Journal officiel
de l'Union européenne

FR
Série L

2025/2050

9.10.2025

RÈGLEMENT DÉLÉGUÉ (UE) 2025/2050 DE LA COMMISSION

du 1er juillet 2025

complétant le règlement (UE) 2022/2065 du Parlement européen et du Conseil en établissant les conditions et procédures techniques selon lesquelles les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne doivent partager des données avec des chercheurs agréés

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

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE ([1]), et notamment son article 40, paragraphe 13,

considérant ce qui suit:

(1) L'article 40 du règlement (UE) 2022/2065 établit des règles concernant l'accès aux données qui doit être accordé par les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne. En particulier, il permet aux chercheurs qui se sont soumis à un processus visant à démontrer qu'ils remplissent les conditions énoncées au paragraphe 8 dudit article (ci-après les «chercheurs agréés») de bénéficier d'un tel accès.

(2) En vertu de l'article 40, paragraphe 4, du règlement (UE) 2022/2065, les chercheurs agréés doivent avoir accès aux données afin de pouvoir étudier les risques systémiques dans l'Union et évaluer l'efficacité des mesures prises pour atténuer ces risques. Leurs conclusions peuvent constituer une contribution précieuse pour l'application du règlement (UE) 2022/2065 et favoriser la responsabilisation des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne. Le présent règlement a pour objet d'établir les conditions techniques et les procédures nécessaires pour permettre cet accès, d'une manière sûre et efficace assurant la cohérence entre tous les coordinateurs pour les services numériques, et de façon à garantir l'égalité de traitement pour les chercheurs et les fournisseurs de données.

(3) Afin de garantir la cohérence du processus d'accès aux données entre tous les coordinateurs pour les services numériques et de rendre ce processus clair et transparent pour tous, il est nécessaire de créer une infrastructure numérique spécifique (ci-après le «portail pour l'accès aux données en vertu du DSA»). Le portail pour l'accès aux données en vertu du DSA devrait permettre aux chercheurs, aux fournisseurs de données et aux coordinateurs pour les services numériques de participer au processus d'accès aux données, d'avoir accès aux informations pertinentes telles que les coordonnées des points de contact spécialisés et de les diffuser, et de communiquer entre eux. Le portail pour l'accès aux données en vertu du DSA ne devrait pas être considéré comme l'une des modalités d'accès à utiliser pour fournir l'accès aux données en réponse à une demande motivée.

(4) Les fournisseurs de données et les chercheurs souhaitant participer au processus d'accès aux données devraient, à cette fin, créer un compte sur le portail pour l'accès aux données en vertu du DSA. Afin de faire en sorte que les coordinateurs pour les services numériques puissent accéder aux informations soumises par l'intermédiaire du portail pour l'accès aux données en vertu du DSA sans avoir à créer un compte distinct sur le portail, ce dernier devrait être interopérable avec le système de partage d'informations AGORA établi par le règlement d'exécution (UE) 2024/607 de la Commission ([2]).

(5) Afin que le processus d'accès aux données soit transparent pour toutes les parties concernées et qu'il soit possible de contrôler l'efficacité et l'efficience du processus d'accès aux données ainsi que le respect de l'article 40, paragraphe 4, du règlement (UE) 2022/2065 et du présent règlement, le portail pour l'accès aux données en vertu du DSA devrait générer des notifications automatiques relatives aux différentes étapes et mises à jour du processus.

([1]) JO L 277 du 27.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.

([2]) Règlement d'exécution (UE) 2024/607 de la Commission du 15 février 2024 définissant les modalités pratiques et opérationnelles du fonctionnement du système de partage d'informations conformément au règlement (UE) 2022/2065 du Parlement européen et du Conseil (règlement sur les services numériques) (JO L, 2024/607, 16.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/607/oj).

(6) Pour fournir aux chercheurs des informations cohérentes sur le processus d'accès aux données, les coordinateurs pour les services numériques devraient veiller à ce que des informations concernant le processus d'accès aux données, y compris des liens vers le portail pour l'accès aux données en vertu du DSA, soient disponibles et facilement accessibles sur leurs interfaces en ligne. Afin de ne pas occasionner de charge administrative inutile et en vue d'accroître l'efficacité et de faciliter la communication entre toutes les parties intervenant dans le processus d'accès aux données, les coordinateurs pour les services numériques sont encouragés à faciliter la gestion des informations relatives au processus d'accès aux données, y compris d'un point de vue linguistique.

(7) Pour permettre aux chercheurs de déterminer les données pertinentes aux fins énoncées à l'article 40, paragraphe 4, du règlement (UE) 2022/2065, les fournisseurs de données devraient mettre à disposition des catalogues de données DSA relatifs à leurs services. Ces catalogues, qui devraient être faciles à trouver et accessibles sur les interfaces en ligne des fournisseurs de données, devraient décrire les actifs de données disponibles, leur structure de données et leurs métadonnées, pouvant faire l'objet d'une demande d'accès en vertu de l'article 40, paragraphe 4, du règlement (UE) 2022/2065. Lorsqu'ils mettent à disposition les catalogues de données DSA, les fournisseurs de données devraient tenir compte des risques pour la confidentialité, la sécurité des données ou la protection des données à caractère personnel pouvant découler de la publication de ces informations.

(8) Afin de contribuer à l'élaboration de projets de recherche pertinents aux fins énoncées à l'article 40, paragraphe 4, du règlement (UE) 2022/2065, les catalogues de données DSA devraient contenir en particulier les données relatives aux risques systémiques dans l'Union que les fournisseurs de données ont recensés dans les évaluations annuelles des risques qu'ils réalisent conformément à l'article 34 dudit règlement, ainsi que les données relatives à toute mesure d'atténuation des risques visée à l'article 35 du règlement. Pour que les catalogues de données DSA restent toujours pertinents et actuels, il convient de les mettre à jour régulièrement en tenant dûment compte des risques systémiques nouvellement recensés et de l'évolution des risques systémiques. Par exemple, les catalogues devraient tenir compte des risques émergents recensés à la suite d'une évaluation ad hoc des risques réalisée conformément à l'article 34 du règlement (UE) 2022/2065 ou à la suite d'un rapport d'audit établi conformément à l'article 37 dudit règlement. Afin de réduire au minimum la charge procédurale pesant sur les fournisseurs de données, ces catalogues peuvent, le cas échéant, s'appuyer sur les ressources existantes en matière de documentation des données utilisées à d'autres fins et pour d'autres publics, tels que la publicité, la création de contenu ou le développement d'applications par des tiers. Les catalogues de données DSA ne devraient pas être soumis à une obligation d'exhaustivité et ne devraient donc ni être contraignants pour les chercheurs demandeurs, ni limiter ces derniers dans leurs demandes d'accès aux données.

(9) Pour permettre au coordinateur pour les services numériques de l'État membre d'établissement de déterminer plus facilement les modalités d'accès et pour alléger l'ensemble du processus d'accès aux données pour tous les acteurs concernés, les fournisseurs de données devraient publier les modalités d'accès proposées pour les données décrites dans les catalogues de données DSA. Les modalités d'accès proposées devraient être proportionnées au caractère sensible des données et inclure des informations sur les éventuelles conditions techniques, organisationnelles et juridiques que les fournisseurs de données jugent appropriées pour permettre la fourniture des données. Les modalités d'accès proposées par les fournisseurs de données ne devraient pas être contraignantes pour les coordinateurs pour les services numériques de l'État membre d'établissement, qui devraient rester compétents pour déterminer les modalités d'accès appropriées.

(10) Afin de garantir l'égalité de traitement des demandes d'accès aux données, indépendamment du coordinateur pour les services numériques auquel la demande d'accès aux données est soumise ou dont émane la demande motivée, il convient de préciser le délai de formulation des demandes motivées pour assurer la cohérence entre tous les coordinateurs pour les services numériques. Si la formulation de la demande motivée nécessite un délai supplémentaire, le coordinateur pour les services numériques de l'État membre d'établissement doit en informer le chercheur principal, en indiquant les raisons du retard. Au nombre de ces raisons peut figurer la nécessité, pour le coordinateur pour les services numériques de l'État membre de l'organisme de recherche ou d'établissement, de procéder à des vérifications supplémentaires, par exemple lorsque les demandes d'accès aux données impliquent des transferts internationaux de données, ou lorsque le coordinateur pour les services numériques de l'État membre d'établissement a identifié des risques potentiels pour la sécurité de l'Union si les données devaient être partagées. En vue d'harmoniser également les étapes du processus d'accès aux données précédant la formulation des demandes motivées, notamment l'évaluation des demandes d'accès aux données et l'octroi du statut de chercheur agréé, les coordinateurs pour les services numériques sont encouragés à mettre au point une méthode de travail cohérente et coordonnée, y compris des critères opérationnels communs, dans le cadre du comité européen des services numériques.

(11) Afin de rationaliser les procédures de formulation des demandes motivées, tous les coordinateurs pour les services numériques de l'État membre d'établissement devraient être tenus de vérifier que certains éléments communs du processus d'accès aux données ont été dûment pris en compte dans les demandes d'accès aux données. À cette fin, les coordinateurs devraient vérifier que tous les chercheurs demandeurs qui sont mentionnés dans la demande d'accès aux données ont donné la preuve de leur affiliation à un organisme de recherche, par exemple en fournissant des justificatifs de contrats de travail ou de toute autre forme de lien juridique avec l'organisme de recherche. Les coordinateurs pour les services numériques de l'État membre d'établissement devraient également vérifier que les chercheurs demandeurs ont démontré leur indépendance à l'égard d'intérêts commerciaux, par exemple en fournissant une déclaration à cet effet.

(12) Les coordinateurs devraient vérifier que le financement du projet de recherche pour lequel les données sont demandées est divulgué dans la demande d'accès aux données. Les chercheurs demandeurs devraient donner, dans les informations qu'ils fournissent, des précisions sur les contributions, telles que l'entité qui finance, le montant, la nature et la durée de la contribution, et notamment indiquer si le financement a déjà été octroyé ou si une demande de financement est toujours en cours d'évaluation, ainsi que, le cas échéant, les références pertinentes aux projets financés par l'Union. La demande d'accès aux données devrait également inclure les résultats des évaluations réalisées par l'entité ou les entités fournissant le financement, lorsqu'ils sont disponibles.

(13) Le coordinateur pour les services numériques de l'État membre d'établissement devrait vérifier que la demande d'accès aux données décrit la manière dont les données et le format des données sont sélectionnés, compte tenu des exigences de nécessité et de proportionnalité liées à la finalité de la recherche envisagée. Lorsque les données demandées sont également disponibles par l'intermédiaire d'autres sources, le coordinateur pour les services numériques de l'État membre d'établissement devrait évaluer, compte tenu des informations figurant dans la demande d'accès aux données, s'il est justifié d'introduire une demande d'accès pour ces données. Une telle demande pourrait, par exemple, être justifiée par la mauvaise qualité ou le manque de fiabilité attestés de ces données lorsqu'elles proviennent d'autres sources, ou par l'inadéquation du format dans lequel ces données peuvent être obtenues auprès d'autres sources pour les besoins du projet de recherche, caractéristiques qui entraveraient la réalisation dudit projet. Le type de données qui peuvent être demandées pour étudier les risques systémiques ou l'atténuation de ces derniers dans l'Union pourrait évoluer à l'avenir. Actuellement, on peut citer comme exemples de ces données les données relatives aux utilisateurs des services, telles que les informations sur les profils, les réseaux relationnels, l'exposition au contenu au niveau individuel et les historiques d'interaction; les données d'interaction telles que les commentaires ou autres types d'interaction; les données relatives aux recommandations de contenu, y compris les données utilisées pour personnaliser les recommandations; les données relatives au ciblage des publicités et au profilage, y compris les données relatives au coût par clic et d'autres mesures des prix publicitaires; les données relatives aux essais de nouvelles fonctionnalités avant leur déploiement, y compris les résultats de tests A/B; les données relatives à la modération et à la gouvernance des contenus, telles que les données sur les systèmes et processus algorithmiques ou d'autres systèmes et processus de modération des contenus, y compris les journaux des modifications, les archives ou les répertoires regroupant les contenus modérés, y compris les comptes, ainsi que les données relatives aux prix, aux quantités et aux caractéristiques des biens ou services fournis ou faisant l'objet d'une intermédiation par le fournisseur de données.

(14) Le coordinateur pour les services numériques de l'État membre d'établissement devrait vérifier si la demande d'accès aux données fournit suffisamment d'informations prouvant que le chercheur est en mesure de satisfaire aux exigences spécifiques de confidentialité, de sécurité et de protection des données à caractère personnel en ce qui concerne les données demandées, recense les risques éventuels découlant de l'accès à ces données et de leur traitement aux fins de la recherche, et documente toute modalité d'accès proposée, y compris les conditions juridiques, organisationnelles et techniques qui seront mises en place pour réduire au minimum les risques recensés, par exemple au moyen d'une lettre d'engagement dans laquelle l'organisme de recherche confirme avoir accès à des moyens pouvant constituer des garanties pertinentes, ou d'autres documents justificatifs.

(15) Lorsque des données à caractère personnel sont demandées, le coordinateur pour les services numériques de l'État membre d'établissement devrait vérifier que la demande d'accès aux données comprend des informations relatives à la base juridique du traitement des données à caractère personnel, y compris des catégories particulières de données à caractère personnel, si nécessaire, et si cette base juridique est conforme à l'article 6, paragraphe 1, point e) ou f), et, le cas échéant, à l'article 9, paragraphe 2, point g) ou j), du règlement (UE) 2016/679 du Parlement européen et du Conseil ([3]). En outre, le coordinateur pour les services numériques de l'État membre d'établissement devrait vérifier que la demande d'accès aux données contient suffisamment d'éléments indiquant que les chercheurs ont évalué les risques pour la protection des données à caractère personnel. Cela pourrait, par exemple, être démontré par une analyse d'impact relative à la protection des données au sens de l'article 35 dudit règlement. Afin de garantir l'accès aux données à caractère personnel conformément au règlement (UE) 2016/679, les coordinateurs pour les services numériques devraient être autorisés à consulter les autorités de contrôle concernées établies en vertu de l'article 51 dudit règlement, qui restent compétentes pour évaluer le respect du règlement (UE) 2016/679.

([3]) 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).

(16) Pour faciliter la formulation de la demande motivée et préserver l'intégrité des informations figurant dans la demande d'accès aux données, le coordinateur pour les services numériques de l'État membre d'établissement devrait vérifier si la demande d'accès aux données comprend un résumé. Ce résumé devrait contenir un aperçu des informations qui feront partie de la demande motivée, publiées sur le portail pour l'accès aux données en vertu du DSA, dans les cas où l'évaluation de la demande d'accès aux données conduit à la formulation d'une demande motivée.

(17) Afin de garantir que les modalités d'accès fixées par le coordinateur pour les services numériques de l'État membre d'établissement sont appropriées eu égard au caractère sensible des données spécifiques faisant l'objet d'une demande d'accès aux données, le coordinateur pour les services numériques de l'État membre d'établissement devrait procéder à une évaluation au cas par cas, sur la base des informations fournies dans la demande d'accès aux données. Les modalités d'accès établies dans la demande motivée devraient être appropriées pour satisfaire aux exigences en matière de sécurité et de confidentialité des données et de protection des données à caractère personnel et, dans le même temps, permettre la réalisation des objectifs de recherche du projet. L'accès aux données peut, par exemple, se faire par la transmission de données aux chercheurs agréés au moyen d'une interface appropriée et d'un stockage de données approprié; par la transmission des données vers un environnement de traitement sécurisé géré par le fournisseur de données ou par un prestataire tiers, auquel des chercheurs agréés ont accès, et où le stockage sera assuré, mais sans qu'aucune transmission de données aux chercheurs agréés n'ait lieu, ou par d'autres modalités d'accès que le fournisseur de données mettra en place ou dont il facilitera l'établissement. Lorsque le coordinateur pour les services numériques de l'État membre d'établissement précise les modalités d'accès, il convient également qu'il énumère toutes les conditions juridiques, techniques ou organisationnelles auxquelles l'accès doit être soumis. Si la fourniture de l'accès implique un transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales au sens du chapitre V du règlement (UE) 2016/679, les modalités d'accès devraient également inclure des informations concernant la nécessité de mettre en place un mécanisme de transfert approprié, afin de veiller à ce que le fournisseur de données prenne les mesures nécessaires pour se conformer audit règlement.

(18) En vue de garantir que les modalités d'accès aux données sont appropriées pour tenir compte d'aspects particulièrement sensibles en matière de protection, de sécurité ou de confidentialité des données, le coordinateur pour les services numériques de l'État membre d'établissement devrait pouvoir exiger, sur la base des informations reçues dans la demande d'accès aux données, que l'accès aux données soit fourni par l'intermédiaire d'environnements de traitement sécurisés. Dans de tels cas, le coordinateur pour les services numériques de l'État membre d'établissement devrait veiller à ce que l'environnement choisi fonctionne conformément à la technologie la plus appropriée et permette aux chercheurs agréés d'atteindre leurs objectifs de recherche.

(19) Afin d'assurer la cohérence des informations transmises aux fournisseurs de données par les coordinateurs pour les services numériques de l'État membre d'établissement, il est nécessaire de préciser le contenu des demandes motivées.

(20) Pour préserver les intérêts des fournisseurs de données, réduire la fréquence des demandes de modification sur la durée et faciliter la formulation des demandes d'accès aux données pertinentes par les chercheurs, le coordinateur pour les services numériques de l'État membre d'établissement qui a émis les demandes motivées devrait publier sur le portail pour l'accès aux données en vertu du DSA un aperçu de chaque demande motivée, y compris toute modification et mise à jour de celle-ci.

(21) Afin de garantir que le coordinateur pour les services numériques de l'État membre d'établissement dispose des informations pertinentes pour évaluer une demande de modification et de faciliter une approche uniforme de l'évaluation des demandes de modification, le fournisseur de données devrait être tenu de préciser les motifs de cette demande, conformément à l'article 40, paragraphe 5, du règlement (UE) 2022/2065. Plus précisément, lorsque le coordinateur pour les services numériques de l'État membre d'établissement évalue une demande de modification justifiée par le fait que le fournisseur de données n'a pas accès aux données, il devrait être en mesure d'examiner si cette allégation est dûment étayée, par exemple par l'inexistence des données demandées, ou par des restrictions techniques telles que le chiffrement, et il devrait disposer des informations nécessaires pour examiner si l'absence d'accès est permanente ou temporaire. Il devrait être clair, à cet égard, que les considérations commerciales ne devraient pas être considérées comme un motif de refus automatique de l'accès aux données demandées, mais plutôt comme un motif de modification du moyen de fournir l'accès aux données, ce qui peut conduire à imposer des exigences supplémentaires en matière de sécurité et de confidentialité des données.

(22) Lorsqu'une demande de modification a été présentée, les fournisseurs de données devraient, pour favoriser un règlement efficace des litiges et encourager la recherche d'une solution mutuellement acceptable, pouvoir demander aux coordinateurs pour les services numériques des États membres d'établissement de participer à la médiation. Cette participation devrait être volontaire tout au long du processus de médiation et ne devrait pas aboutir à un résultat contraignant pour le coordinateur pour les services numériques de l'État membre d'établissement, qui reste compétent pour statuer sur les demandes de modification. Toutes les parties participant au processus de médiation devraient s'engager de bonne foi et s'efforcer de parvenir à un accord équitable et mutuellement acceptable.

(23) Afin d'éviter que la médiation ne prolonge indéfiniment le processus d'accès aux données, la transmission de la demande écrite de médiation, la sélection du médiateur et le processus de médiation proprement dit devraient respecter des calendriers précis. Les coordinateurs pour les services numériques de l'État membre d'établissement devraient fixer un délai pour le processus de médiation en ce qui concerne une demande motivée donnée et le médiateur devrait être habilité à mettre un terme au processus de médiation dans des circonstances particulières.

(24) Afin de maintenir la confiance mutuelle entre les parties participant à la médiation, le coordinateur pour les services numériques de l'État membre d'établissement devrait veiller à ce que le médiateur proposé satisfasse aux exigences d'impartialité et d'indépendance et possède une expertise pertinente de l'objet de la médiation.

(25) Pour faciliter la prise de décision éclairée et efficace en ce qui concerne le processus d'accès aux données, les coordinateurs pour les services numériques devraient avoir la possibilité de demander des avis d'experts sur des éléments spécifiques du processus d'accès aux données, tels que la détermination des modalités d'accès, y compris les interfaces appropriées, la formulation de la demande motivée et toute demande de modification présentée par le fournisseur de données. Les experts consultés devraient posséder une expertise avérée dans le domaine sur lequel leur avis est demandé et être indépendants. En particulier, ils ne devraient pas avoir de conflit d'intérêts découlant, par exemple, d'un quelconque lien avec les chercheurs demandeurs ou avec le fournisseur de données.

(26) Afin d'accroître la transparence et de permettre aux coordinateurs pour les services numériques de s'appuyer sur l'expertise qu'ils ont acquise au fil du temps, il convient d'enregistrer dans AGORA chaque demande de consultation d'experts et le suivi généré par celle-ci.

(27) Pour faciliter le contrôle effectif du respect des conditions énoncées dans la demande motivée, il convient que le fournisseur de données informe le coordinateur pour les services numériques de l'État membre d'établissement, dans un délai de trois jours ouvrables à compter de la date à laquelle l'accès est accordé aux chercheurs agréés et à compter de la date de la fin de l'accès.

(28) Afin de permettre aux chercheurs agréés d'utiliser les données demandées à des fins de recherche et de fournir des informations contextuelles pertinentes, les fournisseurs de données devraient communiquer aux chercheurs agréés les métadonnées et la documentation pertinentes décrivant les données mises à disposition, telles que les livres de codes, les journaux des modifications et la documentation sur l'architecture.

(29) Pour faciliter la réalisation de recherches utiles par les chercheurs agréés, notamment en leur permettant de combiner les données demandées avec les données disponibles par l'intermédiaire d'autres sources, les fournisseurs de données ne devraient imposer aucune restriction aux outils analytiques utilisés par les chercheurs agréés, y compris les bibliothèques logicielles pertinentes, ni formuler des exigences en matière d'archivage, de stockage, de mise à jour et de suppression, à moins qu'elles ne soient explicitement mentionnées dans les modalités d'accès définies dans la demande motivée.

(30) Lorsque les données fournies aux chercheurs agréés comprennent des données à caractère personnel au sens de l'article 4 du règlement (UE) 2016/679, le fournisseur de données devrait respecter les règles énoncées dans ledit règlement. En particulier, l'article 40, paragraphe 4, du règlement (UE) 2022/2065 crée une obligation légale au sens de l'article 6, paragraphe 1, point c), du règlement (UE) 2016/679 pour tout traitement de données à caractère personnel nécessaire pour que le fournisseur de données donne accès aux données spécifiées dans la demande motivée. Lorsque des catégories particulières de données à caractère personnel au sens de l'article 9 du règlement (UE) 2016/679 doivent être traitées, le présent règlement satisfait à l'exigence énoncée à l'article 9, paragraphe 2, point g), du règlement (UE) 2016/679.

(31) 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 ([4]) et a rendu un avis le 4 décembre 2024.

(32) Après consultation du comité européen des services numériques conformément à l'article 40, paragraphe 13, du règlement (UE) 2022/2065 et après son approbation,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet

Le présent règlement établit les procédures et les conditions techniques permettant aux chercheurs agréés d'accéder aux données détenues par les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne, conformément à l'article 40, paragraphe 4, du règlement (UE) 2022/2065, en particulier:

a) les conditions techniques relatives à la mise au point et au fonctionnement d'un portail d'accès aux données;

b) les procédures et les conditions techniques applicables à la gestion du processus d'accès aux données par les coordinateurs pour les services numériques et les fournisseurs de données;

c) les exigences relatives à la formulation de demandes motivées et à l'évaluation des demandes de modification;

d) les conditions techniques applicables à la fourniture de l'accès aux données par les fournisseurs de données.

Article 2

Définitions

Aux fins du présent règlement, les définitions figurant à l'article 4 du règlement (UE) 2016/679 et à l'article 3 du règlement (UE) 2018/1725 s'appliquent. De plus, on entend par:

1) «demande d'accès aux données»: les informations et la documentation pertinente soumises par les chercheurs demandeurs au coordinateur pour les services numériques de l'État membre d'établissement ou au coordinateur pour les services numériques de l'État membre de l'organisme de recherche auquel le chercheur principal est affilié, afin d'obtenir le statut de «chercheur agréé» mentionné à l'article 40, paragraphe 8, premier alinéa, du règlement (UE) 2022/2065, pour un projet de recherche particulier nécessitant l'accès aux données d'un fournisseur de données;

2) «processus d'accès aux données»: les étapes et procédures qui peuvent conduire à la fourniture d'un accès aux données tel que mentionné à l'article 40, paragraphe 4, du règlement (UE) 2022/2065;

3) «chercheur demandeur»: toute personne physique qui demande l'accès aux données tel que mentionné à l'article 40, paragraphe 4, du règlement (UE) 2022/2065, soit individuellement, soit en tant que membre d'un groupe ou d'une entité;

4) «chercheur principal»: le chercheur demandeur qui soumet la demande d'accès aux données à titre individuel ou pour le compte d'une entité ou d'un groupe de chercheurs demandeurs;

5) «fournisseur de données»: un fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne désigné comme tel conformément à l'article 33, paragraphe 4, du règlement (UE) 2022/2065, auquel une demande motivée pourrait être adressée;

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

6) «demande motivée»: une demande motivée d'accès aux données au titre de l'article 40, paragraphe 4, du règlement (UE) 2022/2065;

7) «demande de modification»: une demande de modification au titre de l'article 40, paragraphe 5, du règlement (UE) 2022/2065, présentée par le fournisseur de données au coordinateur pour les services numériques de l'État membre d'établissement à la suite de la réception d'une demande motivée;

8) «environnement de traitement sécurisé»: un environnement de traitement sécurisé au sens de l'article 2, point 20), du règlement (UE) 2022/868 du Parlement européen et du Conseil ([5]).

CHAPITRE II

OBLIGATIONS EN MATIÈRE D'INFORMATION ET DE POINTS DE CONTACT

Article 3

Portail pour l'accès aux données en vertu du DSA

1. La Commission met en place et héberge un portail pour l'accès aux données en vertu du DSA.

2. Les fonctions du portail pour l'accès aux données en vertu du DSA sont les suivantes:

a) soutenir et rationaliser la gestion du processus d'accès aux données pour les chercheurs, les fournisseurs de données et les coordinateurs pour les services numériques;

b) servir de guichet numérique central pour les informations concernant le processus d'accès aux données et faciliter les échanges d'informations au titre du présent règlement entre les chercheurs demandeurs, les chercheurs agréés, les fournisseurs de données et les coordinateurs pour les services numériques.

3. Le portail pour l'accès aux données en vertu du DSA est interopérable avec le système de partage d'informations AGORA établi par le règlement d'exécution (UE) 2024/607. Les coordinateurs pour les services numériques ont accès, dans AGORA, aux informations soumises par l'intermédiaire du portail pour l'accès aux données en vertu du DSA.

4. Les fournisseurs de données disposent d'un compte sur le portail pour l'accès aux données en vertu du DSA.

5. Pour participer au processus d'accès aux données, les candidats chercheurs disposent d'un compte sur le portail pour l'accès aux données en vertu du DSA.

Article 4

Rôles et responsabilités en matière de traitement des données à caractère personnel sur le portail pour l'accès aux données en vertu du DSA

1. Les coordinateurs pour les services numériques sont considérés comme des responsables du traitement distincts en ce qui concerne le traitement des données à caractère personnel qu'ils effectuent aux fins de la gestion du processus d'accès aux données et de la publication des informations pertinentes.

2. La Commission est considérée comme un sous-traitant des données à caractère personnel traitées dans le cadre du portail pour l'accès aux données en vertu du DSA.

3. Les responsabilités de la Commission en tant que sous-traitant pour les activités de traitement des données menées dans le cadre du portail pour l'accès aux données en vertu du DSA sont définies à l'annexe.

([5]) 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).

Article 5

Traitement des données à caractère personnel dans le cadre du portail pour l'accès aux données en vertu du DSA

1. Lorsque des données à caractère personnel sont enregistrées et échangées par l'intermédiaire du portail pour l'accès aux données en vertu du DSA, le traitement n'a lieu que dans la mesure où il est proportionné et nécessaire aux fins du processus d'accès aux données et de la publication des informations pertinentes.

2. Le traitement de données à caractère personnel dans le cadre du portail pour l'accès aux données en vertu du DSA ne peut avoir lieu que pour les catégories suivantes de personnes concernées:

a) les personnes physiques qui disposent d'un compte sur le portail pour l'accès aux données en vertu du DSA;

b) les personnes physiques dont les données à caractère personnel figurent sur le portail pour l'accès aux données en vertu du DSA ou dans tout autre échange en vertu du présent règlement concernant le processus d'accès aux données.

3. Le traitement de données à caractère personnel dans le cadre du portail pour l'accès aux données en vertu du DSA ne peut avoir lieu que pour les catégories suivantes de données à caractère personnel:

a) les données d'identité, telles que le nom, l'identifiant de l'utilisateur;

b) les coordonnées, telles que l'adresse, l'adresse électronique et autres renseignements;

c) les données à caractère personnel contenues dans les documents prouvant l'affiliation à un organisme de recherche, ainsi que toute autre information à caractère personnel jugée nécessaire aux fins de la participation au processus d'accès aux données.

4. Le traitement des données à caractère personnel mentionné au paragraphe 1 s'effectue au moyen d'infrastructures informatiques situées dans l'Espace économique européen.

Article 6

Points de contact et informations publiques sur le processus d'accès aux données

1. Chaque coordinateur pour les services numériques et chaque fournisseur de données établissent un point de contact spécifique, chargé de fournir des informations et un soutien sur le processus d'accès aux données.

2. Les coordinateurs pour les services numériques et les fournisseurs de données communiquent dès que possible leurs points de contact à la Commission. La Commission publie les coordonnées des points de contact mentionnés au paragraphe 1 dans l'interface publique du portail pour l'accès aux données en vertu du DSA.

3. Chaque coordinateur pour les services numériques veille à ce que les coordonnées du point de contact établi en vertu du paragraphe 1 soient disponibles et facilement consultables sur son interface en ligne, et à ce qu'elles soient accompagnées d'un lien vers le portail pour l'accès aux données en vertu du DSA.

4. Les fournisseurs de données veillent à ce que les informations suivantes soient disponibles et facilement consultables sur leurs interfaces en ligne:

a) les coordonnées du point de contact qu'ils ont établi conformément au paragraphe 1;

b) un lien vers le portail pour l'accès aux données en vertu du DSA;

c) un catalogue de données DSA, qui décrit les ressources en données auxquels il est possible d'accéder aux fins énoncées à l'article 40, paragraphe 4, du règlement (UE) 2022/2065, ainsi que leur structure de données et leurs métadonnées;

d) des propositions de modalités d'accès aux données figurant dans le catalogue conformément au point c), adaptées au niveau de sensibilité des différentes ressources en données.

5. Les informations mentionnées au paragraphe 4, points c) et d), sont régulièrement mises à jour, notamment pour refléter les données relatives aux évaluations des risques effectuées conformément à l'article 34 du règlement (UE) 2022/2065 et aux audits réalisés au titre de l'article 37 dudit règlement.

CHAPITRE III

EXIGENCES RELATIVES À LA FORMULATION ET AU TRAITEMENT DES DEMANDES MOTIVÉES

Article 7

Formulation de la demande motivée

1. Dans un délai de 80 jours ouvrables à compter de la présentation d'une demande d'accès aux données, le coordinateur pour les services numériques de l'État membre d'établissement, en tenant dûment compte des conditions préalables énoncées à l'article 8 et, le cas échéant, de toute autre évaluation pertinente à ces fins, décide si une demande motivée peut être formulée et prend l'une des mesures suivantes:

a) il formule une demande motivée, la soumet au fournisseur de données et informe le chercheur principal qu'une demande motivée a été soumise;

b) il informe le chercheur principal des raisons pour lesquelles la demande motivée n'a pas pu être formulée.

2. Lorsque, dans des cas dûment justifiés, le coordinateur pour les services numériques de l'État membre d'établissement a besoin d'un délai supplémentaire pour formuler une demande motivée, il en informe le chercheur principal dès que possible, indique les raisons du retard et communique une nouvelle date pour prendre les mesures mentionnées au paragraphe 1.

Article 8

Conditions préalables à la formulation d'une demande motivée

Le coordinateur pour les services numériques de l'État membre d'établissement décide si une demande motivée peut être formulée en tenant compte des éléments suivants:

a) pour chaque chercheur demandeur:

   i) une confirmation d'affiliation à un organisme de recherche au sens de l'article 2, point 1), de la directive (UE) 2019/790 du Parlement européen et du Conseil ([6]);

   ii) une déclaration d'indépendance à l'égard des intérêts commerciaux pertinents pour le projet spécifique pour lequel les données sont demandées;

   iii) l'engagement de mettre gratuitement à la disposition du public les résultats de ses travaux de recherche;

b) des informations sur le financement du projet de recherche pour lequel les données sont demandées;

c) une description des données demandées, y compris le format, la portée et, si possible, les attributs spécifiques, les métadonnées pertinentes et la documentation relative aux données, en tenant compte également des informations mises à disposition conformément à l'article 6, paragraphe 4, du présent règlement;

d) des informations sur la nécessité et la proportionnalité de l'accès aux données et sur les calendriers des travaux de recherche pour lesquels les données sont demandées;

e) des informations sur les risques recensés en termes de confidentialité, de sécurité des données et de protection des données à caractère personnel, qui sont associés aux données auxquelles il serait possible d'accéder, une description des mesures techniques, juridiques et organisationnelles qui seront mises en place, y compris, dans la mesure du possible, des propositions de modalités d'accès, pour atténuer ces risques lors du traitement des données demandées;

f) une description des activités de recherche à mener avec les données demandées;

g) un résumé de la demande d'accès aux données contenant les éléments suivants:

   i) le sujet des travaux de recherche;

   ii) le fournisseur de données auquel les données sont demandées;

   iii) une description des données demandées, telle que mentionnée au point c).

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

Article 9

Modalités d'accès

1. Le coordinateur pour les services numériques de l'État membre d'établissement détermine les modalités, y compris les mesures techniques, juridiques et organisationnelles, que le fournisseur de données doit utiliser pour octroyer aux chercheurs agréés l'accès aux données.

2. Les coordinateurs pour les services numériques sont autorisés à consulter les autorités de contrôle concernées instituées en vertu de l'article 51 du règlement (UE) 2016/679.

3. Lorsqu'il détermine les modalités d'accès, le coordinateur pour les services numériques de l'État membre d'établissement tient compte des informations fournies dans la demande d'accès aux données, en particulier les informations mentionnées à l'article 8, point e), en tenant également compte des droits et des intérêts des fournisseurs de données et des bénéficiaires du service concerné, y compris la protection des informations confidentielles et des secrets d'affaires, et en préservant la sécurité de leur service et des informations mises à disposition par les fournisseurs de données conformément à l'article 6, paragraphe 4, point d).

4. Outre les éléments mentionnés au paragraphe 3, le coordinateur pour les services numériques de l'État membre d'établissement tient compte, lorsqu'il détermine les modalités d'accès, des éléments suivants:

a) lorsque l'accès implique le traitement de données à caractère personnel:

   i) l'évaluation des risques concernant le traitement des données à caractère personnel telle que décrite à l'article 8, point e), y compris, le cas échéant, les analyses d'impact relatives à la protection des données au sens de l'article 35 du règlement (UE) 2016/679;

   ii) les mesures techniques et organisationnelles envisagées, telles que présentées conformément à l'article 8, point e);

b) les mesures de sécurité du réseau pertinentes, le chiffrement, les mécanismes de contrôle d'accès, les politiques de sauvegarde, les mécanismes d'intégrité des données, les plans de réaction en cas d'incident;

c) le cas échéant, des informations sur la période de conservation prévue et les plans de destruction des données pertinents;

d) toute mesure organisationnelle telle que les procédures d'examen en interne, les restrictions des droits d'accès et le partage d'informations;

e) toute clause contractuelle proposée, telle que des accords de non-divulgation, des accords concernant les données et tout autre type de déclarations écrites, pour convenir d'éventuelles conditions d'accès et de traitement entre le chercheur principal et le fournisseur de données;

f) l'existence d'une formation sur la sécurité des données et la protection des données à caractère personnel reçue par les chercheurs demandeurs;

g) la nécessité éventuelle d'environnements de traitement sécurisés pour traiter les données.

5. Lorsque le coordinateur pour les services numériques de l'État membre d'établissement estime qu'un environnement de traitement sécurisé doit être utilisé pour donner accès aux données demandées, il exige des documents attestant que l'opérateur de cet environnement:

a) précise les conditions d'accès à l'environnement de traitement sécurisé afin de réduire au minimum le risque de lecture, de copie, de modification ou de suppression non autorisées des données hébergées dans l'environnement de traitement sécurisé;

b) veille à ce que les chercheurs agréés n'aient accès qu'aux données couvertes par la demande motivée, au moyen d'identités d'utilisateur individuelles et uniques et de modes d'accès confidentiels;

c) tient des registres identifiables de l'accès à l'environnement de traitement sécurisé pendant la période nécessaire pour vérifier et contrôler toutes les opérations de traitement dans cet environnement;

d) veille à ce que la puissance de calcul dont disposent les chercheurs agréés soit appropriée et suffisante aux fins du projet de recherche;

e) contrôle l'efficacité des mesures énumérées aux points a) à d).

Article 10

Contenu de la demande motivée

1. Une demande motivée contient aux moins les éléments suivants:

a) la date à partir de laquelle le fournisseur de données donne accès aux données demandées et la date à laquelle cet accès prend fin;

b) les modalités d'accès déterminées conformément à l'article 9;

c) le résumé de la demande d'accès aux données mentionné à l'article 8, point g).

2. Le coordinateur pour les services numériques de l'État membre d'établissement peut faire figurer dans la demande motivée les noms et coordonnées de tous les chercheurs agréés mentionnés dans la demande d'accès aux données lorsque cela est nécessaire pour permettre l'accès aux données demandées, conformément aux modalités d'accès précisées dans la demande motivée.

3. Si la fourniture de l'accès implique un transfert de données à caractère personnel vers un pays tiers ou à des organisations internationales au sens du chapitre V du règlement (UE) 2016/679, la demande motivée devrait inclure des informations concernant la nécessité de mettre en place un mécanisme de transfert approprié ou d'y faire référence, afin de garantir le respect des dispositions dudit règlement.

Article 11

Publication d'un aperçu d'une demande motivée sur le portail pour l'accès aux données en vertu du DSA

1. Lorsqu'une demande motivée est formulée, le coordinateur pour les services numériques de l'État membre d'établissement publie un aperçu de cette demande motivée dans l'interface publique du portail pour l'accès aux données en vertu du DSA. L'aperçu contient tous les éléments suivants:

a) le résumé de la demande d'accès aux données mentionné à l'article 8, point g);

b) les modalités d'accès déterminées conformément à l'article 9.

2. L'aperçu prévu au paragraphe 1 est mis à jour pour tenir compte de tout changement résultant d'une modification d'un ou de plusieurs éléments à la suite de l'examen d'une demande de modification ou du résultat d'une médiation conformément à l'article 13.

Article 12

Procédures d'examen des demandes de modification

1. Dès que le coordinateur pour les services numériques de l'État membre d'établissement reçoit une demande de modification au titre de l'article 40, paragraphe 5, du règlement (UE) 2022/2065, il en informe le chercheur principal concerné.

2. Lorsqu'il se prononce sur une demande de modification présentée en vertu de l'article 40, paragraphe 5, point a), du règlement (UE) 2022/2065, le coordinateur pour les services numériques de l'État membre d'établissement tient compte des éléments suivants:

a) l'existence de motifs dûment établis pour expliquer l'absence d'accès aux données alléguée;

b) le caractère permanent ou temporaire de l'absence d'accès aux données.

3. Lorsqu'il statue sur une demande de modification présentée en vertu de l'article 40, paragraphe 5, point b), du règlement (UE) 2022/2065, le coordinateur pour les services numériques de l'État membre d'établissement tient compte de tous les éléments suivants:

a) l'existence d'une motivation dûment établie concernant les vulnérabilités alléguées et leur importance;

b) la probabilité et la gravité du préjudice résultant des vulnérabilités importantes alléguées;

c) la mesure dans laquelle les modalités d'accès énoncées dans la demande motivée atténuent effectivement le risque de survenance d'un tel préjudice.

4. À tout moment au cours de l'évaluation d'une demande de modification, le coordinateur pour les services numérique s de l'État membre d'établissement peut demander au fournisseur de données ou au chercheur principal toute information complémentaire qu'il juge nécessaire pour mener à bien son évaluation.

5. Cette demande d'informations complémentaires est présentée dès que possible afin que le fournisseur de données ou le chercheur principal dispose d'un délai de réponse suffisant et, en tout état de cause, que cela n'ait pas d'incidence sur le délai fixé à l'article 40, paragraphe 6, deuxième alinéa, du règlement (UE) 2022/2065. Lorsque le fournisseur de données ou le chercheur principal ne fournit pas du tout les informations demandées, ne les fournit pas dans un délai fixé par le coordinateur pour les services numériques de l'État membre d'établissement, ou ne les fournit que partiellement, le coordinateur prend sa décision dans le délai fixé à l'article 40, paragraphe 6, du règlement (UE) 2022/2065, sur la base des informations qui ont été mises à sa disposition dans un délai raisonnable.

Article 13

Médiation

1. Si le fournisseur de données est en désaccord avec la décision du coordinateur pour les services numériques de l'État membre d'établissement en ce qui concerne la demande de modification, le fournisseur de données peut, dans un délai de cinq jours ouvrables à compter de la communication faite par le coordinateur pour les services numériques de l'État membre d'établissement conformément à l'article 40, paragraphe 6, deuxième alinéa, du règlement (UE) 2022/2065, demander par écrit au coordinateur de participer à un processus de médiation.

2. Le coordinateur pour les services numériques de l'État membre d'établissement n'est pas tenu de participer au processus de médiation.

3. La demande écrite mentionnée au paragraphe 1 comprend une description concise des éléments spécifiques de la décision, tels que communiqués par le coordinateur pour les services numériques de l'État membre d'établissement conformément à l'article 40, paragraphe 6, deuxième alinéa, du règlement (UE) 2022/2065, qui sont contestés par le fournisseur de données.

4. Le coordinateur et le fournisseur de données conviennent de la désignation d'un médiateur et entament la médiation dans un délai de 20 jours ouvrables à compter de la présentation de la demande de médiation conformément au paragraphe 3.

5. Avant de donner son accord sur la désignation d'un médiateur, le coordinateur vérifie que le médiateur est impartial et indépendant et possède l'expertise pertinente en rapport avec l'objet décrit dans la demande écrite visée au paragraphe 1.

6. Le fournisseur de données supporte tous les coûts de la médiation.

7. Le coordinateur pour les services numériques de l'État membre d'établissement informe le chercheur principal de la demande de médiation mentionnée au paragraphe 1 dans les meilleurs délais et peut décider d'inviter le chercheur principal à participer à la médiation en tant que partie. Lorsque la demande d'accès aux données a été soumise au coordinateur pour les services numériques de l'organisme de recherche, le coordinateur pour les services numériques de l'État membre d'établissement peut inviter le coordinateur pour les services numériques de l'organisme de recherche à participer au processus de médiation. Une invitation à participer au processus de médiation émanant du coordinateur pour les services numériques de l'État membre d'établissement n'oblige pas la partie invitée à prendre part à ce processus.

8. La participation à la médiation ne porte pas atteinte au droit des parties d'engager une procédure judiciaire à tout moment avant, pendant ou après la médiation.

9. Le coordinateur pour les services numériques de l'État membre d'établissement fixe, pour la médiation, un délai qui ne dépasse pas 40 jours ouvrables à compter du jour de l'ouverture du processus de médiation conformément au paragraphe 4.

10. Le médiateur peut mettre fin à la médiation avant l'expiration de ce délai dans l'un des cas suivants:

a) l'une des parties demande explicitement qu'un terme soit mis à la médiation;

b) il apparaît clairement que le comportement des parties au cours de la médiation, notamment l'absence de bonne foi, rend improbable la conclusion d'un accord.

11. Lorsque la médiation aboutit à un accord entre les parties, le coordinateur pour les services numériques de l'État membre d'établissement tient compte de cet accord et, le cas échéant, modifie la demande motivée et en informe le chercheur principal.

12. Lorsque les parties ne parviennent pas à un accord, le coordinateur pour les services numériques de l'État membre d'établissement informe le fournisseur de données que la décision du coordinateur pour les services numériques de l'État membre d'établissement concernant la demande de modification, telle que communiquée en dernier lieu conformément à l'article 40, paragraphe 6, deuxième alinéa, du règlement (UE) 2022/2065, est considérée comme valable et sert de base pertinente pour les étapes ultérieures du processus, et en informe le chercheur principal.

13. Le coordinateur pour les services numériques de l'État membre d'établissement enregistre dans AGORA un compte rendu sommaire de la médiation, établi par le médiateur et signé par toutes les parties. Ce compte rendu contient les informations suivantes:

a) la date de la demande écrite de médiation émanant du fournisseur de données;

b) l'identité et les coordonnées des parties;

c) les dates de début et de fin de la médiation;

d) le résultat de la médiation, y compris tout accord conclu ou le motif pour lequel la médiation a pris fin.

Article 14

Consultation d'experts indépendants

1. Avant de formuler une demande motivée ou de prendre une décision sur une demande de modification, le coordinateur pour les services numériques peut décider de consulter des experts.

2. Les experts sont indépendants et impartiaux, possèdent une expertise pertinente et des compétences avérées et disposent des capacités et des ressources nécessaires pour exécuter la tâche prévue, sans retard injustifié.

3. Pour attester de leur impartialité, les experts signent une déclaration confirmant qu'ils:

a) n'ont aucun lien financier ou personnel avec le fournisseur de données ou les chercheurs demandeurs;

b) ne sont pas intéressés par l'issue du processus d'accès aux données;

c) sont libres de tout conflit d'intérêts.

4. Le coordinateur pour les services numériques encode dans AGORA toute consultation effectuée en vertu du paragraphe 1, ainsi que l'avis d'expert reçu en réponse à la consultation, dans les meilleurs délais.

CHAPITRE IV

CONDITIONS DANS LESQUELLES LES DONNÉES DEMANDÉES SONT FOURNIES AUX CHERCHEURS AGRÉÉS

Article 15

Partage des données et documentation relative aux données

1. Les fournisseurs de données informent le coordinateur pour les services numériques de l'État membre d'établissement, dans un délai de trois jours ouvrables:

a) que l'accès aux données demandées a été accordé à des chercheurs agréés, conformément à la demande motivée;

b) qu'il a été mis fin à l'accès des chercheurs agréés.

2. Les fournisseurs de données communiquent aux chercheurs agréés toute information supplémentaire nécessaire pour accéder aux données demandées et les comprendre, telles que les livres de codes, les journaux des modifications et la documentation relatives à l'architecture. Si la fourniture de ces informations peut être à l'origine d'une vulnérabilité importante des services du fournisseur de données, ce dernier informe le coordinateur pour les services numériques de l'État membre d'établissement de ce risque et propose, dans la mesure du possible, d'autres informations.

3. Lorsqu'ils donnent accès à des données, les fournisseurs de données n'imposent pas aux chercheurs agréés des obligations en matière de gestion des données, telles que des exigences en matière d'archivage, de stockage, de mise à jour et de suppression, ou des limitations à l'utilisation d'outils analytiques standard, susceptibles d'entraver la réalisation de la recherche concernée, à moins que ces exigences ou limitations ne soient explicitement mentionnées dans la demande motivée.

4. Lorsque des données à caractère personnel sont traitées, les fournisseurs de données n'imposent aux chercheurs agréés aucune condition relative au traitement des données à caractère personnel partagées autre que celles spécifiées dans la demande motivée.

CHAPITRE V

DISPOSITIONS FINALES

Article 16

Entrée en vigueur

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

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

Fait à Bruxelles, le 1er juillet 2025.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE

Responsabilités de la Commission en tant que sous-traitant pour les activités de traitement des données menées dans le cadre du portail pour l'accès aux données en vertu du DSA

1. La Commission met en place et garantit, au nom des coordinateurs pour les services numériques, une infrastructure informatique sécurisée et fiable, le portail pour l'accès aux données en vertu du DSA, qui soutient et rationalise la gestion du processus d'accès aux données pour les chercheurs, les organismes de recherche, les fournisseurs de données et les coordinateurs pour les services numériques.

2. Afin de remplir ses obligations en qualité de sous-traitant des coordinateurs pour les services numériques, la Commission peut faire appel à des tiers en tant que sous-traitants ultérieurs. En pareil cas, les responsables du traitement autorisent la Commission à faire appel à des sous-traitants ultérieurs ou à remplacer ces derniers si nécessaire. La Commission informe les responsables du traitement du recours à des sous-traitants ultérieurs ou du remplacement de ces derniers, pour donner ainsi aux responsables du traitement la possibilité de s'opposer à toute modification de ce type. La Commission veille à ce que les mêmes obligations en matière de protection des données que celles énoncées dans le présent règlement s'appliquent à ces sous-traitants ultérieurs.

3. La Commission ne procède au traitement de données à caractère personnel que dans la mesure où cela est nécessaire pour:

   a) l'authentification et le contrôle d'accès à l'égard de tous les utilisateurs du portail pour l'accès aux données en vertu du DSA;

   b) l'autorisation de la mise en œuvre des demandes des utilisateurs du portail pour l'accès aux données en vertu du DSA relatives à la création, la mise à jour et la suppression de toute information contenue dans la demande sur le portail pour l'accès aux données en vertu du DSA;

   c) la réception des données à caractère personnel visées à l'article 5, paragraphe 3, du présent règlement, téléchargées par les utilisateurs du portail pour l'accès aux données en vertu du DSA;

   d) le stockage des données à caractère personnel sur le portail pour l'accès aux données en vertu du DSA;

   e) la suppression des données à caractère personnel à leur date d'expiration ou sur instruction du responsable du traitement;

   f) après la fin de la prestation des services fournis par le portail pour l'accès aux données en vertu du DSA, la suppression de toutes les données à caractère personnel restantes, sauf si le droit de l'Union ou le droit d'un État membre en impose le stockage.

4. La Commission prend toutes les mesures de sécurité à la pointe de la technique nécessaires sur les plans organisationnel, physique et logique pour assurer le fonctionnement du portail pour l'accès aux données en vertu du DSA. À cette fin, la Commission:

   a) désigne une entité responsable de la gestion de la sécurité du portail pour l'accès aux données en vertu du DSA, communique ses coordonnées aux responsables du traitement et veille à sa disponibilité pour répondre aux menaces pour la sécurité;

   b) est chargée d'assurer la sécurité du portail pour l'accès aux données en vertu du DSA, notamment en procédant régulièrement à des essais, des analyses et des évaluations des mesures de sécurité.

5. La Commission prend toutes les mesures de sécurité nécessaires pour éviter de compromettre le bon fonctionnement opérationnel du portail pour l'accès aux données en vertu du DSA. Il s'agit notamment:

   a) de procédures d'évaluation des risques, afin d'identifier et d'estimer les menaces potentielles pour le portail pour l'accès aux données en vertu du DSA;

   b) d'une procédure d'audit et de contrôle destinée:

      i) à vérifier la correspondance entre les mesures de sécurité mises en œuvre et la politique de sécurité applicable;

      ii) à contrôler régulièrement l'intégrité du portail pour l'accès aux données en vertu du DSA, les paramètres de sécurité et les autorisations accordées;

      iii) à détecter les atteintes à la sécurité et les intrusions sur le portail pour l'accès aux données en vertu du DSA;

iv) à appliquer des modifications afin de pallier les failles existantes en matière de sécurité sur le portail pour l'accès aux données en vertu du DSA;

v) à définir les conditions dans lesquelles il convient d'autoriser, notamment à la demande des responsables du traitement, la réalisation d'audits indépendants, y compris des inspections, et d'examens des mesures de sécurité, ainsi que de contribuer à ces opérations, sous réserve de conditions qui respectent le protocole n° 7 du traité sur le fonctionnement de l'Union européenne relatif aux privilèges et immunités de l'Union européenne;

c) d'une modification de la procédure de contrôle afin de documenter et de mesurer l'incidence des modifications avant leur mise en œuvre et de tenir les responsables du traitement informés de toute modification susceptible d'affecter la communication avec leurs infrastructures et/ou la sécurité du portail pour l'accès aux données en vertu du DSA;

d) d'établir une procédure de maintenance et de réparation, afin de préciser les règles et les conditions à respecter lors de la maintenance et/ou de la réparation du portail pour l'accès aux données en vertu du DSA;

e) d'établir une procédure relative aux incidents de sécurité, afin de définir le système de signalement et d'escalade, d'informer sans délai les responsables du traitement concernés, d'informer sans délai les responsables du traitement pour qu'ils avertissent les autorités nationales de contrôle de la protection des données de toute violation de données à caractère personnel, et de définir une procédure disciplinaire pour les atteintes à la sécurité du portail pour l'accès aux données en vertu du DSA.

6. La Commission prend des mesures de sécurité physiques et logiques à la pointe de la technique pour les installations hébergeant le portail pour l'accès aux données en vertu du DSA ainsi que pour les contrôles des données et les contrôles d'accès de sécurité s'y rapportant. À cette fin, la Commission:

a) assure la sécurité physique, afin de mettre en place des périmètres de sécurité distincts et de permettre la détection des atteintes dans le portail pour l'accès aux données en vertu du DSA;

b) contrôle l'accès aux installations du portail pour l'accès aux données en vertu du DSA;

c) veille à ce qu'aucun équipement ne puisse être ajouté, remplacé ou retiré sans l'autorisation préalable des organismes compétents désignés;

d) contrôle l'accès depuis et vers le portail pour l'accès aux données en vertu du DSA;

e) veille à ce que les utilisateurs du portail pour l'accès aux données en vertu du DSA qui accèdent à ce portail soient authentifiés;

f) réexamine les droits d'autorisation relatifs à l'accès au portail pour l'accès aux données en vertu du DSA en cas d'atteinte à la sécurité touchant ce portail;

g) préserve l'intégrité des informations transmises par l'intermédiaire du portail pour l'accès aux données en vertu du DSA;

h) met en œuvre des mesures de sécurité d'ordre technique et organisationnel afin d'empêcher l'accès non autorisé aux données à caractère personnel dans le portail pour l'accès aux données en vertu du DSA;

i) met en œuvre, en tant que de besoin, des mesures visant à empêcher tout accès non autorisé au portail pour l'accès aux données en vertu du DSA (blocage d'une localisation/d'une adresse IP).

7. La Commission:

a) prend des mesures pour protéger son domaine, y compris la rupture des connexions, en cas d'écart important par rapport aux principes et concepts de qualité ou de sécurité;

b) maintient un plan de gestion des risques lié à son domaine de compétence;

c) surveille — en temps réel — la performance de tous les éléments de service du portail pour l'accès aux données en vertu du DSA, produit des statistiques régulières et tient des registres;

d) fournit aux utilisateurs du portail pour l'accès aux données en vertu du DSA une assistance en anglais;

e) aide les responsables du traitement, au moyen de mesures techniques et organisationnelles appropriées, à s'acquitter de leur obligation de répondre aux demandes d'exercice des droits de la personne concernée prévus au chapitre III du règlement (UE) 2016/679;

f) soutient les responsables du traitement en fournissant des informations sur le portail pour l'accès aux données en vertu du DSA, dans le but de mettre en application les obligations énoncées aux articles 32, 33, 34, 35 et 36 du règlement (UE) 2016/679;

g) veille à ce que les données traitées dans le cadre du portail pour l'accès aux données en vertu du DSA soient inintelligibles pour toute personne non autorisée à y accéder;

h) prend toutes les mesures utiles pour empêcher l'accès non autorisé aux données à caractère personnel transmises via le portail pour l'accès aux données en vertu du DSA;

i) prend des mesures pour faciliter la communication entre les responsables du traitement;

j) tient un registre des activités de traitement effectuées pour le compte des responsables du traitement conformément à l'article 31, paragraphe 2, du règlement (UE) 2018/1725.