CONSULTATION ON DIGITAL SERVICES ACT'S TRANSPARENCY DATABASE

CCIA Europe's additional comments

July 2023

The Computer & Communications Industry Association (CCIA Europe) appreciates the possibility to contribute to the European Commission's work to ensure the Digital Services Act (DSA) is appropriately implemented.[1] The questionnaire, content, and structure of the Application Programming Interface (API) constituting the DSA Transparency Database provide a useful starting point for providers of online platforms to comply with Articles 17(1) and 24(5) of the DSA. Article 17 describes the content of the statements of reasons (SORs) the providers should send to their recipients about restrictions relating to their content. The consultation looks at how providers should practically submit these SORs to the Commission, pursuant to Article 24. The Association would like to offer the following additional comments to the European Commission with a view to ensuring a successful rollout of the database.

Timeline of database rollout

Designated very large online platforms (VLOPs) will have to start using the API on 28 August 2023. At best, the final API will be published a month before VLOPs have to fully comply with the DSA. Given that improvements are necessary to make sure the API is both functional and aligned with the DSA, we encourage the Commission to give an express grace period to providers in order to ensure their technical systems are ready to submit their SORs and decisions to the database. Greater flexibility in making submissions to the database for a given period of time would allow providers to appropriately comply with Articles 17(1) and 24(5) of the DSA.

Alignment of the database with the DSA

The API under consultation goes *de facto* beyond the requirements in Article 17 of the DSA, by listing specifications that are not mentioned in the text of Article 17. These new requirements create technical challenges and complexities for online platforms. Because providers of online platforms have been preparing their systems and services to comply with the DSA based on the requirements of Article 17. This will be especially impactful for VLOPs that have an imminent deadline for compliance. The final API should only contain mandatory fields that are clearly aligned with the DSA. This first version should accommodate the need for VLOPs to comply with their obligations under the DSA quickly, without preventing new versions of the API (preferably after meaningful consultation with providers).

Validation protocol of SORs

As it stands, the API requires that all data fields be entered to accept the submission of SORs to the database. This is not workable. Many data fields raise questions regarding their legal validity, and technical and operational feasibility, as detailed in our response to the questionnaire and in the Annex. Overall, more flexibility in the submission process would help providers of online platforms to adapt to the API, and at the very least the data fields

[1] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065&qid=1666857517641

that are not based on the text of the DSA should be optional. This flexibility could be further ensured by allowing corrections to submissions and removing mandatory fields.

Database access and purpose

While Article 24(5) states that the database should be publicly accessible, some type of access control would be necessary to ensure the security and privacy of the information in the database. For example, while still publicly accessible, the Lumen database provides different access rights for researchers and non-researchers. Similar access restrictions here could still support good faith research efforts while mitigating concerns around abuse by malicious actors.

Related to access is the question of the purpose of the database. While the database will most likely be a useful tool for enforcers and researchers, it should be noted that conclusions purely based on it will not necessarily accurately reflect the prevalence of violations on online platforms. For example, the data included in transparency reports will arguably be more reliable as it allows sufficient time for data verification and will account for the full life cycle of content moderation (e.g. possible appeals and reinstatements).

Clarifications regarding submitting SORs "without undue delay"

Article 24(5) mentions that providers should submit SORs and decisions to the European Commission "without undue delay". Question 20 asks what the delay (from immediately to a week) should be. Providers will need time to conduct verification, such as data anonymisation, refinement, and processing, before submitting to the database. Therefore, providers might need up to a week of delay, but the upload would probably be batched, given the expected high volume of submissions. In any case, the wording of the DSA does not need further specification as it will vary from one provider to another and will need to be adapted over time.

Privacy safeguards

SORs sent to recipients may contain personal data, which is why Article 24(5) of the DSA requires that the SORs submitted to the European Commission should not include such information. To do so, the European Commission should set the standards for the API to contain privacy-by-design measures to avoid the inclusion of information that directly or indirectly allow the identification of a natural person. As the data controller of any personal data that could be contained in the database, the Commission should set the necessary anonymisation (including via aggregation and data minimisation) standards.

Communication between Commission and providers

An aspect the consultation fails to address is the need for communication between the European Commission and providers throughout the rollout and operational phase of the database, especially with the potential difficulties caused by very high numbers of submissions. Several elements are needed so that the transmission tools of the providers can work. To remedy this, the Commission could put in place a point of contact for the database (e.g. regarding maintenance, outages, or any other technical issues). A protocol for handling such outages, for both the Commission and providers, would also be beneficial. Further coordination on how the database will scale over time would also help prevent technical issues.

Annex: API requirements go beyond the DSA

As it stands, the information required to complete a submission in the database goes beyond Article 17 of the DSA which describes the content of the statements of reasons. Providers of online platforms prepared their systems to comply with the DSA and have anticipated the requirements of Article 17. The API needs to align with these requirements. Therefore, several changes, clarifications or removal are required:

- **CONTENT_TYPE**: The three categories (text, video, and image) proposed in the API do not reflect some of the most frequent possibilities, such as "audio" and combinations of several categories (e.g. video/text is very common). Further categories and flexibility to select several categories are needed.

- **URL:** The API currently requires the URL to the data that has been moderated. This would pose three immediate issues: (1) as described above, URLs are not required to be included in SORs under the DSA; (2) the URL may have disappeared or changed by the time of submission after deletion, suspension or restriction; or (3) URLs could contain personal data (e.g. user name) or allow for the (re)identification of users (as previously explained). URLs should not be required for, and included in, the database.

- **SOURCE_TYPE**: The API currently offers three possibilities, which are trusted flagger, own voluntary initiative and notice under DSA Article 16. This goes beyond the requirements of Article 17(3)(b) of the DSA, which requires only that a SOR indicate whether the decision was taken pursuant to a notice under Article 16 or based on a voluntary own-initiative investigation. It should also be noted that the current categories only account for EU residents and lack the possibility for them to be the subject of notices by non-EU users. Another category should be added for this situation, as it is required to report them to the database.

- **SOURCE**: Clarifications are needed on what the API requires when it comes to the source of the notification. Article 17(3)(b) mentions the need to contain the identity of the notifier "where strictly necessary", so this should not be a mandatory field. Besides, if the European Commission expects a high level of detail (e.g. name of notifiers), this would contradict data protection and privacy laws, and would not be in line with the very text of Article 24 of the DSA. Finally, the determination of the source type for each decision is not always definitive, as decisions can have multiple sources that may not clearly map out the origin of the decision.

- **START_DATE**: The date the decision took place in YYYY-MM-DD format is sufficient. We note that the HH:MM:SS element of this field is optional; however, removing from the API the need to declare the precise time is necessary as it could undermine the privacy of recipients and the security of systems.

- **END_DATE**: Depending on the content moderation decision, the end date varies (e.g. content can be taken down permanently, whereas an account can be suspended for three days). This field should be deleted or adapted to accommodate these different situations, listed in Article 17(1) of the DSA (i.e. visibility, monetisation, service provision, and account). As with START_DATE, the date the decision took place in YYYY-MM-DD format is sufficient.

- **DECISION_GROUND**: The API requires providers of online platforms to declare whether the decision was taken based on the illegality of the content or its incompatibility with terms and conditions (T&Cs). In practice, it would be difficult to systematically provide that information, as online platforms may not always differentiate content moderation decisions based on T&Cs, the law or both, and in many cases, T&Cs may be broader and stricter than what would be reflected in local law. For example, some platforms may take decisions based on patterns of conduct over time (e.g. harassment).

- **INCOMPATIBLE_CONTENT_ILLEGAL**: The API requires that providers of online platforms indicate whether the content removed was not only incompatible with T&Cs, but was also illegal. The DSA does not require that platforms analyse both legality and incompatibility with T&Cs before taking action. In practice, providers do not always conduct an analysis of both legality and incompatibility with T&Cs for each piece of content. For example, for some platforms, incompatibility with T&Cs results in a global removal, and therefore no analysis of legality is then conducted because no additional remedy exists. This field should either not be required to be submitted in the database or an additional category of "unconfirmed" should be added.

- **DECISION_PROVISION**: Further clarification is needed as the categories could overlap, between the suspension/termination of an account and a service.

- **CATEGORY**: The API *de facto* creates a list of categories to classify each SOR: piracy, discrimination, counterfeit, fraud, terrorism, child safety, non-consent, misinformation, terms of services (TOS) violation, and uncategorised. Articles 17 and 24 of the DSA have not established such a list (whereas Article 17 *does* set out a number of categories to classify other elements of each SOR). Besides, the industry has not been consulted to create such standards. Imposing this categorisation is not supported by the text of the DSA, and would require providers of online platforms to make substantial changes to their systems (in some cases, requiring those systems to be rebuilt entirely), in a short period of time. Further consultation is needed because the categories are not necessarily the right ones for all services, and ignore the fact that content may be part of multiple categories. For now, more flexibility in the categorisation of SORs would be welcomed.

- **Text-based fields** (DECISION_FACTS, ILLEGAL_CONTENT_EXPLANATION, INCOMPATIBLE_CONTENT_EXPLANATION): This would be challenging to implement at scale and would be unlikely to result in any benefits in terms of transparency, given required privacy safeguards. These fields should be removed.

About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policy making since 2009. CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.

For more information, visit: twitter.com/CCIAeurope or www.ccianet.org

For more information, please contact:

CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org