E-Evidence

Fragensammlung

Berlin, 2. Juli 2024

Grundsatzfragen zur Umsetzung der E-Evidence-VO

Die Branche begrüßt grundsätzlich das Vorgehen der EU zu der Verbesserung der Ermittlung und Verfolgung von Straftaten für die Bekämpfung von Kriminalität. Die Notwendigkeit eines besseren Zugangs der Strafverfolgungsbehörden ist vor allem vor dem Hintergrund der vermehrten Nutzung technologischer Dienste und Werkzeuge für die Planung und Begehung von Straftaten ersichtlich und nachvollziehbar. Es ergeben sich jedoch in technischer sowie in rechtlicher Sicht noch eine Vielzahl von ungeklärten Fragen, die vor allem kleine und mittelständische Unternehmen vor erhebliche Herausforderungen stellt und mit dem Versprechen eines geplanten Bürokratieabbaus nicht vereinbart ist. Diese unklaren Regelungen gilt es nun gemeinsam mit der Branche auszudifferenzieren, um Planungssicherheit sicherzustellen. Dies gilt auch im Hinblick auf den Ausbau notwendiger Personal- sowie IT-Strukturen. Es steht zu befürchten, dass eine restriktive Umsetzung der E-Evidence-VO ohne maßvolle Ausnahmetatbestände zu unverhältnismäßigen Belastungen der betroffenen Unternehmen führt; dies gilt in besonderem Maße für kleinere und mittlere Unternehmen. Wie sich zum Beispiel aus Erwägungsgrund 88 der E-Evidence-VO ersehen lässt, sollen gerade solche unverhältnismäßigen Aufwände auf Seiten kleinerer und mittlerer Unternehmen vermieden werden.

Gemeinsam haben wir rechtliche und technische Fragen im Kontext der E-Evidence-VO herausgearbeitet, die es noch zu klären gilt.

A. Rechtliche Fragen Einleitung zu den Fragen

Wir gehen als Vertreter der von der E-Evidence-Verordnung betroffenen Unternehmen (IT- wie Telekommunikationsunternehmen) davon aus, dass den von der Abfrage betroffenen „Provider“ (nachfolgend „Diensteanbieter“ genannt) keine Prüfpflicht in formeller und

materieller Hinsicht zukommt, wenn dieser eine Sicherungs- oder Herausgabeanordnung zu befolgen hat. Allein angesichts des Umstandes, dass das Recht des Anforderungsstaates maßgeblich ist (mithin des anfragenden ausländischen Staates), macht eine Prüfung nahezu undurchführbar. Da sich die Verordnung in Bezug auf die vorstehenden Annahmen nicht eindeutig verhält, stellen sich nachfolgende Fragen zur Prüfpflicht:

I. Einzelfragen zu formellen und materiell-rechtlichen Prüfung

1. Einige Passagen der Verordnung (exemplarisch Art. 10 (5) und (6) sowie Art. 11 (4), (5)) könnten dahingehend verstanden werden, dass dem adressierten Diensteanbieter eine formelle und/oder materiell-rechtliche Prüfpflicht zukommt. Ein weiteres Beispiel stellt ein EPOC/EPOC-PR dar, der nach Art. 4 der RL in einer nicht zulässigen Sprache verfasst ist. Generell stellt sich die Frage, ob ein Diensteanbieter die Daten auch bei einem „offensichtlichen Fehler“ gemäß Anhang III Abschnitt D lit. a) der Verordnung herausgeben darf.

   Darüber hinaus ist zu betonen, dass der Anhang III Abschnitt D lit. a) Gründe zur Auswahl stellen will, die eine Ausführung der Anordnung unmöglich machen. Tatsächlich enthalten die letzten fünf (!) aufgezählten Gründe dieses Abschnitts gar keine Umstände, die eine Ausführung der Anordnung faktisch unmöglich machen. Falls der Verordnungsgeber dennoch gewollt hat, dass diese Umstände zu einer unterlassenen Ausführung der Anordnung führen sollen, bedürfte dies im Gegensatz zur faktischen Unmöglichkeit eines entsprechenden Willens des Adressaten. Den für eine Unterlassung einer Ausführung notwendigen Willen kann der Adressat aber nur nach vorheriger Prüfung und Annahme der genannten Umstände bilden.

   Eine entsprechend weitgreifende Prüfungspflicht der Adressaten wäre vom Verordnungsgeber normenklar im eigentlichen Verordnungstext, anstatt andeutungsweise in einem Anhang aufzuerlegen gewesen. Eine ausdrückliche Prüfungspflicht lässt der Verordnungstext jedoch vermissen. Im Fall der Unmöglichkeit der Ausführung einer Anordnung ist eine Prüfung schon denklogisch entbehrlich. Außerhalb der Unmöglichkeit der Ausführung nennt der Verordnungstext nur in Art. 10 (5) und 11 (4) einen Umstand, der die Ausführung der Anordnung hindern soll. Hierbei wird die Auffassung des Adressaten von einer möglichen Schutzrechtsverletzung der betroffenen Person vorausgesetzt. Die Pflicht, sich überhaupt eine Auffassung zu dieser Möglichkeit zu verschaffen, wird jedoch nicht statuiert. Es handelt sich vielmehr um eine Regelung zur „Selbstheilung“ im Rahmen des Auskunftsverfahrens.

   Dies steht im Widerspruch zu dem Grundverständnis, dass dem Diensteanbieter keine Prüfpflicht in Bezug auf die Anordnungen nach der E-Evidence-Verordnung zukommt. Es muss daher aus Sicht der betroffenen Unternehmen klargestellt werden, dass auch bei vermeintlich offensichtlichen Fehlern keine Obliegenheit seitens der Diensteanbieter besteht die Anordnung überprüfen zu müssen. Denn ansonsten würde die formell und/oder materiell-rechtliche Prüfung einer Anordnung auf die Unternehmen übertragen. Diese Prüfung obliegt hingegen nach diesseitigem Verständnis dem Vollstreckungsstaat respektive der beauftragten Vollstreckungsbehörde.

   Der Diensteanbieter hat das Recht, hingegen nicht die Pflicht, eine Anforderung nach der Verordnung auf formelles und/oder materielles Recht hin zu prüfen. Entsprechend gehen wir davon aus, dass der Diensteanbieter im Falle von Zweifeln an der Rechtmäßigkeit der Anordnung (z. B. ein Konflikt mit dem Recht eines Drittlandes) ein Überprüfungsverfahren nach Art.17 (Einschaltung der Vollstreckungsbehörde) durch Übersenden eines Annex III- Formblatts einleiten kann, aber nicht muss. Für den Diensteanbieter bestünde ansonsten ein nicht hinnehmbares Risiko, wann ein Prozess

in seinem Vollstreckungsstaat hinsichtlich der Rechtmäßigkeit durchgeführt werden muss und wann nicht. Selbst bei einem vermeintlich „offensichtlichen Fehler“ bestünde die Gefahr, dass dies unterschiedlich eingeordnet wird.

2. Wir gehen davon aus, dass die formellen und materiell-rechtlichen Fragen durch den Anordnungsstaat abschließend geprüft werden („In good faith“). Dieses „Vertrauendürfen“ auf die Rechtskonformität einer signierten Anordnung muss auch dann gelten, wenn die Verordnung juristisch gegen geltendes Recht verstößt, da der Umfang der betroffenen Diensteanbieter so weitgehend ist, dass die meisten keinen unmittelbaren Zugriff auf einen rechtskundigen Experten haben.

3. Wird die Übermittlungsfrist durch die Prüfung der Vollstreckungsbehörde gehemmt? Die Vollstreckungsbehörde im Vollstreckungsstaat prüft innerhalb von 10 Tagen, ob die Anordnung rechtskonform ergangen ist. Der Diensteanbieter hat seinerseits aber nur 10 Tage Zeit zu antworten. Entsprechend könnte und dürfte der Diensteanbieter die betreffenden Daten in allen Fällen, bei denen die Vollstreckungsbehörde zwingend einzuschalten ist (d. h. regelmäßig aus Art. 8 (1) i.V.m. Art.10 (2)), stets erst nach Ablauf der 10 Tagesfrist senden, da er ansonsten damit rechnen muss, dass der Vollstreckungsstaat die Anordnung als rechtswidrig einstuft. Wie kann sichergestellt werden, dass die in Art. 10 (2) Satz 2 zur Beschleunigung der Abwicklung vorgesehene Vorab-Notifikation des Anbieters nach erfolgter Prüfung der Anordnung durch die Vollstreckungsbehörde – zumindest in Deutschland – der Regelfall im Prüfverfahren wird und so eine zeitnahe Abwicklung für Diensteanbieter und in Folge den empfangenden Strafverfolgungsbehörden wird?

4. Welche Kostenentschädigungsregelungen finden in Bezug auf das EPOC Anwendung? Nach dem grundsätzlichen Ansatz der Verordnung gilt das Recht des anfragenden Staates. Dies führt dazu, dass nicht gewährleistet ist, dass der mit den Anfragen verbundene Aufwand einheitlich bzw. überhaupt vergütet wird. Wie wird sichergestellt das – unabhängig vom Anforderungsstaat – eine angemessene Entschädigung an den betroffenen Diensteanbieter gezahlt wird? Insofern dies aus Art. 14 (1) derzeit nicht vorgesehen scheint, setzt sich die Bundesregierung für eine europaweite Regelung zur einheitlichen Vergütung von Anbietern mit Sitz im Ausland z. B. im Rahmen einer multilateralen zwischenstaatlichen Vereinbarung, wie diese zur Abwicklung von E-Evidence im Rahmen der Ländergruppe auch an anderer Stelle geplant ist, ein?

II. Haftung

Als maßgeblichster Punkt muss der Provider von der Haftung befreit werden, wenn er einer Anordnung Folge leistet und sich diese im Nachhinein als nicht rechtskonform erweist. Dies gilt unabhängig von Anforderungs-/Vollstreckungsstaat und unabhängig davon, ob es sich um zivil- oder strafrechtliche Haftung handelt. Der betroffene Diensteanbieter muss sich aufgrund der formalisierten Herausgabeanordnung stets exkulpieren können, vgl. § 174 II 5 TKG. Ist eine analoge Klarstellung im Rahmen der nationalen Umsetzung vorgesehen?

III. Datenschutz - Verhältnis zu DSGVO, TKG und TTDSG

Bildet die Verordnung eine ausreichende datenschutzrechtliche Rechtfertigung für die betroffenen Diensteanbieter zur Datenübermittlung (wie z. B. § 170 TKG, der dann nicht anwendbar wäre)? Und geht die Verordnung national der TTDSG, dem TKG und der DSGVO vor, sofern und soweit sie speziellere Regelungen trifft?

Sofern dies fraglich ist, sollten die entsprechenden Regularien in dem nationalen Ausführungsgesetz vorgesehen werden, um Rechtssicherheit für die Provider zu erreichen.

IV. Weitere Fragen zur Systematik, Umsetzung und Anwendung

Unabhängig davon, wer die Prüfpflicht ausübt, stellen sich weitere Fragen, die aus unserer Sicht durch den Verordnungstext nicht ausreichend geklärt werden. Nachfolgende Fragen dienen sowohl dem besseren Verständnis der Gesamtsystematik als auch der Rechtssicherheit der betroffenen Unternehmen:

1. Maßnahmen, die im Anforderungsstaat rechtskonform sind, können im Vollstreckungsstaat gegen geltendes Recht verstoßen und zivil- wie strafrechtliche Konsequenzen nach sich ziehen. Wie werden Kollisionen zwischen nationalen Rechtsnormen gelöst und welche Instanz löst diese Fragen abschließend?

2. Ist der Schutz Berufsgeheimnisträger und mitwirkender Personen (§ 53 und § 53a StPO) (z. B. Rechtsanwälte, Abgeordnete, Steuerberater, Ärzte, Seelsorger) ausreichend gesichert? Wie kann/soll eine diesbezügliche Überprüfung stattfinden? Wie wird sichergestellt, dass eine diesbezügliche Prüfung durch die Anforderungsbehörde sowie insbesondere durch die Vollstreckungsbehörde nicht ausschließlich nach nationalen Maßstäben erfolgt, sondern sich abstrakt an dem Schutz der Berufsgeheimnisträger orientiert (z. B. darf die Stellung als Rechtsanwalt nicht von der Stellung als Rechtsanwalt in Deutschland abhängig sein oder der Schutz als Abgeordneter nicht von der Auflistung in § 53 Abs. 1 Nr. 4 StPO)?

3. Existiert für alle Nationalstaaten der EU ein einheitliches Beweisverwertungsverbot für unrechtmäßig erlangte Informationen?

4. Ist gesichert, dass die in der Verordnung genannten Fristen grenzüberschreitend einheitlich gehandhabt und berechnet werden? In Deutschland enden Fristen immer am Tag um 24:00 Uhr. Sollten sie auf einen Samstag/Sonntag fallen, enden sie montags um 12:00 Uhr. Ist gewährleistet, dass hier grenzüberschreitend einheitliche Fristenregelungen im Kontext E-Evidence existieren? (hiervon unbenommen ist die 8 Stunden-Frist für „Emergency cases“).

5. Sind im Rahmen der nationalen Implementierung weitere Gesetze, Verordnungen oder technische Richtlinien neben den bereits geplanten Bestimmungen der §§ 13a, 24a TTDSG in Planung?

6. Welche Behörden werden welche Rollen übernehmen und als Ansprechpartner dienen?

7. Wie sieht die zeitliche Planung für die rechtlichen Anpassungen in Deutschland aus?

8. In welchem Verhältnis stehen die Regelungen der E-Evidence-VO in Bezug auf Umsetzung der Vollzugsakte innerhalb Deutschlands zu anderen vergleichbaren Pflichten, insbesondere aus den zu erwartenden Vorgaben aus dem „Quick-Freeze-Verfahren“ oder den Auskunftspflichten aus Art. 9 und 10 DSA?

9. Nach Art. 7 Abs. 1 E-Evidence-VO ist die Anordnung unmittelbar an eine **„benannte Niederlassung“** oder einen Vertreter des Diensteanbieters zu richten. Die Benennung ist nach Art. 3 Nr. 6 E-Evidence-VO in Verbindung mit Art. 1 Abs. 1 und Art. 3 Richtlinie 2023-1544 vorzunehmen. Analoges gilt für Vertreter. Art. 1 Abs. 5 der Richtline 2023-1544 bestimmt jedoch:

   „Diese Richtlinie gilt für Diensteanbieter im Sinne des Artikels 2 Nummer 1, die ihre Dienste in der Union anbieten. Sie gilt nicht für Diensteanbieter, die im Hoheitsgebiet nur eines Mitgliedsstaats niedergelassen sind und ihre Dienste nur im Hoheitsgebiet dieses Mitgliedsstaats anbieten“.

   Das heißt, dass Diensteanbieter, die nur in Deutschland niedergelassen sind und nur in Deutschland ihre Dienste anbieten, ausdrücklich keine Niederlassung oder Vertreter nach dieser Richtlinie zu benennen haben. Sind damit auch Telekommunikations-unternehmen gemeint, die Dienstleistungen nur gegenüber nationalen (deutschen) Kunden anbieten, deren Anschlüsse aber aus dem EU-Ausland erreichbar ist?

10. Die Richtlinie 2023-1544 gilt aufgrund Art. 1 Abs. 1 S. 2 im Umkehrschluss für **Diensteanbieter, die in mehreren Mitgliedstaaten Dienste anbieten**. Darunter fällt jedoch folglich keine Muttergesellschaft, die zwar in mehreren Mitgliedstaaten Diensteanbieter-Tochterunternehmen hat, selbst aber als Muttergesellschaft keine Dienste anbietet und somit selbst nicht die Merkmale eines Diensteanbieters gemäß Art. 2 Abs. 1 E-Evidence-VO erfüllt. Ist das richtig?

11. Die Antwortfrist in Notfällen beträgt ab Erhalt des EPOC acht Stunden (Art. 10 Abs. 4 E-Evidence-VO). Eine Ausnahmeregelung gibt es nicht. Für kleinere Netzbetreiber bzw. Anbieter ist diese Vorschrift problematisch, wenn sie aufgrund der nationalen Vorschriften für Behördenauskünfte über kein fachkundiges Personal verfügen, das außerhalb der üblichen Geschäftszeiten Auskünfte erteilen kann und nunmehr allein für diesen Zweck zusätzliches Personal aufbauen müssten.

    Deshalb stellt sich insbesondere hier die Frage: Wie ist „Erhalt“ zu verstehen? Ist damit der Zeitpunkt des Eingangs oder der Zugang (§ 130 Abs. 1 BGB) gemeint?

    Zudem müssen nach nationalem Recht alle Netzbetreiber oder Anbieter von Telekommunikationsdiensten eine Bestandsdatenauskunft lediglich unverzüglich übermitteln (§ 174 Abs. 6 S. 1 TKG). Für Verkehrsdaten gilt für Netzbetreiber und Anbieter von Telekommunikationsdiensten mit weniger als 100.001 Endnutzern, dass diese die Anordnung innerhalb ihrer üblichen Geschäftszeiten unverzüglich entgegennehmen und beauskunften müssen (unter den Voraussetzungen des § 31 Abs. 5 S. 1 TKÜV). Kein fachkundiges Personal, das außerhalb der Geschäftszeiten tätig werden kann, haben insbesondere die Netzbetreiber, die aufgrund der Ausnahmetatbestände von § 3 Abs. 2 TKÜV, z. B. § 3 Abs. 2 Nr. 5 TKÜV (weniger als 10.001 angeschlossene Nutzer), keine betrieblichen Vorkehrungen zur Umsetzung von

Überwachungsmaßnahmen (also z. B. Organisation einer Rufbereitschaft) treffen müssen. Wie ist angesichts dessen die Regelung von Art. 10 Abs. 4 E-Evidence-VO zur Wahrung der Verhältnismäßigkeit zu verstehen?

B. Technische Fragen

Des Weiteren stellen sich im Rahmen der Umsetzung technische Fragen, die möglichst zeitnah geklärt werden sollten, um den betroffenen Diensteanbietern und deren Dienstleistern eine frühzeitige Anbindung bzw. Implementierung an das Gesamtsystem zu ermöglichen.

1. Wie soll die IT-Infrastruktur in Deutschland aussehen? Werden hierfür neue Verwaltungsstrukturen und Verfahren geschaffen? Wie werden die Unternehmen hier eingebunden?

2. Wie wird die Interoperabilität innerhalb des dezentralen IT-Systems sichergestellt? Müssen auf nationaler Ebene Entscheidungen zu Schnittstellen/Übergabepunkten getroffen werden?

3. Erhält der Diensteanbieter eine Positivmeldung der Vollstreckungsbehörde nach erfolgter Prüfung vor Ablauf der Übermittlungsfrist? Wenn ja, in welcher Form wird diese Positivmeldung übermittelt? Ansonsten kann nicht vor Ende der maximalen Frist übermittelt werden (gegebenenfalls zwischenstaatliche Vereinbarungen notwendig).

4. Aus Sicht der betroffenen Unternehmen muss sichergestellt werden, dass digitale Unterschriften in allen Teilbereichen eingesetzt werden. Diese Unterschriften müssen zudem automatisch auf Berechtigung geprüft werden können. Ist dies so vorgesehen? Da bereits zur Erstellung der Audit-Trails alle Anordnungen, Nachrichten und Entscheidungen innerhalb des Systems ablaufen sollen, muss auch sichergestellt werden, dass neben den Diensteanbietern auch alle berechtigten Stellen, anordnenden Behörden sowie die Vollstreckungsbehörden mit allen handelnden Personen im System erreichbar und im zentralen Verzeichnis aufgeführt sind. Wie ist die Umsetzung hierzu in Deutschland vorgesehen? Ist bereits bekannt welche Stelle als Ansprechpartner für die Diensteanbieter zum regelmäßigen Update von Informationen und digitalen Schlüsseln zuständig sein wird?

5. Wie soll eine automatische Prüfung der Legitimierung der berechtigten Interessen vor dem Hintergrund der 27 verschiedenen Rechtssysteme umgesetzt werden? (Anm.: Bei EIO [European Investigation Order] wird die formale Prüfung durch die amtshelfende Stelle durchgeführt).

6. Wird eine Abrechnung der Kostenentschädigung automatisiert oder halbautomatisiert über das System möglich sein?

7. Soll ein standardisiertes Interface für die Anfrage und Antworten verwendet werden?

8. Welchen Datenmengen werden erwartet? Gibt es schon eine Abschätzung wie viele Anfragen pro einer Millionen Teilnehmer pro Jahr? Die Abschätzungen sind maßgeblich für die Skalierung der nationalen Systeme.

9. Werden Übersetzungen (sprachlich und technisch) für das Backend berücksichtigt?

10. An wen wenden sich Diensteanbieter im Falle eines Sicherheits- oder Zuverlässigkeitsvorfalls mit dem geplanten dezentralen IT-System? Wird hierfür ein gesonderter Zugangskanal eröffnet?

11. Wie oft wird die Europäische Kommission ihre technischen Standards für das dezentrale IT-System überprüfen? Ist geplant, das vorhandene Fachwissen technischer Normungsgremien wie ETSI zu nutzen?

Gerne stehen wir Ihnen in Bezug auf die vorgenannten Fragen und weitere Punkte hinsichtlich der E-Evidence-VO auch für ein persönliches Gespräch zur Verfügung. Aufgrund der sehr hohen Komplexität, welche mit der Umsetzung der Verordnung verbunden ist, möchten wir gerne früh in einen Austausch mit dem Ministerium treten, um den Aufwand für die Wirtschaft möglichst in einem vertretbaren Rahmen zu halten.

ANGA Der Breitbandverband e. V., Reinhardtstraße 14, 10117 Berlin
Tel.: 030 / 2404 7739-0, E-Mail: info@anga.de

BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Albrechtstraße 10, 10117 Berlin
Tel.: 030 / 27576-0, E-Mail: bitkom@bitkom.org

BREKO Bundesverband Breitbandkommunikation e. V., Invalidenstraße 91, 10115 Berlin
Tel.: 030 / 58580-415, E-Mail: breko@brekoverband.de

BUGLAS Bundesverband Glasfaseranschluss e.V., Eduard-Pflüger-Straße 58, 53113 Bonn
Tel.: 0228 / 909045-0, E-Mail: info@buglas.de

eco Verband der Internetwirtschaft e.V., Französische Straße 48, 10117 Berlin
Tel.: 030 / 2021567-0, E-Mail: berlin@eco.de

VATM – Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V., Reinhardtstraße 31, 10117 Berlin
Tel.: 030 / 505615-38, E-Mail: vatm@vatm.de