Use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online (temporary derogation from certain provisions of Directive 2002/58/EC)

2020/0259(COD) - 06/07/2021 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 537 votes to 133, with 24 abstentions, a resolution on the proposal for a regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards as the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online.

The European Parliament's position adopted at first reading under the ordinary legislative procedure amends the Commission's proposal as follows:

Purpose and scope

This Regulation lays down **temporary and strictly limited rules** derogating from certain obligations laid down in Directive 2002/58/EC which protect the confidentiality of communications and traffic data, with the sole objective of enabling providers of certain number-independent interpersonal communications services to use specific technologies for the processing of personal and other data to the extent strictly necessary to detect online child sexual abuse on their services and report it and to remove online child sexual abuse material from their services.

This Regulation should not apply to the scanning of audio communications.

Data processing by service providers

The types of technologies used should be the least privacy-intrusive in accordance with the state of the art in the industry. Those technologies should not be used to systematically filter and scan text in communications unless it is solely to detect patterns which point to possible concrete reasons for suspecting online child sexual abuse, and they should not be able to deduce the substance of the content of the communications.

In the case of technology used for identifying **solicitation of children**, such concrete reasons for suspicion should be based on objectively identified risk factors such as age difference and the likely involvement of a child in the scanned communication.

For any specific technology used for the purposes of the Regulation, the provider should be required to have first carried out a data protection **impact assessment** and consultation in accordance with the General Data Protection Regulation (GDPR).

Obligations of service providers

Service providers should (i) establish internal procedures to prevent misuse of personal data; (ii) ensure human oversight of data processing and; (iii) established appropriate procedures and **redress mechanisms** to ensure that users can lodge complaints with them within a reasonable timeframe for the purpose of presenting their views.

Service providers should inform users in a clear, prominent and comprehensible way that they have invoked the exemption provided for in the Regulation. They should also inform users of (i) the remedies available to them; (ii) the possibility of lodging a complaint with a supervisory authority; and (iii) the right to judicial redress where their content has been removed or their account has been blocked.

Data storage and retention

Where a suspected case of online child sexual abuse has been identified, the content data and associated traffic data processed, as well as the personal data generated by such processing, shall be **stored in a secure manner**.

The period during which data is subsequently stored in the event of the identification of suspected cases of online child sexual abuse should be limited to that which is strictly necessary to carry out these activities.

Any data should be immediately and permanently deleted as soon as they are no longer strictly necessary for one of the purposes specified in this Regulation.

Transparency and accountability

Providers should publish **reports** and submit them to the competent supervisory authority and the Commission, no later than six months after the date of entry into force of the Regulation, and no later than 31 January of each year thereafter.

These reports should cover, inter alia, the processing falling within the scope of the Regulation, including the type and volumes of data processed, the specific grounds for processing personal data under the GDPR, the grounds for transfers of personal data outside the EU and the number of identified cases of online child sexual abuse.

Guidelines

In order to support supervisory authorities with their tasks, the Commission should request the European Data Protection Board to issue guidelines on the compliance with the GDPR in the context of processing falling within the scope of the Regulation's derogation.

Public list

Providers will have to notify the Commission of the **names of organisations acting in the public interest** against child sexual abuse to which they report online child sexual abuse under the Regulation. The Commission will make the list public and keep it up to date.

Statistics

No later than one year after the date of entry into force of the Regulation, and thereafter on an annual basis, Member States will be required to make publicly available and submit to the Commission reports including statistics on (i) the total number of reports of online child sexual abuse that have been forwarded

to the competent national law enforcement authorities; (ii) the number of children identified as a result of measures taken under the Regulation, differentiated by gender; and (iii) the number of perpetrators convicted.