Data Access Article 40(4-11) DSA: Harmonized Guidance

Publication date:
November 2026
Version 1.0

Contents Fout! Bladwijzer niet gedefinieerd.

1 Introduction 3

2 Overview of Vetted Researcher status application process 5

3 How to apply 9

4 Application Requirements 10

5 Information to be provided in respect of each of the conditions in Article 40(8) and related requirements in the Delegated Act. 11

6 Further guidance in respect of applications 21

7 Access Modalities 22

8 After an application for Vetted Researcher status is approved 23

Introduction

1.1 This guidance is intended for those interested in the Vetted Researcher Data Access process under Article 40(4-11) Digital Services Act ("**DSA**"). This guidance has been prepared collaboratively by Digital Service Coordinators (DSCs) for the purpose of outlining a harmonized approach to data access provisions and to highlight commonalities that apply. It is important to note however, that national specificities may apply and Applicant(s) should be aware of this prior to submitting a Data Access Application. We strongly recommend that Applicant(s) review all information available from the DSC of the EU Member State where the Applicant(s) affiliated Research Organisation is based (referred to as the DSC of Origin ("**DSCoO**")), and from the DSC of the EU Member State in which the main establishment of the provider of the Very Large Online Platform ("**VLOP**") or Very Large Online Search Engines ("**VLOSE**") is located or, where the provider has no establishment in the EU, where its legal representative resides or is established (referred to as the DSC of Establishment ("**DSCoE**")).

1.2 Prior to submitting a data access application Applicant(s) should engage with the DSC of the Member State of their Research Organisation in the first instance for more information on national specificities regarding any matters discussed within this Guidance.

1.3 In particular, DSCs have developed this Guidance to inform interested parties of the following:

(a) The form and manner in which applications for VR status are to be made; and
(b) An overview of the process for the assessment of applications for VR status.

1.4 This Guidance is not legal advice; it is not binding on any DSC, and it is not intended to have any impact on how any law is interpreted or applied. Applicant(s) are advised to obtain their own independent legal advice on the relevant legislative provisions. This Guidance may be updated and amended as appropriate and as required, subject to the obligations of DSCs under applicable law. DSCs reserve the right to amend their processes as they see fit.

1.5 Article 40 of the DSA makes provision for certain researchers to access data from VLOPs or VLOSEs for the purposes of studying systemic risks in the EU stemming from the design, functioning or use of a VLOP/VLOSE and assessing mitigation measures implemented by the VLOP/VLOSE. Article 40(8) of the DSA sets out the process whereby a researcher, who has been vetted or assessed by a DSCoE to have met the criteria as set out under this provision, can have a request for access to data held by a VLOP/VLOSE submitted on their behalf by the DSC. Amongst the criteria that must be established (as detailed further below), the data requested must be limited in scope in accordance with Article 34 and 35 of the DSA and be deemed necessary and proportionate to the purpose of the research to which the Application relates.

1.6 A Vetted Researcher ("**VR**") is a researcher who

(a) applies to a DSC for VR status for specified research; and
(b) is formally designated as a VR by a DSCoE, having met the conditions that are set out in Article 40(8) of the DSA and Commission Delegated Regulation (EU) 2025/2050 of 1st July 2025 (the "**Delegated Act**") for the purposes of accessing specified data for the purposes of the research outlined in their application. Only a DSCoE may grant VR status.

1.7 It is important to note that VR status is only awarded in respect of specific research as identified in an application. Where a person who has previously been granted VR status wishes to seek access

to specified data held by a VLOP/VLOSE for the purposes of other research, a new application for VR status will need to be submitted for that purpose.

1.8 In order to be designated as a VR for the purpose of specific research, Applicant(s) must submit a detailed application to a DSC (only through the DSA Data Access portal (the "**Portal**")) which demonstrates that each Applicant meet all the conditions as set out in Article 40(8) of the DSA and related requirements set out in the Delegated Act. In summary each Applicant will need **to demonstrate:**

(a) They are affiliated to a Research Organisation[1];
(b) They are independent from commercial interests;
(c) They have disclosed the funding of the research;
(d) They can fulfil the specific data security, data protection and confidentiality requirements that correspond to the requested data and have described the appropriate technical and organisational measures that they have put and will put in place;
(e) Their access to the data and the time frames requested are necessary for, and proportionate to, the purpose of their research;
(f) The planned research will be carried out for the sole purpose of contributing to an understanding of systemic risk in the EU stemming from the design, functioning or use of the relevant VLOP/VLOSE and the assessment of risk mitigation measures implemented by that VLOP/VLOSE; and
(g) They are committed to making the research results publicly available free of charge, within a reasonable period after the completion of the research.

1.9 Where a DSCoE decides to designate a person as a VR for the specified research, the DSCoE will then issue a reasoned request for access to the data described in the application to the relevant VLOP/VLOSE. The VLOP/VLOSE will then be required to provide the VR with access to the specified data by way of the access modalities specified in the request, within a reasonable period specified in the request.[2]

[1] The term 'Research Organisation' has a specific definition, which is detailed further below.
[2] This is subject to the entitlement of a VLOP/VLOSE to request an amendment to the reasoned request, which is detailed further below.

Overview of Vetted Researcher status application process

1.10 The Vetted Researcher status application process begins with the Applicant(s) registration as a researcher on the Portal.

1.11 Once the Applicant(s) has registered as a principal or applicant researcher on the Portal, they will be able to access the private researcher-only area of the site. This is where the Applicant(s) will submit applications for VR status for specific research.

1.12 When the Applicant(s) is submitting an application via the Portal, they will have the option to submit the application to:

(a) The DSC of the EU Member State in which the main establishment of the provider of the VLOP or VLOSE is located or, where the provider has no establishment in the EU, where its legal representative resides or is established (referred to as the DSC of Establishment ("**DSCoE**")); or

(b) The DSC of the EU Member State where the Applicant(s) affiliated Research Organisation is based (and, where this Member State is different from the EU Member State of the DSCoE of the VLOP or VLOSE, this DSC shall be referred to as the DSC of Origin ("**DSCoO**")).

1.13 Where Applicant(s) submit an application to their DSCoO, the DSCoO will carry out an initial assessment of the application before transmitting it to the DSCoE. The DSCoE will then assess the application and will make a final decision on the application. If the DSCoO deems the application is incomplete, the DSCoO will transmit the initial assessment to the DSCoE and notify the DSCoE of this initial view. Upon receipt of the initial assessment, the DSCoE will proceed with consideration of the application.

1.14 It is important for the Applicant(s) to be aware of national specificities, particularly of the DSCoE who will be the decision maker on the application. This may include specific language requirements. Applicant(s) are responsible for ensuring the application and supporting documents are submitted in a language the DSCoE accepts, even when the Applicant(s) chooses to send the application through a DSCoO. Applicant(s) are advised to consult with the DSCoO and DSCoE, as relevant, regarding specific language requirements.

1.15 Applicant(s) are responsible for ensuring that all information in their application is accurate, this includes details regarding the Research Organisation with which they are affiliated, and, in particular contact details for that organisation.

1.16 Where a DSCoO has carried out an initial assessment, this will be considered by the DSCoE in its assessment of the application. The Assessment will involve the DSCoE considering the application and supporting documentation provided with a view to deciding whether the Applicant(s) have demonstrated that the Applicant(s) have met the conditions set out in Article 40(8) of the DSA, and the related requirements set out in Article 8 of the Delegated Act.

1.17 In the course of the Assessment, the DSCoO and/or DSCoE may request further information from the Applicant(s) regarding an application. As detailed below, the DSCoE may also provide the relevant VLOP/VLOPSE with the opportunity to submit comments for the purpose of expressing their views on an application. When requesting information and/or providing the opportunity to

submit comments, a DSCoE will specify a time period in which the information and/or comments should be provided.

1.18 In circumstances where strict timelines are provided for the conduct of an assessment and delivery of a decision by a DSCoE, the delivery of additional information requested and/or comments by the Applicant(s) or a VLOP/VLOPSE, as appropriate, will be time sensitive. A limited time period will apply for delivery of additional information requested and/or submissions by the Applicant(s) or a VLOP/VLOSE as appropriate.

1.19 A DSCoE may consult with subject matter experts (including, but not limited to, Data Protection Authorities (DPAs)) in the course of the Assessment which may require the sharing of documents in the Application.

1.20 The Applicant(s) and VLOP/VLOSE must ensure that any information contained within their application and/or submission(s), respectively, or within supporting documents in respect of which confidentiality is claimed is clearly identified. When claiming that certain content in the Application and/or submission is confidential, Applicant(s) and/or VLOP/VLOSE must include the basis upon which confidentiality is claimed and identification of the harm that would result from the disclosure of the information. Applicant(s) and/or VLOP/VLOSE must confirm that no claim of confidentiality is made in respect of any information other than those specific pieces of information that have been expressly claimed as confidential.

1.21 It may be necessary for a DSCoE to share information contained in an application, the application and supporting documents with the relevant VLOP/VLOSE in order to provide an opportunity to submit comment on the application prior to a decision being made. Similarly, in certain circumstances, it may be necessary for a DSCoE to share information contained in the submissions made by a VLOP/VLOSE with Applicant(s) in advance of a decision being made. In addition, DSCoEs are also obliged to publish an overview of a reasoned request in the DSA data access portal once it is formulated.

1.22 In light of this, if there is any information in an application and supporting documentation and/or submissions which the Applicant(s) and/or VLOPs/VLOSEs consider to be confidential, the Applicant(s) and VLOPs/VLOSEs should clearly identify that information and explain why they believe it should not be shared or published. Confidential information may include commercially sensitive information (whether to the Applicant(s) or VLOP/VLOSE or to another party, such as the Research Organisation with which the Applicant(s) are affiliated).

1.23 When claiming that information is confidential, Applicant(s) and VLOPs/VLOSEs should:

(a) Identify those specific pieces of information in respect of which confidentiality is claimed;
(b) Explain the basis upon which confidentiality is claimed and, in doing so, clearly identify the harm that would result from the disclosure of the information claimed to be confidential;
(c) Provide i) a non-confidential version and ii) a confidential version of each of the relevant documents to the DSCoE. The non-confidential version of relevant documents should redact the information in respect of which confidentiality is claimed; and
(d) Provide a non-confidential summary of information in respect of which confidentiality is claimed.

1.24 Please note that, in general terms, Applicant(s) and VLOPs/VLOSEs may not claim confidentiality over an entire document or whole sections of a document. It should be possible to protect confidential information with limited redactions; entirely blank or blacked-out pages without justification will not be accepted. A DSCoE retains the discretion to share or publish whatever information the DSCoE considers necessary, having regard to the DSCoE's legal and regulatory obligations, including in respect of fair procedures and good administration and in line with applicable law.

1.25 As noted at paragraph 2.11 above, these steps are required in circumstances where it may be necessary for a DSC to share information and documentation, including an application, with the relevant VLOP/VLOSE in advance of a decision being made. A DSC retains the discretion to uphold or reject a claim of confidentiality made by the Applicant(s) over information in an application, having regard to the DSCoE's legal and regulatory obligations, including in respect of fair procedures and good administration and in line with applicable law.

1.26 A DSCoE is required to determine the Applicant(s) application within 80 working days of the date on which it is submitted. This 80 working day period can be extended where this is justified. Where a DSCoE requires additional time to make its decision, it will notify the Applicant(s) of same, explaining the basis on which additional time is required and notifying the Applicant(s) of a new date by which the application will be determined.

1.27 The Applicant(s) will be notified of the DSCoE's decision regarding the application via the Portal (the "**Application Decision**") and any other means required under national law. Where a DSCoE decides to designate the Applicant(s) as a VR for the specified research, a DSCoE will proceed to issue a reasoned request for access to data to the relevant VLOP/VLOSE concerned (the "**Reasoned Request**").

1.28 On receipt of the Reasoned Request, the VLOP/VLOSE must either proceed to provide the Applicant(s) with access to the requested data within the time period specified in the Reasoned Request, in accordance with the terms of the Reasoned Request or, within 15 days of receipt of the Reasoned Request, submit a proposal for an amendment to the Reasoned Request (an "**Amendment Request**") on the basis that:

(a) They do not have access to the data; or
(b) Giving access to the data would lead to significant vulnerabilities in the security of their service or the protection of confidential information, in particular trade secrets.

1.29 A DSCoE will determine any Amendment Request submitted to it in accordance with the DSA and Delegated Act within a further 15 days. To enable a DSCoE to make its determination, it may issue requests for information to the Applicant(s) and/or the VLOP/VLOSE concerned and/or consult with subject matter experts. If the amendment proposal is accepted by a DSCoE, a new Reasoned Request will be formulated by the DSCoE and issued to the VLOP/VLOSE, who will then be required to comply with the revised terms of the Reasoned Request. The Applicant(s) will be notified of the decision of the DSCoE in relation to any Amendment Request and provided with the amended Reasoned Request, where applicable.

1.30 The Applicant(s) will also be notified through the Portal in the event a DSCoE decides that the application does not demonstrate that the Applicant(s) meets the designation conditions and related requirements and, accordingly, refuses to designate the Applicant(s) as a VR for the specified research. Where an application has been refused, if the Applicant(s) wishes to challenge the refusal,

the Applicant(s) will have a set time period from the date of the decision to request a review or otherwise seek to appeal the Decision. National specificities may apply and it is recommended Applicant(s) seek further information from the DSCoE.

How to apply

1.31 Applications must be submitted via the Portal.

1.32 To access the features available on the private area of the Portal, which is necessary in order to make an application, each Applicant needs to have EU Login credentials and a profile created on the Portal.

1.33 Each Applicant participating in a VR status application must have a dedicated profile created on the Portal for submitting VR status applications as principal researcher or as applicant researcher on the VR status application.

Application Requirements

1.34 This section of the Guidance sets out what an application must contain in order for it to be considered by a DSC to be a complete application. Failure to comply with the Application Requirements may lead to the Applicant(s) application being rejected.

1.35 The Applicant(s) is responsible for demonstrating that the Applicant(s) satisfies the conditions set out in Article 40(8) of the DSA and related requirements set out in the Delegated Act. The Applicant(s) must submit all of the information and the documentary evidence specified in this Guidance and/or as may be requested at a later stage by the DSC. It is important that the Applicant(s) ensure **full and accurate information** is provided to avoid any delays to the application process.

1.36 In assessing an application, the DSC will have regard to the information submitted by the Applicant(s) and also to information available to it from its own independent information-gathering and research that may be relevant to its verification of the information submitted by the Applicant(s). A DSC may also take into account information provided to it by the VLOP/VLOSE in connection with an application.

Information to be provided in respect of each of the conditions in Article 40(8) and related requirements in the Delegated Act.

1.37 The DSA and the Delegated Act do not provide for the amendment of Applicant(s) named in an application while that application is being assessed, or those referenced in a reasoned request after it has been issued to the VLOP/VLOSE. If Applicant(s) would like to add additional team members, not included in the original application, then a new application for vetted researcher status for those new team members will be required. There is no limit on how many Applicant(s) can be included in a single application for vetted researcher status. Each applicant must meet the conditions set out in Article 40(8) DSA and related requirements set out in the Delegated Act.

1.38 Applicant(s) are responsible for ensuring that all information submitted as part of their application is accurate. This includes Research Organisation details.

1.39 All Applicant(s) must demonstrate they meet all conditions, to be granted Vetted Research status. All Applicant(s) must commit to informing both the DSCoO (if relevant) and the DSCoE of any changes to their circumstances at any point after submitting an application.

1.40 If it is determined that a vetted researcher no longer meets the conditions as set out in the DSA and the Delegated Act during the defined data access period, access to data may be terminated.

1.41 The below sections contain non-exhaustive suggestions of how an Applicant(s) may demonstrate they meet the relevant conditions. Applicant(s) should be transparent and provide as much detail as possible in their application and/or supporting documents.

1.42 Article 40(8)(a) - Demonstrating Affiliation to Research Organisation

For each Applicant, the application must demonstrate affiliation to a Research Organisation. For these purposes 'Research Organisation' has the definition given to it in Article 2, point (1), of Directive (EU) 2019/790 of the European Parliament and of the Council and includes civil society organisations that are conducting scientific research with the primary goal of supporting their public interest mission (a "**Research Organisation**")

The following, is a non-exhaustive list of possible supporting documents Applicant(s) may choose to submit. This may include, but is not limited to, providing at least one and, in some situations, more than one, of the items listed below. The Applicant(s) should consider, having regard to their particular circumstances, what information and documentation should be provided in order for their application to demonstrate affiliation to a Research Organisation:

<u>Affiliation</u>

(a) Formal letter signed by Research Organisation stating that the Applicant(s) are affiliated with the organisation;
(b) Proof of legal association with a Research Organisation;
(c) Contract of employment for the Applicant(s) in question;
(d) Funding award letter;
(e) Ethical approval letter;
(f) evidence of the organisation's adherence to any code of conduct on research integrity and/or code of ethics governing research activities;
(g) Confirmation that Applicant(s) may rely on Research Organisation's technical and organisational information security measures to address conditions set out in Article

40(8)(d).

Research Organisation

(a) Annual Reports, Financial Statements, Returns etc from the legal entity showing that a significant portion of funding is allocated to research activities and the organisation operates on a not-for-profit basis;
(b) For public institutions, links to the legal text creating the institution;
(c) Links to relevant sections of the of the Research Organisation;
(d) Relevant Articles of Association, or Constitution a public interest mission recognised by an EU Member State;
(e) Governance relating to the board of the Research Organisation;
(f) If on a not-for-profit basis, documentation evidencing the not-for-profit or charity status of the Research Organisation;
(g) If on a 'for profit' basis, evidence that shows that all profits are reinvested in scientific research such as annual reports or financial statements; and/or
(h) Confirmation that the results generated by the organisation's research are not used on a preferential basis by any party that exercises decisive influence on the organisation, including special or exclusive access, early access to findings etc.

1.43 Article 40(8)(b) - Demonstrating independence from Commercial Interest

For each Applicant(s), the application must demonstrate independence from commercial interests. A completed and signed declaration of independence from commercial interests must be provided by each Applicant. Consideration should be given to the following;

Confirmation of the absence of, or if applicable an explanation of any:

(a) Conflict of interest that would result in the Applicant(s) not being independent from commercial interests;
(b) Funding of the research project for which the data are requested from commercial / private / semi-private entities;
(c) Financial interest in any VLOP/VLOSE or competitor of any VLOP/VLOSE;
(d) Previous employment with any VLOP/VLOSE or competitor of any VLOP/VLOSE within the last three years;
(e) A material business relationship with a VLOP/VLOSE or competitor of any VLOP/VLOSE, either directly or through any other organisation in which the Applicant(s) are partners, shareholders, directors, senior employees, etc.;
(f) Close familial ties with any shareholder, director or senior employee of a VLOP/VLOSE.
(g) Any circumstances that could suggest that Applicant(s) may have commercial interests should be explained as transparently as possible.

The following, is a non-exhaustive list of possible supporting documents Applicant(s) may choose to submit. Documentation which may be demonstrative of independence from commercial interests includes but is not limited to documents relating to:

(a) The existence of financing agreements;
(b) The existence of any partnership agreements;
(c) Any codes of conduct and ethical guidelines adhered to by Applicant(s) as well as any conflict of interest policy

(d) The Research Organisation's ownership structure and who makes strategic decisions;
(e) The Research Organisation's financing model (and if the model includes multiple sources of financing, specifying same);
(f) Evidence of the organisation's adherence to any code of conduct on research integrity and/or code of ethics governing research activities.

1.44 Article 40(8)(c) - Information Required in Relation to the Funding of the Research

The application must disclose the funding of the research the subject of the application. To comply with this condition, information and/or documentation must be provided which discloses the funding of the research, to include details on financial and non-financial contributions supporting the research the subject of the application.

The following, is a non-exhaustive list of possible supporting documents Applicant(s) may choose to submit. This may include, but is not limited to, the documents and information listed below. The Applicant(s) should consider their particular circumstances, and determine what information and documentation should be provided in order to demonstrate that their application discloses:

(a) Details of financial contributions, both public or private, supporting the research project for which the data are requested and the dates of any relevant funding. This should include financial contributions already obtained at the time of the submission of the application or possible financial contributions which have been applied for but in respect of which decisions are pending;
(b) Details of non-financial contributions the research project would benefit from, such as contributions in-kind, the use of facilities, or structural reliance on expertise;
(c) Details of any indirect funding, such as sources of salaries or other payments of the Applicant(s);
(d) Copy of any funding award letter;
(e) Copy of any grant agreement;
(f) A declaration signed by each Applicant, declaring that except for the third-party funding disclosed by the Applicant(s), the Applicant(s) do not intend to rely on any funding to perform the research other than indirect funding or non-financial support provided by the Applicant(s) Research Organisation of affiliation;
(g) Information on funding as to any arrangements in place to bridge funding or otherwise support the work should the current funding award end before the data access duration date.

The information provided by the Applicant(s) should include details of any contributions, such as the funding entity, the amount, the nature and duration of the contribution, including whether the funding has already been awarded or is still under evaluation, as well as, where applicable, relevant references to EU funded projects.

External funding is not a pre-condition. However, Applicant(s) should give as much clarity as possible on any funding declared.

In addition to funding sources, Applicant(s) should also provide all details regarding non-financial contributions. Benefits in-kind include (non-exhaustive list) premises, labs/offices, IT equipment, cloud computing resources, software licences, hardware loans or other such materials required for the research, personnel or expertise, any previous funding which may be deemed a conflict of interest, etc.

Where available, the application should also include the outcomes of evaluations conducted by the entity providing the funding.

1.45 Article 40(8)(d) - Demonstrating capability to fulfil specific data security, confidentiality and personal data protection requirements

The application must demonstrate that the Applicant(s) are capable of fulfilling the specific data security and confidentiality requirements corresponding to the requested data and to protect personal data (where relevant).

The application must include 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. This must include:

(a) Identification of data security and confidentiality risks associated with the request;
(b) Description of technical, legal and organisational measures to mitigate the above risks;
(c) Details on proposed access modality and its associated technical security measures;
(d) Description of whether the data is pseudonymised or relates to an individual who is identified or identifiable without the need for any additional information;
(e) Information demonstrating compliance with data protection legislation, including an assessment of the risks that the processing of personal data would entail for data subjects;
(f) Relevant data protection documentation identifying the roles and responsibilities within the meaning of data protection legislation;
(g) Description of the legal basis to be used under GDPR; and
(h) Description of technical, organisational and legal measures to mitigate the risks relating to personal data.

Further guidance in respect of compliance with Article 40(8)(d) is set out below under different headings.

<u>Data Security</u>

The following is a non-exhaustive list of possible supporting documents Applicant(s) may choose to submit. Documents which may be provided in order to demonstrate that the Applicant(s) can fulfil the specific data security requirements corresponding to the requested data include, but are not limited to, one or more of the documents listed below. The Applicant(s) should consider, having regard to the subject matter of the application, what documentation should be provided for this purpose:

(a) ICT Security assessment;
(b) Security accreditation of investigators or entities;
(c) Software security assessments or technical assessments;
(d) Detailed description of technical security measures of proposed access modality;
(e) Privacy policies of Secure Processing Environment (SPE);
(f) Contract and Terms & Conditions of Secure Processing Environment;
(g) ISO Standards certification;
(h) IT security documentation related to Research Organisation IT (if relevant);
(i) Data Management Plan (DMP) with Research Organisation review/ recommendations;
(j) Data Protection Impact Assessment (DPIA) with Data Protection Officer (DPO) review/ recommendations;
(k) Record of Processing Activities (ROPA)
(l) Any other documentation which demonstrate the implementation of data security best practices; and

(m) Declaration signed by Research Organisation that the Applicant(s) may use the Research Organisation's technical, organisational and legal measures to fulfil the data security requirements that correspond to the requested data.

Data Confidentiality

For your consideration, the following, is a non-exhaustive list of possible supporting documents Applicant(s) may choose to submit. Documents which may be provided in order to demonstrate that the Applicant(s) are capable of fulfilling the specific data confidentiality requirements corresponding to the requested data include, but are not limited to, one or more of the documents listed below. The Applicant(s) should consider, having regard to the subject matter of the application, what documentation should be provided for this purpose:

(a) Data Management Plan with Research Organisation review/recommendations;
(b) Data Protection Impact Assessment (DPIA) with DPO review/ recommendation;
(c) Record of Processing Activities (ROPA);
(d) Any involvement with National Data Protection Authority (DPA) should be attached as supporting documentation;
(e) Statement of understanding that only aggregate or summary results should be published;
(f) Statement of understanding that raw or individual level data should not be published;
(g) Declaration signed by Research Organisation that the Applicant(s) may use the Research Organization’s technical and organisational measures to fulfil the data confidentiality requirements that correspond to the requested data;
(h) Data Flow Diagram (DFD).

Personal Data Protection

For your consideration, the following, is a non-exhaustive list of possible supporting documents Applicant(s) may choose to submit. Documents which may be provided in order to demonstrate that the Applicant(s) is capable of fulfilling the specific personal data protection requirements corresponding to the requested data include, but are not limited to, one or more of the documents listed below. The Applicant(s) should consider, having regard to the subject matter of the application, what documentation should be provided for this purpose;

(a) Data Management Plan (DMP) with Research Organisation review/recommendations;
(b) Data Protection Impact Assessment (DPIA) with DPO review/ recommendations;
(c) Record of Processing Activities (ROPA);
(d) Any involvement with National Data Protection Authority (DPA) should be attached as supporting documentation;
(e) Statement of understanding that only aggregate or summary results should be published;
(f) Statement of understanding that raw or individual level data should not be published;
(g) Statement that no attempt to reidentify data subjects will be made;
(h) Declaration signed by Research Organisation that the Applicant(s) may use the Research Organisation's technical organisational and legal measures to fulfil the personal data protection requirements that correspond to the requested data;
(i) Description of the legal basis to be used under GDPR;
(j) Data Flow Diagram (DFD).

Technical Measures to Protect Data

In order to comply with the condition that the Applicant(s) demonstrates in the application the appropriate technical measures that the Applicant(s) have put and will put in place having regard to data security and confidentiality and, if applicable, personal data protection, documents to be provided may include those listed below. Applicant(s) should consider, having regard to the subject matter of the application, what documentation should be provided for this purpose. For your consideration, the following, is a non-exhaustive list of possible supporting documents Applicant(s) may choose to submit:

(a) Detailed description of technical security measures of proposed access modality;
(b) A declaration signed by Research Organisation that the Applicant(s) may use the Research Organisation's technical measures to fulfil the technical measures requirements that correspond to the requested data;
(c) ISO 27001, ISO 27002, ISO 27701 Certification or similar;
(d) SOC2 Attestation Report or similar;
(e) NIS2 Directive compliance or similar;

Organisational Measures to Protect Data

In order to comply with the condition that the Applicant(s) demonstrate in the application the appropriate organisational measures that the Applicant(s) has put and will put in place having regard to data security and confidentiality and, if applicable, personal data protection, documents to be provided may include those listed below. Applicant(s) should consider, having regard to the subject matter of the application, what documentation should be provided for this purpose. For your consideration, the following, is a non-exhaustive list of possible supporting documents Applicant(s) may choose to submit:

(a) Data sharing agreement;
(b) Non-disclosure agreements;
(c) Data management policies;
(d) Ethical or methodological review/approval;
(e) Data Protection Training certificates or similar;
(f) Data Breach policy of Research Organisation;
(g) Undertaking by the Applicant(s) prohibiting them from disclosing the data to any person(s) not named in their applications, prohibition against the use or disclosure of data in any manner that was not described in the application;
(h) Declaration signed by Research Organisation that the Applicant(s) may use the Research Organisation's organisational measures to fulfil the organisational measures requirements that correspond to the requested data.

Legal Measures to protect Data

In order to comply with the requirement that the Applicant(s) demonstrates in their request the appropriate legal measures that the Applicant(s) have put and will put in place having regard to data security and confidentiality and, if applicable, personal data protection, documents to be provided may include those listed below. Applicant(s) should consider, having regard to the subject matter of the application, what documentation should be provided for this purpose. For your consideration, the following, is a non-exhaustive list of possible supporting documents Applicant(s) may choose to submit:

(a) Data sharing agreement;
(b) Non-disclosure agreement;

(c) Data processing agreement with any third party who will process the data on the Applicant(s) behalf;
(d) Other contractual protections.

Special Considerations for International Personal Data Transfers

Some or all of the data that will be accessed by the Applicant(s) if granted VR status might not constitute personal data. However, if the Applicant(s) will access any personal data, the application should indicate whether there will be any 'international personal data transfer' for the purposes of the GDPR. An international personal data transfer is the transfer of personal data to a country outside of the European Economic Area ("**EEA**").

The meaning of transfer is extremely broad. It does not require a physical handover of data or direct transfer and can include remote access from a third country. Some examples of what may constitute an international personal data transfer includes, but is not limited to:

(a) A situation where he Applicant(s) /the affiliated Research Organisation is located/established in a country outside the EEA;
(b) A situation where the Applicant(s) /the affiliated Research Organisation is located/established within the EEA, however the data will be hosted/provided/accessed on a platform which is outside the EEA.

If an international personal data transfer will be involved should the Applicant(s) be granted VR status, the application must demonstrate that the Applicant(s) will ensure compliance with the obligations under the GDPR in connection with such transfer, i.e. that the access will be covered by:

(a) The third country being covered by an 'adequacy decision';
(b) Appropriate safeguards for data subjects' rights (e.g. the Applicant(s) will enter into Standard Contractual Clauses governing the transfer and that a positive Transfer Impact Assessment has been completed).

1.46 Article 40(8)(e) - Demonstrating Proposed Access and Timeframe are necessary for and proportionate to the purpose of the research

The application must demonstrate that access to the data and the time frames requested are necessary for, and proportionate to, the purposes of the Applicant(s) research, and that the expected results of that research will contribute to the purposes laid down in Article 40(4) DSA. Article 40(4) provides for access to data "*for the sole purpose of conducting research that contributes to the detection, identification and understanding of systemic risks in the Union, as set out in Article 34(1), and to the assessment of the adequacy, efficiency and impacts of the risk mitigation measures pursuant to Article 35.*"

The application must contain:

(a) 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 the Delegated Act (i.e. information in the VLOP/VLOSE's DSA data catalogue);
(b) Information on the necessity and proportionality of the access to the data and the time frames for the purposes of the research for which the data are requested; and

(c) A description of the research activities to be conducted with the requested data and an estimation of the required duration of the access.

Further guidance in respect of compliance with Article 40(8)(e) is set out below under different headings.

Necessity and Proportionality of Access

In order to demonstrate that the access to data that the Applicant(s) request is necessary and proportionate, documents to be provided may include those listed below. Applicant(s) should consider, having regard to the subject matter of the application, what documentation should be provided in order to demonstrate that the access to data the Applicant(s) has requested is necessary and proportionate. For your consideration, the following, is a non-exhaustive list of possible supporting documents Applicant(s) may choose to submit:

(a) Data Management Plan (DMP) with Research Organisation review / recommendations;
(b) Data Protection Impact Assessment (DPIA) with DPO review/ recommendations;
(c) Necessity assessment or other such documentation demonstrating the access to data are necessary; and
(d) Proportionality assessment or other such documentation demonstrating the access to data are proportionate.

In respect of the necessity and proportionality of access, an application should consider, and where appropriate, address the following:

(a) A clear description of data variables requested is expected, which should include format, scope and where possible specific attributes, relevant metadata and data documentation. Applicant(s) should ask for the exact data they require access to and that they believe the VLOP/VLOSE may have;
(b) Each variable or groups of variables (particularly where personal data is concerned) must be necessary for the project and this should be described by the Applicant(s);
(c) Applicant(s) should demonstrate that the amount, scope, granularity and type of data requested do not exceed what is necessary to achieve the research objectives;
(d) Applicant(s) should describe how the data and data format were selected;
(e) Whether data requested are aggregate data or individual level data;
(f) Whether data requested are anonymous, pseudonymised or identifiable data;
(g) Applicant(s) should provide a description of why these data must be used (as opposed to aggregate data or anonymous data for example);
(h) Applicant(s) should consider whether there is a less intrusive way to complete the research;
(i) Any data minimisation is clearly described and justified;
(j) That the access requested balances the impact on the rights and interests (e.g. commercial interests, interests in confidential information, intellectual property rights, data protection rights, etc.) of (i) the data subjects; (ii) the VLOP/VLOSE; and (iii) any other affected third parties, and Applicant(s) should describe their assessment of same; and
(k) The importance of the objective should be described.

Necessity and Proportionality of Timeframe of Access:

In order to demonstrate that the timeframe of access to data the Applicant(s) requests is necessary and proportionate, documents to be provided may include:

(a) Data Management Plan (DMP) with Research Organisation review/recommendations;
(b) Data Protection Impact Assessment (DPIA) with DPO review/ recommendations;
(c) Necessity assessment or other such documentation demonstrating the timeframe to data are necessary; and/or
(d) Proportionality assessment or other such documentation demonstrating the timeframe to data are proportionate.

In respect of the necessity and proportionality of timeframe of access, an application should address the following:

(a) A description of the timeframe in relation to the data requested, including whether it is requested as at a set timepoint, or over a time range;
(b) A description of how long the Applicant(s) will need access to data for and a justification of why the timeframe is necessary;
(c) A justification of the data retention period described;
(d) A breakdown of the research project timeline, i.e., the duration of data cleaning, data analysis, report writing, peer review, publication etc;

Applicant(s) should demonstrate why the timeframe for access to data requested is adequate to achieve the envisaged objective of the research.

In cases whereby Applicant(s) request access to live systems, or live data, they should explain why it is proportionate, including why the research could not be achieved through the examination of historical data.

Expected Results

In addition, Applicant(s) must describe how the results sought to be achieved will contribute toward the detection, identification and understanding of systemic risks in the EU, as set out pursuant to Article 34(1) of the DSA, and to the assessment of the adequacy, efficiency and impacts of the risk mitigation measures pursuant to Article 35 of the DSA, and should describe both the benefits and risks associated with the proposed research. A Data Management Plan (DMP) or Data Protection Impact Assessment (DPIA) with Research Organisation review will again be considered by DSCs in this regard.

1.47 Article 40(8)(f) - Demonstrating that research activities will be carried out for the purposes laid down in Article 40(4) DSA

In order to comply with the condition that the Applicant(s) demonstrate that the research activities will be carried out for the purposes laid down in Article 40(4) DSA, the Applicant(s) must provide the following documentation and information:

(a) A description of the research activities to be conducted with the requested data and an estimation of the required duration of the access;
(b) A summary of the application including the research topic; and
(c) A description of the purpose pursuant to DSA Articles 34 and 35. This should cover research activities and methodology and give details of how they are connected to Article 34 (systemic risks) and Article 35 (mitigation measures) and related to the specific VLOP/VLOSE.

A link should be made between the systemic risks and the design or functioning of the VLOP/VLOSE's service and its related systems or use of the VLOP/VLOSE's service. DSCs will assess whether the application demonstrates that the research described will be carried out for the purposes of contributing to the detection, identification and understanding of systemic risks in the EU stemming from the design, functioning or use of the VLOP/VLOSE, and to the assessment of the adequacy, efficiency and impacts of risk mitigation measures.

The application should describe the specific systemic risks in the EU stemming from the design or functioning of the service in question and its related systems, including algorithmic systems, or from the use made of said services that are the intended focus of the research. The following non-exhaustive examples of such systemic risks are set out in the DSA:

(a) The dissemination of illegal content through the VLOP/VLOSE;
(b) Any actual or foreseeable negative effects for the exercise of fundamental rights;
(c) Any actual or foreseeable negative effects on civic discourse and electoral processes, and public security;
(d) Any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being.

Other potential systemic risks include any systemic risks identified by the relevant VLOP/VLOSE in its own risk assessments performed under the DSA.

Applicant(s) should also include a confirmation that there is no other intended use of the data outside of this research.

1.48 Article 40(8)(g) - Demonstrating Commitment to Publication of Research Results

The application must demonstrate that the Applicant(s) are committed to making the research results publicly available, free of charge, within a reasonable period after the completion of the research, subject to the rights and interests of the recipients of the service concerned, in accordance with the GDPR.

Each Applicant must provide, a written and signed commitment to make research results publicly available, free of charge, subject to the rights and interests of the recipients of the service under the GDPR. Information should also be provided as to the way in which it is expected that the results will be made publicly available, free of charge and a timeframe should be proposed for same. Where there is an indication that part of the results will not be made publicly available free of charge, the Applicant(s) should explain the basis for this.

Further guidance in respect of applications

1.49 By submitting an application, the Applicant(s) declares that the information contained in the application form and supporting documents relating to the application is true and correct to the best of each Applicant(s) knowledge and belief.

1.50 All applications must comply with the following:

(a) **False or misleading information:** You must not include any false or misleading information in your application. There may be national specificities Applicant(s) should be aware of in relation to any possible criminal offences should they submit false or misleading information as part of their application. Applicant(s) should, in the first instance, consult with the DSCoO for more information.

(b) **Changes:** The Applicant(s) must notify the DSCoO (where an application was submitted via this route) and the DSCoE promptly of any changes that occur, between the date of submission of your application and the date on which you receive notice of the DSCoE decision on the application, to any material information contained in the application and/or to any supplemental information that was provided subsequent to the submission of the initial application as requested by the DSC to support its assessment of whether the Applicant(s) met the requirements to be awarded VR status.

(c) **Publication:** The DSCoE is required to publish an overview of any reasoned request that is issued to a VLOP/VLOSE in the public interface of the DSA Data Access Portal. This shall include a summary of the application (if successful) and the access modalities as determined pursuant to Art. 9 of the Delegated Act.

(d) **Confidential and Commercially Sensitive Information:** In submitting an application, the Applicant(s) should bear in mind that the DSC may share information contained in the application and supporting documents with the relevant VLOP/VLOSE, where the DSC considers this to be necessary in order to give them an opportunity to submit comments on the application. The DSC is also obliged to publish an overview of a reasoned request in the DSA data access portal once it is formulated. If there is any information in the application or supporting documents which the Applicant(s) considers to be confidential or commercially sensitive (whether to the Applicant(s) or to another party, such as the Research Organisation with which the Applicant(s) is affiliated), to the extent that it should not be shared by a DSC with the relevant VLOP/VLOSE or published, the Applicant(s) should clearly identify that information and explain why you believe it should not be shared or published. This is addressed in further detail at section 3.11 above. The DSC will consider any such explanation but retains discretion to share or publish whatever information the DSC considers necessary.

(e) **Freedom of Information:** Requests for access to records held by DSCs may be made by members of the public under various national legal provisions, subject to certain exemptions and restrictions. Applicant(s) are encouraged to review the privacy policies of the DCSoO, and/or the DSCoE and to seek independent legal advice as appropriate.

(f) **Personal Data:** DSCs are obligated and committed to protecting all personal data submitted in accordance with its obligations under the General Data Protection Regulation (GDPR) and any other applicable data and privacy laws and regulations. Please review the privacy policies of the DCSoO (where relevant) and the DSCoE in this regard.

1.51 Please note that all documents and information submitted as part of a VR status application should only be submitted through the Portal.

Access Modalities

1.52 If the Applicant(s) are designated as a VR and a Reasoned Request is issued, the Reasoned Request will include details of any access modalities that the DSCoE requires the VLOP/VLOSE to use when providing the Applicant(s) with access to the data.

1.53 When determining the access modalities to be included in a Reasoned Request, the DSC is required to take into account any access modalities proposed by the Applicant(s) in the application and any access modalities proposed by the VLOP/VLOSE to be used in connection with data the VLOP/VLOSE has stated is available in its DSA data access catalogue. However, neither of these proposals is binding on the DSC.

1.54 The VLOP/VLOSE and the Applicant(s) will be required to comply with whatever access modalities are specified by the DSCoE in the Reasoned Request. These may include technical, legal or organisational measures to be used by the VLOP/VLOSE when providing you with access to the data. They may include, for example:

(a) Whether a secure processing environment is necessary to process the data;
(b) Relevant network security measures, encryption, access control, mechanisms, backup policies, data integrity mechanisms, incident response plans;
(c) Storage periods and data destruction plans;
(d) Internal review processes, restrictions of access rights and information sharing; and
(e) Any contractual requirements, such as non-disclosure agreements or data sharing agreements.

1.55 If the specified access modalities outlined in the reasoned request include a requirement that the VLOP/VLOSE enters into a data sharing agreement or any other contractual arrangement with the Applicant(s), then the Applicant(s) and the VLOP/VLOSE will be required to enter into that contractual arrangement. As such, both parties may be subject to contractual obligations in connection with the Applicant(s) access to the data.

After an application for Vetted Researcher status is approved

1.56 If the Applicant(s) is designated as a Vetted Researcher and a Reasoned Request is issued, the Applicant(s) must comply with the designation conditions set out in Article 40(8) of the DSA and related requirements set out in the Delegated Act and implement the technical, legal and organisational measures that the Applicant(s) stated would be put in place in the application when accessing the data and performing the research within the scope of the Reasoned Request. If the Applicant(s) fail to do so then this may result, among other things, in the Applicant(s) access to the data within the scope of that Reasoned Request being terminated under Article 40(10) of the DSA.

1.57 A DSC may commence an investigation for the purposes of determining whether Applicant(s) who have been granted the status of VR continue to meet the designation conditions as set out in Article 40(8) of the DSA at any time. A DSC may do this of its own volition or based on information provided to it by any third party including but not limited to the relevant VLOP/VLOSE. Subject to the outcome of such an investigation, a DSCoE may terminate the Applicant(s) data access if it determines that the Applicant(s) no longer meet the designation conditions. If the Applicant(s) data access is terminated, the VLOP/VLOSE will no longer be required to provide the Applicant(s) with access to the data within the scope of the Reasoned Request.

1.58 If the Applicant(s) access to data within the scope of a Reasoned Request is not terminated early, then the Applicant(s) access to that data will expire on the date specified in the Reasoned Request.

1.59 Further to the commitment the Applicant(s) provided in the application, the Applicant(s) will be required to make the results of the Applicant(s) research publicly available free of charge within a reasonable period after the completion of the Applicant(s) research.