E-Evidence-Verordnung ab heute: Was Unternehmen jetzt beachten müssen

Seit heute, dem 18. August 2026, ist die E-Evidence-Verordnung (Verordnung (EU) 2023/1543) unmittelbar in allen EU-Mitgliedstaaten (mit Ausnahme von Dänemark) anwendbar. Strafverfolgungsbehörden aus der EU können damit elektronische Beweismittel unter bestimmten Voraussetzungen unmittelbar bei Diensteanbietern in anderen Mitgliedstaaten anfordern. Der bisher erforderliche (Um-)Weg über die Behörden des Staates, in dem sich der Diensteanbieter befindet, entfällt in diesen Fällen weitgehend. Der Speicherort der Daten ist dabei unerheblich.

Dieser Beitrag fasst die wesentlichen Folgen für Nutzer digitaler Dienste und für Diensteanbieter zusammen.

Was ändert sich gegenüber der bisherigen Rechtslage?

Elektronische Beweismittel wurden grenzüberschreitend bislang im Wesentlichen über die klassische Rechtshilfe oder die Europäische Ermittlungsanordnung (EEA) erlangt. In beiden Fällen sind die zuständigen Behörden des ersuchten bzw. vollstreckenden Staates in das Verfahren eingebunden. Die E-Evidence-Verordnung ergänzt dieses System für gespeicherte elektronische Daten um einen wesentlich direkteren Mechanismus:

	Bisher (Rechtshilfe / EEA)	**Neu (E-Evidence-VO)**
Adressat	Zuständige Behörde des ersuchten Staates	Diensteanbieter direkt (benannte Niederlassung oder Vertreter)
Einbindung des anderen Mitgliedstaats	Prüfung durch die ersuchte Behörde	Grundsätzlich keine; nur bei sensibleren Datenkategorien wird die Vollstreckungsbehörde unterrichtet und kann aus abschließend geregelten Gründen ablehnen
Dauer	Häufig mehrere Wochen bis Monate	Herausgabe grundsätzlich binnen zehn Tagen, in Notfällen binnen acht Stunden
Speicherort der Daten	Grenzüberschreitende Erlangung grundsätzlich über die zuständigen Behörden des ersuchten Staates	Direkte Anordnung an den Diensteanbieter; Speicherort der Daten unerheblich

Wie funktioniert der Zugriff? Europäische Herausgabe- und Sicherungsanordnungen

Die Verordnung schafft zwei zentrale Instrumente:

- Die **Europäische Herausgabeanordnung** wird dem Adressaten mittels einer Bescheinigung, der sogenannten EPOC (European Production Order Certificate), übermittelt. Sie verpflichtet den Diensteanbieter grundsätzlich dazu, die angeforderten Daten binnen zehn Tagen herauszugeben. In einem Notfall verkürzt sich die Frist auf acht Stunden.

- Die **Europäische Sicherungsanordnung** wird mittels einer EPOC-PR (European Preservation Order Certificate) übermittelt. Sie verpflichtet den Anbieter, bestimmte Daten grundsätzlich für 60 Tage zu sichern, damit sie nicht gelöscht werden, bevor ihre Herausgabe erwirkt werden kann. Die Sicherungsfrist kann einmalig um weitere 30 Tage verlängert werden.

Die Verordnung unterscheidet dabei nach der Sensibilität der Daten:

- **Teilnehmerdaten** (etwa Name, Anschrift, Rechnungs- und Zahlungsdaten, E-Mail-Adresse) sowie Daten, die ausschließlich der Identifizierung des Nutzers dienen (insbesondere IP-Adressen samt Zeitstempel), können grundsätzlich im Zusammenhang mit jeder Straftat angefordert werden. Eine Herausgabeanordnung für diese Daten kann auch von einem Staatsanwalt erlassen oder validiert werden.

- **Verkehrsdaten** (Metadaten der Kommunikation, etwa wer wann mit wem kommuniziert hat, Standortdaten des Geräts) und **Inhaltsdaten** (Texte, Bilder, Videos, Sprachaufzeichnungen) unterliegen strengeren Voraussetzungen: Eine Herausgabeanordnung ist grundsätzlich nur bei Straftaten zulässig, die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren bedroht sind, sowie bei bestimmten ausdrücklich genannten Straftaten, insbesondere aus den Bereichen Cyberkriminalität oder Terrorismus. Die Anordnung muss von einem Richter, Gericht oder Ermittlungsrichter erlassen oder validiert werden. Bei Verkehrs- und Inhaltsdaten ist grundsätzlich auch die Vollstreckungsbehörde jenes Mitgliedstaats zu unterrichten, in dem sich der Adressat der Anordnung befindet; sie kann die Anordnung aus abschließend geregelten Gründen ablehnen – etwa bei Immunitäten und Berufsgeheimnissen, offenkundigen Grundrechtsverletzungen oder einem Verstoß gegen das Doppelverfolgungsverbot (ne bis in idem).

Die betroffene Person wird von der anordnenden Behörde grundsätzlich über die Herausgabe informiert. Diese Information kann jedoch aufgeschoben werden, solange und soweit sie die Ermittlungen gefährden würde. Der Anbieter selbst kann zur Vertraulichkeit verpflichtet werden. Unternehmen können also nicht darauf vertrauen, zeitnah zu erfahren, dass ihre bei einem Provider gespeicherten Daten Gegenstand einer Anordnung waren.

Welche Dienste sind betroffen?

Die Verordnung erfasst Diensteanbieter, die eine der folgenden Kategorien in der EU anbieten (Art. 3 Nr. 3 der Verordnung):

- **elektronische Kommunikationsdienste** – neben klassischer Telefonie und Internetzugang auch Messenger-, Internet-Telefonie- und E-Mail-Dienste;

- **Internet-Domain-Namen- und IP-Nummerierungsdienste**, etwa Domain-Registrare und damit verbundene Privacy- und Proxy-Dienste;

- **sonstige Dienste der Informationsgesellschaft**, sofern sie es ihren Nutzern ermöglichen, miteinander zu kommunizieren, oder sofern die Speicherung oder Verarbeitung von Daten einen bestimmenden Bestandteil der Leistung darstellt. Erfasst sein können insbesondere Hosting- und Cloud-Dienste, Online-Marktplätze sowie bestimmte Plattformen für Online-Spiele.

Finanzdienstleistungen im Sinne des Unionsrechts sind ausgenommen.

Nicht erfasst sind hingegen Unternehmen, deren Online-Auftritt sich in der Kommunikation mit den eigenen Kunden erschöpft, sowie Dienste, bei denen die Datenspeicherung nur ein untergeordneter Nebenaspekt ist – die Verordnung nennt als Beispiele online erbrachte Rechts-, Architektur-, Ingenieur- und Buchführungsleistungen.

Drei Punkte überraschen in der Beratungspraxis regelmäßig:

Erstens: Die Verordnung kennt keine allgemeine Größen- oder Umsatzschwelle. Auch kleinere Anbieter und Nischenanbieter können daher in den Anwendungsbereich der Verordnung fallen.

Zweitens: Entscheidend ist nicht allein der Sitz des Anbieters. Auch Anbieter mit Sitz außerhalb der EU können erfasst sein, wenn sie Dienste in der EU anbieten und eine wesentliche Verbindung zu einem oder mehreren Mitgliedstaaten besteht. Dafür können etwa eine Niederlassung in der EU, eine erhebliche Zahl von Nutzern oder eine gezielte Ausrichtung des Angebots auf einen oder mehrere Mitgliedstaaten sprechen.

Drittens: Ergänzt wird die Verordnung durch die Richtlinie (EU) 2023/1544. Sie verpflichtet die Mitgliedstaaten dazu, Regeln vorzusehen, nach denen bestimmte grenzüberschreitend tätige Diensteanbieter eine benannte Niederlassung oder einen rechtlichen Vertreter als Zustelladressaten benennen oder bestellen müssen. Die Richtlinie musste bis zum 18. Februar 2026 in nationales Recht umgesetzt werden. Sie gilt allerdings nicht für Anbieter, die nur in einem Mitgliedstaat niedergelassen sind und ihre Dienste ausschließlich dort anbieten. Welche konkrete Benennungs- oder Vertreterpflicht einen Diensteanbieter trifft, ist daher anhand des jeweils anwendbaren nationalen Umsetzungsrechts zu prüfen.

In Österreich ist die Umsetzung der Richtlinie nach dem derzeit veröffentlichten Stand noch nicht abgeschlossen. Die Europäische Kommission hat deshalb bereits ein Vertragsverletzungsverfahren gegen Österreich eingeleitet. Für österreichische Diensteanbieter entsteht daraus in der Anfangsphase eine zusätzliche Rechtsunsicherheit, insbesondere hinsichtlich der Benennung des Adressaten sowie der nationalen Vollstreckungs- und Sanktionsregelungen.

Was bedeutet das konkret für Ihr Unternehmen?

Für alle Unternehmen als Nutzer digitaler Dienste
Auch Unternehmen, die selbst keine Diensteanbieter im Sinne der Verordnung sind, sind mittelbar betroffen. Unternehmensdaten, die bei Cloud-, Hosting-, E-Mail- oder Kommunikationsanbietern gespeichert sind, können Gegenstand einer Anordnung einer Strafverfolgungsbehörde aus einem anderen teilnehmenden EU-Mitgliedstaat sein – unabhängig davon, wo sich die Server befinden und unter Umständen, ohne dass das betroffene Unternehmen zeitnah davon erfährt. Unternehmen sollten daher insbesondere:

- sich einen Überblick verschaffen, **welche Unternehmensdaten bei welchen externen Anbietern gespeichert oder verarbeitet werden** und welchen Vertraulichkeitsanforderungen diese Daten unterliegen;

  Verträge mit Cloud- und IT-Dienstleistern darauf prüfen, welche Regelungen für den Umgang mit Behördenanfragen bestehen – insbesondere Informationspflichten des Anbieters, soweit eine Information rechtlich zulässig ist, Protokollierungspflichten und interne Ansprechpartner;

- **besonders sensible Datenbestände identifizieren**. Besondere Schutzmechanismen können insbesondere bei Daten greifen, die gesetzlichen Berufsgeheimnissen, Immunitäten oder sonstigen Privilegien unterliegen. Geschäftsgeheimnisse sind davon zu unterscheiden und sollten zusätzlich durch geeignete technische, organisatorische und vertragliche Maßnahmen geschützt werden.

Für Diensteanbieter
Anbieter, deren Leistungen in den Anwendungsbereich der Verordnung fallen können, sollten insbesondere folgende Punkte prüfen:

- **Betroffenheitsanalyse:** Fällt unser Dienst unter Art. 3 Nr. 3 der Verordnung? Besteht eine wesentliche Verbindung zu einem oder mehreren Mitgliedstaaten?

- **Benennungs- und Vertreterpflicht:** Ist nach der Richtlinie (EU) 2023/1544 und dem jeweils anwendbaren nationalen Umsetzungsrecht eine benannte Niederlassung oder ein rechtlicher Vertreter erforderlich? In welchem Mitgliedstaat ist diese Benennung bzw. Bestellung vorzunehmen?

- **Interner Prozess:** Zuständigkeiten und Vertretungsregelungen für eingehende EPOC und EPOC-PR festlegen. Insbesondere wegen der Acht-Stunden-Frist in Notfällen muss geprüft werden, wie eine ausreichende Erreichbarkeit und ein belastbares Fristenmanagement gewährleistet werden können.

- **Prüfschema:** Eingehende Anordnungen müssen auf formale Vollständigkeit, offensichtliche Fehler und die in der Verordnung vorgesehenen Einwendungs- und Kommunikationsmöglichkeiten geprüft werden. Besondere Aufmerksamkeit erfordern insbesondere Immunitäten und Privilegien, Berufsgeheimnisse sowie mögliche Konflikte mit Verpflichtungen nach dem Recht eines Drittstaates.

- **Technik und Datenzugriff:** Es muss sichergestellt sein, dass angeforderte Datenkategorien innerhalb der kurzen Fristen identifiziert, gegebenenfalls gesichert und

sicher übermittelt werden können. Die Verordnung sieht hierfür eine elektronische Kommunikation über ein dezentrales IT-System vor; die technischen Rahmenbedingungen hierfür werden unionsrechtlich näher ausgestaltet.

Fazit

Die E-Evidence-Verordnung beschleunigt den grenzüberschreitenden Zugriff auf elektronische Beweismittel erheblich. Strafverfolgungsbehörden können sich nun in zahlreichen Fällen unmittelbar an den Diensteanbieter bzw. dessen benannte Niederlassung oder rechtlichen Vertreter wenden – unabhängig davon, wo die angeforderten Daten gespeichert sind.

Für Diensteanbieter bedeutet dies kurze Reaktionsfristen und die Notwendigkeit klarer interner Prozesse. Gleichzeitig sollten auch Unternehmen, die digitale Dienste lediglich nutzen, wissen, welche Daten sie bei welchen Anbietern speichern und welche vertraglichen und technischen Schutzmechanismen bestehen.

Zusätzliche Unsicherheit besteht derzeit in Österreich aufgrund der noch ausstehenden Umsetzung der Richtlinie (EU) 2023/1544. Diensteanbieter sollten daher sowohl die unmittelbar anwendbaren Vorgaben der E-Evidence-Verordnung als auch die weitere nationale Umsetzung aufmerksam im Blick behalten.

Gerne unterstützen wir Sie bei der Betroffenheitsanalyse, der Prüfung einer allfälligen Benennungs- oder Vertreterpflicht, der Gestaltung eines internen Prüf- und Reaktionsprozesses sowie bei der rechtlichen Prüfung und Beantwortung einer konkreten E-Evidence-Anordnung.