

# E-Evidence-Verordnung (EEVO)

Die EEVO ermöglicht EU-Strafverfolgungsbehörden, digitale Beweise direkt bei Diensteanbietern in anderen Mitgliedstaaten anzufordern – ohne langwierige Rechtshilfeverfahren. Es ergeben sich zwei neue Instrumente:



## EPOC – HERAUSGABEANORDNUNG

Pflicht zur Herausgabe elektronischer Beweismittel (Inhalts, Verkehrs- oder Bestandsdaten)



## EPOC-PR – SICHERUNGSANORDNUNG

Pflicht zur Datensicherung für bestimmten Zeitraum, damit Daten nicht gelöscht werden



## Wer ist betroffen?

Betroffen sind Diensteanbieter mit EU-Bezug, unabhängig vom Unternehmenssitz. Darunter fallen:

- Messenger / VoIP
- Hosting & Cloud
- Plattformen & Soziale Netzwerke
- Domain-Registriere



## Welche Kriterien müssen erfüllt sein?

EU-Bezug liegt vor, wenn mindestens eines der folgenden Kriterien erfüllt ist:

- Dienste sind für Nutzer in einem EU-Mitgliedstaat zugänglich (Sprache, Währung, Marketing)
- Anbieter hat eine Niederlassung in einem Mitgliedstaat
- Erhebliche Nutzerzahl in einem oder mehreren Mitgliedstaaten



## Pflichten & Fristen im Überblick

|            | HERAUSGABE (ART. 10 EEVO) | SICHERUNG (ART. 11 EEVO)               |
|------------|---------------------------|----------------------------------------|
| NORMALFALL | 10 Tage ab Zugang         | Sofort sichern, 60 Tage Dauer          |
| NOTFALL    | 8 Stunden ab Zugang       | Verlängerung einmalig +30 Tage möglich |



## Sanktionen bei Nichtbefolgung nach Art. 16 EEVO

Geldbußen bis zu 2 % des weltweiten Jahresumsatzes möglich, bei pflichtwidriger Nichtbefolgung ohne akzeptierten Grund. Aktive Kommunikation mit der Behörde (z. B. Meldung von Hindernissen) kann Sanktionen abwenden.



## So reagieren Sie richtig

### HERAUSGABE

1. Frist beachten: 10 Tage / 8h (Notfall)
2. Datenkategorie prüfen: Teilnehmerdaten → direkt ausführen; Inhalts-/Verkehrsdaten → Straftatenpraxis prüfen (Art. 5 Abs. 4 EEVO)
3. Bescheinigung prüfen: Vollständig & fehlerfrei? Sonst: Anhang III Formular
4. Daten übermitteln: Vertraulichkeit wahren, Benachrichtigungsverbot beachten
5. Nachbereitung: Sicherung aufheben, Daten löschen (soweit keine anderen Aufbewahrungspflichten)

### SICHERUNG

1. Sofort sichern: Unverzüglich nach Zugang
2. Dauer: 60 Tage, einmalig +30 Tage verlängerbar; bei Folge-EPOC bis Herausgabe
3. Bescheinigung prüfen: Vollständig & fehlerfrei? Sonst: Anhang III Formular
4. Vertraulichkeit: Integrität sichern, Benachrichtigungsverbot beachten (Art. 11 Abs. 3 EEVO)
5. Nachbereitung: Nach Fristablauf / Mitteilung der Behörde: gesicherte Daten löschen

## Handlungsbedarf aufgrund der EEVO



### Adressaten benennen

mindestens einen Empfänger der Anordnungen nach Art. 3 Abs. 1 EEVO bestellen



### Interne Prozesse etablieren

Workflows für Eingang, Prüfung, Sicherung, Übermittlung & Dokumentation definieren



### Schulungen & Protokollierung

Personal schulen, Nachweisdokumentation implementieren