Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ

24. Oktober 2023

Bericht zur e-Evidence-Vorlage der EU

BJ-D-FFB23401/87

Inhaltsverzeichnis

1 Ausgangslage

Das digitale Zeitalter verändert nicht nur verschiedenste Aspekte unseres Lebens, sondern auch die Methoden, derer sich Kriminelle bei ihren Machenschaften bedienen. Für eine effiziente Strafverfolgung ist daher unerlässlich, dass sich die Strafverfolgungsbehörden und andere an der Verbrechensbekämpfung beteiligte Behörden diesen neuen Entwicklungen anpassen. Dazu gehört auch, die **adäquaten rechtlichen Grundlagen** für eine erfolgreiche Verbrechensbekämpfung zu schaffen.

Um den mit der Digitalisierung einhergehenden Herausforderungen für die Verbrechensbekämpfung zu begegnen, entstanden und entstehen auf internationaler Ebene verschiedene neue Instrumente. So wurde am 17. November 2021 das Zweite Zusatzprotokoll zum Übereinkommen des Europarates über Computerkriminalität betreffend die verstärkte Zusammenarbeit und Weitergabe von elektronischem Beweismaterial verabschiedet und im Rahmen der Vereinten Nationen wird über ein Übereinkommen zur Cyberkriminalität verhandelt. Parallel dazu entwickeln auch die Staaten ihr Recht weiter: Die USA verabschiedeten im November 2018 den **Clarifying Lawful Overseas Use of Data Act (CLOUD Act)**, der im Rahmen von Strafverfahren zu einem erleichterten Zugriff auch auf im Ausland gelagerte Daten führen soll. Aufgrund der praktischen Bedeutung des CLOUD Act hat das BJ diesen aus Sicht des Schweizer Rechts beurteilt und am 17. September 2021 einen Bericht dazu veröffentlicht (Bericht zum US CLOUD Act (Cloud-Gesetz) nachfolgend: Bericht CLOUD Act).

Angesichts dieser Entwicklungen steht auch die Europäische Union (EU) nicht still und erarbeitete eine neue Regelung für elektronische Beweismittel, das sogenannte **e-Evidence-Paket**. Das e-Evidence Paket geht zurück auf die Terroranschläge in Brüssel im Jahr 2016. Zwei Tage nach den Anschlägen forderten die europäischen Justiz- und Innenminister einen besseren Zugang zu elektronischen Beweismitteln. Auch der Rat der Europäischen Union äusserte in der Folge, dass ein wirksamer Zugang zu elektronischen Beweismitteln für die Bekämpfung von schwerer Kriminalität und Terrorismus von wesentlicher Bedeutung ist. Am 17. April 2018 präsentierte die Kommission ihren Vorschlag für eine e-Evidence Richtlinie und Verordnung.

Am 13. Juni 2023 verabschiedete das Europäische Parlament das Gesetzespaket zur e-Evidence, der Rat der Europäischen Union stimmte seinerseits am 27. Juni 2023 dem Gesetzespaket zu. Das e-Evidence-Paket wurde schliesslich **am 28. Juli 2023 formell verabschiedet**. Ziel des Gesetzespakets ist es, einen kohärenten EU-Rahmen für den Umgang mit elektronischen Beweismitteln zu schaffen und deren Erhebung zu beschleunigen. Die neuen Vorschriften ermöglichen es den Strafverfolgungsbehörden der EU-Mitgliedstaaten insbesondere, Beweismittel direkt von digitalen Diensteanbietern (service provider) in anderen Mitgliedstaaten anzufordern (so genannte "Herausgabeanordnungen") oder die Aufbewahrung von Daten für einen Zeitraum von bis zu 60 Tagen zu verlangen, damit relevante Daten nicht zerstört werden oder verloren gehen ("Datenspeicherungsanordnungen"). Dadurch wird ein alternativer Mechanismus zum bisher geltenden Rechtshilfeweg geschaffen.

Die neuen Regelungen dürften auch grosse Auswirkungen auf die Schweiz haben, da hier ansässige service provider, die ihre Dienste in der EU anbieten, unter bestimmten Voraussetzungen unter die Regelungen fallen werden. Zu denken ist hier beispielsweise an Kommunikationsdienste wie Threema oder Protonmail. Die Regelungen könnten aber darüber hinaus noch weitere von Schweizer Firmen angebotene digitale Dienstleistungen treffen.

Ergänzend zum CLOUD Act-Bericht erläutert der vorliegende Bericht den Inhalt des EU e-Evidence-Pakets, nimmt einen Rechtsvergleich vor und beleuchtet die Folgen und Herausforderungen für die Schweiz sowie die Unterschiede zum US Cloud Act. Zum Schluss zeigt der Bericht mögliche Handlungsoptionen für die Schweiz auf.

2 Inhalt des EU e-Evidence Pakets

2.1 Übersicht

Das EU e-Evidence Paket besteht aus einer Richtlinie, welche die wichtigsten Grundsätze der Vorlage festlegt, und aus einer Verordnung mit detaillierten Bestimmungen.

Die **Richtlinie**[1] verpflichtet digitale Dienstleister, die in der EU bestimmte Dienstleistungen anbieten, dazu, eine Niederlassung in der EU zu etablieren oder einen gesetzlichen Vertreter zu benennen, an den die Behörden der Mitgliedstaaten ihre Herausgabe- und Datenspeicherungsanordnungen richten können.

Die **Verordnung**[2] schafft die Europäische Herausgabeanordnung sowie die Europäische Sicherungsanordnung. Sie regelt damit die Voraussetzungen, unter denen digitale Dienstleanbieter in der EU entweder eine Niederlassung haben oder einen gesetzlichen Vertreter ernennen müssen und unter denen die zuständigen (Strafverfolgungs-)Behörden eines EU-Mitgliedstaates im Rahmen eines Strafverfahrens einen solchen service provider direkt zur Herausgabe oder Aufbewahrung von Daten auffordern können.

Die Verordnung findet keine Anwendung auf Verfahren, die eröffnet wurden, um einem anderen EU-Mitgliedstaat oder einem Drittstaat Rechtshilfe zu gewähren.

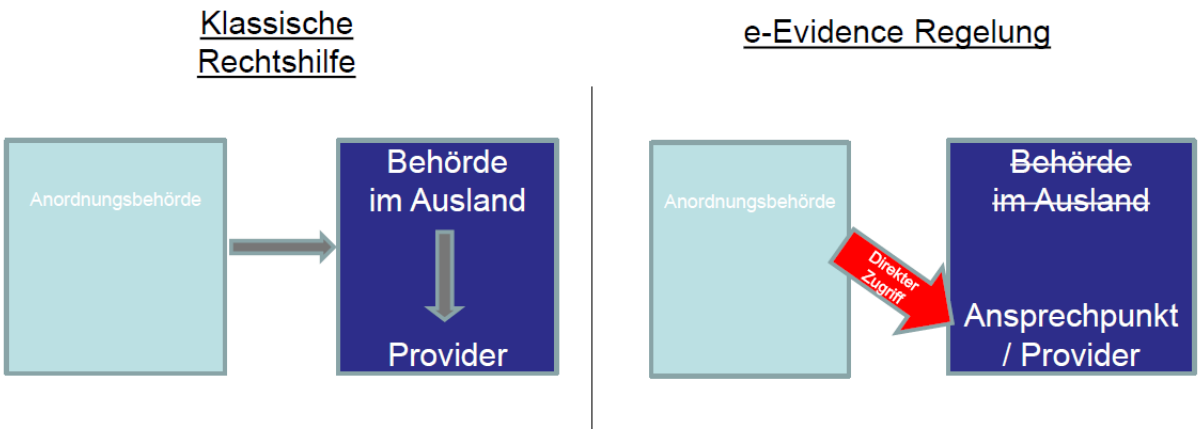

Abb.: Das Funktionieren von e-Evidence im Vergleich mit dem klassischen Rechtshilfeverfahren

2.2 Rechtsgrundlage in der EU

Wie erwähnt, besteht das e-Evidence-Paket aus zwei verschiedenen Instrumenten, einer Verordnung und einer Richtlinie. Diese beiden Instrumente ergänzen einander zwar, sie basieren aber nicht auf denselben primärrechtlichen Grundlagen.

Die Richtlinie beruht auf den Artikeln 53 und 63 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV). Diese beiden Artikel befinden sich unter dem Titel IV des AEUV

[1] RICHTLINIE (EU) 2023/1544 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 12. Juli 2023 zur Festlegung einheitlicher Regeln für die Benennung von benannten Niederlassungen und die Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren, Abl. L 191/181.

[2] VERORDNUNG (EU) 2023/1543 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren, Abl. L 191/118.

über die Freizügigkeit und den freien Dienstleistungs- und Kapitalverkehr. Die Verordnung hingegen stützt sich auf Artikel 82 Absatz 1 AEUV über die gegenseitige Anerkennung von Urteilen und die Stärkung der justiziellen Zusammenarbeit in Strafsachen. Artikel 82 befindet sich unter dem Titel V des AEUV, der den Raum der Freiheit, der Sicherheit und des Rechts regelt.

Auch wenn die unterschiedlichen primärrechtlichen Grundlagen auf den ersten Blick unbedeutend erscheinen, haben diese in der Praxis Konsequenzen, denn sowohl Dänemark wie auch Irland haben sich für ein Opt-out betreffend den Titel V des AEUV entschieden. Während Dänemark ein vollständiges Opt-out hat und sich nicht an Rechtsakten, die auf der Grundlage dieses Titels angenommen werden, beteiligt, handelt es sich bei Irland um ein teilweises Opt-out. Das heisst, dass sich Irland bei Bedarf an bestimmten Initiativen im Bereich des Raums der Freiheit, der Sicherheit und des Rechts beteiligen kann.

Für das e-Evidence-Paket bedeutet dies, dass sowohl Dänemark als auch Irland zwar die Richtlinie des Pakets umsetzen müssen, nicht aber die Verordnung. Im Gegensatz zu Dänemark besteht für Irland aber die Möglichkeit, die Verordnung umzusetzen, wenn es das will. Die Verordnung übernimmt jedoch mehrere EU-Instrumente, die sich auf den Titel V abstützen und die Irland nicht übernommen hat. Eine Umsetzung der Verordnung könnte sich für Irland daher als kompliziert erweisen.[3]

2.3 Anwendungsbereich

2.3.1 Diensteanbieter

Als erstes stellt sich die Frage, welche Diensteanbieter überhaupt vom Gesetzespaket betroffen sind.

Die Verordnung enthält zunächst eine sehr allgemein gehaltene Voraussetzung, wonach darunter **jede natürliche oder juristische Person** fällt, die eine **von der Verordnung umfasste Dienstleistung in der EU** erbringt. Dienstleistungen, die ausschliesslich ausserhalb der Union angeboten werden, fallen nicht in den Anwendungsbereich der Verordnung, selbst wenn der betreffende Dienstleister eine Niederlassung in der EU hat. Welche Dienstleister also von der Verordnung betroffen sind, hängt demnach ab von den Leistungen, welche diese anbieten.

2.3.2 Erfasste Dienstleistungen

Es stellt sich die Frage, **welche Dienstleistungen** konkret von der Verordnung umfasst sind. Diese werden in Artikel 3 Absatz 3 der Verordnung aufgezählt. Es handelt sich um die Leistungen der folgenden Dienste:

2.3.2.1 Elektronische Kommunikationsdienste

Die Verordnung verweist hier auf die Definition in Artikel 2 Absatz 4 der EU-Richtlinie 2018/1972 über den europäischen Kodex für elektronische Kommunikation. Gemäss dieser Richtlinie sind „elektronische Kommunikationsdienste“ gewöhnlich gegen Entgelt über elektronische Kommunikationsnetze erbrachte Dienste, die folgende Dienste umfassen:

- Internetzugangsdienste, also Dienste, die Zugang zum Internet bieten (in der Schweiz wären dies z. B. **Swisscom, UPC-Sunrise** etc.);

[3] Dennoch scheint sich Irland für ein opt-in entschieden zu haben, siehe hinten Ziff. 3.

- interpersonelle Kommunikationsdienste, worunter gemäss Artikel 2 Absatz 5 der Richtlinie 2018/1972 ein gewöhnlich gegen Entgelt erbrachter Dienst zu verstehen ist, der einen direkten Informationsaustausch zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die Kommunikation veranlassen oder daran beteiligt sind (in der Schweiz wären dies z. B. **Protonmail oder Threema**);
- Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für die Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden (z. B. **Anbieter von Blogs, Videoabrufdiensten oder Sozialen Netzwerken**).

2.3.2.2 Domainnamen-Services und IP Nummerierungsdienste

Hierunter fallen IP-Adressanbieter, Dienste, die Domainregistrierungen anbieten sowie Anbieter, die Proxy-Dienste im Zusammenhang mit Domainnamen anbieten (in der Schweiz wären das z.B. **Switch, ProtonVPN** etc.).

2.3.2.3 Andere Dienste, die es ihren Nutzenden ermöglichen, miteinander zu kommunizieren oder die Daten über ihre Nutzenden verarbeiten oder speichern können

Hier verweist die Verordnung auf die Umschreibung in Artikel 1 Absatz 1 litera b der EU-Richtlinie 2015/1535, wonach unter „Dienst“ eine Dienstleistung der Informationsgesellschaft, d. h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung zu verstehen ist.[4]

Diese doch eher komplizierte und nicht leicht zu fassende Umschreibung wird durch Beispiele in Anhang I derselben Richtlinie verständlicher. Demnach fallen **nicht** unter die Dienste gemäss Artikel 1 Absatz 1 litera b:

- Dienste, bei deren Erbringung der Erbringer und der Empfänger gleichzeitig physisch anwesend sind, selbst wenn dabei elektronische Geräte benutzt werden (Untersuchung oder Behandlung in einer Arztpraxis mithilfe elektronischer Geräte, aber in Anwesenheit des Patienten/der Patientin; Konsultation eines elektronischen Katalogs in einem Geschäft in Anwesenheit des Kunden/der Kundin; Buchung eines Flugtickets über ein Computernetz, wenn sie in einem Reisebüro in Anwesenheit des Kunden/der Kundin vorgenommen wird) **(e contrario wären erfasst: Online-Shops, Anbieter von online-Buchungen von Flugtickets etc.)**;
- Bereitstellung elektronischer Spiele in einer Spielhalle in Anwesenheit der benutzenden Person **(e contrario wären erfasst: Anbieter von online-Spielen)**;
- Dienste, die zwar mit elektronischen Geräten, aber in materieller Form erbracht werden (Geldausgabe- oder Fahrkartenautomaten, Zugang zu gebührenpflichtigen Strassennetzen, Parkplätzen usw., auch wenn elektronische Geräte bei der Ein- und/oder Ausfahrt den Zugang kontrollieren und/oder die korrekte Gebührenentrichtung gewährleisten) (e contrario wären erfasst: **Parking-Apps, SBB-App etc.**);
- Offline-Dienste (Vertrieb von CD-ROMs oder Software auf Disketten) **(e contrario wären erfasst: Online-Dienste)**;
- Dienste, die nicht über elektronische Verarbeitungs- und Speicherungssysteme erbracht werden (Sprachtelefondienste; Telefax-/Telexdienste; über Sprachtelefon oder Telefax erbrachte Dienste; medizinische Beratung per Telefon/Telefax; anwaltliche Beratung per Telefon/Telefax; Direktmarketing per Telefon/Telefax) **(e**

[4] „Im Fernabsatz erbrachte Dienstleistung“ bezeichnet eine Dienstleistung, die ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbracht wird; „elektronisch erbrachte Dienstleistung“ eine Dienstleistung, die mittels Geräten für die elektronische Verarbeitung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen wird und die vollständig über Draht, Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen wird; „auf individuellen Abruf eines Empfängers erbrachte Dienstleistung“ eine Dienstleistung, die durch die Übertragung von Daten auf individuelle Anforderung erbracht wird.

contrario wären erfasst: Online-Beratungen in den entsprechenden Bereichen);
- Dienste, die nicht auf individuellen Abruf eines Empfängers, sondern gleichzeitig für eine unbegrenzte Zahl von einzelnen Empfängern erbracht werden (Punkt-zu-Mehrpunkt-Übertragung) (Fernsehdienste (einschliesslich zeitversetzter Video-Abruf; Hörfunkdienste; Teletext (über Fernsehsignal)) **(e contrario wären erfasst, Anbieter die auf den individuellen Abruf abzielen, z.B. online-Zeitungen oder podcasts etc.).**

Des Weiteren präzisiert die Verordnung in Artikel 3 Absatz 4, was unter **«Dienstleistung in der EU erbringen / anbieten»** zu verstehen ist: Der Diensteanbieter muss es einer natürlichen oder juristischen Person in einem Mitgliedstaat ermöglichen, die in Absatz 3 genannten Dienste zu nutzen und eine wesentliche Verbindung **(substantial connection)** zu einem Mitgliedstaat haben. Eine solche liegt dann vor, wenn der Diensteanbieter:

- eine Niederlassung in der EU hat; oder
- eine erhebliche Anzahl Nutzende in einem oder mehreren Mitgliedstaaten hat; oder
- seine Tätigkeiten auf einen oder mehrere Mitgliedstaaten ausrichtet (z. B. durch das Verwenden einer Sprache oder Währung, die in diesem Mitgliedstaat normalerweise verwendet wird oder der Möglichkeit, bei ihm Güter oder Dienstleistungen zu bestellen). Die Ausrichtung von Tätigkeiten auf einen Mitgliedstaat kann sich auch aus der Verfügbarkeit einer App in dem betreffenden nationalen App-Store, aus der Bereitstellung lokaler Werbung oder Werbung in der in diesem Mitgliedstaat allgemein verwendeten Sprache oder aus der Abwicklung von Kundenbeziehungen, etwa durch die Bereitstellung eines Kundendienstes in der in diesem Mitgliedstaat allgemein verwendeten Sprache, ergeben.[5]

Die blosse Zugänglichkeit innerhalb der EU auf eine Webseite des Diensteanbieters oder das Veröffentlichen einer blossen E-Mailadresse oder anderer Kontaktdaten des Diensteanbieters genügen für sich alleine hingegen nicht, um von einer Ausrichtung der Tätigkeiten zu sprechen.[6]

→ Erbringt ein Anbieter einen Dienst im Sinne von Artikel 3 Absatz 3 und besteht eine substantial connection zur EU, so muss der Diensteanbieter entweder eine Niederlassung in der EU haben oder, wenn er keine solche hat, einen gesetzlichen Vertreter benennen.

2.3.3 Betroffene Daten

Das EU e-Evidence-Paket umfasst nur Daten, die sich auf die in der Union angebotenen Dienstleistungen beziehen. Beziehen sich die Daten auf eine solche in der Union angebotene Dienstleistung, so spielt deren Standort keine Rolle (sie können sich also auch ausserhalb der EU befinden).

[5] siehe Vorb. (30) der Verordnung

[6] Siehe Vorb. (29) der Verordnung.

2.3.3.1 Teilnehmer-, Verkehrs- und Inhaltsdaten

Erfasst sind Teilnehmerdaten[7], Daten, die einzig der Identifizierung des Nutzers dienen[8], Verkehrsdaten (Randdaten)[9] und Inhaltsdaten[10] (Art. 3 Abs. 9-12 der Verordnung). Nicht möglich ist hingegen die Echtzeitüberwachung, d. h. beispielsweise das Abhören des Telefons in Echtzeit.

2.3.3.2 Privilegierte Daten

Die Verordnung enthält zudem eine explizite Regelung zu Daten, die nach dem Recht des anordnenden Staates durch das Berufsgeheimnis geschützt sind (siehe Art. 5 Abs. 9 f. der Verordnung). Werden diese Daten von einem Diensteanbieter als Teil einer Infrastruktur, die «privilegierten Berufsangehörigen» (Berufsangehörigen, die unter das Berufsgeheimnis fallen) in ihrer beruflichen Eigenschaft zur Verfügung gestellt wird,[11] gespeichert oder anderweitig verarbeitet, kann eine Herausgabeanordnung zur Erlangung von Verkehrs- oder Inhaltsdaten nur erlassen werden, wenn:

- der oder die privilegierte Berufsangehörige im Anordnungsstaat wohnt;
- die Kontaktaufnahme mit dem oder der Berufsangehörigen den Ermittlungen abträglich sein könnte; oder
- nach dem anwendbaren Recht auf die Privilegien verzichtet wurde.

Hat die anordnende Behörde Grund zur Annahme, dass die ersuchten Verkehrs- oder Inhaltsdaten durch im Recht des ausführenden Staates garantierte Immunitäten oder Privilegien oder durch die Presse- oder Meinungsäusserungsfreiheit geschützt sind, so kann sie dies vor Erlass einer Herausgabeanordnung mit dem ausführenden Staat klären.

2.4 Herausgabe und Speicherung der Daten: Die Herausgabeanordnung (European Production Order; EPOC) und die Datenspeicherungsanordnung (Preservation Order, EPOC PR)

2.4.1 Herausgabeanordnung (Art. 5 der Verordnung)

Mittels der Herausgabeanordnung kann die zuständige Behörde eines Mitgliedstaates die unter das e-Evidence-Paket fallenden Daten direkt von einem Diensteanbieter in einem anderen Mitgliedstaat herausverlangen.

Die Herausgabeanordnung muss **notwendig und verhältnismässig** sein. Die Herausgabe kann nur dann angeordnet werden, wenn sie unter denselben Bedingungen in einem ähnlichen innerstaatlichen Fall auch angeordnet werden könnte (Art. 5 Abs. 2 der Verordnung).

Des Weiteren ist die Herausgabeanordnung nur für **Straftaten mit einem bestimmten Strafmass** zulässig, wobei die Höhe des verlangten Strafmasses von der Art der herausverlangten Daten abhängt:

---

[7] Teilnehmerdaten umfassen einerseits Daten, die auf die Identität des Abonnenten oder Kunden schliessen lassen wie der Name, das Geburtsdatum, die Adresse, Rechnungs- und Zahlungsdaten, Telefonnummer oder E-Mailadresse und andererseits Daten über die Art und Dauer der Dienstleistung.

[8] Dazu gehören IP Adressen und wo notwendig, die entsprechenden Quellports und Zeitstempel, d. h. Datum und Uhrzeit.

[9] Zu den Verkehrsdaten gehören z. B. die Quelle und das Ziel einer Nachricht oder einer anderen Art von Interaktion, der Standort des Geräts, das Datum, die Uhrzeit, die Dauer, die Grösse, der Weg, das Format, das verwendete Protokoll und die Art der Komprimierung sowie andere Metadaten und Daten der elektronischen Kommunikation, die keine Teilnehmerdaten sind und sich auf den Beginn und die Beendigung einer Benutzerzugriffssitzung auf einen Dienst beziehen, wie z. B. das Datum und die Uhrzeit der Nutzung, die Anmeldung beim Dienst und die Abmeldung vom Dienst.

[10] Inhaltsdaten sind alle Daten in einem digitalen Format, wie Text, Sprache, Videos, Bilder und Ton, mit Ausnahme von Teilnehmerdaten oder Verkehrsdaten.

[11] Zu denken wäre hier beispielsweise an ein digitales Geschäftsverwaltungssystem einer Anwaltskanzlei.

- Teilnehmerdaten und Daten, die einzig der Identifizierung dienen, können für alle Straftaten herausverlangt werden sowie für die Vollstreckung von Freiheitsstrafen oder freiheitsentziehenden Massnahmen von mindestens 4 Monaten;
- Verkehrs- und Inhaltsdaten können herausverlangt werden für Straftaten, die im anordnenden Staat mit einer Freiheitsstrafe mit einer Höchststrafe von mindestens 3 Jahren belegt sind, für bestimmte in separaten Richtlinien festgelegte Straftaten (Betrug und Fälschung von Zahlungsmitteln, sexueller Missbrauch und Ausbeutung von Kindern sowie Kinderpornografie, Angriffe auf Informationssysteme) sowie für die Vollstreckung von Freiheitsstrafen oder freiheitsentziehenden Massnahmen von mindestens 4 Monaten.

2.4.2 Datenspeicherungsanordnung (Art. 6 der Verordnung)

Mit der Datenspeicherungsanordnung kann die zuständige Behörde eines Mitgliedstaates einen Diensteanbieter in einem anderen Mitgliedstaat zur Aufbewahrung bestimmter Daten für einen bestimmten Zeitraum verpflichten.

Die Datenspeicherungsanordnung muss **notwendig und verhältnismässig** sein, um die Entfernung, Löschung oder Veränderung von Daten zu verhindern im Hinblick auf ein zukünftiges Rechtshilfeersuchen, eine Europäische Ermittlungsanordnung[12] oder eine Europäische Herausgabeanordnung.

Die Datenspeicherung kann für alle Straftaten angeordnet werden, vorausgesetzt, dass sie unter denselben Bedingungen in ähnlichen innerstaatlichen Fällen angeordnet werden könnte, sowie für die Vollstreckung von Freiheitsstrafen oder freiheitsentziehenden Massnahmen von mindestens 4 Monaten.

2.4.3 Anordnende Behörde (issuing authority)

Die Verordnung regelt auch, welche Behörden der Mitgliedstaaten Daten anfordern können, d. h. eine Herausgabe- oder Datenspeicherungsanordnung erlassen und dem Diensteanbieter direkt zustellen können.

Welche Behörde des anordnenden Staates **(issuing State)** direkt die Herausgabe verlangen kann, hängt von der Art der Daten ab (Art. 4 der Verordnung):

Teilnehmerdaten können von einer Richterin oder einem Richter, vom Gericht, von einem Untersuchungsrichter oder einer Untersuchungsrichterin, von der zuständigen Staatsanwältin oder dem zuständigen Staatsanwalt herausverlangt werden. Zudem kann jede andere Behörde, die gemäss dem Recht des anordnenden Staates zuständig ist, solche Daten herausverlangen, wenn die Anordnung durch eine Richterin, einen Untersuchungsrichter, eine Staatsanwältin oder ein Gericht validiert wurde.

Bei den Verkehrs- und Inhaltsdaten ist die Herausgabe eingeschränkter. Eine solche kann von einer Richterin oder einem Richter, von einem Gericht oder einem Untersuchungsrichter oder eine Untersuchungsrichterin herausverlangt werden sowie von jeder anderen Behörde, die gemäss dem Recht des anordnenden Staates zuständig ist, sofern die Anordnung von einer Richterin oder einem Richter, einem Gericht oder einer Untersuchungsrichterin oder einem Untersuchungsrichter überprüft und genehmigt wurde (Validierung). Im Gegensatz zu Teilnehmerdaten können also Verkehrs- und Inhaltsdaten nicht durch einen Staatsanwalt / eine Staatsanwältin selbständig herausverlangt werden. Die Staatsanwaltschaft könnte aber

[12] Die Europäische Ermittlungsanordnung ist eine gerichtliche Entscheidung, die von einer Justizbehörde eines EU-Mitgliedstaats zur Durchführung einer oder mehrerer Ermittlungsmassnahmen zur Erlangung von Beweisen in einem anderen Mitgliedstaat erlassen wird.

einen entsprechenden Antrag stellen (vgl. Art. 4 Abs. 2 lit. b der Verordnung), der dann durch eine richterliche Behörde genehmigt werden müsste.

Bei der Datenspeicherung wird die Unterscheidung nach Art der Daten nicht getroffen: Eine Datenspeicherung kann für alle Daten von einem Richter oder einer Richterin, einem Gericht, einem Untersuchungsrichter oder einer Untersuchungsrichterin, von einer Staatsanwältin oder Staatsanwalt oder jeder nach dem nationalen Recht des anordnenden Staates zuständigen Behörde angeordnet werden. Wird sie von einer nach dem nationalen Recht zuständigen Behörde angeordnet, so muss ein Gericht, ein Richter oder eine Richterin, ein Untersuchungsrichter oder eine Untersuchungsrichterin oder ein Staatsanwalt oder eine Staatsanwältin die Anordnung für gültig erklären (Validierung).

2.4.4 Adressaten der Anordnung

Adressaten der Herausgabeanordnung sind die Diensteanbieter. Im Grundsatz gilt, dass die Herausgabeanordnung an den Diensteanbieter zu richten ist, der als Verantwortlicher (controller) handelt (Art. 5 Abs. 6 der Verordnung). Wer Verantwortlicher über die Daten ist, ist in der EU-Datenschutzgrundverordnung (DSGVO) Art. 4 Abs. 7 geregelt:[13]

> *"Verantwortlicher" (controller) ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;*

Ausnahmsweise kann die Herausgabeanordnung direkt an den Diensteanbieter gerichtet werden, der die Daten im Auftrag des controllers speichert oder anderweitig verarbeitet (Auftragsverarbeiter (processor))[14], wenn der controller trotz angemessener Bemühungen der anordnenden Behörde nicht ermittelt werden kann oder dessen Adressierung die Ermittlungen gefährden könnte. In diesem Fall hat der processor den controller über die Herausgabe der Daten zu informieren, es sei denn, die anordnende Behörde hat den processor ersucht, den controller nicht zu informieren, um das betreffende Strafverfahren nicht zu behindern (Art. 5 Abs. 7 der Verordnung).[15]

Artikel 5 Absatz 8 der Verordnung enthält zudem eine wichtige Einschränkung in Bezug auf Daten, die von einem Diensteanbieter für eine Behörde gespeichert oder anderweitig verarbeitet werden. Für solche Daten kann eine Herausgabeanordnung nur dann erlassen werden, wenn die Behörde im anordnenden Staat ansässig ist.

Sowohl die Herausgabe- wie auch die Datenspeicherungsanordnung sind direkt an die bezeichnete Niederlassung oder den ernannten gesetzlichen Vertreter des Diensteanbieters zu richten. Reagieren diese nicht, so kann die Herausgabeanordnung in Notfällen auch an eine andere Niederlassung oder einen anderen gesetzlichen Vertreter des Diensteanbieters in der EU gerichtet werden. Zugleich ist in gewissen Fällen auch der ausführende Staat zu informieren (siehe 1.4.5).

---

[13] Die Erwägungen und Bestimmungen in der Verordnung verweisen, wo einschlägig, direkt auf Bestimmungen der DSGVO sowie der Datenschutz-Richtlinie, welche in diesen Fällen anwendbar sind.

[14] Gemäss Art. 4 Abs. 8 der EU-Datenschutz-Grundverordnung ist der „Auftragsverarbeiter" (processor) eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

[15] In diesem Bereich geht die e-evidence Verordnung der DSGVO vor, welche eine Informationspflicht des processors an den controller vorschreibt.

2.4.5 Notifizierung des ausführenden Staates *(executing State)*

Jeder Mitgliedstaat kann eine oder mehrere Zentralstellen benennen, die für die administrative Übermittlung von Zertifikaten, Anordnungen oder Notifizierungen, den Erhalt von Daten und Notifizierungen sowie die Übermittlung offizieller Korrespondenz zuständig ist.

Verlangt die anordnende Behörde die Herausgabe von Verkehrs- oder Inhaltsdaten, so hat sie die zuständige Behörde des ausführenden Staates (executing state = Staat, in welchem der Diensteanbieter niedergelassen ist oder seinen gesetzlichen Vertreter ernannt hat) darüber zu notifizieren, indem sie die Herausgabeanordnung zeitgleich dieser Behörde zustellt (Art. 8 Abs. 1 der Verordnung). Die Notifizierung entfällt in gewissen Fällen, namentlich wenn der anordnende Staat hinreichende Gründe für die Annahme hat, dass die Straftat im anordnenden Staat begangen wurde, wird oder werden könnte und die Person, um deren Daten ersucht wird, im anordnenden Staat wohnt («Wohnsitzkriterium»).

Die ausführende Behörde kann die Anordnung innerhalb von 10 Tagen und in Notfällen innerhalb von 96 Stunden (siehe unten) überprüfen (Art. 12 der Verordnung). Die möglichen Ablehnungsgründe sind in der Verordnung abschliessend geregelt (vgl. dazu 2.4.6.). Erhebt die ausführende Behörde keine Einwände, so hat der Diensteanbieter die Daten herauszugeben, d. h. es ist keine aktive Genehmigung des ausführenden Staates erforderlich (vgl. dazu 2.4.7.).

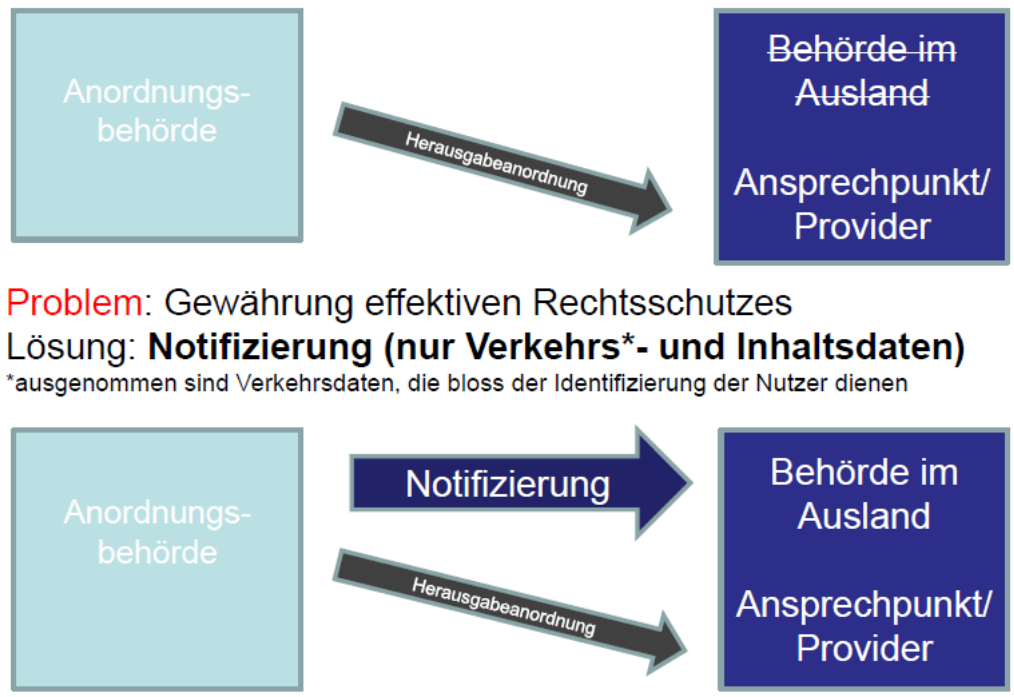

Abb.: Einbezug des Vollstreckungsstaates mittels sog. Notifizierung

Die Notifizierungspflicht ist stark eingeschränkt. So gilt sie gar nicht für Datenspeicherungsanordnungen und nicht für die Herausgabe von Teilnehmerdaten sowie Verkehrsdaten, die alleine der Identifikation des Nutzenden dienen. Letzteres kann insbesondere dann gravierende Konsequenzen haben, wenn die Anordnung auf die Identität von journalistischen Quellen oder Whistleblowern abzielt. In diesem Fall obliegt es alleine dem Diensteanbieter, eine Verletzung der Presse- oder Meinungsäusserungsfreiheit geltend zu machen, da der ausführende Staat gar nicht informiert wird (vgl. 2.4.6). Macht der Diensteanbieter eine solche Verletzung nicht geltend, kann es mitunter zur Herausgabe von Daten kommen, die auf dem heute zu beschreitenden Rechtshilfeweg wegen dieser Verletzung nicht herausgegeben wür-

den. Auch das «Wohnsitzkriterium» ist als problematisch einzustufen, da diese Beurteilung alleine im Ermessen der Strafverfolgungsbehörden des anordnenden Staates liegt, die schliesslich ein beachtliches Interesse an der Vermeidung der Notifizierung haben, um zu vermeiden, dass der ausführende Staat Ablehnungsgründe geltend macht. Gar nicht vorgesehen ist zudem die Notifizierung des Staates, in welchem die betroffene Person ihren Sitz oder Wohnsitz hat. Dies ist insbesondere dann problematisch, wo weder die anordnenden noch die ausführenden Behörden Kenntnis über mögliche Immunitäten gemäss dem Recht des Drittstaates haben, in welchem die betroffene Person ihren Wohnsitz hat.[16]

2.4.6 Ablehnungsgründe

Die Verordnung enthält sowohl für den Adressaten einer Anordnung wie auch für den ausführenden Staat (d. h. dessen notifizierte Zentralstelle) Ablehnungsgründe, die gegen eine Herausgabe- oder Datenspeicherungsanordnung geltend gemacht werden können.

So kann der Adressat einer Anordnung (Diensteanbieter) geltend machen, dass die Anordnung gegen Immunitäten, Privilegien oder die Presse- oder Meinungsäusserungsfreiheit gemäss dem Recht des ausführenden Staates verstösst. Liegt eine solche Rüge vor, hat die anordnende Behörde darüber zu befinden, ob die Anordnung zurückgezogen, angepasst oder aufrecht erhalten bleibt (Art. 10 Abs. 5 und Art. 11 Abs. 4 der Verordnung).

Zugleich kann der ausführende Staat – also die notifizierte Zentralstelle – eine Anordnung dann ablehnen, wenn (Art. 12 Abs. 1 der Verordnung):

- die Daten durch in seinem Recht garantierte Immunitäten oder Privilegien oder durch die Presse- oder Meinungsäusserungsfreiheit geschützt sind;
- in Ausnahmefällen auf der Grundlage konkreter und objektiver Anhaltspunkte stichhaltige Gründe für die Annahme bestehen, dass die Vollstreckung der Anordnung unter Berücksichtigung der besonderen Umständen des Falles eine offenkundige Verletzung eines einschlägigen grundlegenden Rechts, wie es in Artikel 6 des Vertrages über die Europäische Union (EUV)[17] und der Charta der Grundrechte der Europäischen Union (EU-Charta) festgelegt ist, zur Folge hätte;
- die Ausführung der Anordnung gegen das *ne bis in idem*-Prinzip verstösst oder
- keine doppelte Strafbarkeit vorliegt, d. h. der der Anordnung zugrunde liegende Sachverhalt im ausführenden Staat nicht strafbar ist, es sei denn es handle sich um eine Straftat, die unter den in Anhang IV aufgeführten Kategorien von Straftaten aufgeführt und im anordnenden Staat mit einer Freiheitsstrafe oder einer freiheitsentziehenden Massnahme mit einem Höchststrafmass von mindestens drei Jahren bedroht ist.

Gemäss der Einschätzung von NGOs könnte die Tatsache, dass der Ablehnungsgrund der Menschenrechte auf Ausnahmesituationen und einschlägige, fundamentale Rechte eingeschränkt ist, dazu führen, dass Personen, die in Staaten wohnen, in denen Herausforderungen im Bereich der Rechtstaatlichkeit bestehen, besonders beeinträchtigt werden. Denn diese können sich nicht länger dadurch schützen, indem sie bewusst einen Diensteanbieter in einem anderen Staat nutzen. Zu denken ist dabei beispielsweise an Menschenrechtsaktivistinnen und -aktivisten.[18]

---

[16] Siehe dazu Kritik der NGO European Digital Rights (EDRi), e-Evidence compromise blows a hole in fundamental rights safeguards, verfügbar unter: https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/

[17] Art. 6 EUV sieht unter anderem vor, dass die Grundrechte, wie sie in der EMRK gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben, als allgemeine Grundsätze Teil des Unionsrechts sind.

[18] Siehe dazu Kritik der NGO European Digital Rights (EDRi), e-Evidence compromise blows a hole in fundamental rights safeguards, verfügbar unter: https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/

2.4.7 Ausführung

Ist gemäss Artikel 8 der Verordnung die Notifikation der ausführenden Behörde erforderlich und hat diese innerhalb der vorgesehenen Frist (siehe 2.4.5) keine Einwände gegen die Herausgabe erhoben, so hat der Diensteanbieter die ersuchten Daten am Ende der 10 Tage direkt an die zuständige anordnende Behörde oder der in der Anordnung angegebenen Strafverfolgungsbehörden herauszugeben (Art. 10 Abs. 2 der Verordnung). Bestätigt die ausführende Behörde bereits vor Ablauf der 10 Tage, dass sie keinen Ablehnungsgrund geltend machen wird, muss der Diensteanbieter so bald wie möglich, jedoch spätestens nach Ablauf der 10 Tage, tätig werden. Ist eine Notifikation der ausführenden Behörde nicht notwendig, so hat der Diensteanbieter die Daten innerhalb von 10 Tagen direkt der anordnenden Behörde oder der in der Anordnung genannten Strafverfolgungsbehörde herauszugeben (Art. 10 Abs. 3 der Verordnung).

In Notfällen hat der Diensteanbieter die Daten unverzüglich zu übermitteln, spätestens jedoch innerhalb von 8 Stunden nach Erhalt der Herausgabeanordnung (Art. 10 Abs. 4 der Verordnung). In denjenigen Fällen, in denen die ausführende Behörde notifiziert werden muss (also bei Verkehrs- und Inhaltsdaten), kann diese innerhalb von 96 Stunden nach Erhalt der Notifizierung die anordnende Behörde und den Adressaten über ihre Einwände oder Bedingungen zur Verwendung der Daten informieren. Wurden die Daten bereits herausgegeben, sind sie entsprechend zu löschen oder deren Nutzung entsprechend einzuschränken. Problematisch scheint hier insbesondere, dass die Herausgabe der Daten bereits stattgefunden hat, obschon sich deren Herausgabe im Nachhinein als unzulässig erweist.

Kann der Diensteanbieter der Herausgabe oder Datenspeicherung nicht nachkommen, weil die Anordnung unvollständig ist, grobe Fehler oder nicht genügend Informationen zur Ausführung enthält oder es ihm aufgrund von Umständen, die er nicht zu vertreten hat, faktisch unmöglich ist, so hat er unverzüglich die anordnende Behörde zu informieren (Art. 10 Abs. 6 und 7 und Art. 11 Abs. 5 und 6 der Verordnung), allenfalls auch die ausführende Behörde, falls eine Notifikation gemäss Artikel 8 der Verordnung an diese erfolgt ist.

Die Datenspeicherungsanordnung verfällt automatisch nach 60 Tagen, es sei denn, die anordnende Behörde bestätigt, dass eine Herausgabeanordnung ausgestellt wurde (Art. 11 der Verordnung). Innerhalb der 60 Tage kann die anordnende Behörde die Sicherung um 30 Tage verlängern.

2.4.8 Information der Nutzerin oder des Nutzers

Die anordnende Behörde hat die betroffene Person unverzüglich über die Datenherausgabe zu informieren (Art. 13 der Verordnung). Im Anhang I, Abschnitt H ist zudem explizit festgehalten, dass es dem Diensteanbieter untersagt ist, die Person, um deren Daten ersucht wird, zu informieren und es allein der anordnenden Behörde obliegt, diese Person unverzüglich über die Datenherausgabe zu unterrichte. Die anordnende Behörde kann die Information der Person, um deren Daten ersucht wird, nach Massgabe des innerstaatlichen Rechts des anordnenden Staates verzögern, einschränken oder unterlassen, soweit und solange die Voraussetzungen von Artikel 13 Absatz 3 der EU-Datenschutzrichtlinie[19] erfüllt sind. Die anordnende Behörde hat die Gründe für die Verzögerung, Einschränkungen oder Unterlassung in

[19] Siehe Art. 13 Abs. 3: Die Mitgliedstaaten können Gesetzgebungsmassnahmen erlassen, nach denen die Unterrichtung der betroffenen Person [...] soweit und so lange aufgeschoben, eingeschränkt oder unterlassen werden kann, wie diese Massnahme in einer demokratischen Gesellschaft erforderlich und verhältnismässig ist und sofern den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird: a) zur Gewährleistung, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren nicht behindert werden, b) zur Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden, c) zum Schutz der öffentlichen Sicherheit, d) zum Schutz der nationalen Sicherheit, e) zum Schutz der Rechte und Freiheiten anderer.

der Akte aufzuführen und eine kurze Begründung in die Herausgabeanordnung aufzunehmen.

Wie die betroffene Person informiert wird, wenn sie sich nicht auf dem Territorium der anordnenden Behörde befindet, ist in der Verordnung nicht explizit geregelt. Aufgrund des Wortlauts von Artikel 13, der nur die anordnende Behörde anspricht, ist davon auszugehen, dass die Information in jedem Fall durch die anordnende Behörde geschieht, unabhängig davon, wo die Person ihren Wohnsitz hat (kann auch in einem Drittstaat sein). Verlangt beispielsweise eine deutsche Behörde von einem französischen service provider Daten von einer Person, die in Frankreich ihren Wohnsitz hat, so hat die deutsche Behörde diese Person zu informieren.

2.4.9 Sanktionen und Vollstreckung

2.4.9.1 Sanktionen

Die Mitgliedstaaten haben die finanziellen Sanktionen für die Diensteanbieter festzulegen für Verstösse gegen Artikel 10 (Ausführung der Herausgabeanordnung), Artikel 11 (Ausführung der Datenspeicherungsanordnung) sowie Artikel 13 Absatz 4 (Vertraulichkeit, Geheimhaltung, Integrität). Die vorgesehenen finanziellen Sanktionen müssen wirksam, verhältnismässig und abschreckend sein und können bis zu 2% des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahrs des Diensteanbieters betragen (Art. 15 Abs. 1 der Verordnung).

Die Diensteanbieter können nicht für Schäden haftbar gemacht werden, die ihren Nutzenden oder Dritten ausschliesslich durch die Einhaltung der Herausgabe- oder Datenspeicherungsanordnung in gutem Glauben entstehen (Art. 15 Abs. 2 der Verordnung).

2.4.9.2 Vollstreckung

Kommt der Diensteanbieter ohne Angabe von Gründen einer Herausgabeanordnung innerhalb der Frist oder einer Datenspeicherungsanordnung nicht nach und hat die ausführende Behörde ebenfalls keine der in Artikel 12 genannten Verweigerungsgründe geltend gemacht, so kann die anordnende Behörde die ausführende Behörde um Vollstreckung der Herausgabe- oder Datenspeicherungsanordnung ersuchen (Art. 16 Abs. 1 Verordnung).

Die ausführende Behörde hat unverzüglich über die Anerkennung des Vollstreckungsbeschlusses zu entscheiden, spätestens jedoch nach fünf Arbeitstage nach Eingang des Beschlusses (Art. 16 Abs. 2 Verordnung).

Die ausführende Behörde fordert den Diensteanbieter auf, seinen Verpflichtungen nachzukommen und informiert ihn zugleich über:

- die Möglichkeit, gegen die Vollstreckung der betreffenden Anordnung unter Berufung auf einen in der Verordnung genannten Ablehnungsgrund (siehe 2.4.6) Einspruch zu erheben. Macht der Anbieter von dieser Möglichkeit Gebrauch, so hat die ausführende Behörde darüber zu entscheiden, ob die Herausgabe- oder Datenspeicherungsanordnung auf Grundlage der vom Diensteanbieter bereitgestellten Informationen zu vollstrecken ist oder nicht. Die ausführende Behörde kann dazu auch zusätzliche Informationen von der anordnenden Behörde einholen;
- die Sanktionen / Bussen, die im Falle einer Nichteinhaltung verhängt werden;
- die Frist für die Einhaltung oder den Einspruch.

Die Vollstreckung einer Herausgabe- oder Datenspeicherungsanordnung kann von der ausführenden Behörde in bestimmten in der Verordnung abschliessend geregelten Fälle verweigert werden, wenn:

- die Herausgabe oder Datenspeicherung nicht durch die zuständige Behörde angeordnet oder validiert wurde;
- die Herausgabe oder Datenspeicherung nicht für eine in der Verordnung vorgesehene Straftat angeordnet wurde;
- der Diensteanbieter der Herausgabe- oder Datenspeicherungsanordnung nicht nachkommen konnte wegen Gründen, die er nicht zu verantworten hat oder weil die Anordnung gravierende Fehler aufweist;
- die Herausgabeanordnung keine Daten betrifft, die von oder im Auftrag des Diensteanbieters zum Zeitpunkt des Erhalts der Anordnung gespeichert sind;
- die Dienstleistung nicht von dieser Verordnung erfasst ist;
- die angeforderten Daten durch Immunitäten oder Privilegien geschützt sind, wie sie nach dem Recht des ausführenden Staates gewährt werden, oder die angeforderten Daten von der Beschränkung der strafrechtlichen Verantwortlichkeit erfasst sind, die sich auf die Presse- oder Meinungsäusserungsfreiheit in anderen Medien beziehen, welche die Ausführung oder Vollstreckung der Herausgabeanordnung verhindern;
- in Ausnahmesituationen, wenn auf der Grundlage der in der Herausgabeanordnung enthaltenen Informationen ersichtlich ist, dass stichhaltige Gründe für die Annahme bestehen, dass die Vollstreckung der Anordnung unter den besonderen Umständen des Falles eine offensichtliche Verletzung eines einschlägigen Grundrechts gemäss Artikel 6 EUV und der EU-Charta bedeuten würde.

Die ausführende Behörde hat die anordnende Behörde sowie den Diensteanbieter unverzüglich über ihren Entscheid zu informieren. Erlangt die ausführende Behörde die mit der Herausgabeanordnung ersuchten Daten vom Diensteanbieter, so hat sie diese der anordnenden Behörde unverzüglich zu übermitteln.

Kommt ein Diensteanbieter seinen Verpflichtungen aus der Herausgabe- oder Datenspeicherungsanordnung nicht nach, obschon deren Vollstreckbarkeit von der ausführenden Behörde bestätigt wurde, auferlegt ihm die ausführende Behörde eine Busse im Sinne von Artikel 15 der Verordnung.

2.4.10 Gegenläufige rechtliche Verpflichtungen

Ist ein Diensteanbieter der Ansicht, dass die Datenherausgabe einer Verpflichtung gemäss dem anwendbaren Recht eines Drittstaates widerspricht, hat er der anordnenden sowie der ausführenden Behörde innerhalb von 10 Tagen nach Erhalt der Herausgabeanordnung eine begründete Verweigerung zuzustellen. Die Weigerung kann nicht darauf gestützt werden, dass im anwendbaren Recht des Drittstaates keine ähnlichen Bedingungen oder Verfahren für den Erlass einer Herausgabeanordnung bestehen oder alleine darauf, dass die Daten in einem Drittstaat gespeichert sind (Art. 17 Abs. 1 f. der Verordnung).

Hält die anordnende Behörde trotz der begründeten Weigerung an der Anordnung fest, entscheidet das zuständige Gericht im anordnenden Staat. Dieses hat zunächst zu beurteilen, ob eine Pflichtenkollision besteht, indem es untersucht, ob das Recht des Drittstaates überhaupt auf die spezifischen Umstände des Falls anwendbar ist und falls dem so ist, ob das Recht des Drittstaates die Bekanntgabe der betreffenden Daten im konkreten Fall verbietet. Befindet das Gericht, dass kein relevanter Konflikt besteht, bleibt die Anordnung bestehen. Kommt es zum Schluss, dass das Recht des Drittstaates die Herausgabe der betreffenden

Daten verbietet, entscheidet das Gericht, ob die Anordnung aufrechtzuerhalten oder aufzuheben ist. Die Kriterien für diese Beurteilung sind in der Verordnung detailliert aufgeführt (Art. 17 Abs. 6 der Verordnung).

Hier kann zumindest in Frage gestellt werden, inwiefern das Gericht im anordnenden Staat tatsächlich als «neutrale» Instanz betrachtet werden kann, wenn es die Interessen der eigenen anordnenden Behörde gegen die Interessen des Drittstaates abzuwägen hat.

2.5 Rechtsschutz

Der Rechtsschutz ist in Artikel 18 der Verordnung geregelt. Dieser sieht vor, dass der Person, um deren Daten ersucht wird, ein Recht auf wirksame Rechtsbehelfe gegen die Herausgabeanordnung zustehen muss. Handelt es sich bei dieser Person um eine verdächtigte oder beschuldigte Person, so stehen ihr die wirksamen Rechtsbehelfe während des Strafverfahrens zu, in welchem die Daten verwendet werden.

Das Recht auf wirksame Rechtsbehelfe gilt unbeschadet des Rechts, Rechtsbehelfe gemäss der EU-Datenschutzverordnung (DSGVO) einzulegen.

Das Recht auf einen wirksamen Rechtsbehelf ist vor einem Gericht des Anordnungsstaats nach dessen innerstaatlichem Recht geltend zu machen. Dabei kann die Rechtmässigkeit der Massnahme angefochten werden, einschliesslich ihrer Notwendigkeit und Verhältnismässigkeit, unbeschadet der Garantien der Grundrechte im Vollstreckungsstaat.

Wird die Person, um deren Daten um Herausgabe ersucht wird, gemäss Artikel 13 Absatz 1 der Verordnung vom anordnenden Staat über die Herausgabe informiert, hat der anordnende Staat sie auch rechtzeitig über die ihr nach seinem innerstaatlichen Recht bestehenden Möglichkeiten zur Einlegung von Rechtsbehelfen zu informieren. Der anordnende Staat hat dafür zu sorgen, dass diese wirksam ausgeübt werden können.

Zur Einlegung von Rechtsbehelfen gelten dieselben Fristen oder sonstigen Bedingungen wie in vergleichbaren innerstaatlichen Verfahren. Dabei muss gewährleistet sein, dass die betroffene Person ihr Recht auf einen Rechtsbehelf wirksam ausüben kann.

Unabhängig der innerstaatlichen Verfahrensvorschriften haben der anordnende Staat und jeder andere Mitgliedstaat, dem elektronische Beweismittel nach dieser Verordnung übermittelt wurden, sicherzustellen, dass die Verteidigungsrechte und die Fairness des Verfahrens bei der Würdigung der durch die Herausgabeanordnung erlangten Beweismittel gewahrt bleiben.

2.6 Dezentralisiertes IT-System

Das e-Evidence Paket sieht die Errichtung eines dezentralisierten IT-Systems vor, das die sichere elektronische Kommunikation und den Datenaustausch zwischen den zuständigen Behörden und den Diensteanbietern oder nur zwischen den zuständigen Behörden gewährleistet.

Die bezeichnete Niederlassung oder der gesetzliche Vertreter des Diensteanbieters müssen Zugriff auf das dezentralisierte IT System via das jeweilige nationale IT System haben, um Herausgabeanordnungen und Datenspeicherungsanordnungen zu empfangen, die ersuchten Daten zu übermitteln und mit der zuständigen Behörden zu kommunizieren.

Die Kosten für die Errichtung, den Betrieb und die Wartung der dezentralen Zugangspunkte des IT-Systems tragen dabei die jeweiligen Mitgliedstaaten. Zudem trägt jeder Mitgliedstaat die Kosten für die Errichtung und Anpassung seiner nationalen IT-Systeme, um diese kompatibel zu machen.

2.7 Umsetzungsfrist

Die Umsetzungsfrist des e-Evidence-Pakets beträgt 36 Monate und begann mit der Publikation im Amtsblatt der Europäischen Union am 28. Juli 2023 zu laufen.[20]

3 Rechtsvergleichung

Das e-Evidence-Paket wird nicht nur Auswirkungen auf die Schweiz haben wird, sondern auch auf andere Staaten, deren Diensteanbieter in der EU bestimmte Dienste anbieten. Die Schweiz hat daher mit verschiedenen Staaten Kontakt aufgenommen, um sich über deren Position zu den neuen EU-Regeln auszutauschen. Die meisten dieser Staaten haben das neue Gesetzespaket jedoch noch nicht eingehend analysiert.

Das **Vereinigte Königreich** hat mit den USA ein Exekutivabkommen auf der Grundlage des US CLOUD Act geschlossen. Aufgrund seines Austritts aus der EU, ist das Vereinigte Königreich nicht Teil der e-Evidence-Regelung. Zu seiner Positionierung gegenüber dem e-Evidence-Paket hat das Vereinigte Königreich aber noch keine Überlegungen angestellt. Es erscheint aufgrund des Anschlusses UKs an das System des US CLOUD Act aber eher unwahrscheinlich, dass sich UK vertieft für die EU-Regelung interessiert.

Island und **Norwegen**, zwei Staaten, die sich insofern in einer ähnlichen Lage befinden wie die Schweiz, als dass sie ebenfalls nicht EU-Mitgliedstaaten sind, aber als Schengen-Staaten über eine starke Zusammenarbeit mit der EU in den relevanten Bereichen verfügen, scheinen ebenfalls noch nicht mit der Analyse des e-Evidence-Pakets und der internationalen Zusammenarbeit in Strafsachen im Bereich der elektronischen Beweisführung begonnen zu haben. Im Gegensatz zu Norwegen und der Schweiz hat Island das Zweite Zusatzprotokoll (ZP II) zum Übereinkommen über Cyberkriminalität unterzeichnet.

Des Weiteren stand die Schweiz im Austausch mit **Dänemark**. Dänemark ist zwar Mitglied der EU, es verfügt jedoch über ein Opt-out in Bezug auf den Raum der Freiheit, der Sicherheit und des Rechts. Dies bedeutet, dass es Verordnungen, die sich auf diesen Zuständigkeitsbereich stützen, nicht umsetzt. Wie erwähnt stützt sich nur die e-Evidence-Verordnung auf den Raum der Freiheit, der Sicherheit und des Rechts, nicht aber die e-Evidence-Richtlinie. Dies hat zur Folge, dass Dänemark verpflichtet ist, die Richtlinie umzusetzen, nicht aber die Verordnung. Die Richtlinie sieht jedoch hauptsächlich vor, dass die Staaten, die sich nicht an der Verordnung beteiligen, die notwendigen Schritte unternehmen müssen, damit die in ihrem Hoheitsgebiet niedergelassenen Diensteanbieter einen gesetzlichen Vertreter in der EU ernennen. Dänemark evaluiert zurzeit, wie es die Richtlinie ohne die Verordnung umsetzen kann.

Etwas anders gelagert ist die Situation für **Irland**, da es über ein flexibles Opt-out verfügt. Dies erlaubt es Irland, selbst zu entscheiden, an welchen Gesetzgebungsprojekten es sich im Bereich der Freiheit, der Sicherheit und des Rechts beteiligen möchte. Aufgrund der grossen Anzahl von auf seinem Hoheitsgebiet ansässigen Dienstleistern hat Irland ein besonderes Interesse daran, sich am e-Evidence-Paket zu beteiligen, um zu verhindern, dass die Dienste-

[20] ABl. L 191/118 vom 28. Juli 2023.

anbieter einen Vertreter in einem anderen EU-Mitgliedstaat benennen müssen. Gleichzeitig verweist die Verordnung jedoch auf bestimmte Instrumente, die Irland nicht übernommen hat.

Irland hat bereits kurz nach dem Brexit und während der Verhandlungen über das e-Evidence-Paket angedeutet, dass es sich daran beteiligen werde. So ist Irland derzeit daran, sein innerstaatliches Recht anzupassen, damit auf der Grundlage des e-Evidence-Pakets erlassene Herausgabe- und Datenspeicherungsanordnungen direkt an in Irland ansässige Diensteanbieter gerichtet werden können. Auch wenn Irland nicht alle Instrumente übernommen hat, auf denen die Bestimmungen der e-Evidence-Verordnung teilweise beruhen (wie z. B. die Europäische Ermittlungsanordnung), hofft der Staat die Verordnung umsetzen zu können. Durch die Anpassung seines innerstaatlichen Rechts strebt Irland eine Umsetzung der Richtlinie sofort bei deren Inkrafttreten an.

Schliesslich verhandeln die **USA** und die EU bereits seit mehreren Jahren über ein Abkommen, das den Zugang zu elektronischen Beweismitteln zwischen den beiden Entitäten regeln würde. Während die Medien und das DOJ in den USA hauptsächlich von einem *Executive Agreement* sprechen, deuten die der Schweiz vorliegenden Informationen eher darauf hin, dass die beiden Entitäten über ein unabhängiges internationales Abkommen verhandeln, das eine Brücke zwischen dem US-amerikanischen und dem europäischen System schlagen soll. Nachdem die Verhandlungen 2020 aufgrund von COVID 19 und den Diskussionen über das e-Evidence-Paket in der EU auf Eis gelegt wurden, wurden sie nun wieder aufgenommen. Es scheint sich dabei in erster Linie um ein Instrument zu handeln, mit dem vermieden werden soll, dass die Diensteanbieter widersprüchlichen Verpflichtungen unterliegen, da sie de facto sowohl dem CLOUD Act als auch dem e-Evidence-Paket unterworfen wären.

4 Auswirkungen auf die Schweiz

Das e-Evidence-Paket wird zwar hauptsächlich Auswirkungen auf die EU-Mitgliedstaaten oder zumindest auf diejenigen Mitgliedstaaten haben, die an dem Paket beteiligt sind, aber aufgrund der territorialen Nähe der Schweiz zur EU und der engen Beziehungen der Schweiz zu den EU-Mitgliedstaaten dürfte es auch Auswirkungen auf die Schweiz haben. Die Auswirkungen werden hauptsächlich in der Schweiz ansässige Diensteanbieter betreffen, zum Teil jedoch weitere Auswirkungen haben.

4.1 Auswirkungen auf Diensteanbieter

Die in der Schweiz ansässigen Diensteanbieter, welche die vom e-Evidence-Paket erfassten Dienstleistungen auf dem europäischen Markt anbieten oder anbieten wollen (siehe 2.3.1) werden der e-Evidence-Regulierung der EU unterliegen.

Dies hat zur Folge, dass sie einerseits einen gesetzlichen Vertreter in einem EU-Mitgliedstaat ernennen müssen, sofern sie nicht ihre Niederlassung in die EU verlegen. Andererseits können die europäischen Strafverfolgungsbehörden ihre Herausgabe- und Datenspeicherungsanordnungen direkt an den gesetzlichen Vertreter eines in der Schweiz ansässigen Diensteanbieters in einem EU-Mitgliedstaat richten. Der Diensteanbieter muss diesen Anordnungen nachkommen, d. h. er muss die Daten, die von einer EU-Strafverfolgungsbehörde für ein Strafverfahren ausserhalb der Schweiz verlangt werden, herausgeben oder aufbewahren. Dadurch besteht die Gefahr, dass in der Schweiz gelagerte Daten ohne ein Rechtshilfeverfahren und der damit einhergehenden Garantien ins Ausland übermittelt werden.

Darüber hinaus kommt den in der Schweiz ansässigen Diensteanbietern die Aufgabe zu, eine allfällige Kollision bzw. Verletzung des Schweizer Rechts geltend zu machen. Macht der Diensteanbieter einen solchen Rechtskonflikt geltend, hat das Gericht im anordnenden

Staat darüber zu befinden. Folglich wird es den Diensteanbietern, also Privaten, obliegen, die Einhaltung von Schweizer Recht sicherzustellen und mögliche Rechtskonflikte zwischen den Verpflichtungen des Diensteanbieters nach Schweizer Recht und den Verpflichtungen aus dem e-Evidence-Paket zu vermeiden.

4.2 Weitere Auswirkungen

Die Schweiz und die EU haben seit vielen Jahren durch bilaterale Abkommen eine privilegierte Beziehung zueinander aufgebaut. Die internationale Zusammenarbeit in Strafsachen zwischen der Schweiz sowie der EU und ihren Mitgliedstaaten beruht auf den Instrumenten des Europarats und wird ergänzt durch die Assoziierung der Schweiz an das Schengen Abkommen[21] sowie das Betrugsbekämpfungsabkommen[22]. Das e-Evidence-Paket ist jedoch weder Teil der Schengener-Zusammenarbeit noch eines anderen bilateralen Abkommens zwischen der Schweiz und der EU. Abgesehen von den erwähnten Auswirkungen auf in der Schweiz ansässige Diensteanbieter, wird das e-Evidence-Paket daher bei seinem Inkrafttreten keine direkten Auswirkungen auf die Schweiz haben.

Um Kriminalität weiterhin effizient bekämpfen zu können, wird die Schweiz allerdings ihre Gesetzgebung in Bezug auf die Erhebung elektronischer Beweismittel anpassen müssen. Ein Alleingang der Schweiz ist kaum zielführend, denn eine rein nationale Gesetzgebung könnte keinen effektiven grenzüberschreitenden Zugang zu Daten als Beweismittel im Rahmen von Strafverfahren sicherstellen. Bei einem gesetzgeberischen Alleingang müsste die Schweiz vielmehr die Anwesenheit und die Kooperationsbereitschaft aller relevanten Diensteanbieter *in der Schweiz* erwirken können. Das scheint angesichts der geopolitischen Kräfteverhältnisse kaum realistisch. Daher wird die grenzüberschreitende Dimension des Datenzugriffs in der Praxis für die Schweiz sehr bedeutsam bleiben. Da die EU in vielen Bereichen ein wichtiger Partner der Schweiz ist, ist es unumgänglich, dass die Schweiz das e-Evidence-Paket und dessen Chancen und Risiken in ihre Überlegungen zur Neugestaltung der Erhebung elektronischer Beweismittel miteinbezieht.[23]

Des Weiteren wird mit dem e-Evidence-Paket auch ein Register der Diensteanbieter errichtet. Sollte ein solches Register, z.B. über Eurojust, verfügbar sein, wäre dies für die Schweizer Behörden nützlich, da sie wüssten, in welchem Staat die Diensteanbieter eine Niederlassung haben. Sie könnten folglich ihre Rechtshilfeersuchen direkt an den richtigen Staat richten.

5 Unterschiede zwischen dem e-Evidence-Paket und dem US Cloud Act

Der CLOUD Act und das e-Evidence-Paket der EU haben beide das Ziel, den Zugang zu elektronischen Beweismitteln zu erleichtern und so die grenzüberschreitende Kriminalität wirksamer zu bekämpfen. Im Folgenden werden die Unterschiede und Ähnlichkeiten der beiden Instrumente näher beleuchtet.

5.1 Territorialität und transnationaler Zugriff

Der erste Unterschied betrifft die Frage der Territorialität. Das e-Evidence-Paket der EU zielt auf alle Diensteanbieter ab, die ihre Dienste in der EU anbieten. Daher müssen Diensteanbieter, die ausserhalb der EU ansässig sind, einen gesetzlichen Vertreter in einem EU-Mitgliedstaat ernennen. Der CLOUD Act hingegen orientiert sich am engen Bezug, den ein

[21] Abkommen zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands, SR 0.362.31.

[22] Abkommen über die Zusammenarbeit zwischen der Schweizerischen Eidgenossenschaft einerseits und der Europäischen Gemeinschaft und ihren Mitgliedstaaten andererseits zur Bekämpfung von Betrug und sonstigen rechtswidrigen Handlungen, die ihre finanziellen Interessen beinträchtigen, SR 0.351.926.8.

[23] Vgl. dazu die Überlegungen in Ziff. 6.

Diensteanbieter zu den USA haben muss. Wer in den USA angesiedelt ist oder eine US-Tochter oder Zweigniederlassung hat, ist erfasst. Unter gewissen Umständen auch bereits, wer seine Dienste mittels Werbung im US-Markt anpreist. Der CLOUD Act orientiert sich jedoch nicht am Kriterium der Präsenz in den USA und es wird auch nicht verlangt, dass die dem CLOUD Act unterstellten Diensteanbieter eine solche errichten. Die Diensteanbieter sind zur Herausgabe der Daten verpflichtet, die sich auf ihren Servern befinden, unabhängig davon, ob die Daten in den USA oder im Ausland gespeichert sind. So können Herausgabeanordnungen gemäss dem Cloud Act auch an die Schweizer Niederlassung eines in den USA ansässigen Diensteanbieter gestellt werden. Solche «extraterritorialen» Zugriffe auf Daten stellen für das amerikanische Rechtssystem kein Problem dar. Sie können jedoch zu Konflikten mit den Rechtssystemen derjenigen Staaten führen, auf deren Territorium sich die Daten befinden. Das EU-System hingegen «domestiziert» die Daten. Aufgrund der Anwesenheitspflicht der Diensteanbieter wird keine Anordnung in Gebiete ausserhalb der EU gesendet, sondern diese wird immer an den Hauptsitz oder den innerhalb in der EU ernannten Vertreter gerichtet. Dieser muss jedoch Zugang zu allen Daten des Unternehmens haben, unabhängig davon, wo diese gespeichert sind. Diensteanbieter, die von der EU-Verordnung betroffen sind, müssen alle Daten ihres Unternehmens übermitteln, unabhängig davon, wo diese gespeichert sind.

Beide Systeme sehen somit einen länderübergreifenden Zugriff auf die Daten vor und vereinfachen dadurch den grenzüberschreitenden Datenzugriff. Während das EU-System die Diensteanbieter dazu «zwingt», in der EU präsent zu sein, und den Zugriff auf alle Unternehmensdaten von der EU-Zentrale aus verlangt, basiert das US-System auf der Verbindung des Diensteanbieters mit den USA. Ein Diensteanbieter, der diese Verbindung zum US-amerikanischen Rechtssystem, wie es von den USA verstanden wird, hat, ist verpflichtet, alle seine Daten zu liefern, unabhängig davon, wo sie sich befinden.

Darüber hinaus sieht der CLOUD Act die Möglichkeit vor, *Executive Agreements* abzuschliessen, die es den US-Behörden ermöglichen, Anfragen an Diensteanbieter zu senden, die nicht auf US-Territorium ansässig sind, sich aber in den Staaten befinden, mit denen ein *Executive Agreement* geschlossen wurde, und umgekehrt.

5.2 Schutz personenbezogener Daten und Menschenrechtsschutz

Sowohl der US Cloud Act als auch das e-Evidence Paket enthalten Datenschutzbestimmungen. Die Bestimmungen des e-Evidence-Pakets müssen dabei den Datenschutzstandards der EU entsprechen, insbesondere der DSGVO. Die DSGVO ist für die Schweiz als Nicht-Mitgliedstaat der EU zwar nicht direkt anwendbar, da es sich nicht um eine Weiterentwicklung des Schengen-Besitzstands handelt. Die Schweiz hat jedoch ihr Datenschutzrecht revidiert, um den Entwicklungen auf internationaler und europäischer Ebene Rechnung zu tragen. Das totalrevidierte Datenschutzgesetz (DSG, SR 235.1) trat am 1. September 2023 in Kraft. Darüber hinaus gelten die Bestimmungen der DSGVO für Unternehmen in der Schweiz, die in den Anwendungsbereich der Verordnung fallen (Art. 3 DSGVO). Dies ist dann der Fall, wenn der Diensteanbieter in der EU niedergelassen ist oder, bei fehlender Niederlassung, wenn die Datenverarbeitung damit im Zusammenhang steht, betroffenen Personen in der EU Waren oder Dienstleistungen anzubieten oder deren in der EU erfolgendes Verhalten zu überwachen.

Die Schweiz verfügt über einen Angemessenheitsbeschluss der EU, der sie als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt. So wird ein ungehinderter Datenaustausch ermöglicht. Die Schweiz kann davon ausgehen, dass die Anwendung des e-Evidence-Pakets die europäischen Datenschutzstandards erfüllen wird und diese Äquivalenz also nicht

gefährdet, da die betroffenen Unternehmen sowohl den europäischen als auch den schweizerischen Vorschriften unterliegen werden.

Im Gegensatz dazu unterscheiden sich die Datenschutzstandards des CLOUD Act von den Schweizer Standards. Der CLOUD Act Bericht kommt zum Schluss, dass die Datenverarbeitung im Rahmen eines Verfahrens, das auf dem CLOUD Act basiert, aufgrund mehrerer Elemente der DSGVO als problematisch eingestuft werden kann.[24]

Auch im Bereich der Menschenrechte bestehen zwischen dem Schweizer Recht und den e-Evidence-Bestimmungen grössere Parallelen als zum CLOUD Act. Die EU-Mitgliedstaaten sind alle Mitglieder des Europarats und unterstehen als solche der Europäischen Menschenrechtskonvention (EMRK). Die Umsetzung des e-Evidence-Pakets erfolgt daher in Übereinstimmung mit der EMRK, der auch die Schweiz angehört. Dazu gehört insbesondere die in Artikel 6 EMRK verankerte Rechtsweggarantie, wie sie auch Artikel 29*a* BV garantiert. So garantieren auch die e-Evidence-Bestimmungen für die von der Datenübertragung betroffene Person das Recht auf einen wirksamen Rechtsbehelf. Der US CLOUD Act sieht hingegen keine Möglichkeit für die betroffene Person vor, einen Richter oder eine Richterin anzurufen.

5.3 Verfahrensrechtliche Aspekte

Sowohl beim US CLOUD Act als auch beim e-Evidence-Paket werden Anordnungen von Behörden eines Staates direkt an einen Diensteanbieter in einem anderen Staat gerichtet. Die Behörden des Staates, in dem sich dieser Diensteanbieter befindet, müssen zur Datenerhebung grundsätzlich nichts beitragen. Man könnte also von einer «Privatisierung der internationalen Rechtshilfe in Strafsachen» sprechen. Dieser Effekt wird im e-Evidence-Paket durch die Pflicht zur Notifizierung abgeschwächt. So hat die anordnende Behörde bei der Herausgabe von Verkehrs- und Inhaltsdaten sowohl den Diensteanbieter als auch die zuständige Behörde in dem Staat, in dem der Diensteanbieter niedergelassen ist oder seinen gesetzlichen Vertreter ernannt hat, über die Anordnung zu informieren (siehe 2.4.5).

Dieser Mechanismus ist im US CLOUD Act oder im *Executive Agreement* zwischen den USA und dem Vereinigten Königreich nicht vorgesehen. Der Staat, in dessen Hoheitsgebiet sich der Diensteanbieter befindet, erhält keine Kenntnis von den Anfragen, die bei den sich in seinem Hoheitsgebiet befindenden Anbietern eingehen. Dies gilt selbst dann, wenn ein *Executive Agreement* abgeschlossen wurde.

Ein weiterer wichtiger Aspekt, den es zu erwähnen gilt, ist die Anwendung von Zwang oder die Durchsetzung von Anordnungen. Der US CLOUD Act sieht vor, dass die Strafverfolgungsbehörden auf dem Gebiet eines anderen Staates keinen Zwang anwenden dürfen. Wenn sich also ein Diensteanbieter in einem Staat, der mit den USA ein *Executive Agreement* eingegangen ist, weigert, die Daten zu übermitteln, müssen die US-Behörden die Daten durch internationale Rechtshilfe in Strafsachen beschaffen. Das e-Evidence-Paket sieht vor, dass die Anordnung in diesem Fall ohne Rechtshilfeverfahren direkt mit den Mechanismen in der e-Evidence-Verordnung durchgesetzt wird. So kann eine anordnende Behörde in einem EU-Mitgliedstaat unter Einhaltung der in der Verordnung vorgesehenen Verfahren (siehe 1.4.9) eine finanzielle Sanktion gegen einen Diensteanbieter erwirken, der sich in einem anderen EU-Mitgliedstaat befindet.

Das e-Evidence-Paket führt ein zentrales Register der Niederlassungen und gesetzlichen Vertreter von Diensteanbietern ein, die in der EU eine unter die Verordnung fallende Dienst-

[24] BJ, Bericht zum US Cloud Act, S. 24 ff.

leistung anbieten. Dank diesem Register können die Strafverfolgungsbehörden ihre Anfragen schnell an die zuständige Stelle richten. Ein solches Register ist vom US CLOUD Act nicht vorgesehen.

Bezüglich der Datenverschlüsselung sind sowohl der CLOUD Act als auch das e-Evidence-Paket neutral. Denn keines dieser Instrumente sieht vor, dass die Diensteanbieter die ihnen vorliegenden Daten vor dem Versand entschlüsseln müssen, was für die Strafverfolgungsbehörden in der Praxis einige Komplikationen mit sich bringen dürfte.

5.4 Öffnung gegenüber anderen Staaten

Der US CLOUD Act sieht für Staaten, die dies wünschen und aus Sicht der USA einen gewissen rechtstaatlichen Standard erfüllen, die Möglichkeit vor, ein *Executive Agreement* mit den USA abzuschliessen. Dadurch können die Behörden anderer Staaten Anordnungen direkt an US-Diensteanbieter richten und umgekehrt. Angesichts der zunehmenden Globalisierung wird ein solches offenes System zu einer schnelleren internationalen Zusammenarbeit und damit zu einer besseren Bekämpfung der Kriminalität insgesamt führen.

Im e-Evidence-Paket ist keine Möglichkeit der Assoziierung für Drittstaaten vorgesehen. Im Gegenteil: Da es auf mehreren EU-Rechtsakten beruht, darunter Mechanismen zur Vereinfachung der Rechtshilfe wie die Europäische Ermittlungsanordnung, scheint es für einen Drittstaat schwierig zu sein, sich diesem System auf bilateralem Weg anzuschliessen.

5.5 Rechtskonflikte

Beide Systeme sehen Regeln für mögliche Rechtskonflikte vor. Unter dem US CLOUD Act sind diese jedoch sehr begrenzt. Nur der Diensteanbieter selbst – nicht aber der Staat in welchem der Anbieter seinen Sitz hat – kann sich auf einen solchen Rechtskonflikt berufen, und auch nur unter der Voraussetzung, dass ein *Executive Agreement* abgeschlossen wurde. Der Entscheid, ob ein Rechtskonflikt vorliegt oder nicht, obliegt dabei dem Staat, der die Daten anfordert.

Auch unter dem e-Evidence-System der EU ist es primär Sache des Diensteanbieters, einen Rechtskonflikt mit dem Recht eines Drittstaates oder mit dem Recht des Staates, in welchem der Diensteanbieter seine Niederlassung errichtet oder einen gesetzlichen Vertreter ernannt hat, geltend zu machen.[25] Der Diensteanbieter hat über seine Ablehnung zugleich aber auch die zuständige Behörde des Staates zu informieren, in welchem er seine Niederlassung errichtet oder einen gesetzlichen Vertreter ernannt hat. Wie beim US CLOUD Act ist es auch hier der Staat, der die Informationen anfordert, der darüber entscheidet, ob ein solcher Rechtskonflikt vorliegt oder nicht. Macht der Diensteanbieter einen der eingeschränkten Ablehnungsgründe gemäss dem Recht des Staates, in welchem er sich befindet, geltend, so entscheidet die anordnende Behörde (siehe 2.4.6), bei Geltendmachung einer Kollision mit dem Recht eines Drittstaates, obliegt der Entscheid dem zuständigen Gericht im anordnenden Staat (siehe 2.4.10).

Im Gegensatz zum US Cloud Act hat der anordnende Staat aber in bestimmten Fällen den Staat, in welchem der Diensteanbieter seine Niederlassung errichtet oder seinen gesetzlichen Vertreter ernannt hat, über die Anordnung zu notifizieren. Letzterer hat dann die Möglichkeit,

[25] Wobei in Bezug auf das Recht des Staates, in welchem der Diensteanbieter seine Niederlassung errichtet oder einen gesetzlichen Vertreter ernannt hat, die Ablehnung auf im Recht dieses Staates geschützte Immunitäten, Privilegien und die Presse- oder Meinungsäusserungsfreiheit beschränkt ist.

die Anordnung bei Vorliegen einer der in der Verordnung abschliessend genannten Verweigerungsgründe abzulehnen (siehe 2.4.6).[26]

6 Fazit

Die e-Evidence-Regeln der EU stellen einen wichtigen Schritt im Bereich des grenzüberschreitenden Zugriffs auf Daten als Beweismittel im Rahmen von Strafverfahren auf dem europäischen Kontinent dar. Durch die Festlegung klarer Regeln sowohl für die Präsenz von Diensteanbietern in der EU als auch für europäische Herausgabe- und Datenspeicherungsanordnungen stärkt die EU die internationale Zusammenarbeit in Strafsachen und berücksichtigt dabei – zumindest bis zu einem gewissen Grad – die grundlegenden Rechte der Personen, gegen die sich solche Verfahren richten, sowie den Schutz ihrer Daten. Die neuen Regeln dürften bei der Bekämpfung der grenzüberschreitenden Kriminalität eine entscheidende Rolle spielen.

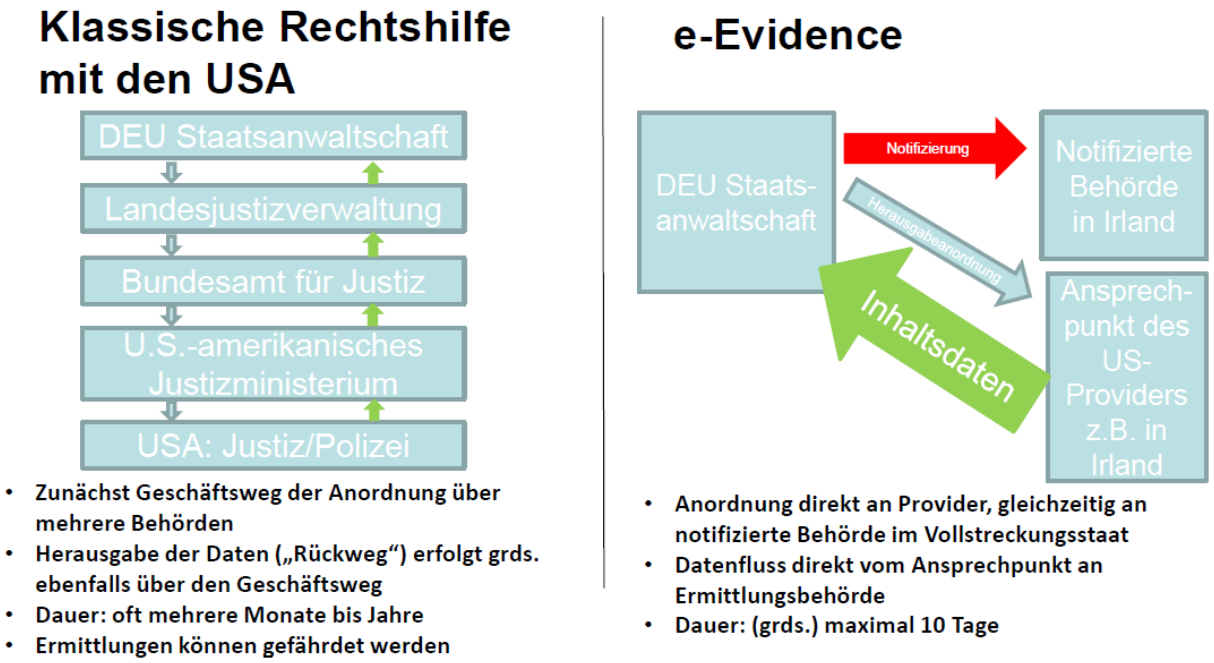

Abb.: Datenzugriff seitens einer deutschen Staatsanwaltschaft bei US-Provider unter e-Evidence-Regelung und unter klassischem Rechthilfeverfahren (Quelle: BMJ Deutschland)

Angesichts der Entwicklung in den Systemen ihrer wichtigsten Partner muss sich auch die Schweiz mit dem Thema e-Evidence auseinandersetzen. Das Schweizer Recht basiert derzeit ausschliesslich auf der Rechtshilfe, die relativ langsam und nicht auf elektronische Beweismittel zugeschnitten ist. Ein Alleingang der Schweiz scheint jedoch nicht zielführend. Elektronische Beweismittel stellen das Konzept der Territorialität in Frage und werden in verschiedenen Staaten von Unternehmen gespeichert, die nicht alle dem Schweizer Recht unterstehen. Vor diesem Hintergrund scheint eine einseitige Schweizer Lösung schwer vorstellbar. Die Schweiz muss in der Lage sein, mit anderen Staaten zusammenzuarbeiten. Zum gegenwärtigen Zeitpunkt scheinen verschiedene Handlungsoptionen zu bestehen:

- Die erste Option besteht darin, nichts zu tun. Wie ausgeführt, handelt es sich hier um einen Bereich, der sich schnell entwickelt und immer häufiger Auswirkungen auf Strafverfahren hat. Nichts zu tun, würde eine Lücke schaffen, die Kriminelle ausnutzen

[26] Die Ablehnungsgründe umfassen dabei aber nicht das ganze Recht des ausführenden Staates, sondern sind beschränkt auf Immunitäten, Privilegien, die Presse- oder Meinungsäusserungsfreiheit, offenkundige Verletzungen eines einschlägigen Grundrechts gemäss der EU-Charta oder Art. 6 EUV, Verstoss gegen das ne bis in idem-Prinzip sowie die fehlende doppelte Strafbarkeit.

könnten. Ausserdem könnte es zu einem Rechtskonflikt (vgl. insb. Art. 271 StGB)[27] kommen, wenn die EU-Regelung zu e-Evidence in Kraft tritt.

- Das zweite Szenario wäre eine Anpassung des nationalen Rechts, um eine eigenständige Lösung zu entwickeln. Bei näherer Betrachtung lässt sich dieses Szenario in zwei Untervarianten unterteilen:

    - Zum einen könnte die Schweiz versuchen, einzig Rechtskonflikte zu vermeiden, die sich mit der e-Evidence-Regelung der EU ergäben. Sie würde ihr nationales Recht so anpassen, dass der ausländische Datenzugriff toleriert wird. Das wäre zwar technisch relativ einfach, hierbei würde die Schweiz den ausländischen Behörden allerdings etwas ermöglichen, ohne für ihre Behörden das entsprechende Gegenrecht zu erlangen.
    - Andererseits könnte die Schweiz versuchen, eine eigenständige Lösung zu entwickeln, die den Schweizer Behörden einen grösseren Zugang zu Daten mit Bezug zur Schweiz ermöglicht. Dies hätte den Vorteil, dass die Schweiz ein System entwickeln könnte, das ihren eigenen Rechtsgrundsätzen entspricht und auf ihre Bedürfnisse zugeschnitten ist. Allerdings bieten Diensteanbieter aus der ganzen Welt ihre Dienste in der Schweiz an. Als kleines Land wäre es für die Schweiz schwierig, all diese Diensteanbieter zur Ernennung einer gesetzlichen Vertretung oder der Errichtung einer Niederlassung in der Schweiz zu bewegen.

- Das dritte Szenario wäre ein Anknüpfen an das eine und/oder andere System. Wie erwähnt, sieht das e-Evidence-Paket eine solche Möglichkeit nicht ausdrücklich vor, der US CLOUD Act hingegen schon. Die EU und die USA verhandeln jedoch über ein Abkommen, um die internationale Zusammenarbeit im Bereich der elektronischen Beweismittel zu erleichtern. Die Schweiz könnte versuchen, ihr nationales Recht unter Berücksichtigung der beiden Systeme – und allenfalls der «Konfliktlösung» zwischen den beiden Akteuren EU und USA – autonom anzupassen. Diese Gesetzesrevision könnte die Möglichkeit vorsehen, mittels Staatsverträgen Brücken zu anderen Rechtssystemen zu bauen.
  Aufgrund der dargelegten engen Verbindungen der Schweiz mit der EU im Bereich der justiziellen Zusammenarbeit und des Datenschutzes (insbesondere im Bereich der Schengener-Zusammenarbeit), jedoch auch aufgrund der Personenfreizügigkeit (auf welche sich die e-Evidence Richtlinie abstützt) und des Zugangs zum Binnenmarkt, gerade auch im digitalen Bereich, erscheint es ratsam, den Blick nicht nur auf die USA, sondern auch auf die EU und die schweizerischen Nachbarstaaten zu richten. Es stellt sich daher gar die Frage, ob die Schweiz evtl. eine Lösung erarbeiten könnte, welche sich auf die e-Evidence-Gesetzgebung der EU abstützt.

In jedem Fall muss die Schweiz handeln und dies rasch. 36 Monate nach dem 28. Juli 2023, also am 28. Juli 2026, wird die neue e-Evidence-Gesetzgebung in Kraft treten. Ab diesem Datum besteht, wenn keine Lösung gefunden werden konnte, die Gefahr, dass es zu einem Rechtskonflikt mit dem neuen EU-System kommt. Einen solchen gilt es zu vermeiden. Dabei ist zu bedenken, dass die Schweiz ihre rechtsstaatlichen Errungenschaften nicht gefährden darf. Sie sollte jedoch grundsätzlich eine Lösung anstreben, die ihren Strafverfolgungsbehörden die Möglichkeit bietet, mit anderen Staaten oder zumindest mit Anbietern, die sich auf dem Territorium anderer Staaten befinden, zusammenarbeiten zu können.

[27] Wenn ein in der Schweiz domizilierter Diensteanbieter gemäss e-Evidence-Regelung einen Ansprechpunkt in einem EU-Staat errichtete, dort EU-Herausgabeanordnungen erhielte und gestützt auf diese Daten, die in der Schweiz liegen, herausgäbe, nähme er nach schweizerischem Verständnis eine Handlung vor, die dem Staat zukommt. Es käme zu einem Konflikt mit Art. 271 StGB – und der Diensteanbieter müsste jedes Mal um eine entsprechende Genehmigung des EJPD ersuchen, was kaum praktikabel wäre.