

Temporary derogation from certain provisions of the ePrivacy Directive to combat online child sexual abuse

2025/0429(COD) - 28/07/2026 - Final act

Regulation (EU) 2026/1881 establishes a temporary and strictly limited derogation from the confidentiality of communications and traffic-data rules in Directive 2002/58/EC. It enables providers of number-independent interpersonal communications services, such as certain messaging and webmail services, to voluntarily use specified technologies to detect, report and remove online child sexual abuse material, and to detect and report the solicitation of children, pending a long-term EU framework.

Scope of the Derogation

The Regulation permits processing of personal and other data only where strictly necessary to:

- detect and remove online child sexual abuse material and report it to law-enforcement authorities and organisations acting in the public interest against online child sexual abuse;
- detect the solicitation of children and report it to those authorities or organisations.

The derogation applies to content data and related traffic data. It does not apply to audio communications or to communications protected by end-to-end encryption, whether encryption is currently, previously or subsequently applied. The Regulation must not be interpreted as prohibiting or weakening end-to-end encryption.

The Regulation does not itself provide a legal basis for processing personal data. Processing remains subject to Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR), where it falls within the scope of the derogation.

Conditions and Safeguards

Providers may rely on the derogation only if the technologies used are state of the art, the least intrusive for privacy, and comply with data protection by design and by default. Technologies used to scan text must only identify patterns suggesting possible online child sexual abuse and must not deduce the substance of communications.

Technologies must minimise false positives as far as possible and allow errors to be corrected without delay. Systems used to detect possible solicitation of children must rely on relevant indicators and objectively identified risk factors, such as an age difference and the likely involvement of a child in the communication.

Providers must carry out a data protection impact assessment and a prior consultation with the competent supervisory authority for each technology. Transitional exemptions until 1 April 2027 apply to certain providers already using relevant technologies before 31 July 2026, provided that they begin the required procedure by 1 September 2026 and cooperate properly with the supervisory authority.

Providers must establish safeguards against unauthorised access, transfers and misuse of data, ensure human oversight and, where needed, human intervention. Material not previously identified as online child sexual abuse material or solicitation of children cannot be reported without prior human confirmation.

Providers must clearly inform users that they rely on the derogation, explain the logic and effect of their measures on communications confidentiality, and indicate that personal data may be shared with law-enforcement authorities or relevant public-interest organisations. Where content is removed, an account is blocked or a service is suspended, users must be informed of available redress, the possibility of complaining to a supervisory authority and their right to a judicial remedy.

Reporting, Retention and Supervision

Cases giving rise to a reasoned and verified suspicion must be reported without delay. Data relating to suspected online child sexual abuse may be stored securely only for specified purposes, including reporting, account or service measures, creating a non-reversible digital signature, enabling redress, and responding to lawful requests from law-enforcement or judicial authorities. Data must be deleted when no longer necessary and, in any event, no later than 12 months after the suspected abuse was identified.

By 1 February 2027, and annually by 31 January thereafter, providers must publish and submit reports to the competent supervisory authority and the European Commission. These reports must cover, among other matters, the data processed, legal grounds under the GDPR, transfers outside the European Union (EU), identified cases, complaints, false-positive rates, retention policies, safeguards and organisations with which data were shared. The Commission must establish a standard reporting form by 1 November 2026.

The Commission must request European Data Protection Board guidelines by 1 September 2026 to support supervisory authorities in assessing compliance with the GDPR. Providers must also submit by that date the names of public-interest organisations to which they report cases. The Commission must publish and update this list from 1 October 2026.

Member States must publish and submit annual statistics from 1 August 2027 on reports received by national law-enforcement authorities, children identified and perpetrators convicted. The Commission must report on implementation to the European Parliament and the Council by 1 February 2028, including the proportionality of the derogation and technological developments affecting accuracy and false-positive rates.

Procedure and Application

The Regulation was adopted following European Parliament positions of 26 March and 9 July 2026, and Council positions and decisions of 2 and 22 July 2026. It was adopted on 24 July 2026.

It entered into force on 31 July 2026, the third day following its publication in the Official Journal of the European Union on 28 July 2026. It applies until 3 April 2028 and is binding in its entirety and directly applicable in all Member States.

This summary was AI-generated and human-reviewed.