Consultation on Digital Services Act (DSA) transparency database

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://ec.europa.eu/info/sites/info/files/digital-services-act-ensuring-safe-accountable-online-environment-2023-en.pdf), and a link to the code of the statements of reasons database can be found in [Github](https://github.com/EU-OSHA/dsa-transparency) and the documentation is [here](https://ec.europa.eu/info.CreateInstance).
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
   Snap Inc

6. Country of Residence
   ID40 - Outside the EU

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

976985829492-08

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

---

At this stage, we have several concerns about using the API for submissions, namely:

**Privacy** - URL field is potentially exposing personal identifiable information, which can be used to trace back to a particular individual and/or lead to scraping of data. URL should not be communicated if companies deem they could lead to privacy breaches.

**Security** - We understand tokens are associated with the EU login which is associated with a company specific email ID. If the integrity of the API token is compromised it can be used by bad actors impersonating the company. At this stage it’s unclear how this will be prevented by the Commission and which security measures will be implemented. Moreover, the public nature of the database is a cause of concern as the public availability of statement of reasons could lead to reverse engineering or abuse by adversarial actors.

**Compliance deadline** - The Commission is expecting a very quick turnaround from the end of discussion/feedback period to the compliance start date. Compliance deadline should be extended to allow companies to prepare internally for implementation, while devoting enough time to testing and working in close collaboration with the Commission to fine tune the database and submission process.

**Database Availability** - At this stage the Commission has given no guidance to operators on what to do if the API becomes unavailable and the database accessibility is compromised. Precise instructions should be issued to help companies deal with possible problems of the system.

**Audit process** - At this stage it is not clear how independent audit should examine/assess the obligation under art. 24. Additional guidance should be produced on this.

**Operational aspects** - The documentation made available by the EC fails to address a number of important points which are critical to effectively operationalize art. 24, namely:

- Batch API - There is no batch API support (batch writing)
- Processing time for database submissions - There are interim and downstream processes associated with abuse detection and enforcement. Not having time to fully process and audit statements compromises the accuracy of data reporting and could force platforms to take premature actions. This in turn could cause bad user experience or exposure to abuse while these processes are completed. Platforms should be able to establish the most appropriate cadence of submissions by taking into account their internal processes and
12. Would you prefer other submission method?

- Web Form
- File upload in a specified format
- Other

Please specify:

No, we agree API is the best submission method.

13. What kind of improvements would you suggest to the API?

We would recommend the following:
- Improve the authorization and security protocols for API access
- Switch to Batch API, or a specific standardized aggregated report
- Let platforms determine the cadence of submissions (i.e. once per month) that works best given their internal operations and constraints, while at the same time introduce a maximum delay (for instance, no later than 3 months). Flexibility in establishing cadence of submissions is important to allow companies resolve cases with better certainty. From Snap’s perspective, once a month would be an appropriate cadence.
- Consult with platforms to define the structure and fields of the API and establish which ones should be mandatory (vs. not required)
- Provide more time for platforms to comply - ideally 3 additional months
- Provide the ability to update and delete a statement of reason
- Provide guidance on how to handle data deletion requests

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
Please specify

Not applicable - but essentially the same concerns expressed in our answer to question 11.

16. Would you prefer other submission method?
   - [ ] API (Sending Statements of Reason Individually)
   - [x] 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?

   N/A

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)
   - [x] API (sending statements of reasons in batches)
   - [ ] File upload in a specified format
   - [ ] Other

19. Please explain your suggestion

   API in batches and non-real time submission or in a specific aggregated format (like a transparency report).

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)
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

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

☐ Yes
☐ No

Why?

Yes, there should be limitations. Especially in the first months, as companies start to integrate the new tool, there is a high risk that the system isn’t working as intended. Overall, safeguards should be put in place to prevent bad actors from abusing the reporting flows (e.g. spamming the tool).

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?

Snap believes that URL links should not be included as they could potentially expose personal data (see also response to question 11). Snap only hosts content for a short period of time and therefore there is no value in providing a URL because no moderated content will be accessible by the time researchers are seeking to access the information due to moderation, user deletion or natural expiry of our short retention period. Additionally, free text fields should be used as little as possible to limit any risk of inclusion of personal data.
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

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.

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) 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) 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. 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