Consultation on Digital Services Act (DSA) transparency database

Fields marked with * are mandatory.

Welcome

Digital Services Act (DSA)

The DSA introduces a comprehensive new set of rules for online intermediary services. The new rules include new responsibilities to limit the spread of illegal content and illegal products online, increase the protection of minors, and give users more choice and better information.

All online intermediaries, except micro and small enterprises, will have to comply with wide-ranging new transparency obligations to increase accountability and oversight. The obligations of different online players match their role, size, and impact in the online ecosystem.

Statement of Reason database - public consultation

Article 24(5) of the DSA prescribes that “providers of online platforms shall, without undue delay, submit to the Commission the decisions and the statements of reasons referred to in Article 17(1) for the inclusion in a publicly accessible machine-readable database managed by the Commission”.

The Commission services have designed and prepared a database for statements of reasons, the DSA Transparency Database, in accordance with the regulation. The purpose of this consultation is to give the opportunity to all interested stakeholders and the wider public to provide feedback and suggestions on the precise way this obligation should be implemented, including the information to be collected, the methods for submission of statements of reasons, and the tools of access for the public.

Currently, submission of the statements of reasons is planned in the following ways:

- An API (Application Programming Interface) which is a software intermediary that allows two applications to talk to each other.
- An online web or HTML form that allows for user input.

The full text of the regulation is available here [The Digital Services Act: ensuring a safe and accountable online environment](https://eur-lex.europa.eu), and a link to the code of the statements of reasons database can be found in Github and the documentation is [here](https://github.com).
Please submit your input until 17 July 2023, so that the Commission services can take it into account in due time before the database becomes operational to ensure compliance with the Digital Services Act.

Who are you?

1. As an interested party in this consultation, please identify yourself under the following categories:
   - ☐ A platform with obligations under the DSA with more than 45 million users
   - ☐ A platform with obligations under the DSA with less than 45 million users
   - ☐ Potential vetted researcher under DSA
   - ☐ Interested non-governmental organisation (not covered under a or b)
   - ☐ Government agency or government funded
   - ☐ Law or legal company
   - ☐ Journalist / media influencer (e.g., high profile on social media)
   - ☐ Political organisation
   - ☐ General Public
   - ☐ Other

2. First Name

3. Last Name

4. Email

5. Organisation Name

6. Country of Residence

If you reply on behalf of a platform, in which EU countries does your platform operate in?

☐ AT - Austria
☐ BE - Belgium
☐ BG - Bulgaria
☐ HR - Croatia
☐ CY - Cyprus
☐ CZ - Czechia
☐ DK - Denmark
☐ EE - Estonia
7. If you are registered in the transparency register, please provide the identification number

03181945560-59

Submission Methods

8. Are you aware of the reporting obligations described above

- Yes
- No

9. Do you have an idea of the volume of statements of reasons you expect to send in a month?

- 1-10
- 11-100
- 101-1.000
- 1.001-10.000
- 10.001-100.000
- 100.001 - 1.000.000
- 1.000.001 - 10.000.000
- More than 10.000.000

Submission of Statement of Reasons via the API

The DSA Transparency Database has an application programming interface (API) that allows individuals and organizations that deal with large numbers of statements of reasons.
10. Will you use the API (documentation here) to submit statement of reasons information?
   - Yes
   - No

11. Do you have concerns in using the API for submissions?
   - Yes
   - No

   What concerns do you have in using the API for submissions?
   - Cost
   - Time
   - Complexity
   - Security
   - Other

Please indicate

We have a number of concerns, including but not limited to some mentioned in the list above. Our core concerns include among other things:

(1) the very short amount of time that has been given to providers of very large online platforms, in particular, to make the technical and operational adjustments required to support the requested data and allow for transmissions to the API. We have concerns about whether timely execution is feasible for very large online platforms and believe a more reasonable timeline should be offered to adapt to the technical specifications given the scale at issue;

(2) the requirement to submit and validate individual statements of reasons (rather than batches of individual statements of reasons) given the anticipated volume of SORs;

(3) the mismatch between the requirements of Articles 17 and 24 of the DSA and the requirements of the API;

(4) the existence of a validation protocol that requires all database fields to be filled in; as well as

(5) re-identification, abuse and circumvention risks given the breadth of information currently required by the API.

12. Would you prefer other submission method?
   - Web Form
   - File upload in a specified format
   - Other

Please specify

13. What kind of improvements would you suggest to the API?
As we also explain in our response to question 19 below, we are concerned that the draft API requires the submission and validation of individual statements of reasons. Given the expected scale and volume of statements of reasons that Google and other online platform providers will be submitting to the database for in-scope services, we would strongly advise, based on our technical expertise, that the API permit batch uploads (i.e. uploads of many statements of reasons in distinct batches, in frequencies that the European Commission determines) to lessen the transmission load on the European Commission servers. While we understand that the European Commission has conducted initial heavy load-testing, we are concerned that the significant volume of statements of reasons expected to be uploaded will unintentionally overwhelm the servers, resulting in transmission delays and potential inaccessibility of the database. There are also other benefits with batch uploads, which we explain in more detail in our response to question 19 below.

Additionally, the draft API requires all data fields provided to be filled for each statement of reasons submission to be validated and accepted to the database. Given technical, operational, and legal challenges relating to certain data points (which we explain in more detail below), and the time it may take for the European Commission to come to final resolution on those, we would welcome the introduction by the European Commission of some flexibility into the validation process, by making some of the now required fields optional.

The draft API as currently documented is not idempotent (e.g., there’s no protection against sending duplicate records). There may be occasions when duplicate records may be inadvertently transmitted (such as when there is a network error in the middle of a request, before a response is received). The draft API should be modified to be idempotent (e.g., by allowing the submitter to provide a unique ID and discarding submissions with IDs that already exist) to support de-duplication.

Submission of Statement of Reasons via the Web Form

This method allows the use of a web or HTML form for submission of statements of reasons to the DSA Transparency Database and would be suitable for low volumes.

• 14. Will you use the web form to submit statement of reasons information?
  ○ Yes
  ○ No

• 15. Do you have concerns in using Web Form submissions?
  ○ Yes
  ○ No

• What concerns do you have in using the Web Form for submissions?
  □ Cost
  □ Time
  □ Complexity
  □ Security
  □ Other

Please specify
16. Would you prefer other submission method?
- API (Sending Statements of Reason Individually)
- API (Sending Statements of Reason in batches)
- File upload in a specified format
- Other

17. What kind of improvements would you suggest to the web form?
As we describe in our responses to questions 13 and 19, we believe that an API that allows transmission of statements of reasons in batch submissions is necessary for a number of reasons and, in particular, for the European Commission database to bear the load of large volumes coming from in-scope online platform providers.

General Views on Submission Methods

18. What methods would you suggest for the Commission to receive the statements of reasons?
- WebForm
- API (sending statements of reasons individually)
- API (sending statements of reasons in batches)
- File upload in a specified format
- Other

19. Please explain your suggestion
Based on our technical expertise, we propose that it be possible to send the required information in batches rather than on a per-statement of reasons basis.

First, as we explain in our response to question 13, given the expected scale and volume of statements of reasons that Google and other online platform providers will be submitting to the database for in-scope services, the API should permit batch uploads (i.e. uploads of many statements of reasons in distinct batches, in frequencies that the European Commission determines) to lessen the transmission load on the European Commission servers. While we understand that the European Commission has conducted initial heavy load-testing, we are concerned that the significant volume of statements of reasons expected to be uploaded will unintentionally overwhelm the servers, resulting in transmission delays and potential inaccessibility of the database.

Second, batching makes it easier for online platforms to detect and recover from delivery errors at the time of transmission or at a time when the European Commission system goes down unexpectedly.

Third, in the event the European Commission continues to require such expansive data elements, a batch submission protocol with an acceptable delay will provide additional protection for users by reducing the possibility that personal data is shared (e.g., by giving online platforms more time to process the submissions to confirm that only data fields that are unlikely to result in an identification of a natural person are shared). It will also help reduce the risk of bad actors attempting to reverse engineer enforcement systems in real time.
Statements of Reason

Article 24(5) requires providers of online platforms to submit statements of reasons without undue delay.

• 20. What should the delay be in your opinion (choose the nearest option)?
  ○ no delay (immediately as it occurs)
  ○ twice per day
  ○ once per day
  ○ every 2 days
  ○ twice per week
  ○ once a week
  ○ less than once a week

Public Access to the DSA Transparency Database

The DSA Transparency Database is the one holding all the submitted statement of reasons from various platforms. In accordance with the DSA, it is publicly accessible, standardised and machine readable.

21. What other tools should be at the disposal of the users of the database to facilitate research and public scrutiny?

☐ Reports
☐ Data extraction
☑ Other

Please specify

The European Commission should design any additional tools for the public and researchers after considering the final data elements that are included in the database, and comprehensively reviewing the re-identification or reverse engineering risks posed by the data available to potential bad actors.

We respectfully suggest that a tiered-access structure may be beneficial for the database, especially if the EC envisages including sensitive data elements in the database. For example, the Lumen database (which, for the sake of clarity, contains a narrower scope of information than what is contemplated here) provides rate-limited access to full notices for the general public (e.g., 1 view of a full notice every 24 hours), while allowing more fulsome access to researchers and other organizations after approval by Lumen staff. Similar to this model, the European Commission may consider a model that allows multiple tiers of access for different use, e.g.:

(1) Highly rate-limited access to the general public, e.g. a particular number of views every 24 hours;
(2) Basic researcher access, which—after successful vetting—results in removal of the rate limiting and access to other functionality, such as filtering; and
(3) Highest level of access (such as data extraction) for vetted researchers who undergo significant vetting akin to that required under Article 40(8) of the DSA.

• 22. Should there be any type of access limitation/restriction to any part of the database?
  ○ Yes
Why?

The API is silent on who will be credentialed to access the Transparency Database. Depending on the granularity of the data that will eventually be included in the database, unfettered public access could allow for abuse or circumvention, by allowing bad actors to glean information on how detection and enforcement tools work, allowing them to reverse engineer targeted attacks. Whereas vetted researchers and authorities could find such data useful to contribute to their assessment of the presence of systemic risks on specific online platforms and/or across the EU, it should be recalled that those stakeholders have other means to get access to this information, with the safeguards duly required by the DSA. Making publicly available, with no limitations or restrictions, a detailed roadmap of content moderation decisions across online platforms should be approached with extreme caution, given the very objectives the DSA pursues.

Additionally, the numerous data fields currently required in the draft API (e.g., URL, source, detailed facts and circumstances) could, in combination, permit the re-identification of users and, therefore, be deemed to constitute personal data, as defined by European data protection authorities (DPAs); and conflict with the express requirement in Article 24 of the DSA not to include personal data in the submissions made to the database.

In those circumstances, the sharing of and making publicly-available these data points could also cause tension with GDPR requirements (e.g., providing adequate notice to affected data subjects about the processing of their personal data). Making this data publicly available without any access control also increases risk to these affected data subjects, compared to a database that would share this data with a limited number of parties.

Data Protection

Article 24 of the DSA regulation requires online platforms to send the statements of reasons to the Commission without any personal data.

23. How will you prevent personal information from being included in the Statement of Reasons submissions? What safeguards should be in place to ensure this?

First and foremost, we would urge the European Commission to design the API in a way that ensures privacy by design and prioritises data minimisation. Limiting the number of required data fields would also be in line with the requirements of Article 24(5) of the DSA, which requires that the information submitted to the database by online platforms does not contain personal data. Additionally, as explained above, we would in part rely on batch uploads to the database to more smoothly operationalise the requirement of personal data redaction.

This said, we are concerned that there is an unresolved conflict between some of the required data fields in the draft API and the broad interpretation given to the concept of personal data by DPAs in the context of sharing information about content moderation decisions. In particular, based on existing DPA decisions, there is a risk that the sharing of URLs may be deemed to constitute the sharing of personal data, to the extent that such URLs, especially when combined with the numerous other data points required by the database, could be used to re-identify users. Submitting this data could conflict with the express language in
Article 24 of the DSA prohibiting platforms from submitting personal data to the database. Similarly, identification of the user who submitted an Article 16 notice, as currently required in the “source” field, conflicts with the express prohibition of sharing personal data in Article 24 of the DSA.

*Content and Structure of the Statements of Reason*

The content and structure of the database is available at https://github.com/digital-services-act/transparency-database.

24. Do you think that the content and/or structure of the database needs any change?

- Yes
- No

What changes would you propose?

***We invite you to see the full response to this question in the PDF document, which is attached to the submission.***

Google understands that the European Commission’s goal for the database is to collect data and publicly share it to inform anonymous, statistical insight on content moderation and enforcement in the EU across online platforms, as defined under the DSA. We would like to offer some pragmatic feedback and concrete suggestions for the API, including:

1. Providing latitude for industry to have more lead time (beyond 28 August 2023) to modify technical systems to implement the statement of reasons database requirements and engage with the EC on certain data fields;

2. Introducing flexibility into the API’s validation protocol while very large online platforms continue to engage with the European Commission on certain data fields, including by allowing very large online platforms to submit statements of reasons that have some, but not all, required data fields;

3. Permitting online platforms to transmit data in batches to the European Commission in a pre-agreed frequency;

4. Providing further clarification about potentially overlapping data fields and convening discussion about implementation challenges relating to certain data fields;

5. Clarifying technical details that would be helpful to building workable transmission systems.

We welcome the opportunity to further discuss operational guidance and our proposals to satisfy the European Commission’s goals for creating and managing this new database while safeguarding user privacy, ensuring the database is scalable and durable, and decreasing potential friction or technical challenges associated with data transmission between systems.

Implementation Timeline: Our first concern is around the implementation timeline. The API will likely be finalized within weeks of 28 August 2023, yet the terms of the draft delegated act on the DSA audit requires that all compliance be in place and auditable by 28 August 2023. Google will work to modify technical systems to ensure statement of reasons submissions that are compliant with the requirements of the final API. However, given the time required for modification of technical systems and iterative industry
engagement with the European Commission to scope and define data points, we recommend providing industry with an express grace period that takes into account the lead time necessary for implementation once requirements are finalized.

Validation Protocol: Likewise, we recommend flexibility around the submission validation protocol to reflect the fact that requirements are still being finalized. Currently, in order for a statement of reasons submission to be “validated” and accepted into the database, all required data fields need to be filled. Some of these data fields present legal, technical, or operational challenges, and the European Commission should host robust stakeholder engagement on these complex topics without the time pressure to conclude all discussions before 28 August 2023. We recommend the European Commission introduce flexibility into the validation process and make certain currently “required” data fields optional.

Batching: As we have discussed in response to prior questions, we are also concerned about the database’s ability to intake large volumes of data from online platforms. We believe the API should permit batch uploads, which would (1) make it easier for online platforms to detect and recover from delivery errors or unexpected server interruptions, (2) ensure that large submitters do not overwhelm the European Commission’s transmission system, (3) in the event the European Commission continues to require such expansive data elements, give online platforms more time to remove personal data.

Data Fields Requiring Further Discussion: We would also welcome further discussion regarding a number of data fields that may pose legal, technical, or operational challenges.

For example, the draft API requires disclosure of a number of elements that are not specified in Articles 17 or 24 of the DSA, even though the scope of disclosures to the database are bounded, in the language of Article 24(5), by Article 17 of the DSA. Accordingly, the DSA appears to make clear that (very large) online platforms are not obligated to submit to the database data points beyond the information they are required to provide to users under Article 17 of the DSA. The draft API’s net-new requirements also pose a significant technical and implementation challenge given that online platforms have been building towards the requirements of Article 17 of the DSA for a significant length of time. Additional specifications will require new resourcing allocations and engineering lead time to modify existing technical builds.

***We invite you to see the full response to this question in the PDF document, which is attached to the submission.***

Additional Information and privacy statement

If you have an additional contribution (e.g., on the content and structure of the database, the submission methods, data protection or additional features), please upload your file(s) with your contribution.

025406cc-57aa-4c2e-ba34-4a3faa615389/FINAL_GOOGLE_PUBLIC_SUBMISSION_-_SOR_DATABASE.pdf

Privacy statement

The European Commission (hereafter ‘the Commission’) is committed to protect your personal data and to respect your privacy. The Commission collects and further processes personal data pursuant to 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 (repealing Regulation (EC) No 45/2001).
This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

The information in relation to the processing of personal data linked to targeted consultation activities organised by the services of the Commission is presented below.

**Why and how do we process your personal data?**

**Purpose of the processing operation:** The Commission collects and uses your personal information within the framework of targeted consultation activities to obtain your views on a specific initiative, policy or intervention.

You are being contacted by the service of the Commission since it has concluded that your views are relevant and necessary to inform the specific initiative, policy or intervention concerned by the targeted consultation.

For reasons of transparency and openness your views will, in principle, be published on a Europa website, in the form of a summary report. The Commission only publishes your identity if you consent to the publication.

To avoid misuse, anonymous contributions to the Commission may not be accepted, regardless whether you consent to the publication of your identity together with your contribution.

- The subject matter of the consultation activity require you to provide personal data in your response that may identify or make you identifiable. These personal data will only be published subject to your explicit consent.
- It is your responsibility if you opt for confidentiality of your personal data to avoid any reference in your submission or contribution itself that would reveal your identity.
- The consultation activity uses the Commission’s online questionnaire tool EUSurvey that requires you to login via your ‘EU Login’ or ‘social media account’. ‘EU Login’ requires certain personal data such as the name, surname and e-mail address of the registrant. For further information, please refer to the privacy statements of ‘EU Login’ and ‘EU Survey’ as well as the processing operations ‘Identity & Access Management Service (IAMS)’ (reference number in the public DPO register: DPR-EC-03187) and ‘EUSurvey’ (reference number: DPR-EC-01488). Should you choose to log in through your social media account, please refer to the pertinent social media platform’s privacy statement.
- Your contribution to the targeted consultation is stored in the Commission’s document management system (for further information on the Commission’s document management system please refer to the processing operation ‘Management and (short- and medium-term) preservation of Commission documents’, reference number: DPR-EC-00536).

The personal data processed may be reused for the purpose of procedures before the EU Courts, national courts, the European Ombudsman or the European Court of Auditor.

Your personal data will not be used for an automated decision-making including profiling.

**On what legal ground(s) do we process your personal data**

We process your personal data, because:

(a) processing is necessary for the performance of a task carried out in the public interest;
The Union law which is the basis for the processing based on Article 5(1)(a) of Regulation (EU) 2018/1725 is the Treaty of the European Union, and more specifically its Articles 1 and 11, Article 298 of the Treaty on the Functioning of the European Union, read in conjunction with Recital 22 of Regulation (EU) 2018/1725), as well as the Protocol 2 on the application of the principles of subsidiarity and proportionality. Further specific legal provisions may be provided in the specific privacy statement.

Which personal data do we collect and further process?
In order to carry out this processing operation the following categories of personal data may be processed:

- name and surname,
- country of residence,
- e-mail address of the respondent,
- the name of a self-employed individual (natural persons) on whose behalf the respondent is contributing,
- personal data related to the physical, economic, cultural, or social identity of the respondent, insofar as they are not falling under Article 10 of the Regulation,
- personal data included in the response or contribution to the targeted consultation activity, including (personal) opinions (if the targeted consultation at hand requires so),
- photos, audio/video recording.

Furthermore, you may spontaneously provide other, non-requested personal data in the context of your reply to the targeted consultation.

Please note that the Data Controller does not request nor expect that data subjects provide any special categories of data under Article 10(1) of Regulation 2018/1725 (that is “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation”) related to themselves or to third persons in their contributions to the targeted consultation activity. Any spontaneous inclusion of these types of personal data is the responsibility of the data subject and by including any of these types of data the data subject is considered to provide his/her explicit consent to the processing, in accordance with Article 10(2)(a) of Regulation 2018/1725.

How long do we keep your personal data?
The Data Controller only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing, namely for a maximum of five years after the closure of the file to which the present targeted consultation belongs. A file is closed at the latest once there has been a final outcome in relation to the initiative to which the targeted consultation contributed.
This administrative retention period of five years is based on the retention policy of European Commission documents and files (and the personal data contained in them), governed by the common Commission-level retention list for European Commission files SEC(2019)900. It is a regulatory document in the form of a retention schedule that establishes the retention periods for different types of European Commission files. That list has been notified to the European Data Protection Supervisor.

The administrative retention period is the period during which the Commission departments are required to keep a file depending on its usefulness for administrative purposes and the relevant statutory and legal obligations. This period begins to run from the time when the file is closed.
In accordance with the common Commission-level retention list, after the ‘administrative retention period’, files including (the outcome of) targeted consultations (and the personal data contained in them) can be transferred to the Historical Archives of the European Commission for historical purposes (for the processing operations concerning the Historical Archives, please see record of processing ‘Management and long-term preservation of the European Commission's Archives’, registered under reference number DPR-EC-00837).

**How do we protect and safeguard your personal data?**

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored on the servers of the Commission (or of its contractors (processors) if contractors are engaged to assist the controller). All processing operations are carried out pursuant to Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the Commission.

In order to protect your personal data, the Commission has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

The Commission’s processors (contractors) are bound by a specific contractual clause for any processing operations of your personal data on behalf of the Commission. The processors have to put in place appropriate technical and organisational measures to ensure the level of security, required by the Commission.

**Who has access to your personal data and to whom is it disclosed?**

Access to your personal data is provided to the Commission staff responsible for carrying out this processing operation and to authorised staff according to the “need to know” principle, in particular to follow-up on the targeted consultation. Such staff abide by statutory, and when required, additional confidentiality agreements.

Certain personal data may be made public on the Europa website, namely:

- any personal data on which you consented to their publication;
- personal data spontaneously provided by you in your contribution (without it being required by the targeted consultation activity).

Please note that pursuant to Article 3(13) of Regulation (EU) 2018/1725 public authorities (e.g. Court of Auditors, EU Court of Justice) which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

**What are your rights and how can you exercise them?**

You have specific rights as a ‘data subject’ under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access your personal data and to rectify them in case your personal data are inaccurate or incomplete. Under certain conditions, you have the right to erase your personal data, to restrict the processing of your personal data, to object to the processing and the right to data portability.
You have the right to object to the processing of your personal data, which is lawfully carried out pursuant to Article 5(1)(a), on grounds relating to your particular situation. Insofar you have consented to the certain processing of your personal data to the Data Controller for the present processing operation, you can withdraw your consent at any time by notifying the Data Controller. The withdrawal will not affect the lawfulness of the processing carried out before you have withdrawn the consent.

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given under Heading 9 below.

Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description (i.e. their Record reference(s) as specified under Heading 10 below) in your request.

In accordance with Article 14(3) of Regulation (EU) 2018/1725, your request as a data subject will be handled within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. In such case you will be informed of the extension of the time limit, together with the reasons for the delay.

**Contact information**

**The Data Controller**

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the Data Controller, whose contact details will be provided in the specific privacy statement of the specific targeted consultation activity.

**The Data Protection Officer (DPO) of the Commission**

You may contact the Data Protection Officer ([DATA-PROTECTION-OFFICER@ec.europa.eu](mailto:DATA-PROTECTION-OFFICER@ec.europa.eu)) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

**The European Data Protection Supervisor (EDPS)**

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor ([edps@edps.europa.eu](mailto:edps@edps.europa.eu)) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.

**Where to find more detailed information?**

The Commission Data Protection Officer (DPO) publishes the register of all processing operations on personal data by the Commission, which have been documented and notified to him. You may access the register via the following link: [http://ec.europa.eu/dpo-register](http://ec.europa.eu/dpo-register).

This specific processing operation has been included in the DPO’s public register with the following Record reference: DPR-EC-01011.

**Contact**

CNECT-DIGITAL-SERVICES@ec.europa.eu