EU regulation facilitates cross-border criminal investigations

E-Evidence on the horizon

Have you heard of the EU's E-Evidence Regulation? If not, it is time to find out more, as it could affect professionals bound by confidentiality obligations, including doctors, dentists and psychotherapists. The regulation aims to streamline the way criminal prosecution authorities in Europe obtain access to digital evidence, such as e-mails, chat logs or stored data on servers, in order to improve the investigation of serious crimes, including terrorism and cybercrime. However, there is also an ongoing debate about data protection and the rights of those affected.

© Peter Maszlen – stock.adobe.com

Regulation (EU) 2023/1543 of the European Parliament and of the Council on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings—known as the E-Evidence Regulation (EEVR)—has been in force since 2023. So far, it has largely escaped the attention of professionals bound by confidentiality obligations, such as physicians, dentists or psychotherapists. In June, the German Federal Government published its draft legislation for transposing the regulation into national law. The three-year transitional period granted to member states will expire in August 2026. After that date, the regulation will be binding across the EU.

Background

The E-Evidence Regulation is a significant step towards modernising criminal prosecutions across the European Union. By simplifying and accelerating access to digital evidence, it aims to improve the

effectiveness of investigations while safeguarding the rights of individuals, according to its authors.

Under the regulation, law enforcement authorities in one member state can request information directly from service providers based in another member state without the involvement of the judicial authorities in the requested country. This applies to all types of electronic evidence, including subscriber data, traffic data and content data.

The European Production Order, introduced by the regulation, enables the direct request and retrieval of digital evidence from service providers. Providers must make the requested data available within ten days, or within eight hours in an emergency. Additionally, a European Preservation Order ensures that data can be secured for later retrieval, even before a production order is issued.

Although the official purpose is to streamline justice, some of the regulation's provisions read like something straight out of Orwell's *1984*. Authorities in other EU member states can compel electronic service providers to release data directly, without the knowledge or approval of domestic judicial bodies. This could include data stored in electronic patient records (EPRs), practice management software or cloud services. In other words: highly sensitive patient data, protected by medical confidentiality, could be disclosed to foreign investigative authorities.

Implementation into national law: the German example

In June 2025, the German Federal Government presented a draft bill designed to transpose the E-Evidence Regulation into national legislation in a legally sound manner. The stated objective was to strike a fair balance between efficient criminal prosecution and the protection of fundamental rights. The draft explicitly emphasises the need for careful handling of data relating to professional confidentiality, such as information held by doctors, lawyers and other professional groups bound by secrecy obligations.

According to the proposal, such sensitive data may only be disclosed under strict conditions, for example, only via German authorities if the person concerned resides in Germany. Furthermore, the draft provides for a notification requirement: if a production order is issued by an authority in another member state, the German authorities must be informed. German authorities may then refuse to execute the order if it breaches data protection rights or contradicts national legislation.

Are dentists affected?

Data from electronic patient records (EPRs), practice management systems and cloud services could be affected, even though the regulation, compared to the original commission proposal, provides for an "effective level of protection for data of professional secrecy holders from access by state investigative authorities".

The German Dental Association (Bundeszahnärztekammer, BZÄK) and the National Association of Statutory Health Insurance Dentists (KZBV) have expressed their concerns in a statement to the federal government: "This level of protection must also be fully and unambiguously guaranteed at national level." The protection of highly sensitive patient data, which is subject to medical confidentiality, is at stake, and this data must now be shielded from access by foreign investigative authorities.

Is medical confidentiality under threat?

The German Medical Association (Bundesärztekammer, BÄK) and the BZÄK fear that the regulation may circumvent national protective provisions such as the seizure ban (Section 97 of the German Code of Criminal Procedure, StPO), because it does not currently provide for automatic exemptions for professional secrecy holders. Furthermore, the persons or institutions affected (e.g., dental practices) are not necessarily informed when their data is disclosed. This makes it more difficult to safeguard the rights of those affected.

There is a lack of clear and comprehensive definitions as to which data fall under professional secrecy and how they are to be protected. For years, the BZÄK and the Council of European Dentists (CED) have been calling for improvements at national and European levels. At the initiative of the German Dental Association, the CED had urged the EU legislator at an early stage to uphold medical and professional confidentiality and to anchor corresponding exceptions in the proposed regulation. These include protection of the EPR and other sensitive storage locations through explicit provisions, as well as the introduction of an automatic seizure ban for confidential data. At least a partial success has been achieved, as outlined above.

Legal measures

To protect medical confidentiality from the kind of access envisaged under the E-Evidence Regulation, a combination of legal and technical-organisational safeguards are required. In terms of legislation, the German Federal Government must actively prevent the disclosure of data held by professionals bound by confidentiality obligations without judicial oversight. In particular, Section 97 of the StPO (prohibition on seizure) would need to be amended to cover electronic data stored in cloud services or digital patient records. Furthermore, affected individuals or institutions must be informed of every data request so that they can take legal action (e. g., an objection or an appeal) in due time. An independent judicial review should be mandatory before any sensitive data is released, including in cross-border requests.

Technical protection of data

Technical and organisational measures range from end-to-end encryption of sensitive data to requirements for national data storage (e. g. on German servers), and access logging to document potential abuse. Ultimately, raising awareness among those bound by professional secrecy is also essential to safeguarding confidential data.

Loss of data subject rights

Germany's Data Protection Conference (DSK), the body comprising the independent data protection supervisory authorities of the federal and state governments, has criticised the EU's E-Evidence Regulation.

Its primary concerns relate to the protection of personal data and the rule-of-law safeguards in the context of cross-border investigations. In its statement dated 12 April 2024, the DSK highlights four core areas of concern:

- Lack of judicial oversight
- Threats to fundamental rights
- Varying data protection standards across EU member states
- Lack of transparency and accountability, including an absence of robust rules for tracing data requests

Preliminary conclusion

Since the EU Commission's original draft of the E-Evidence Regulation, various changes and clarifications have been made, particularly regarding implementation and data protection. Where direct access to data is concerned, sensitive categories of data are now excluded and still require review by the authorities of the receiving member state.

However, as of 18 August 2026, telecommunications providers, internet service providers, cloud service operators, online shops, platforms, forums and other electronic services accessible to users will be required to disclose or temporarily restore certain user data upon request from law enforcement authorities in any EU member state. Failure to comply may result in fines.

AWU

Sources: Data Protection Conference (DSK), IHK, bfdi.bund.de, EUR-lex