

EP Adopted Position on Digital Services Act



Anna Pinggen

News

On 20 January 2022, the European Parliament **adopted** its position regarding the proposal for a **regulation on a Single Market For Digital Services (Digital Services Act)**. The EP amended several dispositions of the Commission proposal (→ [eucrim 4/2020, 273](#)). The DSA primarily concerns online intermediaries and platforms (e.g. online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms). The aim is to create a safer digital space in which the fundamental rights of users are protected.

In order to achieve the objective of ensuring a safe and trusted online environment, the concept of “illegal content” should be understood broadly - it should underpin the general idea that what is illegal offline should also be illegal online.

Among the major amendments by the EP:

- In order to assist Member States and service providers, the Commission should provide guidelines that clarify any potential conflicts between the conditions and obligations laid down in legal acts (referred to in this Regulation), explaining which legal act should prevail;
- Providers of intermediary services should make efforts to ensure that, where automated tools are used for content moderation, the technology can be sufficiently relied on to limit (to the maximum extent possible) the rate of error, namely when information is wrongly considered to be illegal content;
- Member States should not prevent providers of intermediary services from providing end-to-end encrypted services;
- In accordance with the principle of data minimisation and in order to prevent unauthorised disclosure, identity theft, and other forms of abuse of personal data, Member States should not impose a general obligation on providers of intermediary services to limit the anonymous use of their services;
- Member States should ensure full implementation of the Union's legal framework on confidentiality of communications and online privacy as well as on the protection of natural persons with regard to the processing of personal data enshrined in Directive (EU) 2016/680;
- Providers of intermediary services should also be required to designate a single point of contact for recipients of services, which allows rapid, direct, and efficient communication - in particular by easily accessible means using telephone numbers, email addresses, electronic contact forms, chatbots, and instant messaging;
- Online platforms should ensure that recipients can understand how recommender systems impact the way information is displayed and how this can influence how information is presented. They should clearly indicate the parameters for such recommender systems in an easily comprehensible manner in order to ensure that the recipients understand how information is prioritised for them;

AUTHOR

Anna Pinggen 

Researcher
Max Planck Institute for the
Study of Crime, Security and
Law

ISSN: 1862-6947

<https://eucrim.eu>



- Online platforms should not use personal data for commercial purposes related to direct marketing, profiling, and behaviourally targeted advertising of minors. Targeting individuals on the basis of special categories of data, especially targeting vulnerable groups, should not be permitted;
 - The Commission should ensure that it is independent and impartial in its decision-making with regard to both digital services coordinators and providers of services defined in this Regulation.
 - The Commission should carry out a general evaluation of the DSA Regulation and submit a report to the European Parliament, the Council, and the European Economic and Social Committee.
-

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and “criministrative” law.

All news items are freely accessible at: <https://eucrim.eu/news/>

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.

The project is co-financed by the **Union Anti-Fraud Programme (UAFP)**, managed by the **European Anti-Fraud Office (OLAF)**.



**Co-funded by
the European Union**