



Notice to Members

Compliance with the Digital Services Act

The **Digital Services Act** ([Regulation \(EU\) 2022/2065](#), "DSA") is a regulation, i.e. directly applicable in Member States, which updates the rules of the 2000 Electronic Commerce Directive. More particularly, it deals with the liability and content moderation regimes of intermediary services¹ with a particular focus on illegal and harmful activities and user rights.

As of **17 February 2024**, the DSA rules apply to all intermediary services, including online platforms².

If your organisation is **providing an online platform**, such as a MediaWiki installation or a cloud service allowing users to share content, you are likely to be covered by the new set of unified rules. An example would be [WMAT's members wiki](#) on their own website.

If you **use an online platform** that is hosted on Wikimedia Foundation servers, such as the [Wikimedia Belgium wiki](#), then the Wikimedia Foundation is the legal host and responsible for compliance.

If you are **offering an email service**, this qualifies as a hosting service under the DSA. You should enjoy continued protections and little to nothing should change. The DSA preserves the liability regime established in the e-Commerce Directive by Articles 12 to 15, replacing them with Articles 4, 5, 6 and 8. We still recommend you to double-check with a lawyer.

Obligations for providers of online platforms:

If your organisation operates an online platform or another intermediary service that allows users to upload and share content, you should check with a lawyer in your country if an update of your terms of service and your processes is necessary.

The **main obligations** under the DSA include:

¹ See Article 3 letter (g) for the definition of intermediary service and recital 29 of DSA for an illustrative list of economic activities qualifying as intermediary services.

² According to Article 3, letter (f): "online platform" means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation".

- Having a **point of contact** for authorities & users. [Articles 11 and 12]
- Having intelligible **terms of services** that explain any restrictions and content moderation practices by the service provider (i.e. the chapter in your case). [Article 14]
- **Transparency reporting:** You need to publish an annual report covering any content moderation done by the service provider (i.e. the chapter). [Article 15]
- **Notice and Action Mechanism:** You need to offer users an easy way to signal illegal content or activities to you. [Article 16]
- **Statement of reasons:** When you, as a service provider, delete or restrict content, you must provide understandable reasons for doing so to any involved parties (e.g. uploader & notifier). Same goes for restricting or deleting user accounts. [Article 17]
- **Internal complaint handling:** You need to offer an easy way for users to contest your content moderation decisions. You must have an internal process that allows you to double-check your decision in such a case. [Article 20]
- **Out-of-court:** If the user is unhappy with your internal complaint handling, they may go to an out-of-court dispute settlement body designated by the national regulator in your country. You are obliged to participate in this process. This does not preclude the right of the user to go to a regular court of law. [Article 21]
- **Notification of suspected criminal offences:** If you suspect a criminal offence involving a threat to the life or safety of a person or persons, you are under a legal obligation to promptly inform the law enforcement or judicial authorities. [Article 18]
- **Trusted Flaggers:** The national regulator responsible for the DSA in your country will categorise some organisations as “trusted flaggers”. Ideally, these will be organisations with expertise in identifying illegal content or behaviour. You are obliged to provide a contact point to them that guarantees their notices are treated with priority (e.g. a dedicated email address). People or organisations who frequently submit manifestly unfounded complaints can be suspended by the service provider. [Article 22 and 23]
- **Protection of minors:** If minors can access the platforms, there should be measures ensuring a high level of protection of privacy, security and safety in place. [Article 28]

You may already be compliant with some of the obligations, as they are not new. Others will require tweaks to the information you provide or to your internal organisation.

For additional information and questions, please drop us a message:

dimi@wikimedia.be

michele.failla@wikimedia-europe.eu