article 32 *quatervicies*: les ensembles de données spécifiques de forte valeur sont lisibles par machine. Des actes d'exécution peuvent préciser les modalités relatives aux formats de données et de métadonnées ainsi que les modalités techniques de diffusion.<br><br>**Mesures d'interaction de machine à machine:**<br><br>- Article 32 *untricies*: utilisation obligatoire du point d'information unique. Le point d'information unique est compétent pour recevoir les demandes d'information ou les demandes de réutilisation, et les transmet, par des moyens automatisés lorsque cela est possible et opportun, aux organismes du secteur public compétents, ou aux organismes compétents.<br><br>**Autres mesures pertinentes:**<br><br>- article 48 *bis*: modification de l'annexe II du règlement (UE) 2018/1724 (portail numérique unique). Des synergies ont été recherchées;<br>- considérant 52 du règlement omnibus: dans la mesure du possible, l'ENISA devrait tenir compte des solutions techniques nationales existantes qui facilitent le signalement des incidents, telles que les plateformes nationales, lors de | |

| | | |
|---|---|---|
| | l'élaboration des spécifications relatives aux mesures techniques, opérationnelles et organisationnelles concernant la mise en place, la maintenance et le fonctionnement sécurisé du guichet unique. En outre, l'ENISA devrait envisager des protocoles et outils techniques tels que des interfaces de programmation d'applications et des normes lisibles par machine qui permettent aux entités de faciliter l'intégration des obligations de signalement dans les processus opérationnels, et aux autorités de connecter le guichet unique à leurs systèmes nationaux de signalement. | |

**Service public numérique # 2 — Signalement des incidents**

| **Évaluation** | **Mesure(s)** | **Obstacles potentiels restants (le cas échéant)** |
|---|---|---|
| **Alignement sur les politiques numériques et sectorielles existantes**<br>**Énumérer les politiques numériques et sectorielles applicables recensées** | Article 6<br>L'alignement général sur les politiques numériques et sectorielles existantes est assuré par la directive (UE) 2022/2555 (SRI 2), que le règlement omnibus numérique modifie à présent. En outre, le règlement omnibus prévoit des synergies avec le portefeuille européen d'identité numérique pour les entreprises ainsi qu'avec le règlement (UE) 2024/2847 (règlement sur la cyberrésilience). En particulier:<br>• l'article 23, paragraphe 4, rend obligatoire l'utilisation du guichet unique pour les notifications au titre de la directive SRI 2;<br>• l'article 23, paragraphe 1, dispose qu'une notification d'incident grave conformément à l'article 14, paragraphe 3, du règlement (UE) 2024/2847 (règlement sur la cyberrésilience) constitue également une communication d'informations au titre de la directive (UE) 2022/2555 (directive SRI 2). Cette disposition est conforme au principe «une fois pour toutes»;<br>• l'article 23 *bis*, paragraphe 3, point d), prévoit le lien avec les portefeuilles européens d'identité numérique pour les entreprises. | |

| | | |
|---|---|---|
| **Mesures organisationnelles en faveur d'une fourniture transfrontière sans heurts de services publics numériques**<br>**Énumérer les mesures de gouvernance prévues** | Article 6<br>L'article 23 *bis* définit les rôles et les responsabilités. En l'occurrence, l'ENISA:<br>• assure la mise en place et la maintenance d'un guichet unique pour faciliter le signalement obligatoire des incidents et des événements connexes en vertu des actes juridiques de l'Union;<br>• prend des mesures techniques, opérationnelles et organisationnelles afin de gérer les risques pour la sécurité du guichet unique et des informations communiquées ou diffusées. Ce faisant, elle consulte la Commission, le réseau des CSIRT et les autorités compétentes concernées. | |
| **Mesures prises pour garantir une compréhension commune des données**<br>**Énumérer ces mesures** | Article 6<br>L'article 23 *bis* charge l'ENISA d'élaborer des spécifications qui garantissent la capacité nécessaire à l'interopérabilité en ce qui concerne les autres obligations pertinentes en matière de signalement.<br>*NB: les exigences en matière de contenu applicables au signalement des incidents sont définies plus en détail dans les actes juridiques pertinents de l'Union, dont la directive (UE) 2022/2555 (directive SRI 2). L'article 23 bis, paragraphe 3, point c), du règlement omnibus précise que l'ENISA veille à ce qu'il en soit dûment tenu compte.* | |
| **Utilisation de spécifications et de normes techniques ouvertes convenues d'un commun accord.**<br>**Énumérer ces mesures** | Article 6<br>L'article 23 *bis* appelle à l'élaboration de spécifications:<br>• l'ENISA fournit et met en œuvre les spécifications relatives aux mesures techniques concernant la mise en place, la maintenance et le fonctionnement sécurisé du guichet unique. Ces spécifications comprennent, entre autres: | |

| | | |
|---|---|---|
| | ○ la capacité nécessaire pour assurer l'interopérabilité au regard d'autres obligations pertinentes en matière de signalement;<br>○ les modalités techniques permettant aux entités et autorités concernées de consulter, soumettre, retrouver, transmettre ou traiter d'une autre manière les informations provenant du guichet unique, ainsi que les protocoles et outils techniques permettant aux entités et autorités de poursuivre au sein de leurs systèmes le traitement des informations reçues.<br>• Le cas échéant, le guichet unique est interopérable et compatible avec les portefeuilles européens d'identité numérique pour les entreprises. | |

### 4.5. Mesures de soutien de la mise en œuvre numérique

*Description générale des mesures de soutien de la mise en œuvre numérique*

| **Description de la mesure** | **Référence(s) à l'exigence ou aux exigences** | **Rôle de la Commission** (le cas échéant) | **Acteurs à associer** (le cas échéant) | **Calendrier prévu** (le cas échéant) |
|---|---|---|---|---|
| Acte d'exécution: conception d'un logo commun pour les prestataires de services d'intermédiation de données | Article 1er | Définir les caractéristiques du logo commun, y compris en ce qui concerne sa conception et les modalités d'utilisation. | Comité chargé de la procédure d'examen | // |
| Acte d'exécution: conception d'un logo commun pour les organisations altruistes | Article 1er | Définir les caractéristiques du logo | Comité chargé de la procédure | // |

| | | | | |
|---|---|---|---|---|
| en matière de données reconnues | | commun, y compris en ce qui concerne sa conception et les modalités d'utilisation. | d'examen | |
| Contrôle et conformité: les autorités compétentes peuvent contrôler le respect du règlement soit de leur propre initiative, soit à la demande de personnes physiques ou morales. | Article 1er | // | Autorités compétentes, services d'intermédiation de données, organisations altruistes en matière de données | // |
| Acte d'exécution: ensembles de données de forte valeur spécifiques | Article 1er | Établir une liste d'ensembles de données de forte valeur spécifiques. Peut préciser les modalités de publication et de réutilisation des ensembles de données de forte valeur. | Comité chargé de la procédure d'examen | // |
| Lignes directrices:<br>• l'EDIB fournit des conseils sur les lignes directrices relatives aux espaces européens communs des données<br>• l'EDIB adopte des lignes directrices sur les cadres | Article 1er | Recevoir le soutien de l'EDIB | EDIB | // |

| | | | | |
|---|---|---|---|---|
| interopérables | | | | |
| Acte d'exécution: modèle commun pour la notification d'une violation de données à caractère personnel | Article 3 | Adopter un modèle commun sur la base de la proposition du comité européen de la protection des données. | Comité chargé de la procédure d'examen | // |
| Acte délégué: indications automatisées et lisibles par machine des choix de la personne concernée | Article 3 | Établir une obligation applicable aux navigateurs web et aux fournisseurs d'équipements terminaux | Comité chargé de la procédure d'examen | // |
| Acte d'exécution: notifications d'incidents au titre de la directive CER | Article 9 | Préciser davantage le type et le format des informations notifiées conformément à l'article 15, paragraphe 1, de la directive (UE) 2022/2557 (directive CER). | // | // |