Contribution ID: dbf156b6-c805-457a-9302-2a515d1379ef
Date: 09/01/2026 11:28:18

Targeted consultation Article 18 DSA

Fields marked with * are mandatory.

Introduction

The European Commission requests your input on the following questions regarding the obligations of providers of hosting services (HSPs) under Article 18 of the Digital Services Act (DSA). Under this article, HSPs are obliged to notify law enforcement authorities (LEAs) or judicial authorities about suspicions of criminal offences involving a threat to the life or safety of a person or persons when they become aware of such information. The article remains open for interpretation in certain areas, such as regarding the criminal offences considered in scope under national law and which elements of information must be provided to the authorities.

The targeted consultation therefore has multiple **objectives**:

- To obtain feedback on the functioning of the notification process to identify the areas that warrant further clarification;
- To gather good practices concerning the processing of notifications and the identification of the Member State(s) concerned whose authorities should receive the notifications;
- To identify the criminal offences considered in scope of the article under national law and practical examples of such offences.

This information gathering exercise is part of an effort to ensure the consistent application of the provision across the Member States and to help the Digital Services Coordinators (DSCs) to supervise compliance, including by facilitating regular reporting on the notifications received. This should take into account good practices undertaken by DSCs, LEAs, and HSPs.

Contributions are sought from HSPs, DSCs, LEAs and judicial authorities receiving notifications, researchers and experts in the field, civil society organisations, trusted flaggers and internet hotlines, among others.

Where possible, respondents are encouraged to provide supporting evidence in their responses to justify and substantiate their reasoning.

For details on how we process your personal information, see the privacy statement.

Please note that your contribution to the targeted consultation will not be published. It will be used to prepare a summary report that outlines the overall findings. Any personal information will be anonymised before the final report is made public.

About you

* **Response submitted as** (please select):

Business association

* **Please specify and provide a short description of your experience with Article 18 DSA:**

BSA's members are 'hosting service providers' under the DSA and therefore are targeted by the requirements of Art. 18

* **Country of origin** (please add your country of origin or that of your organisation)

BE - Belgium

* **Email address** (please provide a contact point for follow-up questions)

hadrienv@bsa.org

Questions

1. Which aspects of the notification obligation under Article 18 DSA would benefit from further guidance?

Further guidance would be particularly valuable with respect to the scope of offenses covered by Article 18, in order to ensure a proportionate and legally certain application of the notification obligation.

In this regard, such an open-ended definition of “criminal offense” puts the burden on companies to become knowledgeable of criminal law in all 27 EU member states (given that the scope is where the harm may have occurred). As such, a definition of criminal offense should be provided that covers the most egregious and relevant offense that would arise under the DSA.

Moreover, explicit clarification or exclusion concerning child sexual abuse material (CSAM) would be important, especially in circumstances where there is no information indicating the location of a victim or whether there is an imminent risk of harm to the victim(s). Also, while categories like CSAM have standardized definitions, other terms such as "extremism" or "harmful content" remain highly subjective. Without a clear definition, providers are forced to make determinations that vary by jurisdiction and local Member State laws, leading to inconsistent enforcement and potential over-reporting.

In addition, the concept of “threat of harm” would benefit from clearer temporal parameters. Article 18 refers to situations where a threat of harm is likely to, will, or has already taken place. It remains unclear whether this obligation is intended to apply where the underlying harm occurred several months ago or longer in the past. Clear temporal boundaries are necessary to ensure foreseeability of obligations, prevent over-reporting, and uphold the principle of proportionality.

Further guidance is needed on the definition of an “appropriate authority” for the purposes of Article 18, including which authorities should be notified in cross-border or jurisdictionally ambiguous situations. Clear designation of competent authorities would enhance legal certainty and reduce the risk of inconsistent or duplicative reporting and reduce administrative burden.

Additionally, clarification is needed on what exactly “giving rise to a suspicion” and “becoming aware” mean so that it is clear when the notification obligation is triggered.

The language should also clarify whether the article imposes a duty of active monitoring or is triggered only by actual knowledge. If the article requires providers to proactively scan all hosted content, it would necessitate a significant technical and privacy shift.

2. Can you provide any good practices or recommendations concerning notifications under Article 18 DSA? Please refer to any existing documentation, statistics, or resources that underpin or validate the good practices or recommendations proposed. Such good practices or recommendations may concern:

- The process of sending of notifications by providers of hosting services to the law enforcement or judicial authorities;

- How providers of hosting services become aware of information that may give rise to a suspicion of criminal offences in scope of Article 18 DSA (e.g., through third-party notices and/or own-initiative investigations);

- The assessment of third-party notices, including notices submitted in accordance with Article 16 DSA, to determine whether they give rise to a suspicion of the type of criminal offence in scope of Article 18 DSA.

You may upload relevant documentation.

Please upload your file(s)

3. Can you provide any practical examples for the following aspect(s) concerning the receipt and processing of notifications under Article 18 DSA? In your responses, please ensure that any examples you wish to submit are anonymised, meaning without any indication of personal data of victims, perpetrators, or others.

You may upload relevant documentation.

Please upload your file(s) and ensure that any personal data included in the file(s) blurred.

3.a the criminal offences involving a threat to the life or safety of a person or persons

3.b the type (e.g., text, image, video, audio, etc.) and content of information giving rise to a suspicion of a criminal offence

4. What kind of limitations do providers of hosting services face in identifying content, sending notifications and providing all relevant information available under Article 18 DSA? Please indicate any limitations you are aware of, such as legal, technological or other limitations.

Providers of hosting services face significant practical and legal limitations when identifying content and determining whether the threshold for notification under Article 18 is met. These services generally rely on automated detection tools and user reports, which may flag large volumes of content without providing sufficient contextual information to assess the nature, timing, location, or severity of an alleged offense.

Providers might lack access to key information necessary to evaluate jurisdiction, identify affected individuals, or determine whether a genuine and imminent threat to life or safety exists. Providers may also be subject to laws that prohibit the sharing of certain personal data, such as is the case for US-based providers who may be restricted from sharing any CSAM information to non-US authorities.

Additionally, the obligation to notify authorities “without undue delay” may be challenging to operationalize where further internal assessment is required to avoid over-reporting, misreporting, or duplicative notifications across multiple Member States. These limitations highlight the importance of clear, proportionate guidance that takes into account the technical, legal, and operational realities faced by hosting service providers.

5. If available, please provide information and any potential good practices concerning the identification of the Member State concerned as defined in Article 18(2) DSA, whose authorities should receive the notification.

6. If available, please provide any further information or feedback that you believe would be relevant to this consultation, which has not been previously addressed.

Contact

CNECT-DSA-BOARD-WG7@ec.europa.eu