Positionierung zur NATIONALEN E-EVIDENCE UMSETZUNG

Wir bedanken uns für die Gelegenheit, unsere Überlegungen zur nationalen Umsetzung und Durchführung des E-Evidence-Pakets in Deutschland einbringen zu dürfen.

Es ist uns **ein großes Anliegen**, dass **rechtssichere** und **praktikable Rahmenbedingungen** für die Umsetzung grenzüberschreitender Anordnungen geschaffen werden, die es uns als Diensteanbieter ermöglichen, in der geforderten knappen Zeit die **notwendigen technischen** und **organisatorischen Vorkehrungen** zu treffen, ohne hierbei das **Risiko von Fehlinvestitionen** und **späteren Nachbesserungen** eingehen zu müssen.

Unsere Überlegungen beziehen sich auf

- *die Verordnung (EU) 2023/1543 („Verordnung“) und die dazugehörige Richtlinie (EU) 2023/1544 („Richtlinie“)*
- *den Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz vom 04.06.2025: Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2023/1544 und zur Durchführung der Verordnung (EU) 2023/1543 über die grenzüberschreitende Sicherung und Herausgabe elektronischer Beweismittel in Strafverfahren innerhalb der Europäischen Union („Referentenentwurf“)*

1. Fehlende Regelung des Zugangs zum dezentralen IT-System

Die Verordnung sieht vor, dass die Diensteanbieter über das jeweilige nationale IT-System Zugang zum dezentralen IT-System erhalten. Aus unserer Sicht **mangelt es** hier derzeit an einer **verbindlichen Regelung der Zuständigkeit** sowie der **Ausgestaltung des nationalen IT-Systems**. Insbesondere bei der Anbindung an das nationale IT-System wären **klare technische Spezifikationen** und Abläufe wünschenswert, die eine Entwicklung der Anbindung auf Seiten der verpflichteten Unternehmen erst möglich machen.

Die Diensteanbieter haben ihrerseits **geeignete Vorkehrungen** zu treffen, um die **fristgerechte Umsetzung** von Anordnungen sicherzustellen. Als etablierte Telekommunikationsunternehmen rechnen wir mit einem **signifikanten Anfragevolumen**, dessen effiziente Bearbeitung nur durch den **Einsatz unternehmenseigener IT-Lösungen** und **digitaler Workflows** gewährleistet werden kann.

Wir sehen daher folgende Punkte als **notwendig** an, um die **zukunftsorientierte** und **wirtschaftlich tragfähige Umsetzung** zu erreichen:

- Zur Schaffung eines **verlässlichen und praxistauglichen Rechtsrahmens**, sollte die für die Anbindung der Diensteanbieter zuständige Stelle ein **klares Mandat** haben und mit einer **rechtlichen Ermächtigung** ausgestattet werden, um **verbindliche technische** oder **organisatorische Vorgaben** abzustimmen.
- Es bedarf einer **verbindlichen Aussage** zur Möglichkeit, **eigene IT-Lösungen an das nationale IT-System anzubinden** und dabei die **auf Basis des geltenden ETSI-Standards** spezifizierte Schnittstelle zu nutzen. Gerade im Bereich der Telekommunikation können so die **effektiven bestehenden Prozesse** in den Workflowsystemen der Netzbetreiber auch in diesem Bereich genutzt werden. Die in Deutschland **vorhandene Expertise im Bereich der TKÜV / TR TKÜV** mit der **elektronischen Schnittstelle für Behörden** sollte Berücksichtigung finden. Auch dann, wenn das hier zum Einsatz kommende E-CODEX-Verfahren einen anderen Übertragungsweg vorsieht.
- Für die **Koordinierung von Versionsänderungen** sowie als zentraler Ansprechpartner bei der **Fehlerbehebung** sollte eine **klar benannte und dauerhaft erreichbare Stelle** vorgesehen werden.
- Vorgaben für den **stabilen** und **sicheren Datenaustausch** zwischen der unternehmenseigenen IT-Infrastruktur und dem nationalen IT-System sind eine zentrale Voraussetzung für einen **datenschutzkonformen** und **unterbrechungsfreien Betrieb**.

2. Anwendbarkeit der Verordnung

Die in Art. 1 Abs. 5 Satz 2 der Richtlinie vorgesehene **Ausnahme** für **inländische Anbieter mit ausschließlich nationalem Diensteangebot** wirft in der Praxis Auslegungsfragen auf und führt zu erheblicher **Rechtsunsicherheit**.

Aus unserer Sicht besteht der **dringende Bedarf** an einer **rechtlichen Klarstellung**. Eine Orientierungshilfe, etwas **in Form eines Leitfadens** oder eines **standardisierten Betroffenen-Checks**, erscheint unerlässlich, um die bestehenden Unsicherheiten zu beseitigen und eine **konsistente Anwendungspraxis** zu gewährleisten.

Gerade im **Bereich der Telekommunikation**, der eindeutig durch die E-Evidence Regulierung adressiert wird, handelt es sich um **nationale Unternehmen**, die Ihre **Dienste primär national** anbieten und **national reguliert** werden. Dies zeigt sich besonders deutlich im **Festnetz- und Kabelbereich**.

3. Weitere Anmerkungen

Darüber hinaus möchten wir auf Aspekte hinweisen, die zwar nicht unmittelbar dem nationalen Regelungsbedarf zuzuordnen sind, **in der praktischen Umsetzung** jedoch **deutliche Risiken** mit sich bringen.

3.1 Kostenentschädigung

Die Schaffung der **technischen** und **organisatorischen Voraussetzungen** für die Umsetzung sowie der anschließende laufende Betrieb sind mit **erheblichen Kosten für die Anbieter** verbunden. Die in der Verordnung **vorgesehene Regelung zur Kostenerstattung** nach nationalem Recht im Anordnungsstaat dürfte sich **in der Praxis** jedoch als **kaum anwendbar** erweisen.

Während bei einem Rechthilfeersuchen die **Entschädigung nach nationalem Recht** klar gegeben war, ist dies durch die E-Evidence-Regulierung **ersatzlos entfallen**. Vielmehr wurden auch den national operierenden Unternehmen **weitere wirtschaftliche Lasten** auferlegt, ohne dass es hierfür einen Ausgleich gibt. Während die Justiz von den beschleunigten Verfahren profitiert, werden die **Unternehmen** sowohl **im Hinblick auf den Invest** sowie die **laufenden Kosten des Verfahrens benachteiligt**. Die Zuständigkeit der Politik erscheint uns hier sehr einseitig.

Eine EU-weit einheitliche und für alle Mitgliedstaaten verbindliche Entschädigungsregelung würde maßgeblich zur Schaffung von **Rechts- und Planungssicherheit für die Anbieter** beitragen. Derzeit ist eine solche Regelung jedoch nicht absehbar. Abhilfe könnte geschaffen werden, wenn bei jeder Anfrage **standardisierte Informationen** zum **zuständigen Kostenträger** sowie zu den **erstattungsfähigen Leistungen** bereitgestellt würden. Wir bitten das zuständige Ressort, sich aktiv auf europäischer Ebene für eine **praxisnahe** und **interoperable Lösung** einzusetzen.

3.2 Übermittlung und Zugänglichkeit der Kontaktdaten beauskunftender Stellen

Diensteanbieter sind nach § 4 Abs. 1 Referentenentwurf in Verbindung mit Art. 4 Abs. 1 der Richtlinie dazu verpflichtet, dem Bundesamt für Justiz als zuständiger zentraler Behörde gemäß § 6

Referentenentwurf **Kontaktdaten der zu benennenden Niederlassung bzw. Vertreter** mitzuteilen. Prozessual bestehen **Unklarheiten über den Übermittlungsweg**. Insofern ist klarzustellen ist, dass eine derzeit diskutierte Übermittlung **über die bei der EU-Kommission verortete Court Database** als schriftliche Mitteilung an das Bundesamt für Justiz den Anforderungen des § 4 Abs. 1 Referentenentwurf **genügt**.

Darüber hinaus gibt die vorgesehene Regelung in Art. 31 Abs. 2 der Verordnung, wonach die **Kontaktdaten der für die Beauskunftung zuständigen Stellen öffentlich zugänglich** gemacht werden, Anlass zur Sorge – insbesondere im Hinblick auf **potenzielle Sicherheitsrisiken** und **Missbrauchsmöglichkeiten**. Vor dem Hintergrund des **geschlossenen Benutzerkreises im dezentralen IT-System** sowie der vorgesehenen Bereitstellung der Kontaktdaten über das System selbst stellt sich die Frage, ob eine **Bereitstellung im öffentlichen Raum** in dem geforderten Umfang **erforderlich** und **verhältnismäßig** ist. Sicherzustellen ist insofern, dass eine Veröffentlichung von Kontaktdaten im Einklang mit **datenschutzrechtlichen Vorgaben** sowie **IT-Sicherheitsanforderungen** erfolgt. In Konsequenz sollten **bestenfalls keine oder jedenfalls nur zwingend erforderliche** personenbezogene Daten öffentlich zur Verfügung gestellt werden müssen. Überdies ist zur Verhinderung von IT-sicherheitsrelevanten Vorfällen **keinerlei Veröffentlichung solcher (Kontakt-) Daten** vorzunehmen, die die **Erfüllung** der in der Verordnung geregelten **Pflichten beeinträchtigen** könnte.

3.3 Anforderungen an die Verwendung und Herausgabe der Daten

Die Verwendung von im Rahmen einer Sicherungsanordnung gesicherten personenbezogenen Daten ist aus unserer Sicht bislang **nicht hinreichend geregelt**. Um den **datenschutzrechtlichen Anforderungen** Rechnung zu tragen sollte gewährleistet sein, dass diese **Daten getrennt** von anderen Datenbeständen **gespeichert** werden und **ausschließlich in dem Verfahren zur Verfügung** stehen, für das die Sicherungsanordnung erlassen wurde. Eine **Verwendung für andere** als in der **Sicherungsanordnung benannte Zwecke**, etwa zur Beantwortung von Auskunftsersuchen nach der DSGVO, sollte **ausgeschlossen** sein.