EUROPEAN
COMMISSION

Brussels, 1.7.2025
C(2025) 4340 final

COMMISSION DELEGATED REGULATION (EU) …/...

of 1.7.2025

supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council by laying down the technical conditions and procedures under which providers of very large online platforms and of very large online search engines are to share data with vetted researchers

(Text with EEA relevance)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE DELEGATED ACT

On 16 November 2022, Regulation (EU) 2022/2065 of the European Parliament and of the Council, the Digital Services Act (DSA)[1] entered into force. That Regulation provides a harmonised legal framework applicable to all online intermediary services provided in the Union and seeks to create a safer digital space, in which fundamental rights are effectively protected.

Regulation (EU) 2022/2065 includes a special set of obligations for providers of very large online platforms and of very large online search engines, proportionate to their particular role and societal impact in the Union. The obligations imposed on those providers seek to increase their public accountability and include the obligation to maintain public repositories of advertisements, to publish reports at least once a year on the results of their assessment of any systemic risks stemming from the design, functioning or use of their service and its related systems, and on the risk mitigation measures they put in place, as well as reports resulting from independent compliance audits.

Article 40 of Regulation (EU) 2022/2065 requires providers of very large online platforms and of very large online search engines to provide access to the data they hold for the purposes of regulatory supervision, research and scrutiny that contributes to the detection, identification and understanding of systemic risks in the Union, and to the assessment of the adequacy, efficiency and impacts of risk mitigation measures that those providers have to take under that Regulation. The impact of this provision is twofold: researchers who fulfil the conditions set out in the provision will benefit from access to previously undisclosed or under-disclosed data, opening up new avenues for research and increasing the potential of generating knowledge for the benefit of all. At the same time, these insights will contribute to the work of competent authorities in carrying out their supervision and enforcement tasks, including the assessment of the steps taken by providers of very large online platforms and of very large online search engines to fulfil their obligations under Regulation (EU) 2022/2065.

Pursuant to Article 40(13) of Regulation (EU) 2022/2065, the Commission shall adopt delegated acts to supplement that Regulation by laying down the technical conditions under which providers of very large online platforms or of very large online search engines are to share data pursuant to Article 40, paragraphs 1 and 4, of Regulation (EU) 2022/2065 and the purposes for which the data may be used. In addition, the provision states that those delegated acts shall lay down the specific conditions under which such sharing of data with researchers can take place in compliance with Regulation (EU) 2016/679, as well as relevant objective indicators, procedures and, where necessary, independent advisory mechanisms in support of sharing of data, taking into account the rights and interests of the providers of very large online platforms or of very large online search engines and the recipients of the service concerned, including the protection of confidential information, in particular trade secrets, and maintaining the security of their service.

This delegated act specifies the procedures and technical conditions enabling the provision of access to data pursuant to Article 40, paragraph 4 of Regulation (EU) 2022/2065. Given the important role that researchers can play for the detection, identification and understanding of systemic risks in the Union and for the assessment of the adequacy, efficiency and impact of risk mitigation measures that providers of very large online platforms and of very large online

[1] OJ L277, 27.10.2022, p. 1.

search engines are required to take under that Regulation, this delegated act is intended to ensure an effective and harmonised application of the provision regulating access to data for vetted researchers pursuant to Regulation (EU) 2022/2065.

The rules laid down in this delegated act build on existing practices for accessing data from providers of very large online platforms or of very large online search engines, which were set up on a voluntary basis. Considering the innovative nature of the mechanism set out in Article 40(4) of Regulation (EU) 2022/2065 involving different actors, namely researchers, Digital Services Coordinators and providers of very large online platforms or of very large online search engines, specific procedures are set out to develop reliable, consistent and uniform practices, and to protect the rights and interests of all the actors involved.

In particular, the delegated act sets out the procedures to be followed by Digital Services Coordinators for the formulation of reasoned requests for data access to providers of very large online platforms or of very large online search engines. In doing so, this delegated act also clarifies and harmonises the procedures for the management of the data access process, and establishes the Digital Services Act (DSA) data access portal, to underpin the different steps in that process. Moreover, the delegated act sets out the legal, organisational and technical conditions to be taken into account by the Digital Services Coordinator of establishment when determining the appropriate access modalities for the provision of access to data. To this end, the delegated act sets out rules for the interactions between the Digital Services Coordinator of establishment and the providers of very large online platforms or of very large online search engines in the processing of the reasoned request for data access.

The delegated act aims at establishing a consistent and uniform process for data access for vetted researchers, which will protect the rights and interests of those involved – while containing adequate safeguards against any form of abuse.

2. CONSULTATIONS PRIOR TO THE ADOPTION OF THE ACT

Over the two years preceding the adoption of this delegated act, the Commission has collected views from a wide range of different stakeholders, including providers of digital services, such as providers of very large online platforms or of very large search engines, providers of other online platforms and other intermediary service providers, other businesses, civil society organisations as well as an expert group of academics and researchers.

In addition, the Commission conducted a public call for evidence from 25 April to 31 May 2023. 133 contributions were received, gathering input on data access needs from researchers, providers of online platforms, civil society organisations as well as other interested stakeholders. The call also covered operational aspects of data access, such as procedural and technical requirements for data access applications.

The Commission also conducted targeted consultations with specialised stakeholders in the field of research and access to data, including Digital Services Coordinators, in order to gather further technical views and identify areas that would benefit from further specification in this delegated act. Consultations took place with academics, civil society actors and intermediary service providers.

Furthermore, the Commission published a draft of this delegated act for public feedback from 29 October 2024 to 10 December 2024. 109 contributions were received mainly from researchers, Digital Services Coordinators and businesses.

This delegated act addresses the main points raised by stakeholders with a view to ensuring that an efficient and harmonised process is in place, balancing the rights and interests of all

actors involved for the provision of access to data for vetted researchers as required by Regulation (EU) 2022/2065.

3. LEGAL ELEMENTS OF THE DELEGATED ACT

ELEMENTS OF THE DELEGATED ACT

Chapter I sets out the general provisions, namely the subject matter of the delegated act (Article 1) and the definitions of key terms (Article 2).

Chapter II sets out the information and contact obligations in relation to the data access process. First, it establishes the DSA data access portal (Article 3), then it sets out the roles and responsibilities for the processing of personal data carried out in the DSA data access portal (Article 4) and the rules for the processing of personal data in the DSA data access portal (Article 5). Lastly, it sets out requirements regarding the points of contact and information to the public on the data access process (Article 6).

Chapter III lays down the requirements for the formulation and processing of reasoned requests for data access. It provides details on the formulation of a reasoned request for data access by the Digital Services Coordinator of establishment pursuant to Article 40(4) of Regulation (EU) 2022/2065 (Article 7), on the prerequisites for the formulation of a reasoned request for data access (Article 8), on the appropriateness of the access modalities to ensure compliance with the data security, confidentiality and personal data protection requirements corresponding to the data requested (Article 9) and on the content of the reasoned request for data access (Article 10). It then sets out the requirements for the publication of an overview of the reasoned request for data access in the DSA data access portal (Article 11), the procedures for the handling of amendment requests submitted by providers of very large online platforms or of very large online search engines pursuant to Article 40(5) of Regulation 2022/2065 (Article 12) and a mediation process (Article 13). Lastly, it lays down the conditions for independent expert consultations (Article 14).

Chapter IV contains a provision on the conditions for providing access to the data requested to vetted researchers by providing details on the data management and data documentation requirements data providers need to adhere to when providing access to data (Article 15).

Finally, Chapter V contains the final provision of this delegated act concerning its entry into force (Article 16).

COMMISSION DELEGATED REGULATION (EU) …/...

of 1.7.2025

supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council by laying down the technical conditions and procedures under which providers of very large online platforms and of very large online search engines are to share data with vetted researchers

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC ([2]), and in particular Article 40(13) thereof,

Whereas:

(1) Article 40 of Regulation (EU) 2022/2065 lays down rules regarding access to data to be granted by providers of very large online platforms and of very large online search engines. In particular, it enables researchers who have completed a process to demonstrate that they fulfil the conditions laid down in paragraph 8 of that Article ('vetted researchers') to be provided with such access.

(2) Under Article 40(4) of Regulation (EU) 2022/2065, vetted researchers are to be provided with access to data to help them study systemic risks in the Union and assess the effectiveness of measures to mitigate those risks. Their findings can constitute valuable input for the enforcement of Regulation (EU) 2022/2065 and foster accountability of providers of very large online platforms and of very large online search engines. The purpose of this Regulation is to lay down the technical conditions and the procedures necessary to enable such access, in a secure and efficient manner that is consistent across all Digital Services Coordinators, and in a way that ensures equality of treatment for researchers and data providers.

(3) To ensure that the data access process is consistent across all Digital Services Coordinators and to make that process clear and transparent for everyone, it is necessary to create a dedicated digital infrastructure ('the DSA data access portal'). The DSA data access portal should allow researchers, data providers, and Digital Services Coordinators to participate in the data access process, have access to and disseminate relevant information, such as the details of the dedicated points of contact, and communicate with one another. The DSA data access portal should not be considered as one of the access modalities to be used for the provision of access to the data pursuant to a reasoned request.

(4) Data providers, and researchers wishing to participate in the data access process, should create an account on the DSA data access portal for that purpose. To ensure

[2] OJ L 277, 27.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.

that Digital Services Coordinators can access information submitted via the DSA data access portal without needing to create a separate account on the portal, the DSA data access portal should be interoperable with the information sharing system AGORA established in Commission Implementing Regulation (EU) 2024/607[3].

(5) To ensure transparency of the data access process for all the parties involved and to monitor the effectiveness and efficiency of the data access process and compliance with Article 40(4) of Regulation (EU) 2022/2065 and this Regulation, the DSA data access portal should generate automatic notifications in relation to different steps and updates of the process.

(6) In order to provide researchers with consistent information about the data access process, Digital Services Coordinators should make available and easily accessible on their online interfaces information concerning the data access process, including links to the DSA data access portal. To avoid creating unnecessary administrative burden, increase efficiency and facilitate communication among all parties involved in the data access process, Digital Services Coordinators are encouraged to facilitate the management of information related to the data access process, also from a linguistic perspective.

(7) In order to allow researchers to identify the relevant data for the purposes set out in Article 40(4) of Regulation (EU) 2022/2065, data providers should make available DSA data catalogues for their services. Such catalogues should be easily findable and accessible on the online interfaces of data providers, and should describe the available data assets, their data structure and metadata, access to which may be requested pursuant to Article 40(4) of Regulation (EU) 2022/2065. When making available the DSA data catalogues, data providers should have regard to risks to confidentiality, data security or personal data protection potentially deriving from such information being made public.

(8) To contribute to the development of relevant research projects for the purposes set out in Article 40(4) of Regulation (EU) 2022/2065, the DSA data catalogues should include in particular data related to the systemic risks in the Union that data providers have identified in their annual risk assessments pursuant to Article 34 of that Regulation, as well as data related to any risk mitigation measures referred to in Article 35 of that Regulation. To ensure the relevance and timeliness of the DSA data catalogues, those catalogues should be updated regularly with due consideration to newly identified systemic risks and the evolution of systemic risks. For example, they should reflect emerging risks identified following an ad hoc risk assessment pursuant to Article 34 of Regulation (EU) 2022/2065 or following an audit report pursuant to Article 37 of that Regulation. To minimise the procedural burden on the data providers, where appropriate, such catalogues may rely on existing data documentation resources used for other purposes and audiences, such as advertising, content creation, or third-party app development. The DSA data catalogues should not be required to be exhaustive and therefore should not bind or limit applicant researchers in their data access applications.

-

[3] Commission Implementing Regulation (EU) 2024/607 of 15 February 2024 on the practical and operational arrangements for the functioning of the information sharing system pursuant to Regulation (EU) 2022/2065 of the European Parliament and of the Council (Digital Services Act) (OJ L 2024/607, 16.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/607/oj).

(9) In order to facilitate the determination of the access modalities by the Digital Services Coordinator of establishment and reduce the overall burden of the data access process on all actors involved, data providers should publish their suggested access modalities for the data described in the DSA data catalogues. These suggested access modalities should be proportionate to the sensitivity of the data and include information on the possible technical, organisational and legal conditions considered by the data providers as appropriate to enable the provision of the data. The access modalities suggested by data providers should not bind Digital Services Coordinators of establishment, who should remain competent to determine the appropriate access modalities.

(10) To ensure that data access applications are treated equally, independently of the Digital Services Coordinator to which the data access application is submitted or from which the reasoned request originates, the timeframe for the formulation of reasoned requests should be specified to ensure consistency across all Digital Services Coordinators. If the formulation of the reasoned request requires additional time, the Digital Services Coordinator of establishment should notify the principal researcher, giving reasons for the delay. Such reasons may include the need for additional verifications by the Digital Services Coordinator of the research organisation or of establishment, for example where data access applications imply international data transfers, or where the Digital Services Coordinator of establishment has identified potential risks to the security of the Union if the data were to be shared. With a view to aligning also the steps in the data access process preceding the formulation of reasoned requests, including the assessment of data access applications and granting of vetted researcher status, Digital Services Coordinators are encouraged to develop a consistent and coordinated way of working, including common operational criteria, within the framework of the European Board for Digital Services.

(11) In order to streamline the procedures for the formulation of reasoned requests, all Digital Services Coordinators of establishment should be required to verify that certain common elements of the data access process were duly covered in the data access applications. To that end, the Digital Services Coordinators of establishment should verify that all applicant researchers who are mentioned in the data access application demonstrated their affiliation to a research organisation, for example by providing documentary evidence of employment contracts or any other form of legal association with the research organisation. The Digital Services Coordinators of establishment should also verify that the applicant researchers demonstrated their independence from commercial interests, for example, by means of a declaration to that effect.

(12) The Digital Services Coordinator of establishment should verify that the funding of the research project for which the data are requested is disclosed in the data access application. The information provided by the applicant researchers should include details of the contributions, such as the funding entity, the amount, the nature and duration of the contribution, including whether the funding has already been awarded or whether an application for funding is still under evaluation, as well as, where applicable, relevant references to Union funded projects. Where available, the data access application should also include the outcomes of evaluations conducted by the entity or entities providing the funding.

(13) The Digital Services Coordinator of establishment should verify that the data access application describes how the data and data format are selected, with reference to the requirements of necessity for, and proportionality to, the purpose of the envisaged research. Where the requested data are also available through other sources, the Digital

Services Coordinator of establishment should assess whether the request for such data in the data access application is duly justified, having regard to the information in the data access application. Possible justifications may include evidence of poor quality or unreliability of such data deriving from other sources or the unsuitability of the format in which such data may be retrieved from other sources for the purposes of the research project, which would hinder the performance of the research project. Data that can be requested in order to study systemic risks or their mitigation in the Union may evolve in the future. Current examples of such data include data related to users of the services, such as profile information, relationship networks, individual-level content exposure and engagement histories; interaction data such as comments or other engagements; data related to content recommendations, including data used to personalise recommendations; data related to the targeting of advertisements and profiling, including cost per click data and other measures of advertising prices; data related to the testing of new features prior to their deployment, including the results of A/B tests; data related to content moderation and governance, such as data on algorithmic or other content moderation systems and processes, including changelogs, archives or repositories documenting moderated content, including accounts as well as data related to prices, quantities and characteristics of goods or services provided or intermediated by the data provider.

(14) The Digital Services Coordinator of establishment should verify whether the data access application provides for sufficient information that demonstrate that the researcher is capable of fulfilling the specific requirements of confidentiality, security and protection of personal data with respect to the requested data, identifies possible risks deriving from accessing and processing of such data for the purposes of the research, and documents any access modalities proposed, including the legal, organisational and technical conditions that will be put in place to minimise identified risks, for instance by means of a commitment letter from the research organisation confirming access to means that can constitute relevant safeguards, or other supporting documents.

(15) Where personal data are requested, the Digital Services Coordinator of establishment should verify that the data access application includes information on the legal basis for the processing of personal data, including special categories of personal data, where applicable, and whether such legal basis is in line with Article 6(1), point (e) or (f), and where applicable Article 9(2), point (g) or (j), of Regulation (EU) 2016/679. In addition, the Digital Services Coordinator of establishment should verify that the data access application contains sufficient indication that the researchers have assessed risks to personal data protection. For example, this could be demonstrated by a data protection impact assessment within the meaning of Article 35 of that Regulation. To ensure that personal data can be accessed in compliance with Regulation (EU) 2016/679, Digital Services Coordinators should be allowed to consult the relevant supervisory authorities established pursuant to Article 51 of that Regulation, which remain competent to assess compliance with Regulation (EU) 2016/679.

(16) To facilitate the formulation of the reasoned request and preserve the integrity of the information included in the data access application the Digital Services Coordinator of establishment should verify whether the data access application includes a summary. Such summary should contain an overview of the information that will be part of the reasoned request, published in the DSA data access portal, in cases where the assessment of the data access application leads to the formulation of a reasoned request.

(17) In order to ensure that the access modalities the Digital Services Coordinator of establishment determines are adequate to address the sensitivity of the specific data requested in a data access application, the Digital Services Coordinator of establishment should perform a case-by-case assessment, based on the information provided in the data access application. The access modalities established in the reasoned request should be appropriate to fulfil the requirements of data security, data confidentiality and protection of personal data and, at the same time, enable the attainment of the research objectives of the research project. Access to data may take place for example through data transmission to the vetted researchers via an appropriate interface and appropriate data storage; transmission of the data to, and storage in, a secure processing environment operated by the data provider or by a third party provider to which vetted researchers have access but where no data transmission to the vetted researchers takes place, or other access modalities to be set up or facilitated by the data provider. When specifying the access modalities, the Digital Services Coordinator of establishment should also list any legal, technical or organisational conditions to which access is to be subject. In cases where providing access involves a transfer of personal data to third countries or international organisations within the meaning of Chapter V of Regulation (EU) 2016/679, the access modalities should also include information on the need to put in place an appropriate transfer mechanism, to ensure that the data provider takes the necessary action to comply with that Regulation.

(18) To ensure that the data access modalities are appropriate to address specific sensitivities in terms of data protection, of data security or of confidentiality, the Digital Services Coordinator of establishment, on the basis of the information received in the data access application, should be able to require, that access to data be provided via secure processing environments. In such cases, the Digital Services Coordinator of establishment should ensure that the chosen environment operates in line with the most appropriate technology and it allows the vetted researchers to attain the objectives of their research.

(19) In order to ensure consistency of the information transmitted by the Digital Services Coordinators of establishment to the data providers, it is necessary to specify the content of the reasoned requests.

(20) In order to safeguard the interests of data providers and to reduce the frequency of amendment requests over time and facilitate the formulation of relevant data access applications by researchers, an overview of each reasoned request, including any amendments and updates to it, should be made publicly available in the DSA data access portal by the Digital Services Coordinator of establishment who issued the respective reasoned requests.

(21) In order to ensure that the Digital Services Coordinator of establishment has the relevant information to evaluate an amendment request and to facilitate a uniform approach in the evaluation of amendment requests, the data provider should be required to specify the reasons for such request, as referred to in Article 40(5) of Regulation (EU) 2022/2065. More specifically, when assessing an amendment request submitted on the basis of a data provider’s lack of access to the data, the Digital Service Coordinator of establishment should be in a position to examine whether the alleged impossibility is duly justified, for example by the non-existence of the requested data, or by technical restrictions such as encryption and it should have the information necessary to consider whether the lack of access is permanent or temporary. It should be clear, in this respect, that commercial considerations should

not be considered as a ground to automatically refuse access to requested data but rather as a ground to modify the means of providing access to the data, which may result in imposing additional data security and confidentiality requirements.

(22) In order to ensure an efficient resolution of disputes and to encourage the identification of a mutually acceptable solution, following an amendment request, data providers should be able to ask the Digital Services Coordinators of establishment to participate in mediation. Such participation should be voluntary throughout the entire mediation process and should not result in any binding outcome for the Digital Services Coordinator of establishment, which remain competent to decide on the amendment requests. All parties involved in the mediation process should engage in good faith and strive to reach a fair and mutually acceptable agreement.

(23) In order to prevent that mediation indefinitely prolong the data access process, the transmission of the written request for mediation, the selection of the mediator and the mediation process itself should take place within specified timeframes. The Digital Services Coordinators of establishment should set a time limit for the mediation process in relation to a given reasoned request and the mediator should have the authority to terminate the mediation process in specific circumstances.

(24) In order to maintain mutual trust among the parties involved in the mediation, the Digital Services Coordinator of establishment should ensure that the proposed mediator meet the requirements of impartiality, independence and possess relevant expertise on the subject matter of the mediation.

(25) For the purposes of facilitating informed and effective decision-making in relation to the data access process, Digital Services Coordinators should have the possibility to request expert opinions on specific elements of the data access process, such as the determination of the access modalities, including appropriate interfaces, the formulation of the reasoned request and any amendment requests by the data provider. The experts consulted should possess proven expertise in the matter on which their opinion is sought and should be independent. In particular, they should not have any conflict of interests, deriving for example from any ties with the applicant researchers or with the data provider.

(26) In order to increase transparency and allow Digital Services Coordinators to build on their expertise acquired over time, each expert consultation request and the follow-up generated by it should be registered in AGORA.

(27) In order to facilitate the effective supervision of compliance with the conditions set out in the reasoned request, the data provider should notify the Digital Services Coordinator of establishment within three working days of the date on which access has been provided to the vetted researchers and of the date of the access its termination.

(28) In order to enable the vetted researchers to use the requested data for the purposes of the research and to provide relevant context information, data providers should provide vetted researchers with the relevant metadata and documentation describing the data made available, such as codebooks, changelogs and architectural documentation.

(29) In order to facilitate meaningful research by the vetted researchers, also by enabling the combination of the data requested with data available through other sources, data providers should not impose any restrictions on the analytical tools employed by vetted researchers, including relevant software libraries, and should not impose

archiving, storage, refresh and deletion requirements, unless they are explicitly mentioned in the access modalities identified in the reasoned request.

(30) Where the data provided to the vetted researchers include personal data within the meaning of Article 4 of Regulation (EU) 2016/679, the data provider should observe the rules laid down in that Regulation. In particular, Article 40(4) of Regulation (EU) 2022/2065 creates a legal obligation within the meaning of Article 6(1), point (c) of Regulation (EU) 2016/679 for any processing of personal data necessary for the data provider to provide access to the data specified in the reasoned request. Where special categories of personal data within the meaning of Article 9 of Regulation (EU) 2016/679 are to be processed, this Regulation meets the requirement of Article 9(2), point (g) of Regulation (EU) 2016/679.

(31) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[4] and delivered an opinion on 4 December 2024.

(32) After consulting the European Board for Digital Services in accordance with Article 40(13) of Regulation (EU) 2022/2065 and following its endorsement,

HAS ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

This Regulation lays down procedures and technical conditions for providing vetted researchers with access to data held by providers of very large online platforms and of very large online search engines, pursuant to Article 40(4) of Regulation (EU) 2022/2065, in particular:

(a) the technical conditions for the development and functioning of a data access portal;

(b) the procedures and technical conditions for the management of the data access process by Digital Services Coordinators and data providers;

(c) the requirements for the formulation of reasoned requests and the assessment of amendment requests;

(d) the technical conditions for the provision of access to data by the data providers.

-

[4] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

Article 2

Definitions

For the purposes of this Regulation, the definitions in Article 4 of Regulation (EU) 2016/679 and Article 3 of Regulation (EU) 2018/1725 of the European Parliament and of the Council[5] shall apply. The following definitions shall also apply:

(a) ‘data access application’ means the information and relevant documentation submitted by applicant researchers to the Digital Services Coordinator of establishment or the Digital Services Coordinator of the Member State of the research organisation, to which the principal researcher is affiliated, to obtain the status of ‘vetted researcher’ as referred to in Article 40(8), first subparagraph, of Regulation (EU) 2022/2065, for a specific research project involving access to data from a data provider;

(b) ‘data access process’ means the steps and procedures that may lead to the provision of access to the data as referred to in Article 40(4) of Regulation (EU) 2022/2065; ‘applicant researcher’ means any natural person applying for access to data as referred to in Article 40(4) of Regulation (EU) 2022/2065, either individually, in a group or as part of an entity;

(c) ‘principal researcher’ means the applicant researcher who submits the data access application in their individual capacity or on behalf of an entity or a group of applicant researchers;

(d) ‘data provider’ means a provider of a very large online platform or of a very large online search engine designated as such in accordance with Article 33(4) of Regulation (EU) 2022/2065, to which a reasoned request might be addressed;

(e) ‘reasoned request’ means a reasoned request for data access pursuant to Article 40(4) of Regulation (EU) 2022/2065;

(f) ‘amendment request’ means a request for amendment pursuant to Article 40(5) of Regulation (EU) 2022/2065 submitted by the data provider to the Digital Services Coordinator of establishment following the receipt of a reasoned request;

(g) ‘secure processing environment’ means secure processing environment as defined in Article 2, point (20), of Regulation (EU) 2022/868 of the European Parliament and of the Council6.

---

5 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

6 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (OJ L 152, 3.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/868/oj).

CHAPTER II

INFORMATION AND CONTACT OBLIGATIONS

Article 3

DSA data access portal

1. The Commission shall establish and host a DSA data access portal.
2. The DSA data access portal shall have the following functions:
   (a) support and streamline the management of the data access process for researchers, data providers and Digital Services Coordinators;
   (b) serve as the central digital point for information on the data access process and facilitate the information exchanges pursuant to this Regulation among applicant researchers, vetted researchers, data providers and Digital Services Coordinators.
3. The DSA data access portal shall be interoperable with the information sharing system AGORA established by Implementing Regulation (EU) 2024/607. The Digital Services Coordinators shall have access in AGORA to the information submitted through the DSA data access portal.
4. Data providers shall have an account on the DSA data access portal.
5. To participate in the data access process, applicant researchers shall have an account on the DSA data access portal.

Article 4

Roles and responsibilities for processing personal data in the DSA data access portal

1. Digital Services Coordinators shall be separate controllers with respect to the processing of personal data they carry out to manage the data access process and for publication of relevant information.
2. The Commission shall be a processor of personal data processed within the DSA data access portal.
3. The responsibilities of the Commission as processor for data processing activities conducted in the DSA data access portal shall be as set out in the Annex.

Article 5

Processing of personal data in the DSA data access portal

1. Where personal data are registered in and exchanged via the DSA data access portal, the processing shall take place only in so far as it is proportionate and necessary for the purpose of the data access process and publication of relevant information.
2. The processing of personal data shall take place in the DSA data access portal only in respect of the following categories of data subjects:

(a) natural persons having an account on the DSA data access portal;

(b) natural persons whose personal data is contained in the DSA data access portal or in any other exchange pursuant to this Regulation concerning the data access process.

3. The processing of personal data shall take place in the DSA data access portal only in respect of the following categories of personal data:

(a) identity data, such as name, user ID;

(b) contact information such as address, email address, contact details;

(c) personal data contained in the documentation demonstrating the affiliation to a research organisation, and any other personal information deemed necessary for the purpose of participating in the data access process.

4. The processing of personal data referred to in paragraph 1 shall be performed using information technology infrastructure located in the European Economic Area.

Article 6

Points of contact and public information on the data access process

1. Each Digital Services Coordinator and each data provider shall establish a dedicated point of contact, whose task shall be to provide information and support on the data access process.

2. The Digital Services Coordinators and data providers shall communicate their points of contact to the Commission, as soon as possible. The Commission shall publish the details of the points of contact referred to in paragraph 1 in the public interface of the DSA data access portal.

3. Each Digital Services Coordinator shall make available and easily findable on its online interface, the details of the point of contact established pursuant to paragraph 1 together with a link to the DSA data access portal.

4. Data providers shall make the following information available and easily findable on their online interfaces:

(a) the details of the point of contact established by them pursuant to paragraph 1;

(b) a link to the DSA data access portal;

(c) a DSA data catalogue, which describes the data assets, that may be accessed for the purposes set out in Article 40(4) of Regulation EU 2022/2065, as well as their data structure and metadata;

(d) suggested access modalities for the data in the catalogue pursuant to point (c), adequate to the level of sensitivity of the different data assets.

5. The information referred to in paragraph 4, points (c) and (d), shall be regularly updated, in particular to reflect data related to the risk assessments carried out pursuant to Article 34 of Regulation (EU) 2022/2065 and the audits carried out pursuant to Article 37 of that Regulation.

CHAPTER III

REQUIREMENTS FOR FORMULATING AND PROCESSING OF REASONED REQUESTS

Article 7

Formulation of reasoned request

1. Within 80 working days from the submission of a data access application, the Digital Services Coordinator of establishment, taking due account of the prerequisites set out in Article 8 and, where applicable, any other assessment relevant for these purposes, shall decide whether a reasoned request can be formulated and shall undertake one of the following actions:

   (a) formulate a reasoned request, submit it to the data provider and notify the principal researcher of the submission of the reasoned request;

   (b) inform the principal researcher of the reasons why the reasoned request could not be formulated.

2. Where, in duly justified cases, the Digital Services Coordinator of establishment needs additional time to formulate a reasoned request, it shall notify the principal researcher as soon as possible and shall indicate the reasons for the delay as well as a new date for undertaking the actions referred to in paragraph 1.

Article 8

Prerequisites for formulating a reasoned request

The Digital Services Coordinator of establishment shall decide whether a reasoned request can be formulated taking into account the following elements:

(a) for each applicant researcher:

   i. a confirmation of affiliation to a research organisation as defined in Article 2, point (1), of Directive (EU) 2019/790 of the European Parliament and of the Council[7];

   ii. a declaration of independence from commercial interests relevant to the specific project for which the data are requested;

   iii. a commitment to making their research results publicly available free of charge.

(b) information about funding supporting the research project for which the data are requested;

(c) a description of the data requested, including format, scope and, where possible, the specific attributes, relevant metadata and data documentation, also considering the information made available pursuant to Article 6(4) of this Regulation;

[7]Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, p. 92, ELI: http://data.europa.eu/eli/dir/2019/790/oj).

(d) information on the necessity and proportionality of the access to the data and the information on the time frames of the research for which the data are requested;

(e) information on the identified risks in terms of confidentiality, data security and personal data protection related to the data that would be accessed, a description of the technical, legal and organisational measures that will be put in place, including, where possible, suggested access modalities, to mitigate such risks when processing the requested data;

(f) a description of the research activities to be conducted with the requested data;

(g) a summary of the data access application containing the following elements:

i. the research topic;

ii. the data provider from which data are requested;

iii. a description of the data requested, as referred to in point (c).

Article 9

Access modalities

1. The Digital Services Coordinator of establishment shall determine the modalities, including the technical, legal and organisational measures, that the data provider is to use for providing access to the data to the vetted researchers.

2. The Digital Services Coordinators shall be allowed to consult the relevant supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679.

3. When determining the access modalities, the Digital Services Coordinator of establishment shall take into account the information provided in the data access application, in particular the information referred to in Article 8, point (e), considering also the rights and interests of the data providers and the recipients of the service concerned, including the protection of confidential information, trade secrets, and maintaining the security of their service and the information made available by the data providers pursuant to Article 6(4), point (d).

4. In addition to the elements referred to in paragraph 3, the Digital Services Coordinator of establishment shall, when determining access modalities, take into account the following elements:

(a) where the access involves the processing of personal data:

i. the assessment of the risks concerning processing of personal data as described in Article 8(e), including, where applicable, data protection impact assessments within the meaning of Article 35 of Regulation (EU) 2016/679;

ii. envisaged technical and organisational measures as submitted pursuant to Article 8(e).

(b) relevant network security measures, encryption, access control mechanisms, backup policies, data integrity mechanisms, incident response plans;

(c) where applicable, information on the intended storage period and the relevant data destruction plans;

(d) any organisational measures such as internal review processes, restrictions of access rights and information sharing;

(e) any proposed contractual clauses, such as non-disclosure agreements, data agreements and any other type of written statements, laying down possible conditions of access and processing between the principal researcher and the data provider;

(f) existence of training on data security and protection of personal data received by the applicant researchers;

(g) Whether secure processing environments is necessary to process the data.

5. Where the Digital Services Coordinator of establishment considers that a secure processing environment is to be used to provide access to the data requested, the Digital Services Coordinator of establishment shall require documentation attesting that the operator of that environment:

(a) specifies access conditions to the secure processing environment in order to minimise the risk of the unauthorised reading, copying, modification or removal of the data hosted in the secure processing environment;

(b) ensures that vetted researchers have access only to data covered by the reasoned request, by means of individual and unique user identities and confidential access modes;

(c) keeps identifiable logs of access to the secure processing environment for the period necessary to verify and audit all processing operations in that environment;

(d) ensures that the computing power at the disposal of the vetted researchers is appropriate and sufficient for the purposes of the research project;

(e) monitors the effectiveness of the measures listed in points (a) to (d).

Article 10

Content of a reasoned request

1. A reasoned request shall contain at least the following elements:

(a) the date by which the data provider shall give access to the data requested and the date on which such access shall be terminated;

(b) the access modalities determined pursuant to Article 9;

(c) the summary of the data access application referred to in Article 8 point (g);

2. The Digital Services Coordinator of establishment may include in the reasoned request the names and contact details of all vetted researchers mentioned in the data access application where this is necessary to enable access to the requested data, in accordance with the access modalities specified in the reasoned request.

3. If providing access involves a transfer of personal data to a third country or international organisation within the meaning of Chapter V of Regulation (EU)

2016/679, the reasoned request shall include information on the need to put in place or refer to an appropriate transfer mechanism to ensure compliance with Regulation (EU) 2016/679.

Article 11

Publication of an overview of a reasoned request in the DSA data access portal

1. Upon formulation of a reasoned request, the Digital Services Coordinator of establishment shall publish an overview of the reasoned request in the public interface of the DSA data access portal. The overview shall contain all the following:
   (a) the summary of the data access application referred to in Article 8 point (g);
   (b) the access modalities determined pursuant to Article 9.
2. The overview referred to in paragraph 1 shall be updated to reflect any changes resulting from a modification of one or more elements following the examination of an amendment request or the outcome of a mediation in accordance with Article 13.

Article 12

Procedures for examining amendment requests

1. Upon the receipt of an amendment request pursuant to Article 40(5) of Regulation (EU) 2022/2065, the Digital Services Coordinator of establishment shall inform the principal researcher concerned.
2. When deciding on an amendment request made pursuant to Article 40(5), point (a), of Regulation (EU) 2022/2065, the Digital Services Coordinator of establishment shall take into account the following:
   (a) whether the reasons for the alleged lack of access to data are duly substantiated;
   (b) whether that lack of access to data is permanent or temporary.
3. When deciding on an amendment request made pursuant to Article 40(5), point (b), of Regulation (EU) 2022/2065, the Digital Services Coordinator of establishment shall take into account all the following:
   (a) whether the alleged vulnerabilities and their significance are duly substantiated;
   (b) the likelihood and severity of harm resulting from these alleged significant vulnerabilities;
   (c) the extent to which the access modalities set out in the reasoned request effectively mitigate the risk of such harm occurring.
4. At any time during the assessment of an amendment request, the Digital Services Coordinator of establishment may ask the data provider or the principal researcher for any additional information that it considers necessary to complete its assessment.
5. Such request for additional information shall be made as soon as possible to allow the data provider or the principal researcher sufficient time to respond and, in any

event, shall not affect the deadline set in Article 40(6), second subparagraph of Regulation (EU) 2022/2065. Where the data provider or the principal researcher fails to provide the requested information at all or within a period specified by the Digital Services Coordinator of establishment or provides partial information, the Digital Services Coordinator of establishment shall make its decision within the timeframe laid down in Article 40(6) of Regulation (EU) 2022/2065, based on the information that was made available to it within a reasonable delay.

Article 13

Mediation

1. If the data provider disagrees with the decision of the Digital Services Coordinator of establishment on the amendment request, the data provider may, within a period of five working days from the communication by the Digital Services Coordinator of establishment pursuant to Article 40(6), second subparagraph of Regulation (EU) 2022/2065, request in writing the Digital Services Coordinator of establishment to participate in mediation.

2. The Digital Services Coordinator of establishment shall not be obliged to participate in the mediation process.

3. The written request referred to in paragraph 1, shall include a concise description of the specific elements of the decision, as communicated by the Digital Services Coordinator of establishment pursuant to Article 40(6), second subparagraph of Regulation (EU) 2022/2065, to which the data provider objects.

4. The Digital Services Coordinator of establishment and the data provider shall agree on the appointment of a mediator and initiate the mediation within 20 working days from the submission of the mediation request pursuant to paragraph 3.

5. Before agreeing to the appointment of a mediator, the Digital Services Coordinator of establishment shall verify that the mediator is impartial and independent and possesses the relevant expertise related to the subject matter as described in the written request referred to in paragraph 1.

6. The data provider shall bear all costs of the mediation.

7. The Digital Services Coordinator of establishment shall inform the principal researcher of the mediation request referred to in paragraph 1 without undue delay and may decide to invite the principal researcher to join the mediation as a party. Where the data access application has been submitted to the Digital Services Coordinator of the research organisation, the Digital Services Coordinator of establishment may invite the Digital Services Coordinator of the research organisation to participate in the mediation process. Any party invited to join the mediation by the Digital Services Coordinator of establishment shall not be obliged to participate in the mediation process.

8. Participation in mediation shall not affect the right of the parties to initiate judicial proceedings at any time before, during or after the mediation.

9. The Digital Services Coordinator of establishment shall set a time limit for the mediation, which shall not exceed 40 working days starting on the day of the initiation of the mediation pursuant to paragraph 4.

10. The mediator may terminate the mediation earlier in one of the following cases:

(a) one of the parties requests explicitly to terminate the mediation;

(b) it becomes clear that the conduct of the parties during the mediation, including a failure to engage in good faith, makes it unlikely that an agreement will be reached

11. Where the mediation results in an agreement between the parties, the Digital Services Coordinator of establishment shall take such agreement into account and, where appropriate, modify the reasoned request and inform the principal researcher of the modification.

12. Where the parties fail to reach an agreement, the Digital Services Coordinator of establishment shall notify the data provider that the decision of the Digital Services Coordinator of establishment on the amendment request, as last communicated pursuant to Article 40(6), second subparagraph of Regulation (EU) 2022/2065, shall be considered valid and shall serve as the relevant basis for further steps in the process and inform the principal researcher.

13. The Digital Services Coordinator of establishment shall register in AGORA a summary record of the mediation, prepared by the mediator and signed by all parties. The record shall include the following information:

(a) the date of the written request for mediation by the data provider;

(b) the identities and contact details of the parties;

(c) the start and end dates of the mediation;

(d) the outcome of the mediation, including any agreement reached or the reason for termination of the mediation.

Article 14

Independent expert consultation

1. Before formulating a reasoned request, or taking a decision on an amendment request, the Digital Services Coordinator may decide to consult experts.

2. The experts shall be independent and impartial and possess relevant expertise and proven skills and have the capacity and resources to perform the identified task, without incurring undue delay.

3. To attest impartiality, the experts shall sign a declaration confirming that they:

(a) have no financial or personal ties to the data provider or the applicant researchers;

(b) have no interest in the outcome of the data access process;

(c) are free from any conflicts of interest.

4. The Digital Services Coordinator shall encode any consultation carried out pursuant to paragraph 1, along with the expert opinion received in response to the consultation, without undue delay in AGORA.

CHAPTER IV

CONDITIONS FOR PROVIDING THE DATA REQUESTED TO VETTED RESEARCHERS

Article 15

Data sharing and data documentation

1. Data providers shall notify the Digital Services Coordinator of establishment within three working days of the fact:

   (a) that access to the requested data has been provided to vetted researchers, in accordance with the reasoned request;

   (b) that the access for the vetted researchers has been terminated.

2. Data providers shall provide vetted researchers with any additional information needed to access and understand the requested data, such as codebooks, changelogs and architectural documentation. In cases where the provision of such information may result in a significant vulnerability of the data provider's services, the data provider shall notify the Digital Services Coordinator of establishment of that risk and, where possible, propose alternative information.

3. When providing access to data, data providers shall not impose on vetted researchers data management requirements such as archiving, storage, refresh and deletion requirements, or limitations to the use of standard analytical tools, that may hinder the performance of the relevant research, unless such requirements or limitations are explicitly mentioned in the reasoned request.

4. Where personal data are processed, data providers shall not impose on vetted researchers any conditions in relation to the processing of the shared personal data other than those specified in the reasoned request.

CHAPTER V

FINAL PROVISIONS

Article 16

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 1.7.2025

For the Commission
The President
Ursula VON DER LEYEN

EUROPEAN
COMMISSION

Brussels, 1.7.2025
C(2025) 4340 final

ANNEX

ANNEX

to the Commission Delegated Regulation (EU) .../...

supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council by laying down the technical conditions and procedures under which providers of very large online platforms and of very large online search engines are to share data with vetted researchers

ANNEX

Responsibilities of the Commission as processor for data processing activities conducted in the context of the DSA data access portal

1. The Commission shall set up and ensure a secure and reliable IT infrastructure, the DSA data access portal, on behalf of the Digital Services Coordinators, that supports and streamlines the management of the data access process for researchers, research organisations, data providers and Digital Services Coordinators.

2. To fulfil its obligations as processor for the Digital Services Coordinators, the Commission may use third parties as sub-processors. If it is the case, the controllers shall authorise the Commission to use sub-processors or replace sub-processors where necessary. The Commission shall inform the controllers of said use or replacement of sub-processors, thereby giving the controllers the opportunity to object to any such changes. The Commission shall ensure that the same data protection obligations as set out in this Regulation apply to these sub-processors.

3. The processing by the Commission shall process personal data only insofar as necessary for the:

   (a) authentication and access control with regard to all DSA data access portal users;

   (b) authorisation implementation of requests by DSA data access portal users to create, update and delete any information contained in the application within the DSA data access portal;

   (c) reception of the personal data referred to in Article 5(3) of this Regulation uploaded by DSA data access portal users;

   (d) storage of the personal data in the DSA data access portal;

   (e) deletion of the personal data at their expiration date or upon instruction of the controller;

   (f) after the end of the provision of services provided by the DSA data access portal, deletion of any remaining personal data unless Union or Member State laws require storage of such personal data.

4. The Commission shall take all state of the art organisational, physical, and logical security measures to ensure the DSA data access portal functioning. To this end, the Commission shall:

   (a) designate a responsible entity for the security management of the DSA data access portal, communicate to the controllers its contact information and ensure its availability to react to security threats;

   (b) assume the responsibility for the security of the DSA data access portal, including regularly carrying out tests, evaluations and assessments of the security measures.

5. The Commission shall take all necessary security measures to avoid compromising the smooth operational functioning of the DSA data access portal. This shall include:

   (a) risk assessment procedures to identify and estimate potential threats to the DSA data access portal;

(b) audit and review procedure to:

i. check the correspondence between the implemented security measures and the applicable security policy;

ii. control on a regular basis the integrity of the DSA data access portal, security parameters and granted authorisations;

iii. detect security breaches and intrusions into the DSA data access portal;

iv. implement changes to mitigate existing security weaknesses in the DSA data access portal;

v. define the conditions under which to authorise, including at the request of controllers, and contribute to, the performance of independent audits, including inspections, and reviews on security measures subject to conditions that respect Protocol (No 7) to the Treaty on the Functioning of the European Union on the Privileges and Immunities of the European Union.

(c) changing the control procedure to document, measure the impact of a change before its implementation, and keep the controllers informed of any changes that can affect the communication with and/or the security of the DSA data access portal;

(d) laying down a maintenance and repair procedure to specify the rules and conditions to be respected when maintenance and/or repair of the DSA data access portal is to be performed;

(e) laying down a security incident procedure to define the reporting and escalation scheme, inform without delay the controllers affected, inform without delay the controllers for them to notify the national data protection supervisory authorities of any personal data breach and define a disciplinary process to deal with security breaches in the DSA data access portal.

6. The Commission shall take state of the art physical and logical security measures for the facilities hosting the DSA data access portal and for the controls of data and security access thereto. To this end, the Commission shall:

(a) enforce physical security to establish distinct security perimeters and allowing detection of breaches in the DSA data access portal;

(b) control access to the DSA data access portal facilities;

(c) ensure that equipment cannot be added, replaced or removed without prior authorisation from the designated responsible bodies;

(d) control access from and to the DSA data access portal;

(e) ensure that the DSA data access portal users who access the DSA data access portal are authenticated;

(f) review the authorisation rights related to the access to the DSA data access portal in case of a security breach affecting the DSA data access portal;

(g) keep the integrity of the information transmitted through the DSA data access portal;

(h) implement technical and organisational security measures to prevent unauthorised access to personal data in the DSA data access portal;

(i) implement, whenever necessary, measures to block unauthorised access to the DSA data access portal (i.e., block a location/IP address).

7. The Commission shall:

(a) take steps to protect its domain, including the severing of connections, in the event of substantial deviation from the principles and concepts for quality and security;

(b) maintain a risk management plan related to its area of responsibility;

(c) monitor, in real time, the performance of all the service components of the DSA data access portal, produce regular statistics and keep records;

(d) provide support for the DSA data access portal in English to the DSA data access portal users;

(e) assist the controllers by appropriate technical and organisational measures for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of Regulation (EU) 2016/679;

(f) support the controllers by providing information concerning the DSA data access portal to implement the obligations pursuant to Articles 32, 33, 34, 35 and 36 of Regulation (EU) 2016/679;

(g) ensure that data processed within the DSA data access portal is unintelligible to any person who is not authorised to access it;

(h) take all relevant measures to prevent unauthorised access to transmitted personal data via the DSA data access portal;

(i) take measures in order to facilitate communication between the controllers;

(j) maintain a record of processing activities carried out on behalf of the controllers in accordance with Article 31(2) of Regulation (EU) 2018/1725.