

Die europäische Strafverfolgung wird schlagkräftiger: Gesetz zur Umsetzung des E-Evidence-Pakets der EU in Deutschland verabschiedet

Was ist zu beachten?

Einleitung

Die „**E-Evidence-Verordnung**“ der Europäischen Union (Verordnung (EU) 2023/1543¹) tritt nach einer dreijährigen Übergangszeit am **18. August 2026** verbindlich in allen EU-Mitgliedstaaten in Kraft. Sie ermöglicht Strafverfolgungsbehörden den direkten, grenzüberschreitenden Zugriff auf elektronische Beweismittel bei Diensteanbietern.

Ende Januar 2026 hat nun auch der Deutsche Bundestag das Gesetz über Europäische Herausgabe- und Sicherungsanordnungen zu elektronischen Beweismitteln² („**E-Evidence-Gesetz**“) verabschiedet. Das Gesetz dient der Umsetzung der sog. „**E-Evidence-Richtlinie**“ der Europäischen Union (Richtlinie (EU) 2023/1544³). Gemeinsam mit der E-Evidence-Verordnung wird so ein neuer Rechtsrahmen für den grenzüberschreitenden Zugriff von Ermittlungsbehörden auf elektronische Beweismittel geschaffen.

Unternehmen, die als Diensteanbieter in den Anwendungsbereich der Verordnung fallen, sollten rechtzeitig die erforderlichen technischen und organisatorischen Maßnahmen treffen. Welche Maßnahmen das sind, stellen wir im Folgenden dar.

Inhalte

- Einleitung
- Praktische Einordnung
- Regelungsgehalt der E-Evidence-Vorschriften
 - Anwendungsbereich
 - Zentrale Rechtsinstrumente
 - Pflichten der Diensteanbieter
 - Sanktionen
 - Zentrale Stelle in Deutschland
- Empfohlene Maßnahmen

Praktische Einordnung

Ab dem 18. August 2026 können Ermittlungsbehörden innerhalb der EU elektronische Beweismittel direkt bei Diensteanbietern in anderen EU-Mitgliedstaaten anfordern.

Hierdurch wird das bisherige, langwierige Rechtshilfeverfahren über Regierungsstellen ersetzt. Bislang gilt: Erhalten Diensteanbietern Auskunftersuchen von Ermittlungsbehörden im EU-Ausland auf direktem Weg – bspw. per Post oder E-Mail – und ohne Einbindung der heimischen Behörden, können sie die Beantwortung des Auskunftersuchens verweigern. Unter datenschutzrechtlichen Gesichtspunkten konnte eine Verweigerung der Mitwirkung sogar angezeigt sein.

Mit Inkrafttreten der E-Evidence-Regelungen können die Ermittlungsbehörden künftig Telekommunikations- und Internetunternehmen im EU-Ausland unmittelbar verpflichten, elektronische Daten zu sichern und herauszugeben. Dazu gehören Teilnehmerdaten, Verkehrsdaten sowie Inhaltsdaten.

Ziel der neuen Regelungen ist nicht zuletzt eine effektivere Bekämpfung der Cyberkriminalität.

¹ Abrufbar unter: <https://eur-lex.europa.eu/eli/reg/2023/1543/oj/deu>.

² Bundestag Drucksache 21/3904, abrufbar unter: <https://dserver.bundestag.de/btd/21/039/2103904.pdf>.

³ Abrufbar unter: <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32023L1544>.

Regelungsgehalt der E-Evidence-Vorschriften

Anwendungsbereich

Die E-Evidence-Verordnung richtet sich an **Diensteanbieter** im Sinne des Art. 3 Abs. 1 Nr. 3 der Verordnung. Darunter fallen sowohl Anbieter elektronischer Kommunikationsdienste – wie Internet-Telefonie, Sofortnachrichten und E-Mail-Dienste – als auch Anbieter von Diensten der Informationsgesellschaft, sofern sie eine Kommunikation zwischen Nutzern ermöglichen oder Daten im Auftrag ihrer Nutzer speichern oder verarbeiten – bspw. Online-Marktplätze, Plattformen für Online-Spiele, Cloud-Computing und andere Hosting-Dienste.

Erfasst werden Anbieter, soweit sie die genannten Dienste innerhalb der EU anbieten (Art. 2 Abs. 1 und Art. 3 Abs. 1 Nr. 4 der Verordnung). Ein „Anbieten“ liegt vor, wenn der Anbieter die Nutzung der Dienste innerhalb der EU ermöglicht und zudem eine wesentliche Verbindung zur EU hat. Eine solche wesentliche Verbindung kann in einer EU-Niederlassung bestehen, aber auch schlicht in einer gezielten Marktbearbeitung oder einer erheblichen Anzahl von Nutzern in einem oder mehreren EU-Mitgliedstaaten.

Die Beurteilung, ob ein Dienst vom Anwendungsbereich der E-Evidence-Vorschriften erfasst ist, kann sich in der Praxis als schwierig gestalten.

Zentrale Rechtsinstrumente

Die E-Evidence-Verordnung führt zur Erleichterung grenzüberschreitender Ermittlungen zwei neue Instrumentarien ein:

- Die **Europäische Herausgabeanordnung** (*European Production Order Certificate* – EPOC) ermöglicht Ermittlungsbehörden eines EU-Mitgliedstaats, digitale Beweismittel wie Kundendaten oder Inhalte von E-Mails direkt bei Diensteanbietern in einem anderen EU-Mitgliedstaat anzufordern (Art. 10 E-Evidence-Verordnung).

In der Regel müssen Herausgabeanordnungen innerhalb von 10 Tagen befolgt werden (Art. 10 Abs. 2 E-Evidence-Verordnung) – in Notfällen sogar innerhalb von 8 Stunden (Art. 10 Abs. 4 E-Evidence-Verordnung).

- Die **Europäische Sicherungsanordnung** (*European Preservation Order Certificate* – EPOC-PR) verpflichtet Diensteanbieter zur einstweiligen Sicherung von Daten, um deren Löschung zu verhindern, bis gegebenenfalls eine Herausgabeanordnung ergeht (Art. 11 E-Evidence-Verordnung).

Die Verpflichtung ist unverzüglich zu erfüllen und besteht mindestens für 60 Tage (Art. 11 Abs. 1 E-Evidence-Verordnung).

Die E-Evidence-Verordnung enthält mehrere Anlagen mit entsprechenden Musterformularen für die Ermittlungsbehörden sowie die verpflichteten Diensteanbieter.

Pflichten der Diensteanbieter

Diensteanbieter müssen bis zum 18. August 2026 einen festen Ansprechpartner in der EU benennen, an den sich die Ermittlungsbehörden wenden können („**Adressat**“). Hierbei kann es sich um eine (von mehreren) Niederlassungen innerhalb der EU handeln. Verfügt der Anbieter über keine Niederlassung in der EU, ist er verpflichtet mindestens einen in der EU ansässigen Vertreter als Adressat zu bestellen (Art. 7 Abs. 1 der E-Evidence-Verordnung, § 3 E-Evidence-Gesetz). Soweit ein Diensteanbieter erstmalig nach dem 18. August 2026 Dienste im Sinne der E-Evidence-Verordnung in der EU anbietet, muss innerhalb von sechs Monaten ein Adressat benannt werden (§ 3 Abs. E-Evidence-Gesetz).

In Deutschland muss die schriftliche Benennung des Adressaten gegenüber dem Bundesamt für Justiz erfolgen. Mit dem benannten Adressaten muss den Behörden eine Kommunikation in deutscher Sprache möglich sein (§ 4 Abs. 4 E-Evidence-Gesetz).

Nach Erhalt einer Sicherungs- oder Herausgabeanordnung muss der Adressat die angeforderten Daten umgehend sichern und, bei einer Herausgabeanordnung, innerhalb der vorgegebenen Frist an die Ermittlungsbehörde übermitteln. Eine nicht oder nicht rechtzeitig erfolgende Datenübermittlung ist schriftlich zu begründen und grundsätzlich nur unter engen Voraussetzungen rechtlich möglich – bspw. faktische und unverschuldete Unmöglichkeit der Datenherausgabe oder Fehlerhaftigkeit der behördlichen Anordnung (Art. 10 u. Art. 11 E-Evidence-Verordnung).

Sanktionen

Für Verstöße gegen die Mitteilungs-, Sicherungs- und Herausgabepflichten der E-Evidence-Vorschriften drohen bei Diensteanbietern mit mehr als EUR 5 Millionen weltweiten Jahresumsatzes Geldbußen von bis zu 2% ihres weltweiten Jahresumsatzes (§ 18 Abs. 4 u. 5 E-Evidence-Gesetz).

Zentrale Stelle in Deutschland

Zuständig für die Überwachung der Umsetzung der E-Evidence-Verordnung ist in Deutschland das **Bundesamt für Justiz** (§ 6 E-Evidence-Gesetz).

Die technische Umsetzung der Vorschriften soll laut einer früheren Meldung des Bundesministeriums für Justiz und Verbraucherschutz die beim Justizministerium Nordrhein-Westfalen eingerichteten **E-Justiz-Koordinierungsstelle Europa (EKE)** verantworten. Geplant ist, dass eine Anbindung an die **eCodex**-Infrastruktur erfolgen soll.⁴ Hierbei handelt es sich um ein EDV-System für den grenzüberschreitenden elektronischen Datenaustausch, das Nutzern – Ermittlungsbehörden, Rechtsberatern und Unternehmen – ein elektronisches Versenden und Empfangen von behördlichen Formularen, Beweismitteln oder anderen Informationen ermöglicht.

Empfohlene Maßnahmen

Diensteanbieter sollten prüfen, ob sie bzw. welche ihrer Konzerngesellschaften dem Anwendungsbereich der E-Evidence-Vorschriften unterfallen. Ist dies der Fall, sollten jetzt die für die Erfüllung der ab dem 18. August 2026 geltenden Pflichten notwendigen organisatorischen und technischen Maßnahmen angestoßen werden. Dazu zählt:

- Welche Gesellschaft, Niederlassung oder Vertreter ist als **Adressat** im Sinne der E-Evidence-Vorschriften zu benennen? Dabei sollte berücksichtigt werden, dass gegenwärtig noch nicht alle EU-Mitgliedsstaaten nationale Durchführungsgesetze zu den E-Evidence-Vorschriften erlassen haben, sodass nationale behördliche Zuständigkeiten – etwa für die Entgegennahme der Adressaten-Mitteilung – in manchen Mitgliedsstaaten noch unklar sind – bspw. in Österreich, Frankreich oder Spanien.
- Der benannte Adressat ist mit allen erforderlichen Befugnissen auszustatten, um den behördlichen Herausgabe- und Sicherungsanordnungen innerhalb der knapp bemessenen Fristen nachkommen zu können. Das bedeutet auch, dass unternehmensintern **technische Prozesse** – einschließlich der Schnittstellen zu behördlichen Kommunikationswegen – vorzuhalten sind, die eine entsprechend kurzfristige Datenerhebung, -sicherung und -übermittlung ermöglichen. Die Mitarbeitenden sind entsprechend zu schulen und frühzeitig **klare Zuständigkeiten** festzulegen.
- Darüber hinaus ist ein standardisiertes Verfahren zur **inhaltliche Prüfung** eingehender Anordnungen einzurichten. Zwar sehen die E-Evidence-Vorschriften für den Adressaten keine Pflicht zur Vornahme einer Inhalts- bzw. Rechtmäßigkeitsprüfung vor, einer nicht hinreichend bestimmten oder mit (datenschutz-)rechtlichen Verpflichtungen des Adressaten in Drittländern unvereinbare Anordnung muss – und sollte – jedoch nicht Folge geleistet werden.

Angesichts möglicher Sanktionen von bis zu 2% des weltweiten Jahresumsatzes des Diensteanbieters und der praktischen Komplexität der Verfahren ist eine frühzeitige, strukturierte Vorbereitung auf die E-Evidence-Vorschriften aus Unternehmenssicht unerlässlich. Nur so lässt sich eine rechtskonforme, fristgerechte und technisch einwandfreie Umsetzung gewährleisten.

⁴ e-CODEX steht für *e-justice communication via online data exchange* – Kommunikation via Online-Datenaustausch im Rahmen der E-Justiz. Vgl. auch:

https://www.bmjv.de/DE/themen/digitales/digitalisierung_justiz/digitalisierungsinitiative/laendervorhaben/_doc/artikel_vorhaben_09_eevidence.html sowie <https://www.eulisa.europa.eu/activities/large-scale-it-systems/e-codex/access-points>. Bezüglich des geplanten Interfaces siehe auch: https://www.etsi.org/deliver/etsi_ts/104100_104199/104144/01.02.01_60/ts_104144v010201p.pdf.

Ihre Kontakte



Dr. Anika Schürmann, LL.M.

Partnerin | Fachanwältin für Strafrecht,
Düsseldorf

anika.schuermann@bakermckenzie.com



Dr. Lukas Greiner

Associate, Düsseldorf

lukas.greiner@bakermckenzie.com

© 2026 Baker & McKenzie. **Ownership:** This site (Site) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms, including Baker & McKenzie LLP). Use of this site does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All information on this Site is of general comment and for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulation and practice are subject to change. The information on this Site is not offered as legal or any other advice on any particular matter, whether it be legal, procedural or otherwise. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any information provided in this Site. Baker McKenzie, the editors and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents of this Site. **Attorney Advertising:** This Site may qualify as "Attorney Advertising" requiring notice in some jurisdictions. To the extent that this Site may qualify as Attorney Advertising, **PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME.** All rights reserved. The content of the Site is protected under international copyright conventions. Reproduction of the content of this Site without express written authorization is strictly prohibited.

